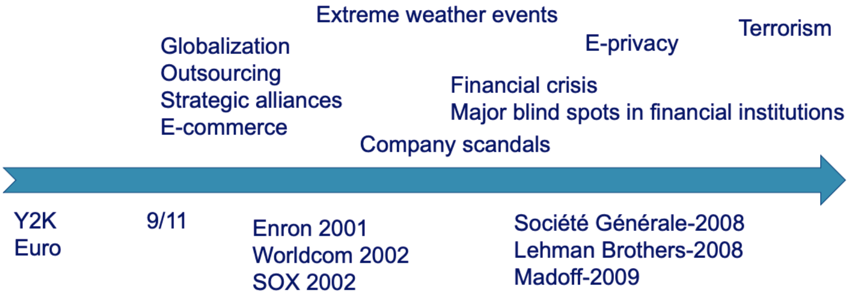
Summary Enterprise Risk Management

Risk Management and Control

How to handle risks…



- The last 15 years we had a series of corporate scandals (Enron, WorldCom, Parmalat, L&H, Societé Générale, etc.) and the financial crisis.
- Also other risks:
  - Technological: Year 2000 problem (millenium bug), cyber threaths
  - Disasters: weather; Katherina Orcane
  - Terrorism
  - Economic: the global financial crisis in 2008 demonstrated the importance of adequate risk management.
    - Some argue: financial crisis demonstrates the failure of risk management
    - We do not agree: rather it demonstrates the failure of organizations to successfully address the risks they face(d) → Need for better risk management
  - As a consequence, risk management has become an increasingly important business driver and shareholders /stakeholders have become much more concerned about risk – not only financial risk, but also operational, strategic, etc. risk.
- An **enterprise-wide approach** to risk management enables an organization to consider the potential impact of all types of risks on all processes, activities, stakeholders, products and services.
- Implementing a comprehensive approach will result in an organization benefiting from what is often referred to as the 'upside of risk'. The last couple of years, there have been a lot of evolutions with new standards, regulation, etc. New risk management standards have been published, including the international standard, ISO 31000 'Risk management – Principles and guidelines'.
- In this course we will discuss in detail different types of risks and how to manage them (controls).

  - This course explores the emerging practice of "enterprise risk management" (ERM) or "integrated risk management"– a new managerial outlook on managing risk
  - **Enterprise risk management** considers all the risks faced by the firm and attempts to integrate these disparate risks into a single unified analytical framework
  - Traditionally, risk has been managed in the compartments of financial risk, operating risk, credit risk, etc. Rather than allowing risk to remain in such "silos," ERM insists that these must be brought together into one system of risk management.
  - As we will see, the methods of ERM are very much a work in progress.

Part 1: Introduction to Risk Management

What is risk?

Definition of **risk** (ISO Guide 73):

= "Risk is the effect of uncertainty on objectives"

- Links risk to objectives
- Effect may be negative, positive or a deviation from expectations

- Therefore, risk may be considered to be related to:
  - A loss
  - An opportunity
  - The presence of an uncertainty for an organization
- Every risk has its own characteristics that require particular management or analysis

- There are **many definitions** of risk and risk management. Risk is often defined in terms of "harm and harmful events" (eg COSO). Committee of Standars in Australia & New Zealand: (basis for new ISO standards) concluded that we should not confine it to harmful events because outcomes can be negative, but also positive. Positive outcomes (return) are also inherent part of risk. Risk should not be seen as something inherently negative. Therefore new definition, also included in ISO now: effect on objectives: thus a SHIFT from "the event" (something happens) to "the effect" (in particular on objectives).
- The definition set out in ISO Guide 73 is that risk is the **"effect of uncertainty on objectives**". Guide 73 also states that an effect may be positive, negative or a deviation from the expected, and that risk is often described by an event, a change in circumstances or a consequence. This definition links risks to objectives. Therefore, this definition of risk can most easily be applied when the objectives of the organization are comprehensive and fully stated. Even when fully stated, the objectives themselves need to be challenged and the assumptions on which they are based should be tested, as part of the risk management process.
- Almost 500 years ago Machiavelli already had these insights!
  - *All courses of action are risky, so prudence is not in avoiding danger (it's impossible), but calculating risk and acting decisively. Make mistakes of ambition and not mistakes of sloth. Develop the strength to do bold things, not the strength to suffer." Machiavelli (1532), Il Principe, Ch. 3.*

- Entrepreneurship/doing business requires **accepting some risks**!
- However, entrepreneurship should be realized within the limits of acceptable risk.
- Through the media we learn that this often not the case, with dramatic consequences for everyone.
- Appropriate controls play an important role in avoiding these risks.

An important part of analyzing a risk is to determine the nature, source or type of impact of the risk.

- Evaluation of risks in this way may be enhanced by the use of a **risk classification system**. Risk classification system are useful for analyzing/evaluating risks
  - Risk classification systems are important because they enable an organisation to identify accumulations of similar risks.
  - A risk classification system will also enable an organisation to identify which strategies, tactics and operations are most vulnerable.
  - Risk classification systems are usually based on the division of risks into those related to financial control, operational efficiency, strategic and regulatory activities, as well ass hazard risks.
- However, there is no risk classification system that is universally applicable to all types of organizations.
  - Select/develop an appropriate one
  - There are many risk classification systems available and the one selected will depend on the size, nature and complexity of the organization. ISO 31000 does not recommend a specific risk classification system and each organization will need to develop the system most appropriate to the range of risks that it faces. (e.g. market risk, credit risk, financial risk, operational risk, legal risk, etc).

    - You could divide risk in financial risk, operational risk, … or you can classify them as LT, ST, … → different classes → there is no 'best' practice, it depends on the kind organization, objective, … the essence is to discuss those risks above these risks. How you classify them is up to the company itself.
- ISO Guide 73: risks are divided into three categories (based on impact):
    - **Hazard** (or pure) risks: mainly operational risks, day-to-day going concern risk
    - **Control** (or uncertainty) risks: uncertainty like projects or ad hoc risks
    - **Opportunity** (or speculative) risks: mainly financial. For example, you are responsible of the treasury of the company, you could play around with that money and buy all kind of financial products that are high risk and then you make high bonusses, but this can also go the other way where you fail. The same goes when you decide to change machines etc. It correlates with operational risk.

HAZARD or pure risks

= Risk events that can only result in negative outcomes

- Are associated with a source of potential harm or situation with the potential to undermine objectives in a negative way
- Often thought of as operational risks: backups, locks, etc…. Typical internal controls
- Often insurable
- Normal efficient operations may be disrupted by loss, damage, breakdown, theft, and other threats

The application of risk management tools and techniques to manage hazard risks is the best and longest-established branch of risk management

May include:

- People:
    - Lack of skilled people and resources
    - Unexpected absence of key personnel
    - Ill-health, accident or injury to people
- Premises:
    - Inadequate or insufficient premises
    - Damage to and contamination of premises
- Assets:
    - Breakdown of plant or equipment
    - Theft or loss of physical assets
- Suppliers
    - Disruption caused by failure of supplier
    - Delivery of defective goods or components
- Inefficient operation
    - Transport failure or disruption
- IT
    - Failure of IT systems
    - Disruption by hacker or computer virus
    - Inefficient operation of computer software

Hazard "tolerance"

- Companies will have a "tolerance" of hazard risks
- Need to manage these risks within these levels of tolerance
- Examples:
    - *Theft*
        - Office environment: *some theft of stationary, including paper, envelops and pens may be tolerated because the cost of eliminating these risks may be very large, so it becomes cost-effective to accept that these losses occur*
        - Jewel shop: *high security cost to eliminate impact of theft*

- *Health and safety risks*
    - Generally accepted: take all appropriate actions to eliminate them. *It is generally accepted that companies should be intolerant and should take all appropriate actions to eliminate them.*
    - In practice: it is not possible so manage safety risks to the lowest level that is cost-effective and in compliance with law

OFTEN: trade-of between preventive and corrective measures

→ You need to know what the tolerance is. As a management you need to make sure you stay within this tolerance. It's the maximum loss you can have as a company. You need to manage those risks.

CONTROL or uncertainty risks

= Risk that give rise to uncertainty about the outcome of a situation

- Uncertainty represents a deviation from the required or the expected outcome
- Extremely difficult to quantify: are associated with unknown and unexpected events
- Frequently associated with project management: difficult to predict and control

These risks are more sudden and unexpected. They are difficult to quantify because of the uncertainty.

Example: project management, it's not on a going Conner basis it's something that happens and disturbs. You don't know what the outcome will be and it's very hard to quantify this. It's hard to make calculations about what the financial effect is. What we usually do in practice is put percentages on it for example, 'X% chance that situation X happens'.

Control management: is concerned with reducing the uncertainty and minimizing the potential consequences of these events

- In general: companies have an aversion to control risks. If you can push the control risks out of the window, then the chance that you will see those will be limited.
- Danger that organizations become obsessed with control risks: over-focus on internal control and control management "might suppress entrepreneurial efforts"

    → *Very important. It's important to have this kind of risk reduced which will have a benefit for the company but you will have to put effort to it to put those systems in place in order to control those risks. You need to find <u>a balance</u> between how much time, risk and money you need to have for having these control risk under control.*
- When undertaking projects and implementing change companies have to accept a level of uncertainty: uncertainty or control risks are an inevitable part of undertaking a project

OPPORTUNITY (or speculative) risks

= Occur when companies deliberately take risks, especially market or commercial risks, in order to achieve a positive return

→ When it's a choice we talk about opportunity risk.

- Two aspects:
    - Risks/dangers associated with **taking** an opportunity
    - Risks/dangers associated with **not taking** the opportunity

      → Two sides which you need to take into account
- Often of a financial nature
- Are normally associated with the development of new or amended strategies but ....
- Can also arise from enhancing the efficiency of operations and implementing change initiatives
- You can make calculations. Even when you have a case when you did not well then it should not be a surprise because you should have thought about those risks

Opportunity management is the approach that seeks to maximize the benefits of taking entrepreneurial risks

- Each organization has its specific appetite for investment in such risks
    - **Risk appetite**: Here risk appetite comes into play. This is how much risk you are willing to take as an organization. It's a decision that needs to be taken by the board of directors of the company. Risk appetite is something that is defined by the board! Those people give the framework to the management, they set boundaries. (The boundaries is the risk appetite)
        - Averse
        - Seeking

      ! Risk appetite does not mean: go for it – even if you are risk seeking!

      → Should be within risk CAPACITY
    - Difference between **risk tolerance and risk appetite**: risk appetite is how much risk are you willing to take and risk tolerance is how much risk you can handle
    - You always have to remember the goal of your enterprise. Then you can talk about how much risk you are willing to take.
        - Imagine you are a venture capitalist → very big risk appetite
        - Imagine you are a hospital → much smaller appetite
            - ➔ Really depends on what kind of organization you are
            - ➔ Risk appetite is the starting point of risk management: if you don't have a clear definition of risk appetite it will not go well, there needs to be a discussion about risk appetite within the board

- There is a clear link between opportunity management and strategic planning: the goal is to maximize the likelihood of a significant positive outcome from investments in business opportunities
- Examples: moving business to a new location, acquiring new property expanding a business, diversifying into new products, development of new products
- Relationship between level of risk and the anticipated reward – not all business activities offer the same return for risk taken

No universal classification (some examples):

There is allot of debate about this topic: which classification? In practice it does not make a huge difference as long as it makes sense for the organization.

- Impact: hazard, control, opportunity risks
- Time scale: risks can impact organizations in the short (operations), medium (tactics) and long term (strategy)
- COSO: strategic, operations, reporting, compliance
- FIRM risk scorecard: Financial, Infrastructure, Reputational and Marketplace
- Internal vs. external condition

- Many debates about risk management terminology
- Important to note that there is no 'right' or 'wrong' subdivision of risks
- The most important is that companies adopt a risk classification system that is most suitable for its own circumstances
- It's also about making people aware of risk. An easy way to make a company aware is discussion and also digging out those risk from management and operational staff.

Why invest in risk management?

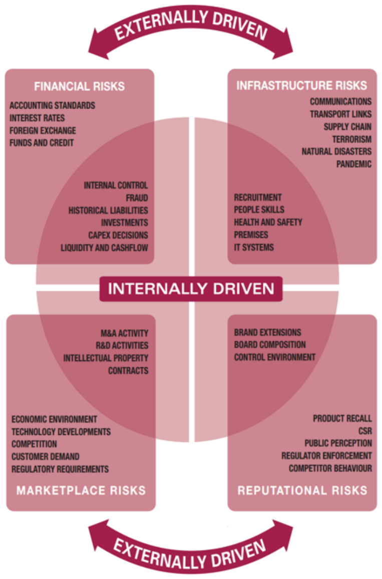
Steps in a circle

1. Inventory of risks / investigate the risks: you are looking for risks
2. Asses risk: What do these risks means? Do I care about those risks?
3. Think about risk and reward
4. Implement countermeasures (put controls into place)
5. Monitor these controls (are they working?)
6. Report (report when something is going on)

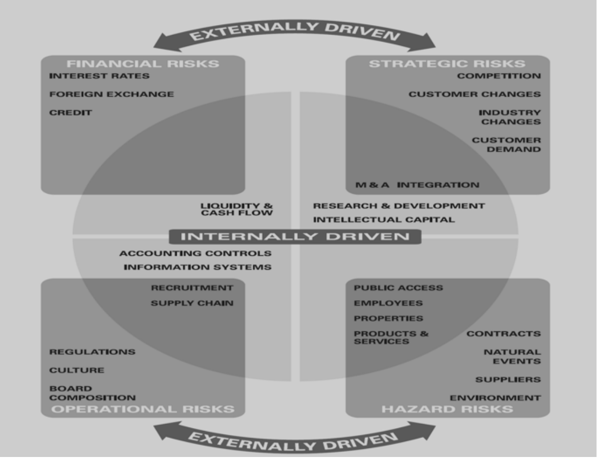
→ risk maturity of organization will increase if they do all these steps (= how mature is the organization dealing with risk? How explicit are they in taking measures against certain risk?)

= ADDED VALUE for the organization (here you see the benefits of ERM)

Internal and external factors can give rise to risks. Figure 5 is based on the FIRM Risk Scorecard risk classification system and it provides examples of internal and external key risk drivers. Some risk classification systems have strategic risk as a separate category. However, the FIRM Risk Scorecard approach suggests that strategic (as well as tactical and operational) risks should be identified under all four headings.
Here you can find the different classifications in one chart. You have externally and internally driven risk. You can have them in a ST and LT perspective.



Is a classification
Typical risks
But no classification works for ALL companies; develop own classification



What is control?

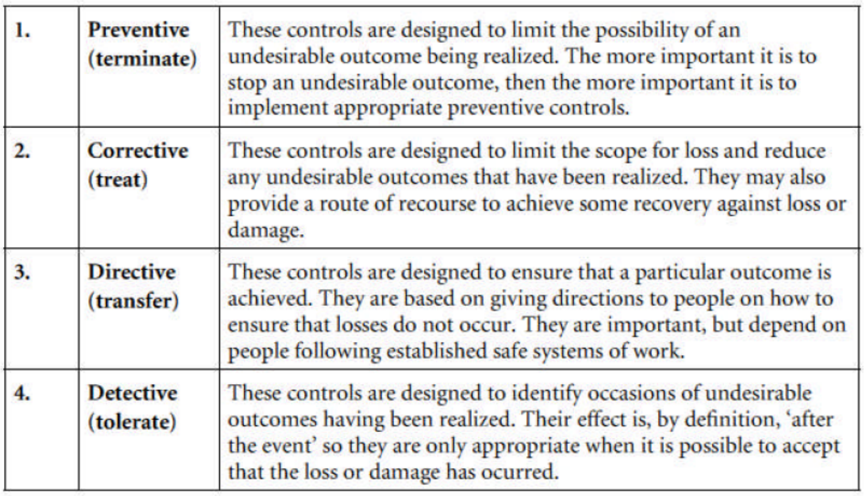
“Control” is a general term used in various domains, for which many definitions exist, but in general control mechanisms are all those arrangements and procedures in place to ensure that business objectives may be met

Control is to stop the risk making sure the risk does not occur. Usually formalized. On the other hand, you can also have soft controls for example culture, the tone that is set on the top of the organization. But you can also have hard controls, like procedures, regulations, …
It has many definitions.

Many different classifications exist; a typical way to break them down is (COSO, 1992):

- **Preventive**:
    - Taken by a firm to detect noncompliance with policies and procedures
    - These controls ensure that sytems work in the first place (e.g. employing competent staff, high moral standards, segregation of duties, physical and controls (locks, passwords, etc)
- **Detective**: to detect something
    - Aimed at uncovering problems after they have occurred
    - Designed to pick up errors that have not been prevented (supervisory checks, internal checks, variance analysis, reconciliations)
    - Necessary in a good internal control system
    - But detection of an independence violation after the fact is less desirable than prevention in the first place
    - Rarely work well as a deterrent in the absence of severe penalties

- **Corrective**: to correct something
  - When violations or problems are identified, some corrective action is required
  - These controls ensure that where problems are identified, they are properely dealt with
  - E.g. counseling and additional training, with more severe disciplinary action in cases of continued noncompliance.
- **Directive**: to give some directions
  - To ensure compliance, a clear, consistent message from management that policies and procedures are important is required
  - POSITIVE arrangements to motivate people and to give them a clear sense of direction (and the ability) to make good progress. – eg staff awarness training.
  - Important: Rewarding exemplary conduct or zero-tolerance policies for violation
- **(Compensating)**: Compensating controls are intended to make up for a lack of controls elsewhere in the system (e.g. a hard copy of the client list -- such a list would compensate for downtime in electronic systems and difficulties in locating client names in an electronic system)



1.	**Preventive (terminate)**	These controls are designed to limit the possibility of an undesirable outcome being realized. The more important it is to stop an undesirable outcome, then the more important it is to implement appropriate preventive controls.
2.	**Corrective (treat)**	These controls are designed to limit the scope for loss and reduce any undesirable outcomes that have been realized. They may also provide a route of recourse to achieve some recovery against loss or damage.
3.	**Directive (transfer)**	These controls are designed to ensure that a particular outcome is achieved. They are based on giving directions to people on how to ensure that losses do not occur. They are important, but depend on people following established safe systems of work.
4.	**Detective (tolerate)**	These controls are designed to identify occasions of undesirable outcomes having been realized. Their effect is, by definition, 'after the event' so they are only appropriate when it is possible to accept that the loss or damage has ocurred.

⇨ Preventive control is the strongest control. Second strongest: corrective
Problem with directive is it is strong, but humans perform it, and they can make mistakes. It's the third strongest. Detective is fourth: if you detect problems then the risk already occurred it already happened. Detection is fine but it's not the strongest.

Two important **dimensions of control** (LINK Management control):

- Formal
- Informal
  - Behavior control (task or action control) = the process of finding ways to control behavior so that a job is completed in a pre-specified manner (e.g. pre defined procedures)
  - Output control (results control) = methods focus on measuring employee performance against stated objectives (e.g. predefined objectives)
  - Social control (people control) = informal control based on unwritten rules within the organisation (e.g. values, ethics, interaction between different groups, personnel selection procedures, culture of the organisation)

Preventive: mainly for hazard risks

- Supervision
- Training
- IT access approval
- Locks: physical access

Corrective

- Correcting financial records after mistake was discovered
- Changing IT access if people change jobs/lefs

Directive

- Corporate policies/procedures

Detective

- Bank reconciliations
- Monitor actual expenditures vs budget
- Post incident review

As a risk manager you want to make sure that you reduce the amount of detective controls and directive and increase the preventive and corrective ones. But the restriction is that if you have to put allot of resources to increase those and it cost you more than not doing that than it might be a discussion

Some traditional **control mechanisms**:

- ○ Authorization: the process of granting permission on behalf of the organization - normally associated with a signature from the authorizing officer
- ○ Physical access restrictions (9/11 led to a compete rethink of security)
- ○ Supervision: double function: staff controlled /observed by their line manager (immediate intervention), but at same time offer help and assist
- ○ Compliance checks: special steps taken to check whether authorized procedures are being applied as prescribed
- ○ Procedures manuals (input/behavior)
- ○ Recruitment and staff development practices: to make sure that staff are competent, motivated, honest and alert
- ○ Segregation of duties: idea is to stop one person from undertaking a transaction from start to finish → involve at least one other person → check each other's work + prevent fraud → typical example: payment system: preparation, authorization, processing and dispatching of the check should each be done by different person (Formal + preventive)
- ○ Organizational structure with clear reporting lines: clear reporting lines help establish links between accountability, responsibility and authorization
- ○ Sequential numbering of documents → especially for valuable documents (checks, orders, etc) → missing, duplicated or inconsistent documents can be readily isolated
- ○ Reconciliations → balancing one system with another

Development of Enterprise Risk Management

→ Risk management is nothing new:

- Historically, the term risk management has been used to describe an approach that was applied only to hazard risk
- Has developed in a way that it enables improved management of control risks and opportunity risks
- Little recognition that these risks were CONNECTED ("silo-approach")
- Early 2000 Enterprise(-wide) Risk Management or ERM emerged as an attempt to manage enterprise risks in a integrated way
- ⇨ Risk management is a constantly developing and evolving discipline
    - ○ 2009: ISO Guide 73 provides the definitions of generic terms related to risk management → common/consistent terminology
    - ○ Current developments: ISO 22300 series: business continuity and crisis management

Risk management became more wide-spread better coordinated

- In 1950s in US: cost of insurance had become excessive and the extent of coverage was limited: people/organizations became aware that buying insurance was insufficient if there was inadequate attention to the protection and of property and people
- In 1970s in Europe: concept of "total cost of risk" – became obvious that many risks were not insurable
- The link with insurance is much less strong: insurance is now seen as one of the risk control techniques – but many other techniques exist – and insurance is only applicable to a portion of hazard risks. Risks related to finance, commercial risks, reputational issue = very important but outside scope of insurance

- In addition there has also been the consideration that many risks are INTERRELATED – and that traditional risk management fails to address the relationships between risks.
- ERM developed to take COORDINATED actions.

September 2004: Committee of Sponsoring Organizations of the Treadway Commission (COSO) issued guidelines that defined ERM as

> *"a **process**, effected by an entity's board of directors, management, and other personnel, **applied in strategy setting** and **across the enterprise**, designed to identify **potential events** that may affect the entity, and **manage risk** to be **within its risk appetite**, to provide reasonable assurance regarding the **achievement of entity objectives**"*

→Publication of this definition was a milestone in ERM

- **Intentionally broad**: applies to all organizations encompasses all risks no matter what industry, what country, etc…
    - A HOLISTIC APPROACH to ERM: from "silos" to "an integrated, strategic and enterprise wide system"
    - The past practice of silo-based approaches for managing pockets of risk, leads to unclear responsibilities and a lack of visibility, thereby exposing the organization to unnecessary risk

⇨ **Analyzing the definition**:
- A process applied in strategy setting
    - Based on an entity's mission/strategy, management sets strategic objectives, which if achieved, will create, and preserve value for the organization. Management will take into account the risks associated with different objectives/alternatives.
- Across the enterprise
    - Coordinated by top management, but also part of every employee's job
- Identify potential events
    - Management identifies potential events affecting its ability to achieve objectives
        - Events with potentially negative consequences represent RISK.
        - Events with potentially positive consequences represent OPPORTUNITY.
- Manage risk
    - Management assesses likelihood and impact of negative events (qualitatively and quantitatively).
- Risk Appetite
    - Is directly linked to entity's strategy: expressed either quantitatively (high, medium, low) or quantitatively (key indicators for growth, return and risk)
    - Linked with Risk Tolerance: acceptable level in risk appetite
- Achievement of entity objectives
    - Effective ERM will provide management reasonable assurance that the entity's objectives will be achieved

Corporate governance and regulatory context

Corporate Governance (CG) is the way organizations are directed and controlled (Cadbury 1992); it is a set of codes, guides, regulations and standards

→ Actually, governance is a synonym for **CONTROLLING**!

- CG is thus an umbrella concept: that provides guidance for all actors on how to achieve corporate goals: organizations need to achieve performance it was established for + at same time adhere at all standards, rules, laws, regulations, policies.
- In that sense, CG heavely depends on effective risk management and good internal controls. CG general framework; ERM is cornerstone for good CG.
- Many countries developd a CG code (we will discuss some examples in a minute). These codes should be concise, understandable and accessible. OECD recognizes that there is no single good model of CG and principles are evolutionary and change with innovations of corporations. Codes are now moving towards non-binding OECD Principles of Corporate Governance → global context.

Last decades many scandals (some examples): Guiness (1986); Maxwell (1991); Baring Futures Signapore (1995); Metropolitan Police (1995); L&H (2001); Enron (2001); Worldcom (2002); Parmalat (2003); Chiquita (2007); Société Générale (2008); Lehman Brothers (2008); Fortis (2008); Madoff (2009); Merill Lynch (2008); Fannie May/Freddie Mac (2008); Northern Rock (2010); etc. + Recently: VW, Ikea, etc.

→Development of CG codes to re-establish performance/conformance balance

- E.g. Guidelines of the European Commission
- The general law in Belgium is that you comply to the code, or you explain. It's okay not to comply but you will have to inform stakeholders why you are not compliant with CG. Why CG in ERM? Because CG tells you itself to do risk management. It tells you to have an audit committee. The CG is a way to ensure that there is some form of ERM implemented in those larger organizations. So, it tells you something that this subject is taken very seriously by those regulatory bodies in Belgium and even everywhere.

Definition of corporate governance (IIA): "The combination of processes and structures, implemented by the board to inform, direct, manage and monitor the activities of the organization towards the achievement of its activities."

SCANDALS (ik denk niet belangrijk)

- *The **Guinness share-trading fraud** was a famous British business scandal of the 1980s. It involved an attempt to manipulate the stock market on a massive scale to inflate the price of Guinness shares and thereby assist a £2.7 billion take-over bid for the Scottish drinks company Distillers.*
- ***Maxwell**: Robert Maxwell, founder and ceo, manipulated funds to give the impression that the company was financially liquid to disguise a huge fraud. The results of the investigation: too long relationship with external auditor – auditor rotation + more idnependence*
- ***Baring Futures Signapore**: Nick Leeson unexperienced trader trading on Signapore exchange → opened an unauthorized account to cover up his large trading losses → lack of internal controls → led to bankrupcy Barings – changes in regulations to make senior executives more accountable for actions of junior staff*
- ***Metropolitan Police**: Anthony Williams Director for special highly sensitive operation against terrorist (1986-1994) → had to set up secret bank account → only his signature needed – stole during many years for private purposes – due to lack of internal control + external control failure; only discovered by tax authorities because Williams had so many houses + renovatations*
- ***Lernout & Hauspie** was een door Jo Lernout, Pol Hauspie en Nico Willaert opgericht spraaktechnologiebedrijf Lernout & Hauspie Speech Products. Het bedrijf kwam in opspraak na onderzoek door The Wall Street Journal omtrent het bestaan van spookbedrijven en boekhoudkundige onregelmatigheden met het doel de koers van de aandelen de hoogte in te jagen. De aandelen van het bedrijf kelderden in nauwelijks een half jaar tijd en uiteindelijk ging L&H failliet in 2001.*
- *Parmalat[3] accounting scandal & mutual fund fraud -- **Parmalat SpA** is a multinational Italian dairy and food corporation. Having become the leading global company in the production of ultra high temperature (UHT) milk, the company collapsed in 2003 with a €14 billion ($20bn; £13bn) hole in its accounts in what remains Europe's biggest bankruptcy.[2] Today, Parmalat is a company with a global presence, having major operations in Europe, Latin America, North America, Australia, China and South Africa. Since 2011, it is a subsidiary of French group Lactalis. Decade of fraudulant accounting.*

⇨ CG covers **a wide range of topics**, and risk management is an integral part of a successful corporate governance of every organization

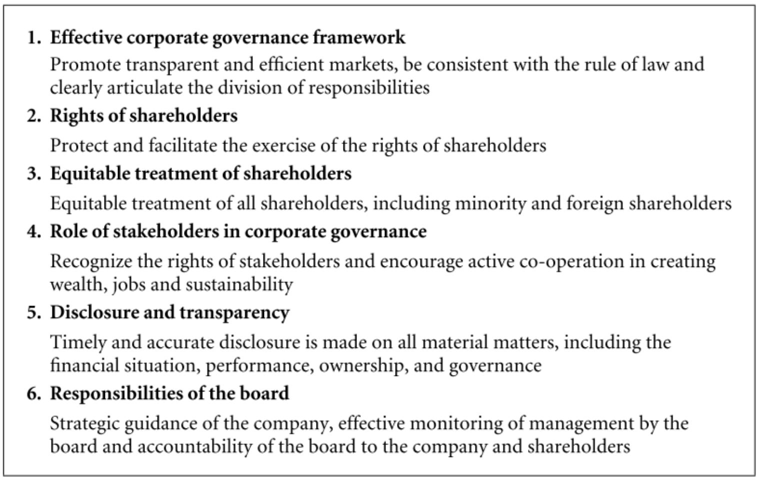
- But CG also comprehends other elements, e.g. strategic direction and business model
- Most countries have placed corporate governance requirements on companies- two main approaches:
  - Comply or explain
  - Full compliance with detailed requirements
- These requirements are particularly strong to companies quoted on stock exchanges

- ***Chiquita Brands International** Financing terrorist organizations. On March 14, 2007, Chiquita Brands was fined $25 million as part of a settlement with the United States Justice Department for having ties to Colombian paramilitary groups. According to court documents, between 1997 and 2004, officers of a Chiquita subsidiary paid approximately $1.7 million to the right-wing United Self-Defense Forces of Colombia (AUC), in exchange for local, employee protection in Colombia's volatile banana harvesting zone. Similar payments were also made to the Revolutionary Armed Forces of Colombia (FARC), as well as the National Liberation Army (ELN) from 1989 to 1997, both left-wing organizations.[8][9] All three of these groups are on the U.S. State Department's list of Foreign Terrorist Organizations.*
- *In January 2008, the bank **Société Générale** lost approximately €4.9 billion closing out positions over three days of trading beginning January 21, 2008, a period in which the market was experiencing a large drop in equity indices.[1] The bank states these positions were fraudulent transactions created by Jérôme Kerviel, a trader with the company. The police stated they lacked evidence to charge him with fraud and charged him with breach of trust and illegally accessing computers. Kerviel states his actions were known to his superiors and that the losses were caused by panic selling by the bank.*

- ***Bernard Lawrence "Bernie" Madoff** (born April 29, 1938) is a former American businessman, stockbroker, investment advisor, and financier. He is the former non-executive chairman of the NASDAQ stock market, and the admitted operator of a Ponzi scheme that is considered to be the largest financial fraud in U.S. history.[In March 2009, Madoff pleaded guilty to 11 federal felonies and admitted to turning his wealth management business into a massive Ponzi scheme that defrauded thousands of investors of billions of dollars. Madoff said he began the Ponzi scheme in the early 1990s. However, federal investigators believe the fraud began as early as the 1970s,[5] and those charged with recovering the missing money believe the investment operation may never have been legitimate.[6] The amount missing from client accounts, including fabricated gains, was almost $65 billion.[7] The court-appointed trustee estimated actual losses to investors of $18 billion.[6] On June 29, 2009, he was sentenced to 150 years in prison, the maximum allowed.[8][9]*
- *Lehman Brothers filed for Chapter 11 bankruptcy protection on September 15, 2008. The **bankruptcy of Lehman Brothers** remains the largest bankruptcy filing in U.S. history with Lehman holding over $600 billion in assets.*
- *Op 7 september 2008 werd **Fannie May**, alsook sectorgenoot **Freddie Mac**, door de Amerikaanse overheid onder curatele geplaatst, waarbij de leiding van het bedrijf werd overgenomen door de Federal Housing Finance Agency. Directeur Daniel Mudd werd ontslagen. Tot deze stappen werd besloten naar aanleiding van een rapport van Morgan Stanley in opdracht van de Amerikaanse Minister van Financiën[1]. Daaruit bleek dat de onderneming - na herrekening van de financiële positie - niet over de voorgeschreven hoeveelheid eigen vermogen beschikte. Voortdurende verliezen op hypotheken leidden tot een gestage stroom verliezen, die tot aanmerkelijke financiële steun van de Amerikaanse overheid noodzaakten. In november 2009 had de Amerikaanse overheid, in diverse vormen, circa $ 60 miljard in Fannie Mae geïnvesteerd[3].*
- ***Northern Rock** (uk) The bank was split into two parts, assets and banking on 1 January 2010.[84] On 15 June 2011, it was announced that the bank was to be sold to a single buyer in the private sector by the end of the year.[85] On 22 March 2011, the bank issued its first mortgage securitisation since the 2007 recession which nearly brought the bank down.[86] On 17 November 2011 it was announced that Virgin Money were going to buy Northern Rock plc for £747 million.[16]*

⇨ **The purpose of CG** is to facilitate accountability and responsibility for efficient and effective performance and ethical behavior. The purpose is to make it efficient and effective but also sustainable and see your company as part of society. Think about all kinds of targets that companies want to achieve in terms of targets.

- CG requirements should be viewed as obligations placed on the board of an organization
    - Legislation
    - Codes of practice
- It should protect executives and employees in the work they are required to do
- It should ensure stakeholder confidence in the ability of an organization to identify and achieve outcomes that its stakeholders value. In these troubling times we live in allot of investors look for security and stability. If you can provide that to your shareholders, it's a good thing.



1. **Effective corporate governance framework**
   Promote transparent and efficient markets, be consistent with the rule of law and clearly articulate the division of responsibilities
2. **Rights of shareholders**
   Protect and facilitate the exercise of the rights of shareholders
3. **Equitable treatment of shareholders**
   Equitable treatment of all shareholders, including minority and foreign shareholders
4. **Role of stakeholders in corporate governance**
   Recognize the rights of stakeholders and encourage active co-operation in creating wealth, jobs and sustainability
5. **Disclosure and transparency**
   Timely and accurate disclosure is made on all material matters, including the financial situation, performance, ownership, and governance
6. **Responsibilities of the board**
   Strategic guidance of the company, effective monitoring of management by the board and accountability of the board to the company and shareholders

- One of the most influential guidelines has been the OECD Principles of Corporate Governance—published in 1999 and revised in 2004.
- The OECD guidelines are often referenced by countries developing local codes or guidelines.
- Building on the work of the OECD, other international organizations, private sector associations and more than 20 national corporate governance codes formed the United Nations Intergovernmental Working Group of Experts on International Standards of Accounting and Reporting (ISAR) to produce their Guidance on Good Practices in Corporate Governance Disclosure. This internationally agreed benchmark consists of more than fifty distinct disclosure items across five broad categories: Auditing,

Board and management structure and process, Corporate responsibility and compliance, Financial transparency and information disclosure and Ownership structure and exercise of control rights

    - Disclosures should include foreseeable risk factors

CG in the Belgian context

- ○ Corporate governance code 2004 ("Code Lippens") à Corporate governance code 2009 ("Code 2009")
- ○ Corporate governance code for non-listed enterprises 2005 ("Code Buysse")
- ○ Law of April 6, 2010: Law to strengthen corporate governance
    - Article 96 Corp. Law already required a description of the main risks the company is exposed to in the management report
    - For listed enterprises this is now extended by a Corporate Governance Statement, including a description of the main features of the company's internal control and risk management systems in relation to financial reporting process and a remuneration report
- ○ RD of June 6, 2010: Code 2009 as "reference code" for listed companies

- *In 2004 the Committee on Corporate Governance was installed in Belgium. This Commission was established on the initiative of the Commission for Banking, Finance and Insurance Commission, the Federation of Enterprises in Belgium and Euronext Brussels. The Commission had to establish a unique reference code for Belgian listed companies. The Belgian Corporate Governance Code was published on 9 December 2004, often referred to as Code Lippens.*
- *Since 1 January 2005 the Lippens Code (named after Count Maurice Lippens) effective for listed companies. The Code is not mandatory, but who deviates, must explain why. The Code does not provide for sanctions against any "bad" drivers which raises questions on the strength of the code. Main elements:*
    - ***Publish a corporate governance charter on their website***
    - ***Must include in their annual report a separate section on corporate governance***
    - ***Limits the number of directorships in Belgian listed companies to five***
    - ***Puts more emphasis on the transparency of the remuneration policies (eg compensation of the Board of Directors)***
- *On 12 March 2009 the Commission published the 2009 edition of the Belgian Corporategovernacecode published. It replaces the 2004 version. After the failure of Fortis (with Lippens as head of the board of directors) it was not longer a good idea to all the CG code "Code Lippens".*
    - *Strictly speaking the code asks companies report on internal control system/risk management with respect to all risks (not only financial as in the law of 2010), but also operational, strategic….(this is almost impossible!)*
- *On 6 June 2010, the legislature by means of the KB Code 2009 appointed the reference code for listed companies.*
- *The Code is based on the 'comply or explain' principle ("comply or explain"). This principle, recommended by the OECD, is recognized by the European Directive 2006/46/EC, which stipulates that listed companies should publish a corporate governance statement.*
    - *The flexibility that this principle provides, was preferred to a strict and rigorous application of a detailed set of rules, because this allows to take into account the specific characteristics of the company such as their size, shareholding structure, activities, risk profile and management structure.*
    - *Listed enterprises should publish a Corporate Governance Statement, including a description of the main features of the company's internal control and risk management systems in relation to financial reporting process and a remuneration report*
    - *Buysse Code for non-listed companies and SMEs: Corporate governance also contributes in non-listed companies, family businesses and SMEs to a more dynamic management, improved business performance, sustainable development and improved business continuity. The Code is the result of a bilingual group led by Baron Paul Buysse.*
- *The 'Buysse Code "contains a first general chapter, a chapter with specific recommendations for family businesses and finally the very concrete and innovative best practices for small businesses. Self-regulation and awareness are key. But also external legal and economic advisers play an important role. The code contains a number of innovative proposals and rightly argues for a corporate governance statement. It provides a "framework" a "reference" for governance in smaller organizations. The code is unique and Belgium was the first country worldwide to introduce such a code. Many countries followed afterwards (eg UK 2010).*
- *The Code Buysse is the first in the world, with a separate chapter devoted to family. The Code calls for the creation of a family forum, the editors of a family charter and calls attention to the family succession. But corporate governance remains customization, especially for family businesses and SMEs that need flexible and practical solutions.*

The Code 2009 asks to describe the steps taken w.r.t. remuneration policies and to communicate on how the remuneration is determined, e.g. preparation of a proposal by the management, presentation and discussion of the remuneration committee, explanations and approval of the board, submission to and approval by the general meeting. With respect to fees the law asks to explain a) the principles on which the remuneration was based, with indication of the relationship between remuneration and performance; b) the relative importance of the various components of the remuneration; c) the characteristics of performance bonuses in shares, options or other rights to acquire shares d) information on the remuneration policy for the next two years.

- *20% is still not compliant with the lippens code, it does get better but companies are still working on getting the code operational and getting it 100% right*

FSMA (niet besproken tijdens de les)

Financial Service and Market Authority: The FSMA is responsible for supervising the financial markets and listed companies, authorising and supervising certain categories of financial institutions, overseeing compliance by financial intermediaries with codes of conduct and supervising the marketing of investment products to the general public

FSMA (2010; study 38): compliance of 122 stock listed enterprises with:

- Renewed Corporate Governance Code (2009)
- Corporate Governance Legislation (2010)
    - Almost all organizations declare to use the Code as framework (few organizations refer to other/older Codes)
    - Only 44 % provides a description of the internal control and risk management system (BEL 20: 73 %)
        - Huge variation in depth/details of description (but often very limited)

- FSMA (study 40 and 42): follow-up
    - Improvement (especially wrt remuneration); but still huge variety in quality of information

  → In this review, only new provisions were scrutinized
    - a statement that the company uses the Code as a reference code (legal anchoring Code + comply or explain)
    - a description of the main features of the internal control and risk management systems
    - information on the main characteristics of the working method for evaluating the board of directors, its committees and its individual directors
    - the remuneration report (since the CG Act limits the amount of severance payments and sets limits on the payment of variable remuneration)

  → CHARACTERISTICS INTERNAL CONTROL AND RISK MANAGEMENT SYSTEM: much variation
    - no concrete guidelines on how it should be defined
    - Fully under development!!!!
    - CBFA (Financial Services and Markets Authority (FSMA)) calls for more attention to thorough definition!!!!
    - Also on board evaluation, remuneration and severance pay very limited info in annual reports: too little!!!!
- Study 42: much improvement (especially wrt remuneration); but still huge variety in quality of information

Similar evolutions worldwide

- Sarbanes-Oxley Act 2002 in US: sets new or enhanced standards for all U.S. public company boards, management and public accounting firms
- Enacted as a reaction to a number of major corporate and accounting scandals
    - Top management must now individually certify the accuracy of financial information
    - Penalties for fraudulent financial activity are much more severe
    - Increased independence of the outside auditors
    - Increased the oversight role of boards of directors
    - Creation of PCAOB: oversees, regulates, inspects and disciplines accounting firms in their roles as auditors of public companies
- Debate continues over the perceived benefits and costs of SOX
- Most well-known articles 302 and 404

*The **Sarbanes–Oxley Act of 2002** and more commonly called **Sarbanes–Oxley**, **Sarbox** or **SOX**, is a United States federal law that set new or enhanced standards for all U.S. public company boards, management and public accounting firms. It is named after sponsors U.S. Senator Paul Sarbanes (D-MD) and U.S. Representative Michael G. Oxley (R-OH).*

- *As a result of SOX, top management must now individually certify the accuracy of financial information. In addition, penalties for fraudulent financial activity are much more severe. Also, SOX increased the independence of the outside auditors who review the accuracy of corporate financial statements, and increased the oversight role of boards of directors.*
- *The bill was enacted as a reaction to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These scandals, which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets.*
- *The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the law. It created a new,*

quasi-public agency, the Public Company Accounting Oversight Board, or PCAOB, charged with overseeing, regulating, inspecting and disciplining accounting firms in their roles as auditors of public companies. The act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

- *Debate continues over the perceived benefits and costs of SOX. Opponents of the bill claim it has reduced America's international competitive edge against foreign financial service providers, saying SOX has introduced an overly complex regulatory environment into U.S. financial markets. Proponents of the measure say that SOX has been a "godsend" for improving the confidence of fund managers and other investors with regard to the veracity of corporate financial statements.[*
- *Most well-known articles 302 and 404.*
  - ***Article 302 deals with the control of the dissemination of information (disclosures). The management of a company should periodically report on the effectiveness of controls at two levels: design of controls (design effectiveness) and operation (operating effectiveness).***
  - ***Article 404 lays down rules for the internal control and financial reporting. The management is obliged to publish an explicit statement on the reliability of the internal controls in the company. The CEO (Chief Executive Officer, Managing Director) and the CFO (Chief Financial Officer, Finance Director) should formally declare that all controls are waterproof. In addition to his usual duties in the area of financial reporting, the auditor should add an explicit statement about his/her agreement with the statements of the CFO and the CEO.***
- *The Netherlands: Corporate Governance Code (Tabaksblat Code). In addition to the existing legislation on corporate governance, Dutch listed companies have drawn up their own code of conduct: the Corporate Governance Code. It explains how a company's directors must be organised. Listed companies are not obliged to observe the code, but if they do not they must explain why. Greater emphasis is put on the importance of integral risk management. This starts with assessment of the risks connected with the strategy and financial structure of the company. The next stage is the design and effectiveness of an adequate internal risk management system. The process is concluded by risk reporting and accounting. The supervisory board is closely involved in the strategy stage and monitors the quality of the internal risk management and reporting.*

Risk management and control frameworks

- The **Cadbury Report**, titled *Financial Aspects of Corporate Governance*, is a report of a committee chaired by Adrian Cadbury that sets out recommendations on the arrangement of company boards and accounting systems to mitigate corporate governance risks and failures. The report was published in 1992. The report's recommendations have been adopted in varying degree by the European Union, the United States, the World Bank, and others.

- **The Standard for risk management (AS/NZS 4360),** first published in 1995, has just been replaced by a joint Australia/New Zealandadoption of the newly published ISO 31000:2009. The new ISO Standard has been substantially based on the original AS/NZS 4360 Standard.

- The **Committee of Sponsoring Organizations of the Treadway Commission** (**COSO**) is a voluntary private-sector organization, established in the United States, dedicated to providing guidance on CG. COSO has established a **common internal control model** against which companies and organizations may assess their control systems.
  - Origin: questionable corporate political campaign finance practices and foreign corrupt practices in the mid -1970s. The Treadway Commission, a private-sector initiative, was formed in 1985 to inspect, analyze, and make recommendations on fraudulent corporate financial reporting. COSO was formed in 1985 to sponsor the Treadway Commission. The Treadway Commission was originally jointly sponsored and funded by five main professional accounting associations and institutes headquartered in the United States: the American Institute of Certified Public Accountants (AICPA), American Accounting Association (AAA), Financial Executives International (FEI), Institute of Internal Auditors (IIA) and the Institute of Management Accountants (IMA). The Treadway Commission recommended that the organizations sponsoring the Commission work together to develop integrated guidance on internal control. These five organizations formed what is now called the Committee of Sponsoring Organizations of the Treadway Commission.
  - In September 1992, the four volume report entitled *Internal Control— Integrated Framework* was released by COSO and later re-published with minor amendments in 1994. This report presented a common definition of internal control and provided a framework against which internal control systems may be assessed and improved. This report is one standard that U.S. companies.
  - In 2004 COSO published *Enterprise Risk Management - Integrated Framework*. COSO believes this framework expands on internal control, providing a more robust and extensive focus on the broader subject of enterprise risk management.

- Some users of the COSO report have found it difficult to read and understand. A model that some believe overcomes this difficulty is found in a report from the Canadian Institute of Chartered Accountants, which was issued in 1995. The report, *Guidance on Control*, presents a control model referred to as **Criteria of Control (CoCo**). The CoCo model, which builds on COSO, is thought to be more concrete and user-friendly.

- **ISO 31000 : the new International Risk Management Standard.** ISO 31000 is an International Standard for Risk Management which was published on 13 November 2009 by the International Standards Organization . An accompanying standard, ISO 31010 - Risk Assessment Techniques, soon followed publication (December 1, 2009) together with the updated Risk Management vocabulary ISO Guide 73. ISO 31000:2009 (an untypically brief 34 pages) is the new international standard on risk management. Its foundation is AS/NZS 4360:1999, the Australian standard originally published in 1995. ISO 31000 provides a generic framework for establishing the context of, identifying, analyzing, evaluating, treating, monitoring and communicating risk. The good news is that ISO 31000 is compatible with COSO ERM. ISO 31000 could be considered an update to COSO that reflects current risk management thinking internationally. In general, ISO 31000 has some significant advantages over COSO:
    - It is more practical (and less theoretical); it is more clearly written, easier for CEOs, CIOs, risk pros to understand
    - Terms are explicitly defined; more detail is provided
    - The standard can be adapted to develop guidelines to assess existing risk management methodologies

  → The most significant difference is in the definition of risk for ISO 31000 and COSO ERM. The ISO risk definition is the “effect of uncertainty on objectives.” The ISO standard has more focus on the consequences of uncertainty and allows for different views of risk than COSO. The focus on consequences provides a framework to help consider the 'flow on' consequences of an event occurring. COSO ERM defines risk as “the possibility that an event will occur and adversely affect the achievement of objectives.” This definition is more focused on events rather the consequences of events

- **Control Objectives for Information and Related Technology** (**COBIT**) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. ISACA first released COBIT in 1996; ISACA published the current version, COBIT 5, in 2012. COBIT aims "to research, develop, publish and promote an authoritative, up-to-date, international set of generally accepted information technology control objectives for day-to-day use by business managers, IT professionals and assurance professionals". COBIT, initially an acronym for "Control objectives for information and related technology" (though before the release of the framework people talked of "CobiT" as "Control Objectives for IT"[2][3]), defines a set of generic processes for the management of IT. The framework defines each process together with process inputs and outputs, key process-activities, process objectives, performance measures and an elementarymaturity model. The framework supports governance of IT by defining and aligning business goals with IT goals and IT processes.
    - COBIT provides a set of recommended best practices for governance and control process of information systems and technology with the essence of aligning IT with business. COBIT 5 consolidates COBIT4.1, Val IT and Risk IT into a single framework acting as an enterprise framework aligned and interoperable with TOGAF and ITIL.
- **INTOSAI** International Organization of Supreme Audit Institutions à 2004 guidelines for public sector (based on COSO)
- **Basel norms**

Control responsibilities: Internal control

- Definition (COSO, 1992):
  - Internal control is a process, effected by an entity's board of directors, management and other personnel.
  - This process is designed to provide reasonable assurance regarding the achievement of objectives in:
    - effectiveness and efficiency of operations,
    - reliability of financial reporting, and
    - compliance with applicable laws and regulations.
- Characteristics of internal control
  - Process, not an end in itself: Internal control is a process. It is a means to an end, not an end in itself
  - People at every level of the organization: Internal control is not merely documented by policy manuals and forms. Rather, it is put in by people at every level of an organization.
  - Reasonable assurance: Internal control can provide only reasonable assurance, not absolute assurance, to an entity's management and board.
  - Achievement of objectives: Internal control is geared to the achievement of objectives in one or more separate but overlapping categories.

→ It helps to accomplish the goals of the organization.

- The system of internal control plays an important part in the successful management of risks by an organization
- When designing effective internal controls, the company should look to achieve the following objectives of internal control (IIA):
  - Accomplishment of objectives and goals
  - Efficient use of resources
  - Compliance with policies, plans, procedures, laws, regulation, etc.
  - Safeguarding of assets and prevention of fraud
  - Reliable financial and operational reporting (internal + external)
- Effective financial controls, including maintenance of proper accounting records, are an important element of internal controls
  - These financial controls help ensure that the company in not unnecessarily exposed to financial risks and that financial information used to manage the business and for public reporting purposes is reliable

Evolution from Internal control toward Enterprise Risk Management (ERM)

- From individual ("silo's") risk assessment toward overall portfolio risk
  - Evaluates all risks that an organization faces across all its operations that can impact the objectives
  - Addresses the relationship between risks: two or more risks can have an impact on the same activity or objective
- Risk is seen as an effect and not an event
  - Management of control and hazard risks
  - Management of opportunities
- Risk appetite linked to corporate strategy
  - Risico-appetijt is het risico dat een onderneming bereid is te nemen in haar streven de ondernemingsvisie en doelstellingen te bereiken – risico-appetijt is direct gerelateerd tot de ondernemingsstrategie. → en dus een taak van de RvB (cf later)

Control responsibilities: internal audit

- Definition (Institute of Internal Auditing – IIA, 1999):
  - Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

    - Internal audit is part of the internal control of a company and can be seen as the culmination (capstone: sluitstuk) of reasonably designed IC.
    - Internal controls, like direct supervision by superiors, administrative procedures and good financial reporting, are control elements of first order. Internal audit is referred to as control of second order.
- Role of internal auditor: validation of the controls and procedures in place to manage risks
    - Internal auditor controls but cant be part of the control
- Important task of the internal auditor is set audit priorities for the testing of controls
- In general, head of internal audit will have direct reporting line to top in the organization/board level (audit committee)

Responsibility of internal auditor

    - Giving assurance on the risk management processes
    - Giving assurance that risk are correctly evaluated
    - Evaluating the reporting of key risks
    - Reviewing the management of key risks
- Provides thus an assurance service on ERM processes: monitors the effectiveness of the ERM processes designed and implemented by management
- Not involved in developing and imposing ERM processes, nor in managing risks, establishing enterprise risk appetite, etc.
- Part of internal control:
    - Internal control: control of first order
    - Internal audit= control of second order: control of internal control

Internal Control	Internal Audit
Part of line function	Staff function
Within hierarchy	Independent (except top and audit committee)
Responsible for activities & their execution	Only responsible for reporting
Administrative manual	Audit charter
No formal standards	Generally accepted standards (IIA)

Part of line function: part of function of every employee – just part of the job
Staff function: separate function – external to normal hierarchy /structure of the organization
Administrative manual: procedures on how to operate – but not specifically focused on risks
Audit charter focusses on risks. There is a clear line between internal control and internal audit

Control responsibilities: external audit

- Does NOT belong to the internal control of the company
- Performed by persons independent of the company:
    - on a contractual basis
    - or in accordance with statutory provisions
- Many different types of external controllers exist
- Most common: external auditor provides an expert opinion on the financial statements of the company

Although there are different types of external auditors that deliver various services, we find here mainly external auditors (e.g. chartered accountants – commissaris revisor → bedrijfsrevisor) to provide an expert opinion (statement) on the financial statements of the company. They give expert opinions usually on annual accounts looking whether they are reliable. An interesting debate is how independent is an external auditor?

***Nuance** of "Role of external auditor": is a bit dubious, why? You pay the fees of an external auditor, but an external auditor just like an internal auditor has to comply to their own code. You really have to comply, so that's partially a guarantee that despite the fact that you are the subject to what you are auditing (who is paying you to audit that) you are still kind of independent.*

Internal audit	External audit
Employee of organization	External contractor
Independent through a) position within organizational chart and b) audit charter	Strictly independent of the organization
Works on behalf of the organization	Works for a third party: shareholders
Not regulated	Regulated
Quality label: Certified Internal Auditor	Quality label: Certified Public Accountant
Broad scope: opinion on adequacy and effectiveness of systems of risk management and internal control (incl. prevention of fraud)	More narrow scope: opinion on true and fair view of accounts (fraud detection is not an objective)
Focus op operational audit	Focus on financial audit
Continuous	Periodic (annual)
Future-oriented	Past period

How do internal and external auditors differ and how should they relate?

- Although they are independent of the activities they audit, internal auditors are integral to the organization and provide ongoing monitoring and assessment of all activities. On the contrary, external auditors are independent of the organization, and provide an annual opinion on the financial statements.
- The work of the internal and external auditors should be coordinated for optimal effectiveness and efficiency. Internal and external auditors have mutual interests regarding the effectiveness of internal financial controls. Both professions adhere to codes of ethics and professional standards set by their respective professional associations.
- There are, however, major differences with regard to their relationships to the organization, and to their scope of work and objectives. The internal auditors' are part of the organization. Their objectives are determined by professional standards, the board, and management. Their primary clients are management and the board. External auditors are not part of the organization, but are engaged by it. Their objectives are set primarily by statute and their primary client - the board of directors.
- The external auditor should work strictly independent of the organization. The Internal Audit team is also independent, but through its position within the organizational chart and through its audit charter. The charter of the internal audit activity is a formal written document that defines the activity's purpose, authority, and responsibility. The charter should (a) establish the internal audit activity's position within the organization; (b) authorize access to records, personnel, and physical properties relevant to the performance of engagements; and (c) define the scope of internal audit activities.
- The internal auditors scope of work is comprehensive. It serves the organization by helping it accomplish its objectives, and improving operations, risk management, internal controls, and governance processes. Concerned with all aspects of the organization - both financial and non-financial - the internal auditors focus on future events as a result of their continuous review and evaluation of controls and processes. They also are concerned with the prevention of fraud in any form.
- The primary mission of the external auditors is to provide an independent opinion on the organization's financial statements, annually. Their approach is historical in nature, as they assess

whether the statements conform with generally accepted accounting principles, whether they fairly present the financial position of the organization, whether the results of operations for a given period of time are accurately represented, and whether the financial statements have been materially affected.

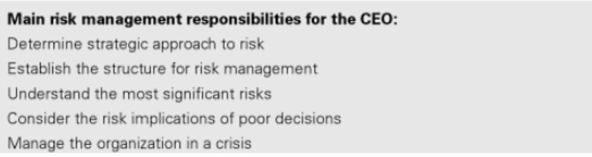
- The internal and external auditors should meet periodically to discuss common interests; benefit from their complementary skills, areas of expertise, and perspectives; gain understanding of each other's scope of work and methods; discuss audit coverage and scheduling to minimize redundancies; provide access to reports, programs and working papers; and jointly assess areas of risk. In fulfilling its oversight responsibilities for assurance, the board should require coordination of internal and external audit work to increase economy, efficiency, and effectiveness of the overall audit process.
- Professional association: Institute of Internal Auditors (IIA) vs American Institute of Certified Public Accountants (AICPA); Instituut der Bedrijfsrevisoren (IBR); Quality label: België: bedrijfsrevisor.Professional organizations play an important role in the training and continuing education of accountants. Also they promote the quality of the audit work by drawing/deigning standards . The national professional bodies for accountants have l united themselves in the International Federation of Accountants (IFAC).

LET OP!
External audit looks at past period, that is indeed true. An internal auditor is future-oriented but that is not really true as an auditor you look in the past, its ex post / after the facts. But the difference here is that you can have debate with the managers on how to improve, how to find a solution… As an internal auditor I have to add value to the company. An external auditor must not deliver added value.

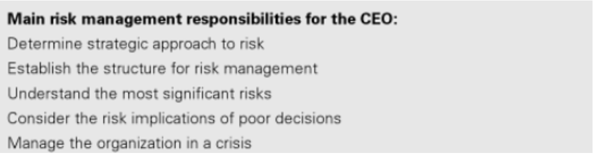
Control responsibilities: Senior management

- Responsible for day-to-day management of risk
  - responsible for enterprise-wide view of risk management

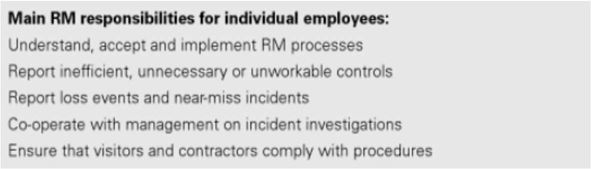
  <-> employees responsible for risks within their area of responsibility
- Responsible for risk reporting to board of directors
- Risk manager / Lead in risk management:
  - Often: Chief Financial Officer (CFO) or Chief Audit Executive (CAE)
  - More and more: Chief Risk Officer (CRO)
- Four major CRO roles (Mikes 2008):
  - Compliance champion
  - Modeling expert
  - Strategic controller
  - Strategic advisor
- No single established reporting position in the structure of an organization for the risk manager: may report to HR, CFO, or sometimes CEO
- The origin of the CRO
  1950s: professional insurance manager
  1970s: focus on financial risks (especially financial sector)
  Early 2000s: CRO a more strategic role (also other industries)
  2010s: CRO important function with various roles



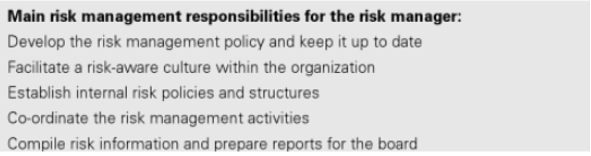
Main risk management responsibilities for the CEO:
Determine strategic approach to risk
Establish the structure for risk management
Understand the most significant risks
Consider the risk implications of poor decisions
Manage the organization in a crisis



Main risk management responsibilities for the CEO:
Determine strategic approach to risk
Establish the structure for risk management
Understand the most significant risks
Consider the risk implications of poor decisions
Manage the organization in a crisis



Main RM responsibilities for individual employees:
Understand, accept and implement RM processes
Report inefficient, unnecessary or unworkable controls
Report loss events and near-miss incidents
Co-operate with management on incident investigations
Ensure that visitors and contractors comply with procedures



Main risk management responsibilities for the risk manager:
Develop the risk management policy and keep it up to date
Facilitate a risk-aware culture within the organization
Establish internal risk policies and structures
Co-ordinate the risk management activities
Compile risk information and prepare reports for the board

Control responsibilities: board of directors

- Not responsible for day-to-day management of risks
- Responsible for strategy, policies, values and risk appetite of the organization → willingness to take risks
- BUT **oversight** responsibility to ensure that ERM processes are
    - comprehensive and tailored to each category of risk
    - in line with the organization's strategy
    - functioning as designed
- Oversight of ERM process employed by an organization is one of the most important and challenging functions of the organization's board of directors
- Boards can also ask independent outside consultants to evaluate the ERM processes for an independent opinion
- ANYWAY: To avoid liability, boards must exercise its OVERSIGHT role – managing risks informally or on an ad hoc basis is no longer tolerable
- **How?** Monitoring systems
    - Periodically review the monitoring systems
    - Make inquiries of management as to their robustness
    - Consider an outside consultant for an independent assessment
    - Be sensitive for "red flags": violations of existing risk limits
    - Developing a culture of risk-aware decision making
    - Violations must be investigated

Driving factors for risk oversight responsibility by board of directors

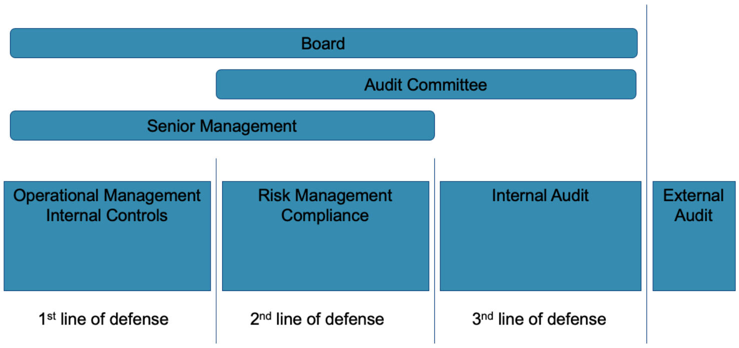
- Fiduciary duty owed to corporate shareholders with TARP (cf state law)
- Court cases (e.g. Delaware courts)
    - Dellaware courts have developed guidelines for Board oversight responsibilities through a series of court cases
        - Guidelines for board oversight responsibilities (Delaware courts)
            - Boards should ensure that their organizations have comprehensive monitoring systems
                - Periodically review these monitoring systems
                - Make inquiries of management as to their robustness
                - Consider an outside consultant for an independent assessment
            - Boards should be sensitive for "red flags", violations of existing risk limits
                - Violations must be investigated
- Recent regulations (e.g. EESA (TARP), SOX)
    - eg Emergency Economic Stabilization Act of 2008, Sarbanes-Oxley Act:
    - *The **Emergency Economic Stabilization Act of 2008**, commonly referred to as a **bailout of the U.S. financial system**, is a law enacted in response to the subprime mortgage crisis authorizing the United States Secretary of the Treasury to spend up to US$700 billion to purchase distressed assets, especially mortgage-backed securities, and make capital injections into banks (however, the plan to purchase distressed assets has been abandoned). Both foreign and domestic banks are included in the program. The Federal Reserve also extended help to American Express, whose bank-holding application it recently approved. The Act was proposed by Treasury Secretary Henry Paulson during the global financial crisis of 2008. President George W. Bush signed the bill into law within hours of its congressional enactment, creating the $700 billion Troubled Asset Relief Program (TARP) to purchase failing bank assets. Supporters of the plan argued that the market intervention called for by the plan was vital to prevent further erosion of confidence in the U.S. credit markets and that failure to act could lead to an economic depression. Opponents objected to the plan's cost and rapidity, pointing to polls that showed little support among the public for "bailing out" Wall Street investment banks, claimed that better alternatives were not considered, and that the Senate forced passage of the unpopular version through the opposing house by "sweetening" the bailout package. TARP (Troubled Asset Relief Program): the act requires that BOARDS OF FINANCIAL INSTITUTIONS participating in TARP institute certain restrictions on executive compensation (related to risk management). Although only applicable to certain financial institutions, the requirements of the act /legislation will also influence organizations in other sectors (sets a standard!)*
- New York Stock Exchange listing requirements
- Industry-specific regulations
- Corporate best practices (e.g. COSO ERM framework)
- Fear for reputation damage (shareholder activism, adverse media coverage, credit rating)
- Risk oversight responsibility often delegated to a committee of the full board
- Often: the Audit Committee
- More and more: a dedicated Risk Management Committee

Responsibility of the Audit Committee on Internal Audit function

  - Review internal audit and its relationship with external auditors
  - Review and assess the annual internal audit plan
  - Review promptly all reports from internal auditors
  - Review management response to the findings of the internal auditor
  - Review activities, resources and operational effectiveness of internal audit
- However, full board remains responsible for monitoring the ERM program

  - *The **Sarbanes–Oxley Act of 2002**, also known as the 'Public Company Accounting Reform and Investor Protection Act' (in the Senate) and 'Corporate and Auditing Accountability and Responsibility Act' (in the House) and commonly called **Sarbanes–Oxley**, **Sarbox** or **SOX**, is a United States federal law which set new or enhanced standards for all U.S. public company boards, management and public accounting firms. It is named after sponsors U.S. Senator Paul Sarbanes and U.S. Representative Michael G. Oxley. The bill was enacted as a reaction to a number of major corporate and accounting scandals including those affecting Enron, Tyco International, Adelphia, Peregrine Systems and WorldCom. These scandals, which cost investors billions of dollars when the share prices of affected companies collapsed, shook public confidence in the nation's securities markets. The act contains 11 titles, or sections, ranging from additional corporate board responsibilities to criminal penalties, and requires the Securities and Exchange Commission (SEC) to implement rulings on requirements to comply with the law. Harvey Pitt, the 26th chairman of the SEC, led the SEC in the adoption of dozens of rules to implement the Sarbanes–Oxley Act. It created a new, quasi-public agency, the Public Company Accounting Oversight Board, or PCAOB, charged with overseeing, regulating, inspecting and disciplining accounting firms in their roles as auditors of public companies. The act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. As a testament to the need for stricter financial governance SOX-type laws have been subsequently enacted in Japan, Germany, France, Italy, Australia, India, South Africa, and Turkey. Debate continues over the perceived benefits and costs of SOX (cf ARTICLE). Opponents of the bill claim it has reduced America's international competitive edge against foreign financial service providers, saying SOX has introduced an overly complex regulatory environment into U.S. financial markets. Proponents of the measure say that SOX has been a "godsend" for improving the confidence of fund managers and other investors with regard to the veracity of corporate financial statements.*

Control responsibilities: summarizing the 'lines of defense'



= important!

1st line: the business

Management has ownership, responsibility and accountability for:

- *Assessing, controlling and mitigating risks;*
- *Maintaining effective internal controls*
  - Development of policies, procedures
  - Description of process flows
  - Identification of risks and key controls
  - Design evaluation of key controls
  - Testing of key controls
  - Reporting of deficiencies
  - Follow-up on deficiencies

2nd line: risk function

3nd line: Internal Audit (IA): responsible for risk assurance

- Internal auditing is an independent, objective assurance and consulting activity designed to **add value** and **improve** an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Part II: A closer look at ERM

Major drivers of ERM development

What are the benefits of ERM?

- Financial benefits: direct financial benefit is that you can say to people that are willing to invest in your company that your company is in control, it's safe to invest money in your company. So, in terms of capital expenditure, in terms of sealing deals where you can acquire more funding, it's a very good thing to have a risk management system in place.
- Preventive controls → which can prevent you from losing allot of money
- There are many drivers we can think of …

External drivers

- Corporate scandals (Enron, WorldCom, etc)
- Economic crisis: some see the economic crisis as proof of ERM not working, during the economic crisis allot of companies lost allot of money <-> proof some /may organizations are not there yet!! Here you could also think about geopolitical crisis like a war, what would that do in your company in terms of managing risks? How to deal with them?
- Studies
    - Joint Australian/New Zealand Standard for Risk Management
    - COSO - US
    - CoCo (Criteria of Control model – Canada)
    - Cadbury Report UK
    - Code Lippens/Buysse/nieuwe Code 2009
- Corporate governance requirements/legal Developments
  Many countries demanded by law to have a risk management system in place. Including credit rating agencies (if you are a triple A company that has an excellent risk management system in place it will be easier to find resources for extra funding).
    - SOX 2002: greater responsibility to board of directors to understand and monitor risks
    - *Een jaar na de CG code werd de Corporate Governance wet (hierna de CG-Wet) gepubliceerd. Zij strekt o.m. tot omzetting van een Europese Richtlijn mbt beloning van bestuurders van beursgenoteerde ondernemingen*
- Regulatory pressure (e.g. rating agencies such as Moody's and Standard & Poor's include ERM system as a factor in their rating methodology)

In other words these are all external drivers that increase the need and necessity to have a decent risk management in place.

Internal drivers

- ERM standards/frameworks/best practices
    - Optimize processes, detect flaws faster within the organization and because you thought about which controls you want to put in place to mitigate that risk you can react faster to this risk. You get to understand your business a bit better, and you can turn that around into more advantaged positions. So, there are really some good decent reasons why risk management must have a place. These are drivers **we** are talking about

- Regulatory pressure including credit rating agencies
- Management and board of directors increasingly accountable for risks
    - Management responsible for considering the probabilities and impact of various possible risk scenarios tied to the overall business strategies – even for risk events that may not be foreseeable (eg 9/11, Hurricane Katrina).
    - Management and board are not expected to foresee these types of events, but they are responsible for and expected to consider and be proactive about thinking of responses to events (i.e. contingency plans) for destroyed operations, lack of cash flow, drastic shifts in regulation etc

- Rising volume and complexities of risks affecting firms – but few organizations have robust key risk indicators: rapid changes in IT, outsourcing, competition, …
- Few have robust risk indicators
    - Inability to recognize shift risks and to proactively act and change strategic initiatives in advance of risk events occuring!
    - SILO approach: risks are managed by BU (Business Unit) managers with little oversight or communication to other BU and the enterprise as a whole (no insights into how particular risks migth impact other risks, including strategic risk)

Internal drivers as ERM can increase value: good ERM leads to better understanding of business (risk & opportunities) and ultimately to increased competitive advantage

→ ERM should create VALUE!

→ BUT is there any direct evidence that risk management increases firm value? The answer is yes, but the evidence is fairly limited yet. At a minimum, whether hedging adds value appears to depend on the types of risk to which a firm is exposed. *(See article on TOLEDO, BUT NOT FOR EXAM)*

→ Research indicates: *"This ranking suggests that while external regulations may have provided the initial impetus for ERM, the promised benefits of a truly enterprise-wide risk management system—better diagnosis and control of strategic and operating risks—only become evident over time. This suggestion is supported by the fact that the Canadian respondents to our survey put this second driver at the top of their list, perhaps reflecting their longer experience with regulatory requirements for risk management that started in the 1990s."*

Major benefits of ERM

If you translate those drivers into benefits, you can have real benefits like listed here below.
This is something that people are looking at. The amount and level of controls you have of your risk and the amount and level of having an ERM system. Some form of ERM is something that people will look at more and more. It is more control driven than it is by looking at the figures, annual reports etc…
Tax bodies for example are also more and more looking at whether companies are in control of their 'VIT risks'. We are evolving from where tax officials were really auditing companies and start auditing them to having a debate and a discussion with management *(are you in control or not?).*

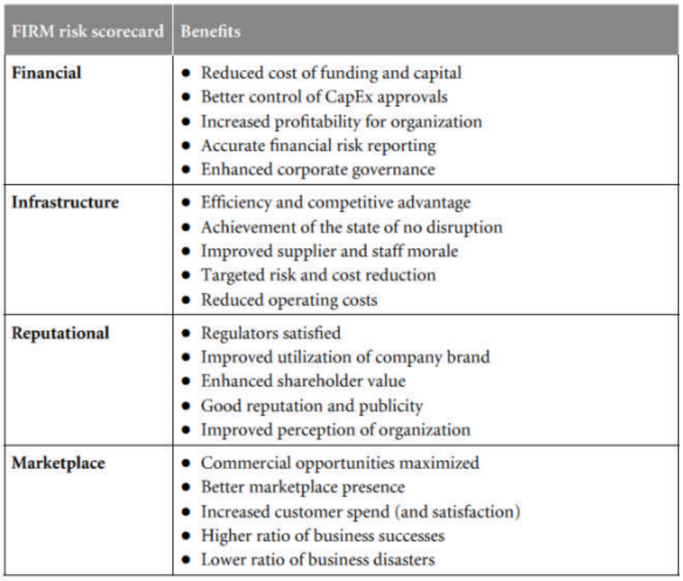
It is for each organization to decide how the enterprise risk management initiative will be structured and how these benefits will be achieved. The key feature of ERM is that the full range of significant risks facing the organization is evaluated.

In order to identify all of the risks facing an organization, a structure for risk identification is required. **Formalized risk classification systems** enable the organization to identify where similar risks exist within the organization. Classification of risks also enables the organization to identify who should be responsible for setting strategy for management of related or similar risks. Also, appropriate classification of risks will enable the organization to better identify the risk appetite, risk capacity and total risk exposure in relation to each risk, group of similar risks or generic type of risk.

The **FIRM risk scorecard** provides such a structure, but there are many risk classification systems available. The FIRM risk scorecard builds on the different aspects of risk, including timescale of impact, nature of impact, whether the risk is hazard, control or opportunity, and the overall risk exposure and risk capacity of the organization. The headings of the FIRM scorecard provide for the classification of risks as being primarily Financial, Infrastructure, Reputational or Marketplace in nature.

The FIRM risk scorecard can also be used as a template for the identification of corporate objectives, stakeholder expectations and, most importantly, key dependencies. The scorecard is an important addition to the currently available risk management tools and techniques. It is compiled by analyzing the way in which each risk could impact the key dependencies that support each core process. Use of the FIRM risk scorecard facilitates robust risk assessment by ensuring that the chances of failing to identify a significant risk are much reduced.

The four headings of the FIRM risk scorecard offer a classification system for the risks to the key dependencies in the organization. The classification system also reflects the idea that 'every organization should be concerned about its finances, infrastructure, reputation and commercial success'. In order to give a broader scope to commercial success, the headings of the FIRM risk scorecard are as follows:



FIRM risk scorecard	Benefits
Financial	● Reduced cost of funding and capital ● Better control of CapEx approvals ● Increased profitability for organization ● Accurate financial risk reporting ● Enhanced corporate governance
Infrastructure	● Efficiency and competitive advantage ● Achievement of the state of no disruption ● Improved supplier and staff morale ● Targeted risk and cost reduction ● Reduced operating costs
Reputational	● Regulators satisfied ● Improved utilization of company brand ● Enhanced shareholder value ● Good reputation and publicity ● Improved perception of organization
Marketplace	● Commercial opportunities maximized ● Better marketplace presence ● Increased customer spend (and satisfaction) ● Higher ratio of business successes ● Lower ratio of business disasters

The features of the FIRM risk scorecard are set out in the Table.

- **Financial** and **infrastructure** risks are considered to be internal to the organization, while **reputational** and **marketplace** risks are external to the organization.
- Financial and marketplace risks can be easily quantified in financial terms, whereas infrastructure and reputational risks are more difficult to quantify.

The inclusion of reputational risks as a separate category of risk in the FIRM risk scorecard is not universally accepted. It is sometimes argued that damage to reputation is a consequence of other risks materializing and should not be considered as a separate risk category. However, if a broader view of risk is taken, it becomes obvious that reputation is vitally important. This is particularly important when organizations are seeking to use their brand name to enter additional markets or achieve 'brand stretch' as it is sometimes called. In any case, there is a broader argument that all risks are a consequence of the broader business decisions. Adopting a particular strategy, undertaking a project and/or continuing with the established operations all involve risks. If the organization did not undertake these strategic, change or operational activities, risks would not be present.

Risk management standards

Many different Risk Management Standards exist (ISO 31000, COSO, CoCo, etc.). A risk standard is a document that produces information on both:

- The risk management process (**8R-4T**) = RMP
- The risk management framework (RASP)
    - Risk Architecture: communications and reporting structure
    - Strategy: overall risk management strategy that is set by the organization
    - Protocols**:** set of guidelines and procedures

Risk management needs to offer an integrated approach to the evaluation, control and monitoring of these types of risk.

- RMP identifies, assesses and treats risks
- RMP is applied to every decision in the organization
- RMP is supported by risk communication, consultation, monitoring and review

The risk management process is well established, although it is presented in a number of different ways and often uses differing terminologies.

Role of ERM **framework** is to facilitate the Risk Management Process (RMP). The risk management process cannot take place in isolation. It needs to be supported by a framework within the organization. Once again, the risk management framework is presented and described in different ways in the range of standards, guides and other publications that are available. In all cases, the key components of a successful risk management framework are **the communications and reporting structure (architecture),** the overall risk management strategy that is set by the organization **(strategy)** and the set of guidelines and procedures **(protocols)** that have been established. The importance of the risk architecture, strategy and protocols (RASP) is discussed in detail.

The combination of risk management processes, together with a description of the framework in place for supporting the process, constitutes a **risk management standard**. There are several risk management standards in existence. There is eg the American COSO ERM framework. The latest addition to the available risk management standards is the international standard, ISO 31000, published in 2009.

Some definitions:
Risk attitude indicates the long-term view of the organization to risk. Different organizations will have different attitudes to risk: Risk averse - Risk aggressive

Risk appetite (risk criteria) indicates the short-term willingness to take risk. It is the total value of the corporate resources that the board of the organization is willing to put at risk = Very important concept in risk management but very difficult to precisely define. This should be taken within the context and not as a stand-alone decision.

The risk management process

The basic explanation of the risk management process is referred to as the **8Rs and 4Ts.** There are many ways to represent the Risk Management Process. ISO standard slightly differ – but basic building blocks are the same. This is a basic representation – 8Rs and 4Ts - makes it easy to remember.

Recognition of risk: recognition or identification of the nature of the risk and the circumstances in which it could materialize. Ways to find out about risk:

- Compare yourself to other companies.
- Test up research
- Reporting → red flags in these reports
- Talk to people: step into organization, talk to management, …

Rating of risks: in terms of magnitude and likelihood to produce the "risk profile" that is recorded in the risk register → How?

- Using a scale from 1-10
- However, there is some <u>bias</u> there it is not fully objective → if I ask a person who is very risk avoiding how they would you rate a specific type if risk this would be different from someone who is risk seeking.
- We should think about the **likelihood** of this risk appearing.
- What **impact** does that risk have? For example, the risk of an earthquake in Leuven. How would you assess the impact? How likely is it that we have a 7-point earthquake in Leuven? Almost zero. Impact however would be massive. This is a start to rate the risk that would happen.

⇨ Start to **prioritize** some risks depending on the **likelihood** and **impact**.

Ranking of risks: ranking current risk against established risk criteria or risk appetite. This leaves a philosophical question
→ if I talk to a risk averse or risk lover this would affect which ranking, they will give so you need **criteria**: some form of items that states when a score of 1 is a 1 in terms of likelihood/impact and when a score of 5 is a 5 in terms of likelihood/impact → you should think about this from a <u>risk management perspective</u>.
*Example: if X happened X times a year then it is a 5. You should define this and talk to people in the firm about this. It's important to **communicate** about them.*
Also here important is the risk appetite: if the board decides the risk appetite for the company, its very important to compare that to how you rank those risks.

Responding to risks *(This matches good with what we have seen in the previous lecture (4 types of controls). These are the controls you want to put in place)*: including the decisions on the appropriate action regarding the following options **(4Ts)**:

- Tolerate: After assessing the Impact and Likelihood of the risk and assessing the control measures required to further reduce the risk, it may be decided that the risk will be accepted without further mitigation
- Treat: Control measures or processes to reduce the risk by addressing the causes, impact and/or likelihood of the risk. Control measures must be proportionate to the risk and provide value for money.
- Transfer: Some risks can be transferred to another body or organisation, e.g. insurance, outsourcing. Care needs to be taken that the risk is actually transferred. Some risks cannot be transferred e.g. reputation
- Terminate: Although unusual there may be occasions when the residual risk is considered unacceptable and the only acceptable course of action is to cease all or part of an activity e.g. Field trips to high risk places

Resourcing controls: to ensure that adequate arrangements are made to introduce and sustain necessary control activities. You want to put a control in front of a risk. If you have a risk with score 1 vs one with score 25 on which one do you want to put your control? (25 of course)

- When you think about internal control you want to think about the most pressing one within your company. Does that mean that it is forbidden to put controls before a risk with score 1? No, but the key is that you must always think about how much time and resources you need for a control to be put in place and what will be the benefit of that.
- If the benefit is greater than time & money invested than you should do it. If it turns out that you have to reorganize your whole financial software system for example or if you have to put in allot of effort to mitigate a risk with score 1 than maybe it's not worth it.

Reaction (and event) planning: for hazard risks this will include disaster recovery or business continuity planning.

- When you are **responding** (←→ reaction) to risk you upstream the process. You think about what to do about the risk before the risk happens.
- When you think about **reaction**, you think about what you are going to do after the risk happens. How can I make sure that there is continuity in my business when something bad happens? That's why there are back up plans in place, recovery produces…

Reporting (and monitoring) risk performance: actions and events and communicating on risk issues, via the risk architecture of the organization. When you think about the process you want to report about how that process is going. You need red flag reports to indicate that something is going wrong.

Reviewing the risk management system: including internal audit procedures and arrangements for the review and updating of the risk architecture, strategy and protocols. If nobody is taking notes or reports on the risks, everything falls apart.

To ensure that risk management remains a DYNAMIC activity, organizations should ensure that the risk management process is repeated as often as necessary → feedback loops. When you think in terms of the risk management process vs risk management framework → for the process you need to think about the 8Rs.

Risk management framework

Each Risk Management Standard refers to the Risk Management Framework, but in different ways. Role of ERM framework is to facilitate the Risk Management Process (RMP). The risk management process cannot take place in isolation. It needs to be supported by a framework within the organization.

Once again, the risk management framework is presented and described in different ways in the range of standards, guides and other publications that are available. In all cases, the key components of a successful risk management framework are **the communications and reporting structure (architecture),** the overall risk management strategy that is set by the organization **(strategy)** and the set of guidelines and procedures **(protocols)** that have been established.

RASP (Risk, Architecture, Strategy and Protocol) has been developed to provide a simple explanation of the scope of the Risk Management Framework

- The organization structures which encompass roles, responsibilities, communication and risk-reporting structure (**architecture**)
    - The British Standard BS 31100: objectives, directive and commitment to manage information risk
- The objectives, **appetite**, attitudes to manage risk, directive (**strategy**), and
    - It's important that when you implement a risk management framework that you know what your **risk appetite** is. It's important to figure out what your architecture is going to be like. What will you do within the structure of your organization to make sure that risk management is happening. Who is responsible for the risk management? Which tools and techniques are we going to use? Coso, basel, …? **It's important to have a good understanding of appetite, how to embed this, who is responsible and what tools will be used.**
    - The British Standard BS 31100: plans, relationship, accountabilities, resources, and activities
- The risk management methodologies, tools and techniques (**protocols**)
    - The British Standard BS 31100: the company strategic and operational policies and practice

Very important: tone at the top and owner share. *If for example the head of bookkeeping wants to implement a risk management system but it doesn't have approval of senior management than it will not happen. You really need <u>ownership</u>.*

*Who should be the **owner** of the risk* management framework? It's the board. They set the risk appetite. The risk manager is ***responsible*** for the risk management <u>process</u>. So, the FRAMEWORK is set by the board and the risk manager is the one that gets the risk management system going.
Is the risk manager the one responsible for risk within a company (if the risk happens)? Management is actually responsible for handling and dealing with those risk. It's the shareholder who sets the tone but it's the manager who has to deal with that. They have to put controls in place. If there is a major operational catastrophe and its risk induced, then the first person to talk to is the COO.

The combination of risk management processes, together with a description of the framework in place for supporting the process, constitutes a **risk management standard**. There are several risk management standards in existence. There is eg the American COSO ERM framework. The latest addition to the available risk management standards is the international standard, ISO 31000, published in 2009.

These standards state that risk management should take place within the context of the business environment, the organization and the risks faced. ISO 31000 places considerable importance on context:

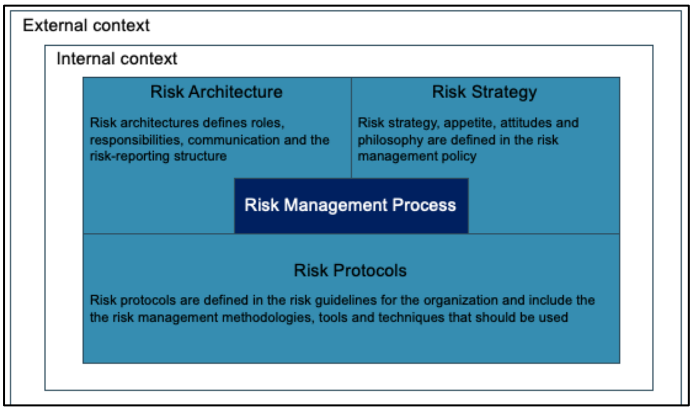
- Internal context: how do you organize your own organization
- External context
- Risk management context: you have to think about risk management as a process itself and there are risks within the risk management

Context is closely related to risk management culture and the benefits that will be derived from enhanced risk management within the organization.
The control environment and the internal environment are measures of the risk culture and the level of risk awareness within the organization. An overall improvement in risk performance will be achieved through improvements in the internal context, risk management context, control environment or internal environment.

RMP should be used for any decision in the organization. It identifies, assesses and treats risks and is supported by risk communication, consultation as well as monitoring and review.

If we tie all these things together, you have your risk framework:

- External context → the world you are in as a company
- Internal → how you organize yourself as an organization, and then within that you have your risk architecture, your role, your responsibilities, your strategy. And you have your protocols, your guidelines.



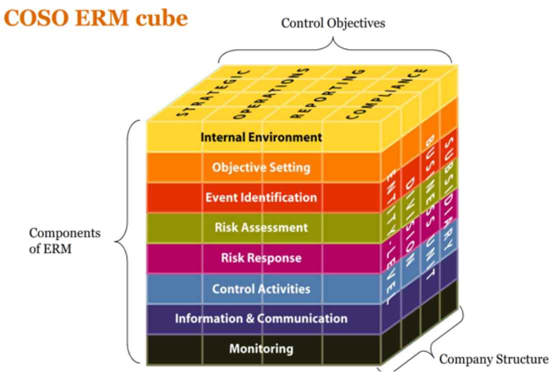
Risk architectures defines roles, responsibilities, communication and the risk-reporting structure

Risk strategy, appetite, attitudes and philosophy are defined in the risk management policy

Risk protocols are defined in the risk guidelines for the organization and include the the risk management methodologies, tools and techniques that should be used

How does the risk management process work? What do you do if something happens? Contigency plans… at the center of that there is the risk management process itself.
If you are a decent risk manager, you know what to do and how to get the process going. Where it usually goes wrong is the framework where the board is not involved enough. It's important that you communicate within your organization and towards your shareholders. It's important that your CEO and CFO and the chairman of the board are really involved in the process. The challenge is to make that risk framework and implement that well and to make that a continuous process.
In general terms these standards are the general rules that are in place when you think about how to implement a risk management process and framework.

COSO ERM Cube



One of the most widely used risk management standards is the COSO framework. For organizations that are listed on the New York stock exchange, the approach outlined in the COSO Internal Control framework (1992) is recognized by the Sarbanes–Oxley Act of 2002 (SOX). The requirements of SOX also apply to subsidiaries of US-listed companies around the world. Therefore, the COSO approach is internationally recognized and, in many circumstances, mandated. It is worth noting that SOX requires the approach described in the COSO Internal Control framework (1992). This is not the same as the COSO ERM framework (2004) described later, although the COSO ERM framework does contain all of the elements of the earlier Internal Control version.

The COSO Internal Control framework has become the most widely used internal control framework in the United States and it has been adapted and/or adopted by numerous countries and businesses around the world. An enterprise risk management (ERM) version of the COSO framework was produced in 2004 and this has both risk management and internal control within scope. The COSO **ERM approach** suggests that enterprise risk management is not strictly a serial process, where one component affects only the next. It is considered to be a multidirectional, iterative process in which almost any component can and does influence all other components.

In the COSO ERM framework, there is a direct relationship between objectives, which are what an entity strives to achieve, and **enterprise risk management component**s, which represent what is needed to achieve them. The relationship is depicted in a three-dimensional matrix, in the form of a cube.

This cube tells you things in **three dimensions.**

First it thinks about **the *company structure***: subsidiary, business unit, division and entity level
→ you can think about risk on all those levels.

Then when you look at **the *control objectives*** it tells you that you can look at risk from a strategic, operational, reporting and compliance perspective.

⇨ The idea behind this cube is that it is possible for example to look at a divisional level in terms of your control objectives of compliance. You can combine two dimensions.

The COSO ERM cube is a very influential risk management framework and it consists of eight interrelated components. These are derived from the way management runs an enterprise and are integrated with the management process. A brief description of the COSO ERM components is set out in the next slide.

COSO ERM describes the framework by stating: 'within the context of the established mission or vision of an organization, management establishes strategic objectives, selects strategy and sets aligned objectives cascading through the enterprise.' This enterprise risk management framework is geared to achieving corporate objectives, set out in four risk categories:

- Strategic: high-level goals, aligned with and supporting its mission.
- Operations: effective and efficient use of its resources.
- Reporting: reliability of reporting.
- Compliance: compliance with applicable laws and regulations.

Third dimensions: the *components of ERM*

Internal environment	The internal environment encompasses the tone of an organization and sets the basis for how risk is viewed and addressed *Tone at the top, which kind of company? How are risks viewed? What is the risk appetite? The COSO model tells you that if you think about the strategic objectives of the company, operational, reporting and compliance, how does the board, senior management, interact with those? On which level are we looking? Divisional? Business unit?*
Objective setting	Objectives must exist before management can identify potential events affecting their achievement. You have to set you objectives before talking about risks. *You have to set goals. What objectives are in place?*
Event identification	Internal and external events affecting achievement of objectives must be identified, distinguishing between risks and opportunities. *It is important to figure out how these events affect the objectives you want to achieve. You need to make the distinction between risk and opportunities. You can look at the event on a compliance level, from a subsidiary point of view for example.*
Risk assessment	Risks are analyzed, considering likelihood and impact, as a basis for determining how they should be managed *If you asses risk in a decent way you can think about response (see below)*
Risk response	Management selects risk responses – avoiding, accepting, reducing, or sharing risk (4Ts)
Control activities	Policies and procedures are established and implemented to help ensure the risk responses are effectively carried out. *How do you respond to the risk and then what contros arel in place to reduce, mitigate the risk?*
Information and communication	Relevant information is identified, captured, and communicated so that people can fulfil their responsibilities. *It's vital that if you put a control in place that you know that the control is doing its job. It's crucial to know that if it is not that it is reported somewhere.*
Monitoring	The entirety of enterprise risk management is monitored and modifications made as necessary

The Risk Management Standards: ISO 31000 standard

There are thus many opinions regarding what risk management involves, how it should be implemented and what it can achieve.
The **International Organization for Standardization (ISO) standard 31000** was published in 2009 and seeks to answer these questions. ISO 31000 was published in 2009 **as an internationally agreed standard** for the implementation of risk management principles. ISO 31000 framework is current best practice: it incorporates COSO and other frameworks.

This chapter provides a structured approach to implementing risk management on an enterprise-wide basis that is compatible with both COSO ERM and ISO 31000. However, more emphasis is placed on ISO 31000 because it is an international standard, and many organizations have international operations.

The purpose of ISO 31000 (2009) is to be applicable and adaptable for "any public, private or community enterprise, association, group or individual.“ Accordingly, the general scope of ISO 31000 - as a family of risk management standards - is not developed for a particular industry group, management system or subject matter field in mind, rather to provide best practice structure and guidance to all operations concerned with risk management.

ISO 31000 (2009) provides generic guidelines for the design, implementation and maintenance of risk management processes throughout an organization. ISO 31000 describes thus a framework for **implementing risk management**, rather than a framework for supporting the risk management process.
The scope of this approach to risk management is to enable all strategic, management and operational tasks of an organization throughout projects, functions, and processes to be aligned to a common set of risk management objectives.

It leaves some latitude to organizations – but the expectation is that the organization’s ERM framework can easily be identified as a ISO 31000 framework. This provides the benefit of a common understanding based on standard terminology and processes. Many ERM failures are due to use of non-standard terminology and hence misinterpretation/misunderstanding. ISO Guide 73 terminology should be used. (E.g. environmental scan → should be linked to ISO term “external context”).

- Advantage of common understanding based on **standard terminology and processes** (ISO Guide 73 terminology; ISO 31010 Risk Techniques)
  One of the key paradigms shifts in ISO 31000 is how risk is conceptualized, under the ISO 31000 (2009) and a consequential major revision of the terminology in ISO Guide 73, risk with respect to the "effect of uncertainty on objectives".

- Overarching ISO principle is that ERM should have **net value for its stakeholders**
  The underlying premise of enterprise risk management is that every entity exists to provide value for its stakeholders. Value: make money, enhance reputation, improve sustainability, reduce harm, etc.
  In other words, enhancement of positive risks and reduction in negative risks must have a net effect that is more than the cost of risk management and risk controls. ERM seeks therefore to deal with risk in a consistent, structured and value-added way by identifying, analyzing and evaluating risks to determine if they should be modified by risk treatment(s) to meet established risk criteria. Throughout this risk management process, there is ideally regular communication and consultation with stakeholders.

- Underlying concept of quality management using **Deming paradigm of Plan-Do-Check-Act (PDCA):** quality of decision making is enhanced by continuously improving the ERM framework.
  - It’s crucial and is used allot in practice. Plan →Do → Check → Act.
  - However, in practice the ‘check’ part is not used allot while this is actually crucial! This is something that is important also in terms of risk management. If you are not checking things, the risk might increase. The final step is that if you have checked something, depending on the outcome you don’t have to do anything because you are on track. You also have to ‘act’, you have to act out what you checked in the previous step. If you do that, if you adjust the course or you repair, solve issues than you come back to where you originally started. If you get these things started like this it will be a motor, a cycle, something that keeps going. And if you do this well. If you want to improve your company, implementation of risk management than this paradigm is always something that has to be going in background.

- **Principle-based** rather than prescriptive: adapt to situation

  The framework has to be practical. Managers are usually overworked. Extra responsibilities need to be manageable and be done effectively. Prescriptive detailed approaches may be counterproductive, therefore principle-based – easy to adapt to circumstances! It is principle based because it has to adapt to different situations.

  → **Unique** for every organization and thus not certifiable

Principles of risk management (ISO 31000, clause 4)

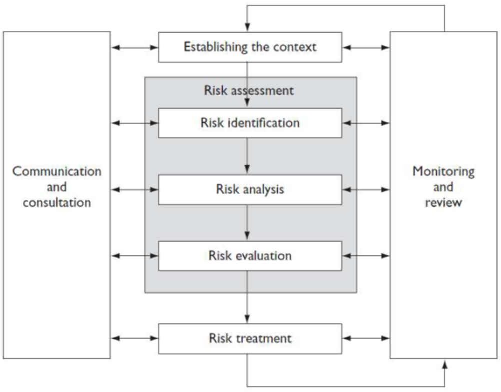
Risk Management should:

- Create and protect value
  - Use risk management to create and protect value. Create and protect value by using risk management to help achieve your organization's objectives and improve its performance.
- Be an integral part of all processes
  - Make risk management part of every process within your organization at every level.
  - Make risk management a responsibility of every manager within your organization.
- Be part of decision making
  - Make risk management part of your decision making process at every level.
    - Use risk management to make informed choices.
    - Use risk management to prioritize actions.
- Be used to deal with uncertainty
  - Use risk management to address the uncertainty that your organization faces.
    - Use risk management to identify and define the nature and type of uncertainties that your organization must deal with.
    - Use risk management to figure out what you can do to address your organization's uncertainties.
- Be structured, systematic and timely
  - Make sure that your risk management approach is structured, systematic, and timely.
    - Make sure that your approach contributes to organizational efficiency.
    - Make sure that your approach generates consistent and reliable results.
- Be based on the best information
  - Make sure that the inputs you use to manage risk are based on the best available information sources.
  - Make sure that decision makers understand and consider the limitations and shortcomings of the data they use to manage risk.
- Be tailored to the environment
  - Make sure that your organization's approach to risk management is aligned with its unique internal and external context.
  - Make sure that your organization's approach to risk management is aligned with its risk profile.
- Consider both human and cultural factors
  - Make sure that your approach to risk management recognizes and considers the human and cultural factors that can influence the achievement of your organization's objectives.
    - Consider how human capabilities can facilitate or hinder the achievement of your objectives.
    - Consider how human perceptions can facilitate or hinder the achievement of your objectives.
    - Consider how human intentions can facilitate or hinder the achievement of your objectives.
- Be transparent, inclusive and relevant
  - Make sure that your approach to risk management is transparent.
    - Make sure that your organization's approach to risk management is open, visible, and accessible.
  - Make sure that your approach to risk management is inclusive.
    - Involve your organization's stakeholders.
    - Involve decision makers from all parts of your organization.

- Be dynamic, responsive and iterative
    - Make sure that your organization’s approach to risk management is dynamic and responsive.
        - Make sure that your approach to risk management continually senses change and responds to it.
    - Make sure that your organization’s approach to risk management is iterative (a process that repeats itself).
        - Repeat your risk management process whenever and wherever objectives need to be achieved.
- Facilitate continual improvement
    - Use risk management to continually improve all aspects of your organization.
    - Develop strategies to continually improve your approach to risk management.

Although there are many ways of representing the risk management process, the basic steps are all similar:

- o RMP in ISO has many similarities with COSO (Link hoofdletters).
- o RMP is used for all decisions in the organization
    - o Routine operations/decisions
    - o Unique strategic decisions



PwC

Risk Management Process (RMP) consist of five activities:

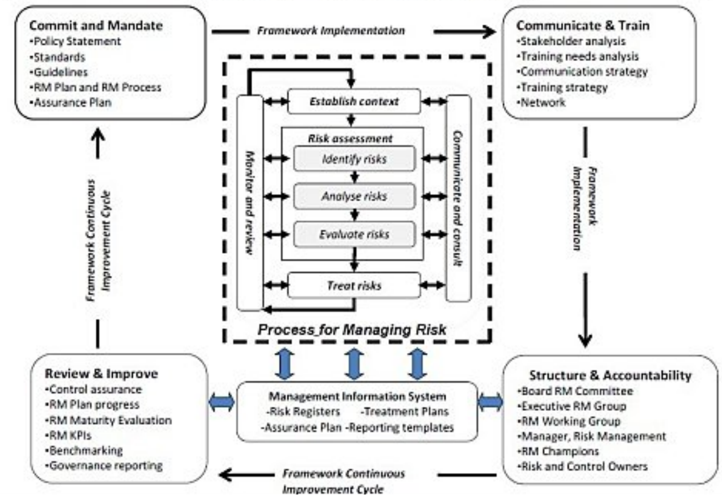
1) **Context**: context of activity or decision requiring risk management - INTERNAL ENVIRONMENT/OBJECTIVE SETTING
   What are our objectives and what do we need to take into account? think in terms of risk appetite
2) **Risk assessment**: identifies, analyzes and evaluates risks - EVENT IDENTIFICATION /RISK ASSESSMENT
    a. Identify - What might happen? How, when and why? *Think about the risk logs, the risk databases where you look them up.*
    b. Analyse - What will this mean for our objectives? What is the likelihood of a risk occurring ?
    c. Evaluate - Which risks need treating? And what is our priority of attention? Think about scoring.

⇨ The core !!

3) **Risk treatment**: reduce risks to acceptable levels - RISK RESPONSE/ CONTROL MEASURES
   How should we best deal with them?
4) **Communication and consultation**: to engage stakeholders in ERM / INFORMATION/COMMUNICTION
   Who are our stakeholders, what are their objectives, and how shall we involve them? Having a debate on all levels of the company
5) **Monitoring and review**: keep close watch to risks and controls & review - MONITORING
   Have the risks and controls changed? You monitor the process and based on that you adjust the process. So, a risk manager in the company is someone who is continuously working on these fields. To ensure that risk management remains a DYNAMIC activity, organizations should ensure that the risk management process is repeated as often as necessary.

*It is important to **distinguish** between a risk management <u>standard</u> and a risk management <u>framework</u>. A risk management standard sets out the overall approach to the successful management of risk, including a description of the risk management process, together with the suggested framework that supports that process. In simple terms, a risk management standard is the combination of a description of the risk management process, together with the recommended framework.*

An ISO 31000 compatible framework for implementing ERM



This illustration shows a typical framework for implementing ERM according to ISO 31000 (source: Broadleaf) The first steps to implementing ERM is to have a list of components. Then these components must be designed and implemented. Most ERM frameworks, including ISO31000, do not specify these components, but rather give conceptual guidance on the framework and its relational structure. We discuss a set of seven main components and their subcomponents for the ISO framework.

It shows the different components + other processes and functions necessary for implementation and continuous improvement. Although the diagram appears complex, it illustrates some essential elements of an ERM framework (ISO 31000, Clause 4):

- **RMP** = inner box. It is the first component that we discuss because it is used to support all decisions in the organization. RMP consists of a traditional set of risk management tasks or activities to support decision making by any manager anywhere in the organization. It consists of 5 main tasks or activities.
- **MIS** box= administrative activity
  It provides the interface between the organization's overall risk management framework and the 100s or 1000s RMPs. It provides the linkage of risk management that is an integral part of the organization through its IT management systems. The management information system includes a risk register, listing the risks, their owners, the risk treatment selected and the continuingmonitoring and review of results for each identified risk. Some organizations, such as global resources giant BHP Billiton, have more than 80,000 risks in their risk register as well as more than 12,000 risk assessments and resulting risk treatments.

Unlike other, more prescriptive regimes, the ISO 31000 framework, since it is fully integrated with existing management processes, can be implemented with a risk management department of only a few people. Typical sizes are from one to four people for the initial phases, often reducing to a single chief risk officer once maturity in risk management with an effective risk culture is achieved. The implementation phase may involve additional resources for training, information systems and so forth. For larger organizations, an implementation period of three to five years is normally required.

Mars Incorporated, a private confectioner and manufacturer of food products, with about 40,000 employees in 40 countries, implemented ERM over a four-year period with one facilitator, who was in high demand to run implementation workshops once the board had embraced the risk management principle (Warner, 2008). Hydro One Inc. in Ontario has developed a fully functioning risk management ERM program over the past decade so that all decisions will include application of the ISO 31000 risk management process (Fraser, 2010).

The PCDA is actually here implemented implicitly. Commit is 'plan', communicate and structure is 'do', the MIS is the 'check', and the review is the 'act'. This has allot of similarities with COSO

RMP (inner box)

Context
= defines the risk management environment and formulates organization-wide risk appetite.
"Context" is a relatively new activity; added to the framework in 2004 New Zealand and Australia Risk Management Standard → included in ISO31000.

Main output:

- Risk criteria to be used to determine the acceptability of the risks
  - are used to evaluate the significance of the risk by comparison of risks with existing or proposed controls. If risk not acceptable, then other treatments are proposed.
- Helps to specify other risk management activities (e.g. risk communication, risk assessment)

Needs to be practical: Boiler plate context checklists + brainstorming for additional items, best practices, industry norms, conferences, special software tools, etc.

Context may be organized into **three components**:

1. **External context**: anything outside the organization that must be taken into account in risk management. *Examples? Stakeholders, regulators, contracts, trends in business drivers, competition, employment situation, norms, etc.*
2. **Internal context**: anything inside the organization that must be taken into account in risk management. *Examples? Capabilities, resources, people and their skills, systems and technology, information flows, internal stakeholders, policies and strategies, etc*.
   - Culture is an important element of the Internal Context
     In an ERM context, a strong culture induces "disciplined decision making"
   - Telling point: pressure for decisions with trade-offs between ST gain and LT risk-adjusted value
   - Culture may also discourage good risk taking when people are punished
     - for taking risks that do not work out even if it was a correct decision to take the risk
     - for hedging against risks that do not materialize
   - A good risk-aware culture is therefore "failure-tolerant":
     - Good decision based on a disciplined approach are right decisions
     - Undisciplined decisions are wrong regardless of whether they result in profit
   - IMPORTANT: tone at the top!!
3. **Risk management context**: any activity in the RMP that requires attention to set the appropriate level of risk. Examples? Scope of the RMP, responsibilities for the different risks, risk assessment methods to be used, time available for RMP, etc.

Risk Assessment – involves three tasks:

1. Risk identification:
   - Risk identification involves the application of a systematic process to understand what could happen, how, when and why.
   - Identifying the risks is a first critical step to inform risk treatment.
   - All risks should be identified and placed in a risk register or risk log (even if later it turns out that risk with associated controls is within acceptable levels)
   - Also identification of existing controls that aim to modify the consequences of the risks.
   - This requires an intimate knowledge of the organization and its environment, as well as an understanding of strategic and operational objectives: knowledge of the factors critical to success and the threats and opportunities related to the achievement of objectives.
   - It should be approached in a methodical way to ensure that all value-adding activities within the organization have been evaluated and all the risks flowing from these activities defined
   - **Categorization** with clear risk names: mutually exclusive categories with main risks and subrisks
   - Room for revision to add unidentified or new risks
   - May use brainstorming, what if analysis, black swan identification

- Failure to employ a systematic approach for risk identification can lead organizations to concentrate their attention to the “known known” risks, and hence miss those that are the “known unknown” or “unknown unknowns” – that never may be treated adequately

2. Risk analysis
    - Risks analysis is concerned with developing an understanding of each risk, its consequences and the likelihood of those consequences.
    - This goes much further than simply the application of a risk matrix (tool we will discuss in later chapter)
    - It also includes an understanding of existing controls and any control gaps: level of risk is most often determined as it is at present: taking into account existing controls and their level of effectiveness: residual risks
        - ➔ There is always a risk that the controls are not working -> internal control risks.
        - ➔ Residual risk: the risk after you implemented the controls to mitigate that risk and after the controls did or did not do their jobs. It’s important to understand what residual risks means. The controls are in place, then the auditor will control whether these internal controls work sufficiently or not. That is where the term residual risk comes from. You have inherent risk; you filter them out with internal controls and what is left is the residual risk.
    - Includes estimates of likelihood of events and consequences of events

3. Risk evaluation: (score of your risk → which one to prioritize?)
    - Risk evaluation involves making a decision about the level of priority of each risk through the application of criteria developed when the context was established
    - Risks are prioritized for attention
    - Cost benefit analysis is deployed to determine whether risk treatment is worthwhile
    - If there no acceptable risk treatment can be found, than it is determined if there is any way to make the risk tolerable – usually with more extensive controls
    - The range of available risk response treatments include tolerate, treat, transfer and terminate. An organization may decide that there is also a need to improve the control environment.
    - Risk evaluation by comparing residual risk against the risk criteria
    - Risk prioritization and cost benefit analysis of risk treatment

→ These three tasks are not done as separate tasks, but with methods that combine the tasks (often also risk treatment (next activity) is included)!

(RISK MATRIX (see book pg 108) is a combined risk assessment method and widely used → see later chapters.)

<u>Risk Treatment</u>

- Includes:
    - Identification of control options
    - Selection of control options
    - Implementation of the selected control
- Approaches to risk treatment → Management selects a *risk response strategy* for specific risks identified and analyzed, which may include:
    - Avoidance: Conscious decision to avoid or pursue a risk → be involved or not, exiting the activities giving rise to risk
    - Remove or isolate risk source
    - Change nature and magnitude of likelihood
    - Change nature and magnitude of consequences
      → Reduction: taking action to reduce the likelihood or impact related to the risk
    - Share or insure: share risk with other parties, transferring or sharing a portion of the risk, to finance it
    - Accept: retain the risk → no action is taken, due to a cost/benefit decision

Monitoring and Review

Monitoring is typically performed by management as part of its internal control activities, such as review of analytical reports or management committee meetings with relevant experts, to understand how the risk response strategy is working and whether the objectives are being achieved.

- Review whether risks and controls have changed
- Is key to continuous improvement of risk management
- Should be applied to the three "line" activities of context, assessment and treatment:
  - Has the context of the risks changed (e.g. crisis)
  - Has the risk changed in character?
  - Are there new risks?
  - Is the risk treatment plan implemented as planned?
  - Are controls effective?
  - Can monitoring be improved?
  - Etc.

Communication and Consultation

- Essential: without communication ERM cannot be effective
- Communicate and consult with all stakeholders
- RMP is a team activity requiring extensive team communication
- Should also be applied to the three "line" activities of context, assessment and treatment

Outer box

Management Information System (MIS)

- Risk management activities should be recorded - needed for
  - Traceability of decisions
  - Continuous improvement of ERM
  - Data for other management activities
  - Legal and regulatory requirements
  - Etc.
- Systems for record keeping, storage, protection, retrieval and disposal need to be carefully designed, implemented, monitored and reviewed
- MIS links the RMP to the risk management framework

Commit and Mandate to the ERM framework

- ERM should be fully integrated in management of the organization
- This requires a mandate/commitment from board and top management for a new or improved/revised ERM framework
- Agreement to proceed with ERM: decision to review ERM framework: assignment of champions & resouces
- Commitment must be continuous/ongoing: framework not only implemented + also maintained and sustained
- Supported by policies: Policies for the ERM framework + Definitions/key terminology

  Policies for risk management decisions
  - Risk appetite = amount and type of risk an organization is prepared to pursue or take
    - For normal/expected outcomes
    - For unexpected/'worst case' outcomes
  - Risk criteria
    - Sets out what risks the organization will take and what risks it will not take
    - Provides for each decision guidance on acceptable risk levels
  - Internal risk reporting
    - Policies on how to aggregate different risks
    - Policies on how to disaggregate risk appetite over managers

Review of policies

Policies should be simple to understand, applied and reviewed

- Check effectiveness of policies over time
- Check whether they are not poorly implemented

Communication and consultation are the continual and iterative processes that an organization conducts to provide, share and obtain information and to participate in dialogue with stakeholders and others regarding the management of risk (ISO guide 73)

- The framework should identify the responsibilities for risk communication
- Particular importance: communication during crisis situations
- Consultation: Process of informed communication prior to decision making. Is a process not an outcome
- Communication: Needed for internal and external stakeholders → To inform and to be informed

Structure and accountability

- Risk ownership:
  - Specify who is accountable for every identified risk
  - Specify who is responsible for controls to treat the risk
- Risk register
  - Everyone in the organization should know who "owns" each risk or risk control
  - Usually contained in a (risk) management information system: contains risk registers, treatment plans, reporting templates, and assurance plans
- The ERM framework itself should also have an owner
  - Accountable for ERM implementation and continuous improvement

Review and continuous improvement

- Risk management performance is monitored and improved through:
  - Self-evaluation by the decision makers
  - Internal audit
  - External audit for critical risks and controls
  - External review through participation in standards organizations, industry-wide user groups, etc
- Monitoring activities for continuous improvement of ERM framework may result in a measure for "risk management maturity" – excellence characteristics (ISO 31000, Appendix A):
  - Formal process for continuous improvement in the framework
  - Accountability for risks with lists of risk owners
  - Documentation of use of RMP in all decision making processes
  - Effective communication about all aspects of RMP
  - High profile for risk management as a core commitment in the organization

Link between ERM and strategy development

Recall ERM definition (see earlier = herhaling)):

> *"a process, effected by an entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives"*

Intentionally broad*: applies to all organizations encompasses all risks no matter what industry, what country, etc…*

- *A HOLISTIC APPROACH to ERM: from "silos" to "an integrated, strategic and enterprise-wide system"*
- *The past practice of silo-based approaches for managing pockets of risk, leads to unclear responsibilities and a lack of visibility, thereby exposing the organization to unnecessary risk*

Analyzing the definition:

- *A process applied in strategy setting*
  - *Based on an entity's mission/strategy, management sets strategic objectives, which if achieved, will create and preserve value for the organization. Management will take into account the risks associated with different objectives/alternatives.*
- *Across the enterprise*
  - *Coordinated by top management, but also part of every employee's job*
- *Identify potential events*
  - *Management identifies potential events affecting its ability to achieve objectives*
    - *Events with potentially negative consequences represent RISK.*
    - *Events with potentially positive consequences represent OPPORTUNITY.*
- *Manage risk*
  - *Management assesses likelihood and impact of negative events (qualitatively and quantitatively).*
- *Risk Appetite*
  - *Is directly linked to entity's strategy: expressed either quantitatively (high, medium, low) or quantitatively (key indicators for growth, return and risk)*

        - *Linked with Risk Tolerance: acceptable level in risk appetite*
    - *Achievement of entity objectives*
        - *Effective ERM will provide management reasonable assurance that the entity's objectives will be achieved*

⇨ Clearly relates ERM to STRATEGY: **STATEGY and ERM need to be aligned and connected**

⇨ Requires a strategic view of risk and a consideration of how external and internal events will affect the ability of an organization to achieve its objectives

Three **key elements** of this ERM definition relate to STRATEGY

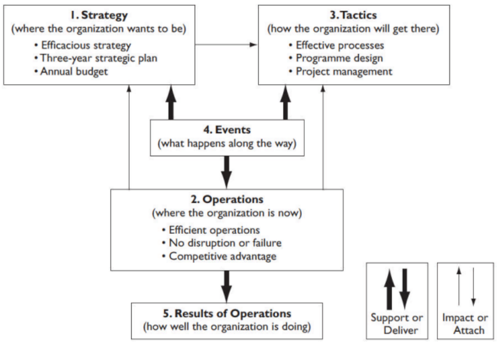
- ERM is directly related to strategy setting. To be effective, it must be embedded in and connected directly to the enterprise's strategy development and strategy execution processes
- ERM is designed to identify events that could affect the company and the performance of its strategy
- A fundamental goal of ERM is to provide reasonable assurance that the enterprise achieves its strategic objectives

→ STATEGY and ERM need to be aligned and connected

→ Requires a strategic view of risk and a consideration of how external and internal events will affect the ability of an organization to achieve its objectives

→ ERM as a **holistic & value-adding**, approach: From "compliance orientation" to "strategic or value-adding orientation"

In order to embed risk management in strategy development, it is useful to consider a business development model:



A basic business development model has the following elements:

- Strategy: "where the organization wants to be"
- Operations: "where the organization is now"
- Tactics: "how the organization will get there"
- Events: "what happens along the way"
    - In many circumstances, these events will represent RISKS that could materialize
- Reporting of results: "how well the organization is doing

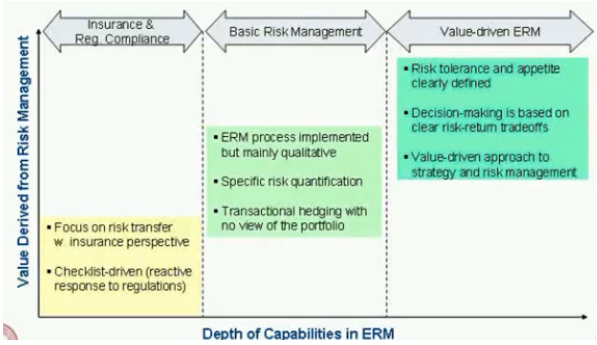
This three-stage approach to development of the business model has EVENTS at its center

This is basically strategy management; with each aspect you can directly link to risk management.

1. **Strategy**
    - Identification of a strategy will require an approach based on opportunity management
    - Opportunity risks: organizations deliberately take risks, especially in market or commercial risks, in order to achieve a positive return
    - Opportunity management is the approach that seeks to maximize the benefits of taking entrepreneurial risks
    - Each organization has its specific appetite for investment in such risks
    - There is a clear link between opportunity management and strategic planning / strategy setting: the goal is to maximize the likelihood of a significant positive outcome from investments in business opportunities

2. **Tactics**
    - Delivery of tactics, often by ways of projects, will require attention to uncertainties and management of control risks will be important
    - Control management: is concerned with reducing the uncertainty and minimizing the potential consequences of these events
    - In general: companies have an aversion to control risks
    - Example: uncertainty about the delivery of a project on time, within budget and to the specifications
    - Over-focused internal control and control management "might suppress entrepreneurial efforts"
    - Risk assessment of strategic plans
        - Make sure that management and board understands the key strategies that create stakeholder value
        - Key strategies: boost revenues, reduce costs, external growth
        - Some of the most valuable assets of an organization aren't on the balance sheet: genuine assets include the most tangible and intangible resouces that make an organization and its offering unique – they are the BUILDING BLOCKS of strategy
    - Identification of critical risk scenarios
        - One approach is to regularly assess strategic risks from three perspectives: risk, opportunities and capabilities
            - Risks are about the risk of loss (loss of revenu, loss of assets, etc)
            - Opportunities are the upside of risk such as opportunities ofr gain in revenu, profitability, etc
            - Capabilities are about distinctive strengths of an organization that can be used to manage the risks and opportunities
            - Define an overriding risk management goal: without understanding of stakeholders appetite for risks, neither board nor management knows what strategic risks to be managed/to be accepted
    - Countermeasures
    - Continuous monitoring
        - Performance measurement: many people believe that the financial crisis is largely attributable to the failure to link performance incentives with the risk management activities within the enterprise (book p 46 example TARP)
3. **Operations**
    - Delivery of effective and efficient operations will require particular attention to the successful management of hazard risks
    - Hazard risks are "pure risks": risk events that can only result in a negative outcome
    - Organizations are faced with a wide range of hazard risks
    - In practice companies will have a "tolerance" of hazard risks, will tolerate a hazard risk exposure and they need to manage these risks within these levels of tolerance
    - Hazard management involves the analysis and management of three aspects of hazard risk:
        1. Actions to prevent the loss
        2. Limit the damage that the event could cause
        3. Contain the cost of recovering from the event

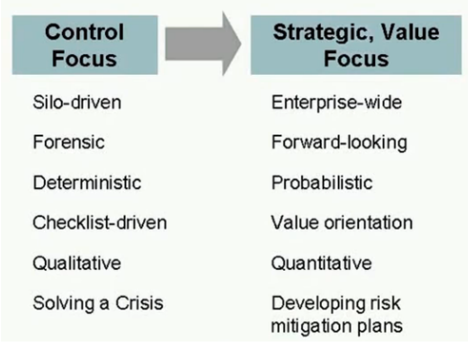
Value-adding ERM: leading organizations are applying ERM as an integral part of strategy setting: This requires higher levels of risk management sophistication


Insurance & Reg. Compliance
Basic Risk Management
Value-driven ERM
• Risk tolerance and appetite clearly defined
• Decision-making is based on clear risk-return tradeoffs
• Value-driven approach to strategy and risk management
• ERM process implemented but mainly qualitative
• Specific risk quantification
• Transactional hedging with no view of the portfolio
• Focus on risk transfer w. insurance perspective
• Checklist-driven (reactive response to regulations)
Value Derived from Risk Management
Depth of Capabilities in ERM

You can look here at how mature the organization is:

- Basic Risk Management → critical issue! Checklists+ hedging some risks → false feeling of "risk management"
  →Many agree this was a key driver of current crisis
  → If it is checklist driven, then here is not allot of ERM going on. If we know our risk appetite and we know we want to create value, then there is allot of ERM working and high value for your organization.
- ERM as a holistic, value-adding, approach: From "compliance orientation" to "strategic or value-adding orientation"
- We usually see that big companies find themselves in right segment and KMOs in left segment. What we see with corporate governance is that shareholders, stakeholders, the government want to push the organization to the right segment.

Thus, value driven or strategic ERM includes a shift in approach from:
Control focus → Strategic, value focus
From silo approach → enterprise wide at company level
Replacing backward-looking forensic approach → assessing risks with a forward-looking approach that takes changing (market) conditions into consideration
Instead of deterministic single point estimate of view of the future → companies apply probabilistic analyses to analyzing portfolios of new investment opportunities: measure risks and rewards



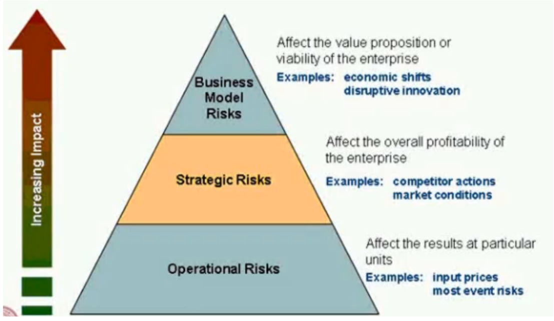
Control Focus	Strategic, Value Focus
Silo-driven	Enterprise-wide
Forensic	Forward-looking
Deterministic	Probabilistic
Checklist-driven	Value orientation
Qualitative	Quantitative
Solving a Crisis	Developing risk mitigation plans

Value-driven ERM requires also a focus on Business Model Risks/Strategic Risks – often very difficult to identify and to quantify

Based on increasing value impact

- Fire in operations → insurance → repaired → no strong value impact
- Development of iPhone → very risky → difficult to assess/predict → competitors are losing market share

For basic risks: heat maps
Strategic risks: statistical approach (we come back on this in later chapters)


Increasing Impact
Business Model Risks
Affect the value proposition or viability of the enterprise
Examples: economic shifts
disruptive innovation
Strategic Risks
Affect the overall profitability of the enterprise
Examples: competitor actions
market conditions
Operational Risks
Affect the results at particular units
Examples: input prices
most event risks

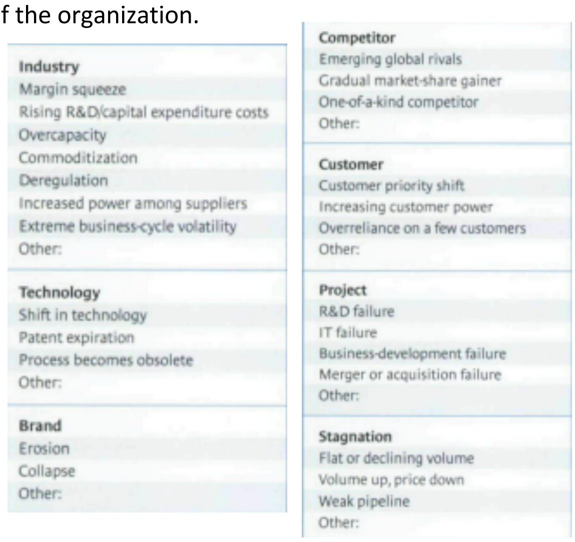
The higher in the pyramid, the more impact on the entire enterprise.

Strategic risk is not a game changer, but it can change the profitability of the organization.

- An array of strategic risks … (not discussed during lecture)

An Array of Strategic Risks and Countermeasures
They categorize strategic risk into seven major classes: industry, technology, brand, competitor, customer, project, and stagnation. Within each class, there are different types of risks. We will describe a particularly dangerous risk from each category and how individual companies have - or have not - deployed countermeasures to neutralize the threat and, in many cases, capitalize on it. (For a list of these risks and countermeasures, see the exhibit "Preventive Measures.")

- and potential (preventive) countermeasures or controls (not discussed during lecture)



Industry
Margin squeeze
Rising R&D/capital expenditure costs
Overcapacity
Commoditization
Deregulation
Increased power among suppliers
Extreme business-cycle volatility
Other:

Technology
Shift in technology
Patent expiration
Process becomes obsolete
Other:

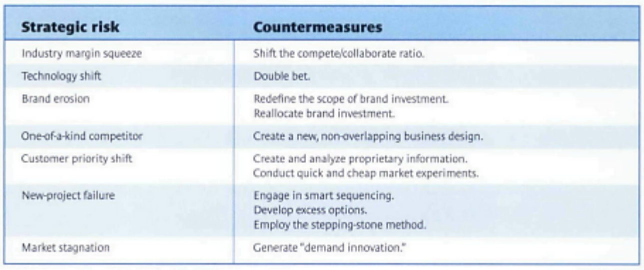
Brand
Erosion
Collapse
Other:

Competitor
Emerging global rivals
Gradual market-share gainer
One-of-a-kind competitor
Other:

Customer
Customer priority shift
Increasing customer power
Overreliance on a few customers
Other:

Project
R&D failure
IT failure
Business-development failure
Merger or acquisition failure
Other:

Stagnation
Flat or declining volume
Volume up, price down
Weak pipeline
Other:



Strategic risk	Countermeasures
Industry margin squeeze	Shift the compete/collaborate ratio.
Technology shift	Double bet.
Brand erosion	Redefine the scope of brand investment. Reallocate brand investment.
One-of-a-kind competitor	Create a new, non-overlapping business design.
Customer priority shift	Create and analyze proprietary information. Conduct quick and cheap market experiments.
New-project failure	Engage in smart sequencing. Develop excess options. Employ the stepping-stone method.
Market stagnation	Generate "demand innovation."

Part III: Risk Assessment

Risk attitude and risk appetite

Many organizations make adequate profits but take too much risk or make inappropriate use of the risk capacity of the organization.

- **Risk attitude** indicates the long-term view of the organization to risk. Different organizations will have different attitudes to risk:
    - Risk averse
    - Risk aggressive
- **Risk appetite** (risk criteria) indicates the short-term willingness to take risk
    - It is the total value of the corporate resources that the board of the organization is willing to put at risk
    - Very important concept in risk management
    - But very difficult to precisely define
    - Should be taken within the context and not as a stand-alone decision
- **Risk capacity** is the capability of the organization to take risk
    - is not the same as the total of all of the individual values at risk within the organization.
- **Risk exposure** is the cumulative total of all of the individual values at risk associated with the risks facing the organization

Most organizations have not determined the value they should risk (risk appetite), nor calculated how much value is actually at risk (risk exposure), nor the capability of the organization to take risk (risk capacity).

An organization should be able to decide how much it wishes to put at risk. Agreeing the risk appetite will ensure that the organization does not put too much (or too little) value at risk.

The risk capacity of the organization needs to be fully utilized to ensure that risk taking is at the optimal level and delivers maximum benefit. Similarly, the organization should not put more value at risk than is appropriate, given the sector in which it operates and prevailing market conditions.

Inherent risk and residual risk

When describing risks it is important to make a distinction between:

- Inherent risk: the level of risks before any actions have been taken to change the likelihood or magnitude of a risk
- Residual risk

Inherent level of risk - controls in place = Residual (or reduced or current level or managed) level of risk

Internal audit recommends describing the Inherent level of risk → Can be compared with current level of risk → Gives indication of quality of controls. But often very difficult to assess Inherent level.

The effort that is required to reduce the risk from its inherent level to its residual or current level can be indicated on **the risk matrix**. A risk map (risk matrix) plots the likelihood of an event against the magnitude or impact should the event materialize.

Risk assessment: definition and description

Risk Assessment is the overall process of risk identification, risk analysis and risk evaluation. The purpose of risk assessment is to identify the significant risks.

1. **Risk identification**
   - Is the process of finding, recognizing and recording risks
   - Includes identifying the causes and source of the risk, events, situations or circumstances which could have a material impact upon objectives

   Risk identification *methods* can include:
   - Evidence based methods (e.g. check-lists and reviews of historical data)
   - Systematic team approaches using a structured set of questions (eg brainstorming)
   - Inductive reasoning techniques (e.g. root cause)
2. **Risk analysis** consists of determining the consequences and their probabilities for identified risk events, taking into account the presence (or not) and the effectiveness of any existing controls
   - Combined to determine a level of risk
   - Impacts may have a low consequence but high probability, or a high consequence and low probability, or some intermediate outcome. In some cases, it is appropriate to focus on risks with potentially very large outcomes, as these are often of greatest concern to managers. In other cases, it may be important to analyze both high and low consequence risks separately. For example, a frequent but low-impact (or chronic) problem may have large cumulative or long-term effects. In addition, the treatment actions for dealing with these two distinct kinds of risks are often quite different, so it is useful to analyse them separately.
   - A common approach is to divide risks into three bands:
     - an upper band where the level of risk is regarded as intolerable whatever benefits the activity may bring, and risk treatment is essential whatever its cost;
     - a middle band (or 'grey' area) where costs and benefits, are taken into account and opportunities balanced against potential consequences;
     - a lower band where the level of risk is regarded as negligible, or so small that no risk treatment measures are needed.
   - *Methods* used in analyzing risks can be qualitative or quantitative: can vary from a simple description of outcomes to detailed quantitative modelling or vulnerability analysis.
     - Qualitative assessment defines consequence, probability and level of risk by levels such as "high", "medium" and "low".
     - Semi-quantitative methods use numerical rating scales for consequence and probability and combine them to produce a level of risk using a formula. Scales may be linear or logarithmic, or have some other relationship.
     - Quantitative analysis estimates values for consequences and their probabilities, and produces values of the level of risk in specific units. Full quantitative analysis may not always be possible or desirable due to insufficient information about the system or activity being analysed, lack of data, influence of human factors, etc. or because the effort of quantitative analysis is not warranted or required. In such circumstances, a comparative semi-quantitative or qualitative ranking of risks by specialists, knowledgeable in their respective field, may still be effective.
   - How?
     - Historical data
     - Expert opinions
     - Probability forecasts using predictive techniques such as fault tree analysis and event tree analysis
3. **Risk evaluation** involves comparing estimated levels of risk with risk criteria - Decisions may include:
   - Whether a risk needs treatment
   - Priorities for treatment

Note that when a risk is identified it may be relevant to more than one of the organization's objectives, its potential impact may vary in relation to different objectives, and the best way of addressing the risk may be different in relation to different objectives (although it is also possible that a single treatment may adequately address the risk in relation to more than one objective). Risk identification and formulation may therefore require different levels of analysis.

Risk description and risk register

Risk description

In order to fully understand a risk, a **detailed description** is necessary so that a common understanding of the risk can be identified and ownership/responsibilities may be clearly understood

- Risks are best expressed as **a cause and effect/consequence relationship**
- For instance, if organizational risks are not managed well, there will likely be consequences for the objectives and performance of the organization, e.g. in terms of: reputation and trust, financial performance, operational performance, and staff.
    - Cf. definition of risk: *"Risk is the effect of uncertainty on objectives"*
        - Understanding cause: helps treating the root cause
            - helps formulate the best possible actions to manage an uncertainty (i.e. treating the root cause instead of the symptom).
        - Understanding the event triggering the risk
        - Understanding consequence: helps formulating contingency plan in case an uncertainty does happen with negative impact.

⇨ Risk is thus characterized by an uncertain event (or uncertainty) that may carry a potential impact on the objectives of the organization. The key word in the definition of risk is uncertain event. The challenge is to identify a potential event which, if it happened, could trigger a set of undesirable consequences for the organization. Needed to allow the identification of the causes leading to the event, their effect or consequence.

Formulating a risk may be a complex exercise which requires **correctly differentiating** between the causes, the event triggering the risk, and its consequences / impact. Furthermore, risks or uncertainties must be assessed and prioritized in relation to objectives (this can be done at any level of objective from personal objectives to organizational objectives). It is important not to confuse risks/uncertainties with consequences or what happens if the risk materialized or from converse statement of the objective. To avoid inadequate risk formulation, a statement of risk should encompass the cause of the risk and its possible impact on the objective (= it should encompass cause and consequence).

- Example: objective = to travel by train from A to B for a meeting at a certain time in the cheapest way possible
- Failure to get from A to B on time for the meeting
    - NO – This is simply the converse of the objective (it does not shed light on what can be done to help achieve the objective)
- Being late and missing the meeting
    - NO – This is a statement of the impact of the risk, not the risk itself. It does not provide insight into the cause
- Get up late, miss the train and being to late for the meeting
    - YES – This is an uncertainty (a threat), within your sphere of direct influence, it can be managed by making sure you allow plenty of time to get to the station

Risk description can also include:

- Name or title of risk
- Causes of the risk
- Consequences should the risk materialize at current/residual level
- Likelihood and magnitude of event
- Stakeholders in the risk, both internal and external
- Responsibility for developing risk strategy and policy
- Existing control mechanisms and activities
- Inherent and residual risk
- Confidence in existing controls and potential for risk improvement
- Risk improvement recommendations and deadlines for implementation
- Responsibility for implementing improvements
- Responsibility for auditing risk compliance
- …
- Often also prioritization of risks needed

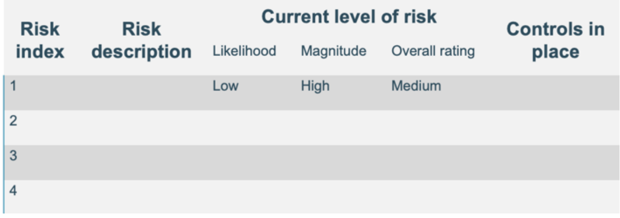
Risk register

= the 'document used for recording the risk management process for identified risks

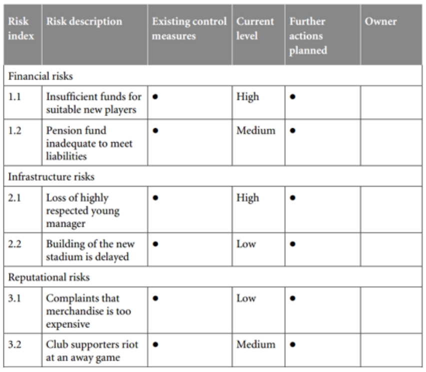
- Provides a structured overview of the results of the risk assessment
- Typically, the risk register will cover the significant risks facing the organization or the project
- Typically includes
  - Ranking or evaluation of risks in terms of magnitude and likelihood to produce the 'risk profile' that is recorded in a risk register
    - With colors: makes it visible
  - Information on current controls and details of intended additional controls
  - Ownership of each risk
- No fixed format
- The risk register should **not become a static document**
  - It has to be refreshed on a daily basis: risk will change, will come

→ Proof that you are doing a risk assessment process

Example of risk register



Risk index	Risk description	Current level of risk			Controls in place
		Likelihood	Magnitude	Overall rating	
1		Low	High	Medium	
2					
3					
4					

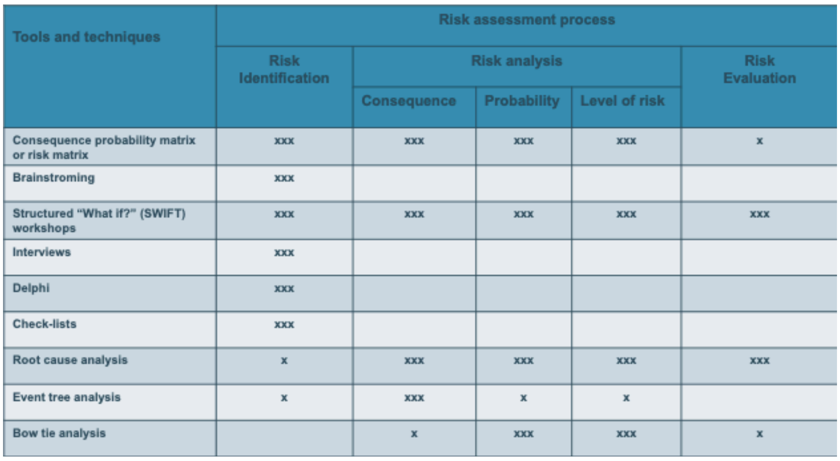


Risk index	Risk description	Existing control measures	Current level	Further actions planned	Owner
Financial risks					
1.1	Insufficient funds for suitable new players	•	High	•	
1.2	Pension fund inadequate to meet liabilities	•	Medium	•	
Infrastructure risks					
2.1	Loss of highly respected young manager	•	High	•	
2.2	Building of the new stadium is delayed	•	Low	•	
Reputational risks					
3.1	Complaints that merchandise is too expensive	•	Low	•	
3.2	Club supporters riot at an away game	•	Medium	•	

Risk assessment tools and techniques

The manner in which the risk assessment process is applied is dependent not only on the context of the risk management process but also on the methods and techniques used to carry out the risk assessment

- Standard ISO 31010 published in 2009 provides detailed information on the full range of risk assessment techniques that can be used



Tools and techniques	Risk assessment process				
	Risk Identification	Risk analysis			Risk Evaluation
		Consequence	Probability	Level of risk	
Consequence probability matrix or risk matrix	xxx	xxx	xxx	xxx	x
Brainstroming	xxx				
Structured "What if?" (SWIFT) workshops	xxx	xxx	xxx	xxx	xxx
Interviews	xxx				
Delphi	xxx				
Check-lists	xxx				
Root cause analysis	x	xxx	xxx	xxx	xxx
Event tree analysis	x	xxx	x	x	
Bow tie analysis		x	xxx	xxx	x

3 X means that it is a strong tool, 2 that it can be used…

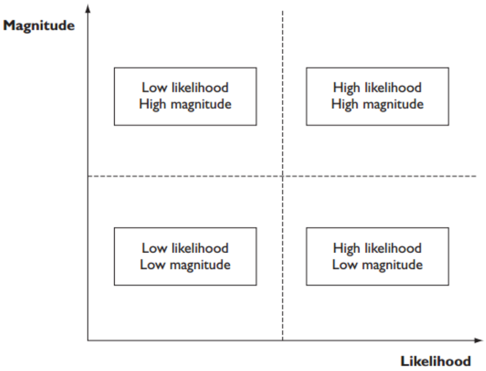
Risk map

A risk map (risk matrix) plots the likelihood of an event against the magnitude or impact should the event materialize

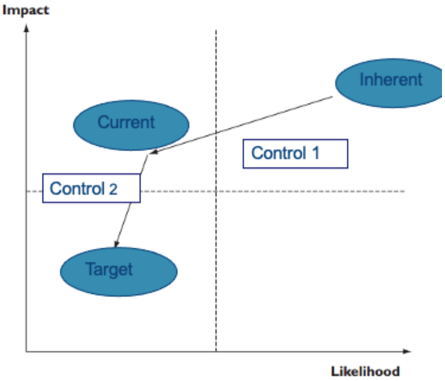
- Is a means of combining qualitative or semi-quantitative ratings of consequence and probability to produce a level of risk or risk rating
- Risk maps can be produced in many formats, but most common:

- Impact/magnitude on Y-axis (impact for residual risks and magnitude for inherent risks)
  - Likelihood on X-axis
- Commonly used as a screening tool when many risks have been identified, for example to define which risks need further or more detailed analysis and which risks need treatment first

As risks move towards the top- right hand corner of the risk matrix, they become more likely and have a greater impact → the risk becomes more important and immediate and effective risk control measures need to be introduced



Can be used both for inherent and residual risks: risk matrix indicating <u>inherent, current (or residual) and</u> <u>target level of risk</u>:



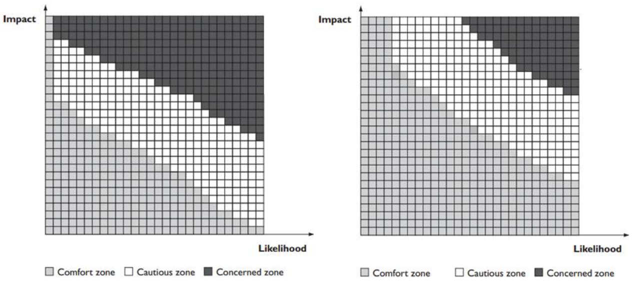
In terms of when you look at the inherent risk: a high likelihood and a like impact but you have a control in place somewhere to mitigate that risk, the residual risk or current risk is less likely but still have a high impact. So, the goal is to reduce the likelihood of the risk. It moves from one quadrant to another. And when you look at the graph you want to your risk to be in the lower left quadrant, then you need to come up with a control number 2 (an extra control) that not only reduce the likelihood of the risk but also the impact of the risk and then you migrate from top right to bottom left of the graph.

Color coding is often used to provide a visual representation of the importance of each risk under consideration: often three or four sections

- Comfort
- Cautious
- Concerned
- Critical

Red - orange – yellow – green

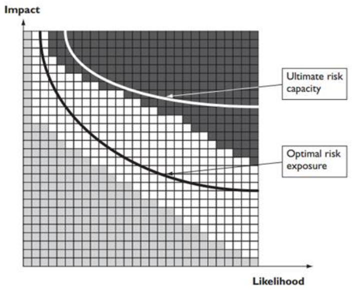
By placing the various risks on the matrix, the relative importance of the risks can be easily identified


Impact
Likelihood
▨ Comfort zone □ Cautious zone ■ Concerned zone
Impact
Likelihood
▨ Comfort zone □ Cautious zone ■ Concerned zone

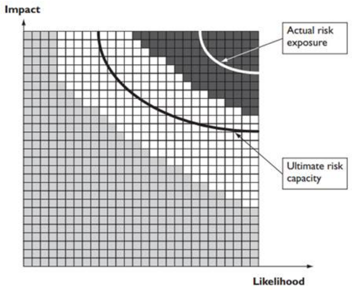
(risk averse)

(risk aggressive)

This risk matrix can be used to decide whether the risk exposure (or risk profile) is acceptable and within the risk appetite and/or risk capacity of the organization:



Risk appetite, exposure and capacity (optimal)



Risk appetite, exposure and capacity (vulnerable)

  - to determine if a given risk is broadly acceptable, or not acceptable according to the zone where it is located on the matrix.

- These figures illustrate the concepts of risk appetite, risk exposure and risk capacity.
  - Risk appetite is illustrated by way of shaded squares on the risk matrix
  - Risk exposure and risk capacity of the organization are shown as a curved line.

⇨ There is a correlation between risk appetite and risk exposure

- The illustration at the left represents risk appetite, exposure and capacity for a risk-averse organization. The lighter area represents a situation where the organization is comfortable with taking the risk. The medium-shaded area represents a cautious zone, where management judgement is required before the risk is accepted. Accepting risks in the darker area will cause the organization concern, and these risks will only be accepted when there is a business imperative. The curved lines represent the overall risk exposure of the organization and this is the optimal position, where the overall exposure cuts through the lighter section. The risk capacity of the organization is shown as higher than both the risk appetite and the risk exposure and is embedded well in the darker area. This represents an optimal state of affairs. This ensures that the organization is taking risks that are within the appetite of the board and not exceeding the ultimate risk capacity of the organization.
- Figure at the right represents a risk-aggressive organization with a much larger comfort zone for accepting risk. The lighter-shaded or cautious zone is smaller and the darker zone is an even smaller part of the overall figure. This situation can be described as representing an approach to risk that has a very limited universe of risk. The universe of risk for the organization is represented by the darker squares and it is only in this area that the board of the organization will consider that the risks are significant. The ultimate risk-bearing capacity of the organization is shown as within the medium-shaded zone. This represents a situation where the organization may be taking risks that are beyond the ultimate risk capacity of the organization. To make circumstances worse, the actual risk exposure of the organization is shown as well within the darker area. This makes the organization vulnerable to risk, because its actual risk exposure is shown to be well beyond its ultimate risk-bearing capacity.

Strengths:

- Relatively easy to use
- Provides a rapid ranking of risks into different significance levels

Limitations:

- Use is very subjective and there tends to be significant variation between raters
- Risks cannot be aggregated
- It is difficult to combine or compare the level of risk for different categories of consequences

Brainstorming

- Involves stimulating free-flowing conversation amongst a group of knowledgeable people to identify potential risks, criteria for decisions and/or options for treatment
- Try to trigger people's imagination by the thoughts statements of others in the group
- Effective facilitation is very important
- Can be formal and informal

Strengths:

- It encourages imagination to help identify new risks and novel solutions
- It involves key stakeholders and hence aids communication overall
- It is relatively quick and easy to set up

Limitations:

- Participants may lack the skill and knowledge to be effective contributors
- Relatively unstructured → may not be comprehensive
- Some people with valuable ideas may stay quiet while others dominate the discussion

Structured "What-if" Technique (SWIFT)

- Is a systematic, team-based study, utilizing a set of 'prompt' words or phrases that is used by the facilitator within a workshop to stimulate participants to identify risks
- Discussion is facilitated with 'what-if' phrases
- Results in discussion/description of the context, the risk, its causes, consequences and (expected) controls

Strengths:

- Widely applicable
- Needs minimal preparation by the team
- Creates a risk register & risk treatment plan
- Involvement in the workshop reinforces accountability/responsibility

Limitations:

- It needs an experienced and capable facilitator to be efficient
- Careful preparation by facilitator is needed
- If workshop team not wide enough experience → may not be comprehensive

Interviews

- Structured interviews: individual interviewees are asked a set of prepared questions from a prompting sheet which encourages the interviewee to identify risks from a different perspective
- Semi-structured interviews: are similar, but allows more freedom for a conversation to explore issues which arise
- Are useful where it is difficult to get people together for a brainstorming session or where free-flowing discussion in a group is not appropriate

Strengths:

- One-to-one communication → more in-depth consideration of issues
- Enable involvement of a larger number of stakeholders than brainstorming which uses a relatively small group

Limitations:

- Time-consuming for the facilitator
- Bias is tolerated and not removed through group discussion
- The triggering of imagination (cf. brainstorming) may not be achieved

Delphi technique

- Procedure to obtain a reliable consensus of opinion from a group of experts
- Experts express their opinions individually and anonymously while having access to the other expert's views as the process progresses:
    - sending the questionnaire to panelists individually.
    - information from the first round of responses is analyzed and combined and recirculated to panelist's;
    - panelist's respond and the process is repeated until consensus is reached

Strengths:

- Views are anonymous → unpopular opinions are more likely to be expressed
- All views have equal weight, which avoids the problem of dominating personalities
- People do not need to be brought together in one place at one time

Limitations:

- It is labor intensive and time consuming
- Participants need to be able to express themselves clearly in writing

Check-lists

- Are lists of hazards, risks or control failures that have been developed usually from experience, either as a result of a previous risk assessment or as a result of past failures
- Are most useful when applied to check that everything has been covered after a more imaginative technique that identifies new problems

Strengths:

- They may be used by non-experts
- They combine wide ranging expertise into an easy to use system
- They can help ensure common problems are not forgotten

Limitations:

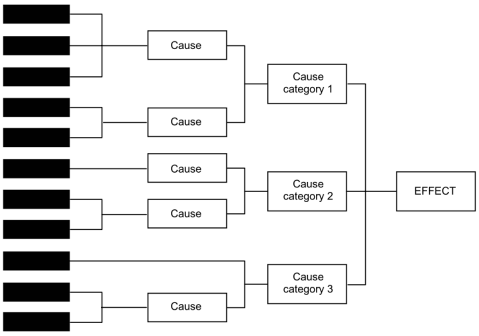
- They tend to inhibit imagination in the identification of risks
- They address the 'known known's', not the 'known unknown's or the 'unknown unknowns'
- They encourage 'tick the box' type behavior

Root cause analysis (RCA) /cause-and effect analysis

- Is a technique for identifying and analyzing causal factors that can contribute to a specified undesired event (called the "top event")
- Attempts to identify the root or original causes instead of dealing only with the immediately obvious symptoms
- Causal factors are deductively identified, organized in a logical manner, and represented pictorially
- Structured analysis techniques may consist of one of the following:
    - "5 whys" technique, i.e., repeatedly asking 'why?' to peel away layers of cause and sub cause
    - Fault tree analysis
    - Fishbone or Ishikawa diagrams

It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyze losses on a more global basis to determine where improvements can be made.

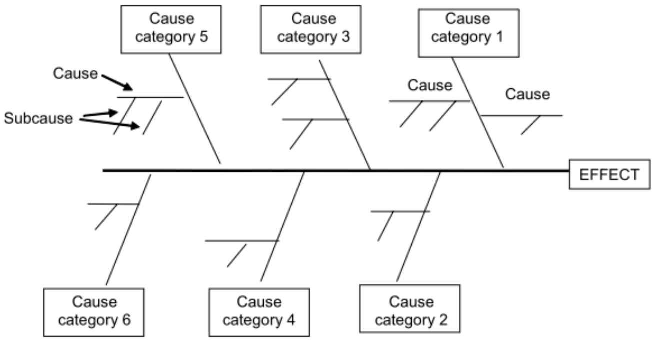
Tree formulation of cause-and-effect analysis:



The tree representation is similar to a fault tree in appearance, although it is often displayed with the tree developing from left to right rather than down the page. However, it cannot be quantified to produce a probability of the head event as the causes are possible contributory factors rather than failures with a known probability of occurrence

The results are normally displayed as either a **Fishbone or Ishikawa diagram or tree diagram.** The Fishbone diagram is structured by separating causes into major categories (represented by the lines off the fish backbone) with branches and sub-branches that describe more specific causes in those categories.

It is recognized that corrective action may not always be entirely effective and that continuous improvement may be required. RCA is most often applied to the evaluation of a major loss but may also be used to analyze losses on a more global basis to determine where improvements can be made.



Strengths:

- Structured /systematic analysis
- Consideration of all likely hypotheses
- Useful for analyzing systems with many interfaces/interactions
- Pictorial representation leads to an easy understanding

Limitations:

- Uncertainties in the probabilities of base events are included in calculations of the probability of the top event
- Can be difficult to ascertain whether all important pathways to the top event are included

Event tree analysis (ETA)

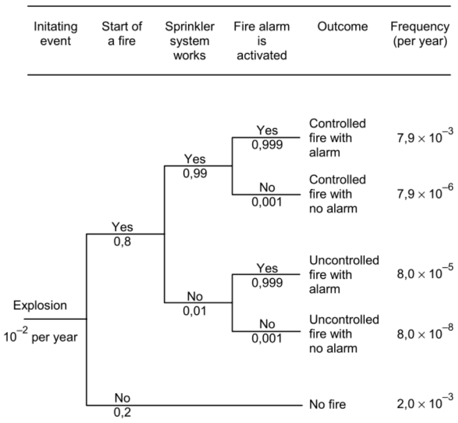
- Is a graphical technique for representing the mutually exclusive sequences of events following an initiating event according to the functioning/not functioning of the various systems designed to mitigate its consequences
- ETA can be used for assessing different accident scenarios following the initiating event
- Most often used to model failures where there are multiple safeguards

Strengths:

- Displays potential scenarios and influence of the success or failure of mitigating systems in a clear diagrammatic way
- Takes into account dependence and domino effects

Limitations include:

- Always a potential for missing some important initiating events
- Difficult to incorporate delayed success or recovery events

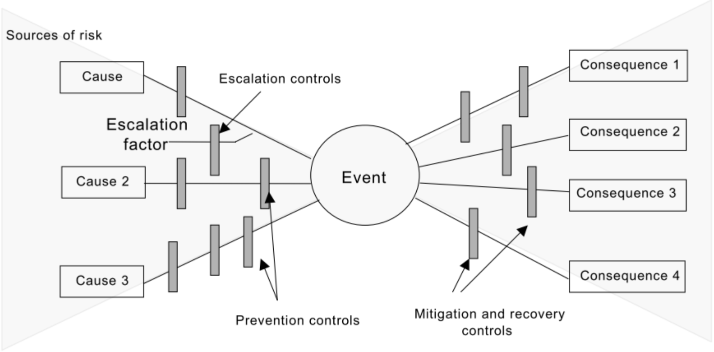


Bow tie analysis

- Is a simple diagrammatic way of describing and analyzing the pathways of a risk from causes to consequences
- Can be considered to be a combination of a fault tree analyzing the cause of an event and an event tree analyzing the consequences
- However the focus of the bow tie is on the barriers between the causes and the risk, and the risk and consequences → ensuring that there is a control for each failure pathway

The bow tie is drawn as follows:

- A particular risk is identified for analysis and represented as the central knot of a bow tie.
- Causes of the event are listed considering sources of risk (or hazards in a safety context).
- The mechanism by which the source of risk leads to the critical event is identified.
- Lines are drawn between each cause and the event forming the left-hand side of the bow tie. Factors which might lead to escalation can be identified and included in the diagram.
- Barriers which should prevent each cause leading to the unwanted consequences can be shown as vertical bars across the line. Where there were factors which might cause escalation, barriers to escalation can also be represented. The approach can be used for positive consequences where the bars reflect 'controls' that stimulate the generation of the event. On the right-hand side of the bow tie different potential consequences of the risk are identified and lines drawn to radiate out from the risk event to each potential consequence.
- Barriers to the consequence are depicted as bars across the radial lines. The approach can be used for positive consequences where the bars reflect 'controls' that support the generation of consequences.
- Management functions which support controls (such as training and inspection) can be shown under the bow tie and linked to the respective control. Some level of quantification of a bow tie diagram may be possible where pathways are independent, the probability of a particular consequence or outcome is known and a figure can be estimated for the effectiveness of a control. However, in many situations, pathways and barriers are not independent and controls may be procedural and hence the effectiveness unclear. Quantification is often more appropriately carried out using FTA and ETA.



A simple and common way to describe risks is to focus on three aspects: cause, event and consequence Often this is also represented in a bow tie analysis (cf. infra): a simple diagrammatic way of describing and analyzing the pathways of a risk from causes to consequences

Strengths:

- Simple to understand; clear pictorial representation of the problem
- Focuses attention on controls: both prevention and mitigation

Limitations include:

- Cannot depict where multiple causes occur simultaneously
- It may over-simplify complex situations, particularly where quantification is attempted

Part IV: Risk Response

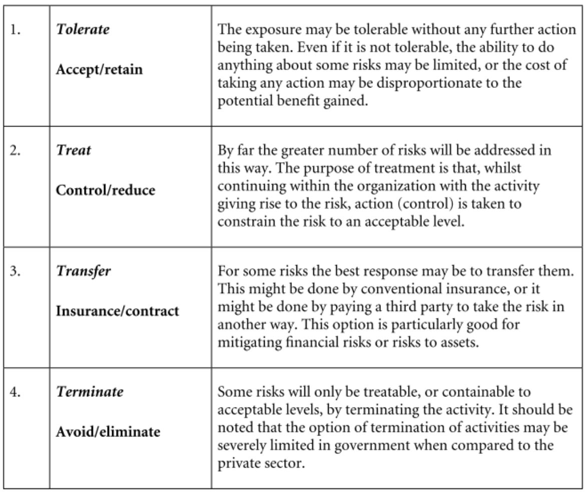
Risk response or Risk treatment:

- The process of developing, selecting and implementing controls (BS 31100)
- Development and implementation of measures to modify risk (ISO 31000)

Priority significant risks:

- High or very high impact in relation to the benchmark test for significance
- High or very high likelihood of materializing at or above the benchmark level
- High or very high scope for cost-effective improvement in control

Generally speaking, it is only priority significant risks that require attention at the most senior level of the organization. However, it is appropriate that regulatory risks also receive board-room attention. In practice, the board will expect these regulatory risks to be properly managed and the board will only receive routine/annual reports describing risk performance, or a special report if a specific issue has arisen.



1.	***Tolerate*** **Accept/retain**	The exposure may be tolerable without any further action being taken. Even if it is not tolerable, the ability to do anything about some risks may be limited, or the cost of taking any action may be disproportionate to the potential benefit gained.
2.	***Treat*** **Control/reduce**	By far the greater number of risks will be addressed in this way. The purpose of treatment is that, whilst continuing within the organization with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.
3.	***Transfer*** **Insurance/contract**	For some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way. This option is particularly good for mitigating financial risks or risks to assets.
4.	***Terminate*** **Avoid/eliminate**	Some risks will only be treatable, or containable to acceptable levels, by terminating the activity. It should be noted that the option of termination of activities may be severely limited in government when compared to the private sector.

TOLERATE

When the hazard risk is considered to be within the risk appetite of the organization, the organization will **tolerate** that risk. Risk tolerance is shown as the approach that will be adopted in relation to low-likelihood risks with low impact. However, an organization may decide to tolerate risk levels that are high because they are associated with a potentially profitable activity or relate to a process that is fundamental to the nature of the organization.

It is unusual for a hazard risk to be accepted or tolerated before any risk control measures have been applied. Generally speaking, a risk only becomes tolerable when all cost-effective control measures have been put in place, so that the organization is accepting or tolerating the risk at its current level. Certain control measures may have been applied because the inherent level of the risk may have been unacceptable. Control effort seeks to move the risk to the low-likelihood/low-impact quadrant of the risk matrix.

Sometimes risks are only accepted as part of an arrangement whereby one risk is balanced against another. This is a simple description of neutralizing or hedging risks, but on a business level this may represent a fundamentally important strategic decision. For example, an electricity company operating independently in the northern states of the United States may have to accept the impact of variation in temperature on electricity sales.

By merging (or setting up a joint venture) with an electricity company in the southern states, the north/south combined operation will be able to smooth the temperature-related variation in electricity sales. The combined operation will then sell more electricity in the northern states during cold weather, when demand in the southern states is low. Conversely, the combined operation will sell more electricity for air-conditioning units in the southern states in the summer, when demand for electricity in the northern states may be lower.

- Risk tolerance (ISO Guide 73): The organization's readiness to bear the risk after risk treatments in order to achieve its objectives
- Risk tolerance relates to a specific risk <-> more general approach of risk appetite
- Often risks only become tolerable when all cost-effective control measures have been put in place: often for residual risks

Risk tolerance can be influenced by legal or regulatory requirements.
An organization may have to tolerate risks that have a current level beyond its comfort zone and its risk appetite. On occasions, an organization may even have to tolerate risks that are beyond its actual risk capacity. However, this situation would not be sustainable and the organization would be vulnerable during this period.

When the hazard risk is considered to be within the risk appetite of the organization, the organization will tolerate that risk. Risk tolerance is shown as the approach that will be adopted in relation to low-likelihood risks with low impact. However, an organization may decide to tolerate risk levels that are high because they are associated with a potentially profitable activity or relate to a process that is fundamental to the nature of the organization.

It is unusual for a hazard risk to be accepted or tolerated before any risk control measures have been applied. Generally speaking, a risk only becomes tolerable when all cost-effective control measures have been put in place, so that the organization is accepting or tolerating the risk at its current level. Certain control measures may have been applied because the inherent level of the risk may have been unacceptable. Control effort seeks to move the risk to the low-likelihood/low-impact quadrant of the risk matrix, as illustrated in Figure 27.1.

TREAT

- Often when level of risk exposure (likelihood) associated with a particular risk is high but the potential loss (impact) associated with it is low
- Often undertaken with the risk at the inherent and/or current level so that when the risk has been treated, the new current level or target level may become tolerable

TRANSFER

- Often when the likelihood of a risk materializing is low but the potential is high
- Insurance is a well-established mechanism for transferring the financial consequences of losses arising from hazard risks
- Other examples: contractual agreement, outsourcing, joint-venture
  - can be achieved by conventional insurance and also by contractual agreement. It may also be possible to find a joint-venture partner, or some other means of sharing the risk. Risk hedging or neutralization may therefore be considered to be a risk transfer option, as well as a risk treatment option.

In some cases, risk transfer is closely related to the desire to eliminate or terminate the risk. However, many risks cannot be transferred to the insurance market, either because of pro-hibitively high insurance premiums or because the risks under consideration have (traditionally) not been insurable.

TERMINATE

- When a risk is both of high likelihood and high potential impact, the organization will wish to terminate or eliminate the risk
  - It may be that the risks of trading in a certain part of the world or the environmental risks associated with continuing to use certain chemicals are unacceptable to the organization and/or its stakeholders. In these circumstances, appropriate responses would be elimination of the risk by stopping the process or activity, substituting an alternative process or outsourcing the activity that is associated with the risk.
- Stopping the process or activity, substituting an alternative process

→ Sometimes not possible: it could be the case that the activity that gives rise to it is fundamental to the ongoing operation of the organization. In such circumstances, the organization may not be able to terminate or eliminate the risk entirely and thus will need to implement alternative control measures.

This is a particular issue for public services. There may be certain risks that are high likelihood and high impact, but the organization is unable to terminate the activities giving rise to them. This may be because the activity is a statutory requirement placed on a government agency or public authority. The public service imperative may restrict the ability to cease the activity, so the organization will need to introduce control measures, to the greatest extent that is cost-effective. It is likely that such control measures will be a combination of risk treatment and risk transfer. As these control measures are applied, the level of risk will move to a level where the organization will be able to tolerate the risk. Because of the variable nature of risks, it may not be possible to get all risks to a level that is within the risk appetite of the organization. The organization may find that it has to tolerate risks beyond its empirical risk appetite in order to continue to undertake a certain activity.

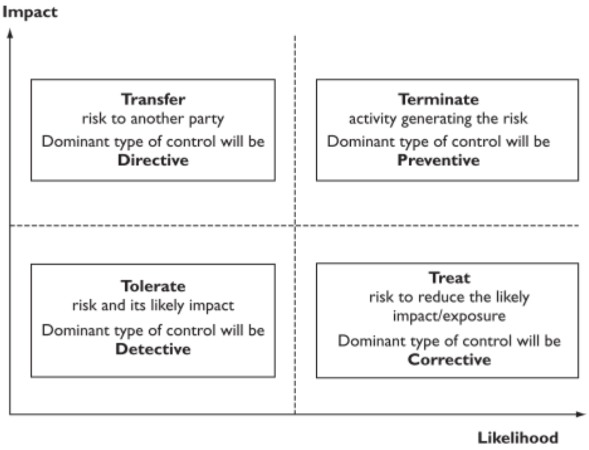

Impact
Transfer
risk to another party
Dominant type of control will be
Directive
Terminate
activity generating the risk
Dominant type of control will be
Preventive
Tolerate
risk and its likely impact
Dominant type of control will be
Detective
Treat
risk to reduce the likely
impact/exposure
Dominant type of control will be
Corrective
Likelihood

Figure suggests that there is a dominant response in relation to each of **the 4Ts**, according to the position of the risk on a risk matrix. For risks that are low likelihood/low impact, the main response is tolerate. For risks that are high likelihood/low impact, the main response is treat. For risks that are low likelihood/high impact, the main response is transfer, and for risks that are high likelihood/high impact, the main response is terminate.

“Control” is a general term; difficult to give definition. Many different types of conrol exist. The Committee of Sponsoring Organizations of the Treadway Commission (COSO, 1992) identified one purpose of an internal control system as providing reasonable assurance that an entity complies with “applicable laws and regulations.” Effective controls can be developed with different purposes, including directive, preventive, compensating, detective, and corrective. Often we work with the classifications:

- **Preventive**: Preventive controls relate to measures taken by a firm to deter noncompliance with policies and procedures. These controls ensure that sytems work in the first place (e.g. employing competent staff, high moral standards, segregation of duties, physical and controls (locks, passwords, etc)
- **Detective**: Detective controls are aimed at uncovering problems after they have occurred. They are designed to pick up transaction errors that have not been prevented (supervisory checks, internal checks, variance analysis, reconciliations). Although necessary in a good internal control system, detection of an independence violation after the fact is less desirable than prevention in the first place. Detective controls rarely work well as a deterrent in the absence of severe penalties.
- **Corrective**: When violations or problems are identified, some corrective action is required. These controls ensure that where problems are identified, they are properely dealt with. This could entail counseling and additional training, with more severe disciplinary action in cases of continued noncompliance.
- **Compensating**: Compensating controls are intended to make up for a lack of controls elsewhere in the system (e.g. a hard copy of the client list -- such a list would compensate for downtime in electronic systems and difficulties in locating client names in an electronic system)
- **Directive**: Although a firm may have policies and procedures, policies and procedures do not always work as intended. To ensure compliance, a clear, consistent message from management that policies

and procedures are important is required. Often managers point out that their busy schedules cause them to pay insufficient attention to policies and procedures. Not only must the firm ensure that firm members have the time to pay attention to independence requirements, but firm members must also perceive the policy as being of sufficient importance to warrant their time. Top management may emphasize the importance of policies either by rewarding exemplary conduct or by zero-tolerance policies for violation. They should ensure that there is clear direction and drive towards achieving the stated objectives. These are POSITIVE arrangements to motivate people and to give them a clear sense of direction (and the ability) to make good progress. – eg staff awarness training.

Part V: Controls of selected risks

Financial risk

= Financial risk is an umbrella term for multiple types of risk associated with financing

→ Credit risk = change in credit worthiness

→ Market risk = currency price volatility, interest rate changes, commodity price fluctuations, liquidity risks (risk that a given security or asset cannot be traded quickly enough in the market to prevent a loss)

→Foreign investment risk (risk of rapid and extreme changes in value due to: smaller markets; differing accounting, reporting, or auditing standards; nationalization, expropriation or confiscatory taxation; economic conflict; or political or diplomatic changes

It has two necessary characteristics

- Exogenous event with potential effect on a financial outcome (e.g., reduced cash flows, reduced market value)
- Can be reduced by entering into a financial contract with cash settlement (e.g., using derivate financial instruments)

Financial risk management ("hedging")

= taking an investment to reduce the risk of adverse price movements in an asset - normally, a hedge consists of taking an offsetting position in a related security, such as a futures contract

- ⇨ Hedging employs various techniques but, basically, involves taking equal and opposite positions in two different markets (such as cash and futures markets). Hedging is used also in protecting one's capital against effects of inflation through investing in high-yield financial instruments (bonds, notes, shares), real estate, or precious metals.
- ⇨ **Financial risk management** is thus the practice of creating economic value in a firm by using financial instruments to manage exposure to financial risk (particularly credit risk and market risk).
- ⇨ A risk management strategy used in limiting or offsetting probability of loss from fluctuations in the prices of commodities, currencies, or securities. In effect, hedging is a transfer of risk without buying insurance policies.
- ⇨ **Example: derivatives** are securities (options, swaps, futures and forward contracts) that move in terms of one or more underlying assets. The underlying assets can be: stocks, bonds, commodities, currencies, indices or interest rates.

Derivatives can be effective hedges against their underlying assets, since the relationship between the two is more or less clearly defined.

Reasons for hedging financial risks:

- ○ Reduces probability and thus cost of financial distress
  - Costs associated with bankruptcy (**financial distress hypothesis**)
    - Not hedging can lead to financial distress.
    - Costs of financial distress = often considered as costs associated with bankruptcy (e.g. legal and accounting fees, management time with dealing with bankruptcy, but also distressed asset sales, higher cost of capital, etc.)
    - Hedging can reduce/eliminate these costs
  - Costs of underinvestment (**underinvestment hypothesis**)
    - Hedging will solve the firm's inability to take advantage of valuable investment opportunities (i.e. underinvestment problem).
- ○ Creates more debt capacity (debt capacity argument)
  - If hedging of financial risk reduces a firm's probability of distress, its optimal action might be INCREASE its debt.
  - We said already that firms might benefit from a reduced cost of capital (because of smoother cash flows/earnings).

        - Recent research provides evidence for the “debt capacity” argument and that the advantages are important on average. More specific, they show that an “average user” of interest rate and/or currency derivatives has a higher debt ratio than a non-hedger of financial risk + this higher debt ratio provides more than 1 percent extra value, on average, through tax benefits.
        - An important benefit of reducing risk by hedging are thus the **INCREMENTAL TAX BENEFITS** accruing from additional debt after the firm readjusts its capital structure. →Hedging creates thus value because extra debt allows for additional tax benefits.
        - Hedging to enable greater debt capacity might be beneficial beyond providing extra value through tax benefits. Extra debt might be used to increase the firm’s capital base and provide funds for pursuing valuable investment opportunities. Hedging creates thus also value because extra debt allows to finance valuable investment opportunities.

    - Aligning the incentives of the firm’s management and board
        - A firm’s financial risk management strategy may be a function of the incentives of its senior management (as well as its board).
        - Mostly recommended: not pure stocks (focus too much on ST), but stock options (focus more on LT)
        - Research indicates that senior management who hold significant amounts of wealth in OPTIONS may have greater incentives to INCREASE rather than decrease firm risk because the extra volatility makes the option more valuable.
        - On the other hand: senior management who hold significant amounts of STOCKS, reinforce personal risk aversion and therefore will be more likely to hedge.
        - The fact that senior management has incentives to pursue self-interested policies (possible at the expense of other stakeholders) suggests that the **board may have an important oversight role in the company’s hedging policy.**
        - Research finds that evidence that outside directors can play an important influence on risk management strategy and its value on the firm.

Does hedging affect firm value?

- Extant research is inconclusive
- Can be a valuable strategy, but only if investors have a clear understanding of the benefits and if the benefits outweighs the costs associated with it – not playing on the market, not taking positions without underlying economic reason!

Market risk

Market risk

= the potential for gain or loss due to changes in market conditions such as interest rates, commodity prices, exchange rates and other economic and financial variables

- Examples of market risks:
    - Currency risk: direct (currency) and indirect (loss of sales): the risk that changes in exchange rates impact the expected cash flow (direct (currency risk) or indirect (loss of sales because not competitive))
    - Interest rate risk: risk that changes in interest rate impact the expected cash flow
    - Commodity price risk: risk that changes in commodity prices (e.g., oil, natural gas, gold, silver, coffee, etc.) impact the cash flow of an entity
    - Equity price risk: : risk that changes in equity prices impact the expected cash flows of an entity
    - Economic risk (GDP growth, housing prices, consumer confidence): GDP growth, housing prices, consumer confidence
    - Liquidity risk (security of asset cannot be traded quickly enough): the risk that a given security or asset cannot be traded quickly enough in the market to prevent a loss (or make the required profit)

→ Combination of these risk caused the financial crisis

Credit risk
= the potential for gain or loss due to changes in the creditworthiness

The combination of these risks can have important implications:

Simple perception of these risks (accurate or not) can have significant implications (e.g. banking crisis – people withdrawing money)

  - can have significant implications for a corporate entity and all its stakeholders

- Actively managing them can lead to strategic/competitive advantages (e.g. Southwest Airlines hedging fuel costs)
  E.g. Southwest airline → in 2008/2009 hedging fuel costs at beginning of the year before prices of crude oil went up to 150$ per barrel → gained a significant cost advantage over competitors → could offer lower prices than competitors
- Can have significant effects on other risks (eg strategic and operational risk)
  Eg car companies offering cheap credit = part of their operating strategy

⇨ Both risks differ from other risks such as operational risk because they are PRICED and OBSERVED in the CAPITAL MARKETS

⇨ As such: relatively objective tools and strategies exist to measure and manage these risks (for other risks it is often more subjective!)

⇨ Very quantitative + existing models → so often managed by risk managers; but it is still not exact science!!!

The case for actively managing market risk

- More predictable cash flows
  - is preferred by shareholders and creditors
  - aids in operational planning/forecasting
  - ensures that necessary investments can be made regardless of economic conditions
- Reduction of financial costs
  - reduction of capital raising costs
  - shareholders/credit providers reward more stable companies
  - less financial stress which itself leads to lower cost
- Fiduciary responsibilities (= your governance is better)
  - legal cases where management was sued for failing to be active in market risk management
- Avoidance of uncertainty ("fear factor")
  - fear or sleep factor: management does not have to worry about market risk if it is actively managed
- To maintain focus on core business strategy
  - if actively managed, it is one less thing to worry about → more time to focus on core strategy

The case for not actively managing market risk:

- Costly
  - Fees for hedging instruments
  - Need for information systems + professional risk manager
  - Increased complexity of accounting and reporting requirements
- Potentially not in shareholders' best interest (e.g., institutional investors)
  - if shareholders are large institutional investors – they may want to actively self-manage market risk and have the scale, technology, and capabilities to do so
- Diffficult to do properly
  - derivates, collaterated effects, etc – more art than science

Measuring market risk (not need to know in details)

Markets provide many indicators of risks – assumed to be an effective indicator because it represents the collective judgement of a wide group of people

- Stock market (major indices → economy & single stock prices → single company)

- Publicly traded future markets (gives indications about the prices that investors, trader, speculators are willing to trade commodities, interest rates and currencies at a given time in the future)
  → Also important: volatility of prices (standard deviation) & correlation of price changes
    - Volatility: gives information about the level of UNCERTAINTY
    - Correlation: even more important – risks not independent!

Value at Risk (VaR) (he said less important)

- Combines amount of potential loss, probability of that amount of loss, and the time frame
- Estimates how much a set of investments might lose, given normal market conditions, in a set time period such as a day
- Probability of losing more than a given amount of assets
- Common parameters: 1% and 5% probabilities; one day and two week horizons
- VaR break = loss which exceeds the VaR threshold
  - For example, a financial firm may determine that it has a 5% one month value at risk of $100 million. This means that there is a 5% chance that the firm could lose more than $100 million in any given month. Therefore, a $100 million loss should be expected to occur once every 20 months.
  - For example, if a portfolio of stocks has a one-day 5% VaR of $1 million, that means that there is a 0.05 probability that the portfolio will fall in value by more than $1 million over a one day period if there is no trading. Informally, a loss of $1 million or more on this portfolio is expected on 1 day out of 20 days (because of 5% probability).

VaR is thus a risk management model that calculates the largest possible loss that an institution or other investor could incur on a portfolio. Value at risk describes the probability of losing more than a given amount of assets, based on a current portfolio.

- *This has a couple of important implications: one, that it is a snapshot, a picture of what the risk level is now, based on what you hold now. The longer the time period you apply it to, the fuzzier it is likely to become.*
- *Two, it is a lower bound for loss, not an upper bound – if your model says that at a 95 per cent VaR, the value at risk is half of your assets, you can expect to lose half or more of your assets one day in 20. It should be used to make sure you can withstand these losses, not necessarily to prevent them.*

VaR is a mathematical model that purports to estimate the maximum future losses expected from a trading portfolio, with a degree of statistical confidence. VaR's calculation can be extremely technical, or it can be as simple as looking at a subjective past period and then projecting future risks from there. A big problem with VaR is that it can very easily gravely misrepresenting true exposures. Relying on the past can be treacherous: a quiet past period need not imply future quietness, historical volatility and correlation may betray you.
VaR played a key negative role in the 2008 credit crisis, by severely underestimating the danger from toxic mortgage products and by allowing banks to enjoy excessive levels of leverage on their trading positions. Recognising all this, the Basel Committee for Banking Supervision, which had enthusiastically adopted VaR since 1995, has been busy at work disowning the model and tweaking the bank capital formula. Just a few weeks ago, Basel announced that it no longer wants to keep using VaR.

"Natural" or nonderivative-based market risk management

- Involves using operating, marketing, and/or financing strategies that minimize or potentially eliminate the need for complicated financial instruments
- Techniques:
  - Diversify product lines
  - Diversify geographically (operations and marketing)
  - Diversify funding sources (type of funding and country of origin)
  - Diversify exchange rates globally
  - Cost-plus contracts
    → *see this a lot in construction. The risk if for example steel prices go up than as a contractor you might loose on your contract, so often there is a cost-plus contract; a base price + adding a surplus of the real costs*
    → *is passing on costs to customers when there are more costs. You transfer part of the risk to the customer.*
  - Backward and forward supply chain integration
- Drawbacks
  - Not in operational comfort zone anymore

    - Seldom as well-fitted as financial-based hedges
    - Long-term hedges

Market risk management with forward-type products

(Not know by heart but they are indications of what you can have to manage these risks)

- **Forwards**
    - Bi-lateral agreements to exchange an asset or a cash flow at a preset price and a preset time in the future
    - is a non-standardized contract between two parties to buy or to sell an asset at a specified future time at a price agreed upon today, making it a type of derivative instrument
    - Reduce uncertainty, but no profit from favorable moves
    - Over the counter (OTC) contracts traded between a corporate and a financial counterparty
    - Can be highly customized: available on a wide variety of financial indices /economic variables
    - Not as liquid as future contracts
- **Futures**
    - Is a standardized forward contract which can be easily traded between parties other than the two initial parties to the contract. The parties initially agree to buy and sell an asset for a price agreed upon today (the *forward price*) with delivery and payment occurring at a future point, the *delivery date*.
    - Are exchange traded products: contracts are negotiated at futures exchanges, which act as a marketplace between buyers and sellers. The buyer of a contract is said to be long position holder, and the selling party is said to be short position holder.
    - Standardized forward products to facilitate trading & create liquidity
    - Basis risk: difference in risk being hedged and price changes in derivative instrument being used for the hedging (e.g. heating fuel vs. jet fuel)
    - Margin requirements
        - *As both parties risk their counterparty walking away if the price goes against them, the contract may involve both parties putting a margin of the value of the contract with a mutually trusted third party. For example, in gold futures trading, the margin varies between 2% and 20% depending on the volatility of the spot market.*
        - *At the inception of the trade both the buyer and the seller need to post margin to ensure monies are available to settle the contracts at expiry or settlement*
        - *Each day the future exchanges calculate the gains or losses to each account → falls below a certain level (the maintenance level) , then that account will receive a margin call to post additional margin*
        - *This virtually eliminates counterparty credit risk issues*

- **Swaps**
    - Multi-period forward-type contracts

Market risk management with option-type products

- Is a contract which gives the buyer (the owner or holder of the option) the right, but not the obligation, to buy or sell an underlying asset or instrument at a specified price on or before a specified date, depending on the form of the option. The seller has the corresponding obligation to fulfill the transaction – to sell or buy – if the buyer (owner) "exercises" the option.
- Options to hedge market risk
- Allow to profit from favorable moves in market price
- Two main types of option
    - Call options: right but no obligation to buy
    - Put options: right but no obligation to sell
- Options trade on all assets that futures do + individual stock and bonds
- Traded on exchange and over-the-counter market
- Asymmetric instruments: because the buyer has the OPTION to transact (choice), while the seller must transact if the buyer chooses to do so.
    - The buyer must therefore pay an option premium to seller (therefore many organizations prefer to hedge with futures that do not have an upfront fee)
- Pricing is complex (Black-Scholes Option Pricing model)

- Caps = multi-period options

Operational issues of using derivatives

- In theory easy to understand, in practice much more complicated
    - highly dependent on their specific structural features
- International Swaps and Derivative Association: ISDA master agreement
    - Agreement between financial institution and corporation when they start trading – start from standard ISDA and add specific clauses
    - Specifies all the terms that might come up in the life of a trade between counterparties (how payments are done, how interest rates are calculated, etc)
- Each individual trade will be documented with a CONFIRMATION → spells out the details of each individual transaction such as the notional size, time to maturity, strike prices, etc.
- Choosing hedge counterparties (price, flexibility, advice, etc.)
    - Price is important – but not the only criterium
    - Flexibility: ability to unwind a hedging transaction in a timely manner and at reasonable value
    - Quality and amount of advice
- Ask a variety of sources to ensure fairness of the valuation + ask for bid and ask side of trade so that they cannot bias the answer to increase
- Strong and knowledgeable oversight: risk philosophy
    - Making it a profit-generating activity is highly questionable
- Tools and techniques for credit and market risk are among the most highly developed and quantitative of all the classes of risks
  ←→ Require a good understanding of tools + good understanding of underlying business

Credit risk

= the potential for gain or loss due to changes in the credit worthiness

- Almost always a downside risk; almost always unexpected
    - Unexpected: No one extends credit to a customer or executes a loan to a counterparty, expecting that this will not be paid <->Market risk: not always downside risk
- Measuring credit risk is not trivial:
    - In lending (homes, autos, credit cards, commercial lending, etc.) a third concept is introduced to emphasize that most loans are repaid over time and therefore have a declining outstanding amount to be repaid.
    - Additionally, loans are typically backed up by a collateral whose value changes *differently* over time vs. the outstanding loan value.

Expected loss = probability of default (PD) x exposure at default (EAD) x loss given default (LGD)

Probability of default (PD) *"probability of default of a borrower"*

- Measures the probability over some point in time – usually one year – that the debtor or payer will default (not pay a contractual obligation after 90 days). PD is a vital concept
    - For loans to individuals or small businesses, credit quality is typically assessed through a process of **credit scoring**. Prior to extending credit, a bank or other lender will obtain information about the party requesting a loan. In the case of a bank issuing credit cards, this might include the party's annual income, existing debts, whether they rent or own a home, etc.
    - Larger cooperations: Many banks, investment managers and insurance companies hire their own credit analysts who prepare credit ratings for internal use. Other firms—including Standard & Poor's, Moody's and Fitch—are in the business of developing credit ratings for use by investors or other third parties. These firms are called **credit rating agencies**. Institutions that have publicly traded debt hire one or more of them to prepare credit ratings for their debt. Those credit ratings are then distributed for little or no charge to investors.
    - Generally speaking, the higher the default probability a lender estimates a borrower to have, the higher the interest rate the lender will charge the borrower (as compensation for bearing higher default risk).

Exposure at default (EAD) *"amount to which the bank was exposed to the borrower at the time of default, measured in currency"*[

- EAD shows your potential TOTAL dollar loss and asset exposure at the time of default. EAD is equal to the current amount outstanding in case of fixed exposures like term loans.

Loss given default (LGD) «*magnitude of likely loss on the exposure, expressed as a percentage of the exposure"*[1]

- LGD is the share of an asset that is lost when a borrower defaults (expressed as %). Loss given default is facility-specific because such losses are generally understood to be influenced by key transaction characteristics such as the presence of collateral and the degree of subordination. The LGD calculation is easily understood with the help of an example: If the client defaults with an outstanding debt of $200,000 and the bank or insurance is able to sell the security (e.g., a condo) for a net price of $160,000 (including costs related to the repurchase), then the LGD is 20% (= $40,000 / $200,000).

Example (not important but take note on how you can calculate this):

- *Original home value $100, loan to value 80%, loan amount $80*
  - *outstanding loan $75*
  - *current home value $70*
  - *liquidation cost $10*
- *Probability of default = since there is negative equity, 50 homeowners out of 100 will "toss the keys to the bank and walk away", therefore: 50% probability of default*
- *Exposure at default = outstanding loan of $75*
- *Loss given default*

  = magnitude of likely loss on the exposure / exposure at default

  = $15/$75 = 20%
    - *-$75 loan receivable write off*
    - *+$70 house sold*
    - *-$10 liquidation cost paid = -$15 Loss*
- *Expected loss in % = 20% x 50% =10%*
- *Expected loss in currency = currency loss x probability = $15 * 0.5 = $7.5*
  - *Check: LGD x PD x EAD = 20% * 50% * $75 = $7.5*

Fundamental analysis of credit default probability

- “Five C’s” of credit analysis:
  - Capacity: ability to pay obligations out of cash flows generated
  - Capital: amount of cash on hand
  - Collateral: quality of assets that can be sold to repay obligations
  - Conditions: business conditions specific to company and its industry
  - Character: reputation and integrity of firm and its management

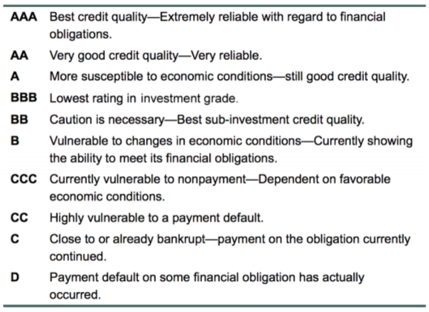
- Accounting measures to assess credit worthiness
  - Short-term ability to cover exposures
    - Current ratio = current assets / current liabilities
    - Quick ratio = current assets – inventory / current liabilities
    - Burn rate = annual expenses / 365 (= very actual especially in the IT sector)
    - Days cash on hand = available cash / burn rate
  - Longer-term financial flexibility
    - Debt ratio = total liabilities / total assets
    - Debt ratio = total long-term debt / shareholder’s equity

How to measure?

→ Look when firms do not pay their clients on time and no reason is given!

→ Look at ratings form rating agencies

Example →



AAA	Best credit quality—Extremely reliable with regard to financial obligations.
AA	Very good credit quality—Very reliable.
A	More susceptible to economic conditions—still good credit quality.
BBB	Lowest rating in investment grade.
BB	Caution is necessary—Best sub-investment credit quality.
B	Vulnerable to changes in economic conditions—Currently showing the ability to meet its financial obligations.
CCC	Currently vulnerable to nonpayment—Dependent on favorable economic conditions.
CC	Highly vulnerable to a payment default.
C	Close to or already bankrupt—payment on the obligation currently continued.
D	Payment default on some financial obligation has actually occurred.

Credit risk mitigation:

- Credit policy towards clients
- Policy for customers that fail to make timely payments (for ex reminders)
- Sell receivables to a special purpose company: factory company (= outsourcing your receivables to another company → transferring the risk to the factor)
- Package receivables into a structured note (packing your receivables and trading it with the underlying value (=credit derivatives))
- Credit derivatives for most public companies

Operational risk

Operational risk (Basel Committee):

> =The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events

- Operational risk is a broad term: often debate on what is included and what not
- The Basel Committee decided that operational risk management (ORM) is focused on managing the risks that appear during the day-to-day activities of executing the organization's strategy
    - This excludes risks from taking poor strategic business decisions (i.e. strategic risk)
    - But it includes the failure to effectively and efficiently execute the strategy of an organization (which is a major source of operational risk)
- However, the Basel Committee recognizes that operational risk is a term that has a variety of meanings and therefore, for internal purposes, banks are permitted to adopt their own definitions of operational risk, provided that the minimum elements in the Committee's definition are included.

- Operational risk may be considered to be the type of risk that will disrupt normal everyday activities.
- In earlier times (90s), much of the risk management focus was on techniques for measuring and managing market risk and later also credit risk.
- By the end of the decade, firms and regulators were increasingly focusing on risks "other than market and credit risk." These came to be collectively called operational risks. This catch-all category of risks was understood to include,
    - employee errors,
    - systems failures,
    - fire, floods or other losses to physical assets,
    - fraud /criminal activity
- Firms had always managed these risks. The new goal was to do so in a more systematic manner.
- Operational risks are usually hazard risks, and historically this has been an area of strong application of risk transfer by way of insurance. However, operational risk now has a more extensive application.

Scope exclusions

- The Basel II definition of operational risk excludes, for example, strategic risk - the risk of a loss arising from a poor strategic business decision.
- Other risk terms are seen as potential consequences of operational risk events. For example, reputational risk (damage to an organization through loss of its reputation or standing) can arise as a consequence (or impact) of operational failures - as well as from other events.

Types of operational risks

- Internal fraud (misappropriation of assets, tax evasion, bribery)
- External fraud (theft, hacking, forgery)
- Employment practices and workplace safety
- Clients, projects and business practices
- Damage to physical assets
- Business interruption and system failures
- Execution, delivery, and process management

Employee errors
System failures
Fraud/criminal activity
Events: fire, flood, etc.

- Expected losses can have a direct and indirect cost

How to evaluate operational risk management effectiveness?

- Identify and quantify the risks associated with a particular strategy so that the potential impact that these risks can have on operational objectives can be understood
- Evaluate the existing risk treatment -- within risk tolerance?
    - Tollerable → no further action needed
    - Over-managed → reallocate some resources to more sign. risks
    - Under-managed → consider additional risk treatments
- Develop an adaptive risk response capability to bring the risk within the defined risk tolerance
    - Change potential likelihood of the risk -- (i.e., reduce/increase PREVENTION activities)
    - Change potential impact of the risk -- (i.e., reduce/increase MITIGATION activities)

The development of interest in operational risk has been based on the need to quantify operational risk in financial institutions. The challenges of quantifying operational risk have been considerable. Expected levels of loss can only be estimated, even if the probability of loss is accurately known. Although statistical approaches have been adopted and developed, a universally accepted approach is still not available.

The expected losses can have a direct and indirect cost. Indirect costs are often larger and include the loss of a customer. This loss can be represented by the present value of that customer and all future gains from that relationship

Risk response/treatment is some combination of prevention and mitigation measures
Typical internal control measures:

- Prevention measures (preventing breakdown):
    - Segregation of duties (preventive control)
    - Authorization of transactions and activities
    - Procedures
    - Security access to assets and information

- Detection/mitigation of errors (detecting process breakdown)
    - Testing against reality
    - Testing against ex-ante information

Financial reporting and disclosure risk

- ERM reporting and disclosure provides forum to discuss key vulnerabilities and risks and should be adequate and broad-based
- US: SOX Act of 2002 profoundly impacted the financial reporting and disclosure environment
- Belgian: Law of April 6, 2010: Law to strengthen corporate governance
    - Article 96 Corp. Law already required a description of the main risks the company is exposed to in the management report
    - For listed enterprises this is now extended by a Corporate Governance Statement, including a description of the main features of the company's internal control and risk management systems in relation to financial reporting process and a remuneration report
- Two sections of SOX impact internal control reporting directly and ERM reporting indirectly
    - Section 302: Financial reporting responsibility – "signature clause"
        - CEOs/CFOs/other senior executive officers of public corporations
            - Must certify the veracity of firm's public statements
                - True representation of financial and operational results
                - No misleading or material untrue information
            - Review and sign off on internal controls

- Section 404: Internal control (IC) and compliance management
    - Firms must establish and test internal financial controls (including those to protect against fraud) + disclose weaknesses
    - External auditor must review and independently assess the IC
    - Management responsible for reporting on quality and effectiveness of IC
    - Requires firms to follow an accepted internal control framework (e.g., COSO) – [cf. Belgian CG law]

More info:
302

- *Section 302 of the Act mandates a set of internal procedures designed to ensure accurate financial disclosure.*
- *The signing officers must certify that they are "responsible for establishing and maintaining internal controls" and "have designed such internal controls to ensure that material information relating to the company and its consolidated subsidiaries is made known to such officers by others within those entities"*

404

- *The most contentious aspect of SOX is Section 404, which requires management and the external auditor to report on the adequacy of the company's internal control on financial reporting (ICFR).*
- *This is the most costly aspect of the legislation for companies to implement, as documenting and testing important financial manual and automated controls requires enormous effort.*
- *Management is required to produce an "internal control report" with an assessment of the effectiveness of the internal control structure and procedures*
- *To do this, managers are generally adopting an internal control framework such as that described in COSO.*
- *External auditors are required to issue an opinion on whether effective internal control over financial reporting was maintained in all material respects by management. This is in addition to the financial statement opinion regarding the accuracy of the financial statements. The requirement to issue a third opinion regarding management's assessment was removed in 2007.*

SOX 404 compliance costs represent a tax on inefficiency, encouraging companies to centralize and automate their financial reporting systems. This is apparent in the comparative costs of companies with decentralized operations and systems, versus those with centralized, more efficient systems. For example, the 2007 Financial Executives International (FEI) survey indicated average compliance costs for decentralized companies were $1.9 million, while centralized company costs were $1.3 million.[36] Costs of evaluating manual control procedures are dramatically reduced through automation.
To help alleviate the high costs of compliance, guidance and practice have continued to evolve. The Public Company Accounting Oversight Board (PCAOB) approved Auditing Standard No. 5 for public accounting firms on July 25, 2007. The SEC also released its interpretive guidance [on June 27, 2007. It is generally consistent with the PCAOB's guidance, but intended to provide guidance for management.

- *Both management and the external auditor are responsible for performing their assessment in the context of a top-down risk assessment, which requires management to base both the scope of its assessment and evidence gathered on risk. This gives management wider discretion in its assessment approach.*

However, as a result of the passage of Auditing Standard No. 5, which the SEC has since approved, external auditors are no longer required to provide an opinion on management's assessment of its own internal controls.

Financial reporting challenges today

- Paring down internal control: Auditing standard 5 (AS5)
    - Paring down means *reducing* the risk of having an external framework and an external audit, internal audit. The auditor is auditing the work of the auditor who is auditing the controller who is controlling the work of the CFO…. So, it gets very cluttered. That can kill entrepreneurial spirit. How are we going to make sure that it is not too much?
    - SEC issuers, especially smaller firms, were critical of section 404 → unreasonable expensive and time-consuming
    - In response to criticism, PCAOB adopted a new standard AS5 (in 2007) which still requires an auditor to test the effectiveness of a company’s internal controls, but t allows a more principle-based approach, including relying on the work of others: more top-down instead of bottom-up
- Global financial crisis and ERM
    - Shows that many organizations lack the tools to identify, prioritize, measure and REPORT risks at the enterprise level → big challenge for ERM
- Conflicts with International Standards: rules vs principles
    - IFRS (IASB) is more principle-based than rules-based in US (FASB): move to IFRS?
    - Aftermath of global financial crisis: substantial changes may be expected to the reporting and measurement of financial instruments (changes will be as severe as SOX)
    - This highlight importance of ERM
- Adding ERM to company credit rating

Legal risk

- Prior to SOX: almost no legal framework for legal and reputational risk
    - Little incentives to report violations (attorneys, employees)
        - Counseler/attorney: risk losing client
        - Employee: risk losing job
- SOX represented a revolution (but not sufficient)
    - Rules of professional responsibility for attorneys
        - Reporting of material violations of certain laws at Qualified Legal Compliance Committee (QLCC) a lot of risk/uncertainty for attorneys, solved with QLCC
        - *Qualified Legal Copmpliance Committee (QLCC): committee of the board investigates reportings of violations, asks oustide opinions and provides recommandations + reports to SEC if recommendations are ignored*
        - Advantage: whistle-blower protection for attorneys + Board has high incentives to avoid director liability
        - But it is optional and only very few LISTED firms have implemented (for non-listed it even does not apply)
    - Whistle-blower protections (e.g. litigation support + fines for interfering)
        - But it is not working/not sufficient to overcome the powerful social mores of being a "snitch" or "rat"
        - What else? Omnibus statute, monetary rewards for whistle blowers, assuring anonymity
    - Audit reform
        - PCAOB: public company accounting oversight board
        - Audit committee for public firms -> SOX thus mandated corporate governance structures
        - Encourages ethical codes of conduct + disclosure of it

→ But recent evolutions (e.g. subprime mortgage fiasco) indicate that SOX is not sufficient to reduce legal and reputational risk to an optimal level

- Toward optimal reputational and legal risk management
    - Install QLLC; make it mandatory <u>for all firms</u>
    - Enhance QLLC responsibilities
        - Not just violations as defined by SEC
        - All legal and reputational risks and violations of code of conduct should be reported to QLCC (eg environmental or racism violations or harassment) → can have huge impact on legal and reputational risk

    - Definition of "violation of certain laws" should be broader
        - Any violation (environmental, racism, etc.)
        - Any corporate agent
    - Ensure close relationship between QLLC and audit committee
    - Broader whistle-blower protection is needed
    - Create anonymous means of reporting violations
    - Have an ethics code/ code of conduct
    - Not only attorneys or lawyers, but ANY corporate agent having information about violations should be required to report to the QLCC to maximally protect the firm from legal and reputational risk

IT risk *(niet besproken in detail)*

IT risk management (ISACA): is the application of risk management methods to Information Technology to manage IT risk, i.e.:

The business risk associated with the use, ownership, operation, involvement, influence, and adoption of IT within an enterprise or organization

- IT risk management can be considered a component of a wider enterprise risk management system
- It covers *all* IT-related risks, including:
    - Information security breaches
    - Obsolete or inflexible IT architecture

- Not achieving enough value from IT/ wasted investments
- System crashes
- Compliance
- IT project failure/late delivery
- IT service delivery problems

The effective use of IT is critical to the success of enterprise strategy:

- Information is a key resource for all enterprises.
- Information is created, used, retained, disclosed and destroyed.
- Technology plays a key role in these actions.
- Technology is becoming pervasive in all aspects of business and personal life.

While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this even more so in the future

IT also carries risks:

- It is clear that in these days of doing business on a global scale around the clock, system and network downtime has become far too costly for any enterprise to afford.
- In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage, while in many others it determines survival, not just prosperity.

IT risk is not limited to information security !!!

- theft of computers and other hardware;
- unauthorized access into IT systems;
- introduction of viruses into the system;
- hardware or software faults and failures;
- user error, including loss or deletion of information;
- IT project failure

Drivers for IT risk management:

- Concern over the generally increasing level of IT expenditure
- Business managers and boards demanding better returns from IT investments, i.e., IT delivers what the business needs to enhance stakeholder value
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g. SOX), and in specific sectors such as finance, pharmaceutical and healthcare
- Increasingly complex IT-related risks, such as network security
- The growing maturity and consequent acceptance of well-regarded frameworks, such as the Information Technology Infrastructure Library (ITIL), Control Objectives for Information and related Technology (CobiT), ISO/IEC 27002, etc.
- Statements by analysts recommending the adoption of best practices

Benefits of IT risk management

- Maintain quality information to support business decisions
- Achieve operational excellence through reliable and efficient application of technology
- Generate business value from IT-enabled investments, i.e., achieve strategic goals and realise business benefits through effective and innovative use of IT
- Maintain IT-related risk at an acceptable level
- Optimise the cost of IT services and technology

IT risk management frameworks/ best practices widely adopted around the world:

- **CobiT**
- **ITIL**
- **ISO/IEC 27005: 2011**

⇨ Implementation of best practices should be consistent with the enterprise's risk management and control framework, appropriate for the enterprise, and integrated with other methods and practices that are being used.

Control Objectives for Information and related Technology (CobiT)

- Published by Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI)
- Positioned as a high-level governance and control framework
- Based on a generic set of IT processes
- Widely accepted as "best practice"

- Includes:
  - Framework: 34 high-level control objectives, grouped into four domains: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate
  - Process descriptions
  - Control objectives
  - Management guidelines
  - Maturity models

ISACA recognised in the early 1990s that auditors, who had their own checklists for assessing IT controls and effectiveness, were speaking a different language to business managers and IT practitioners. In response to this communication gap, CobiT was created as an ***IT control framework for business managers, IT managers and auditors*** *based on a generic set of IT processes meaningful to IT people and, increasingly, business managers. The best practices in CobiT are* ***a common approach to good IT control—implemented by business and IT managers, and assessed on the same basis by auditors.*** *Over the years, CobiT has been developed as an open standard and is now increasingly being adopted globally as the control model for implementing and demonstrating effective IT governance.*

Executives need confidence that they can rely on information systems and the information produced by those systems and get a positive return from IT investments. CobiT enables business executives to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. CobiT provides the tools to direct and oversee all IT-related activities.

CobiT is ***a globally accepted framework for IT governance based on industry standards and best practices****. Once implemented, executives can ensure IT is aligned effectively with business goals and better direct the use of IT for business advantage.* ***CobiT provides a common language for business executives to communicate goals, objectives and results with audit, IT and other professionals.***

CobiT provides best practices and tools for monitoring and managing IT activities. The use of IT is a significant investment that needs to be managed. CobiT helps executives understand and manage IT investments throughout their life cycle and provides a method to assess whether IT services and new initiatives are meeting business requirements and are likely to deliver the benefits expected.

The difference between enterprises that manage IT well and those that do not, or cannot, is tremendous. CobiT enables clear policy development and good practice for IT management. The framework helps increase the value attained from IT. It also helps organisations manage IT-related risk and ensure compliance, continuity, security and privacy.

Because CobiT is a set of proven and internationally accepted tools and techniques, implementation of CobiT is a sign of a well-run organisation. It helps IT professionals and enterprise users demonstrate professional competence to senior management. As with many generic business processes, there are specific IT industry standards and good practices that enterprises should follow when using IT. CobiT captures these and provides a framework for implementing and managing them. Once the key CobiT principles relevant to an enterprise are identified and implemented, executives gain confidence that the use of IT can be managed effectively.

Includes:

- Framework—Explains how CobiT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements. The framework contains a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor and Evaluate.
- Process descriptions—Included for each of 34 IT processes, covering the business and IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility and measure performance
- Maturity models—Provide profiles of IT processes describing possible current and future states

Executives can expect the following results from the adoption of CobiT:

- IT staff and executives will understand more fully how the business and IT can work together for successful delivery of IT initiatives.
- Full life-cycle costs of IT will become more transparent and predictable.
- IT will deliver better quality and more timely information.
- IT will deliver better quality services and more successful projects.
- Security and privacy requirements will be clearer and implementation more easily monitored.
- IT-related risks will be managed more effectively.
- Audits will be more efficient and successful.
- IT compliance with regulatory requirements will be a normal management practice.

Information Technology Infrastructure Library (ITIL)

- Published by the UK government (Office of Government Commerce (OGC))
- Provides a best practice framework for IT service management
- Gives guidance at the lowest level
- Describe approaches, functions, roles and processes, upon which organizations may base their own practices
- Contains five core publications or ITIL books with best practices for 5 phases of the IT service lifecycle
    - ITIL Service Strategy
    - ITIL Service Design
    - ITIL Service Transition
    - ITIL Service Operation
    - ITIL Continual Service Improvement

The UK government recognized very early on the significance of IT best practices to government and, for many years, has developed best practices to guide the use of IT in government departments. These practices have now become de facto standards around the world in private and public sectors. ITIL was developed more than 15 years ago to document best practice for IT service management, with that best practice being determined through the involvement of industry experts, consultants and practitioners. ISO/IEC 20000, which is aligned with ITIL, superseded BS 15000 in 2005 as a new global service management standard.

Business must ensure that high-quality IT services are provided that are:

- *Matched to business needs and user requirements*
- *Compliant with legislation*
- *Effectively and efficiently sourced and delivered*
- *Continually reviewed and improved*

IT service management is concerned with planning, sourcing, designing, implementing, operating, supporting and improving IT services that are appropriate to business needs. ITIL provides a comprehensive, consistent and coherent best practice framework for IT service management and related processes, promoting a high-quality approach for achieving business effectiveness and efficiency in IT service management.

ITIL is intended to underpin but not dictate the business processes of an organization. In this context, OGC does not approve of the term 'ITIL-compliant'. The role of the ITIL framework is to describe approaches, functions, roles and processes, upon which organizations may base their own practices. The role of ITIL is to give guidance at the lowest level that is applicable generally. Below that level, and to implement ITIL in an organization, specific knowledge of its business processes is required to tune ITIL for optimum effectiveness.

BOOKS are periodically reviewed and updated as technologies change. Each book collects best practices for each major phase of the IT service lifecycle. ITIL Service Strategy explains business goals and customer requirements. ITIL Service Design shows how to move strategies into plans that help the business. ITIL Service Transition shows how to introduce services into the environment. ITIL Service Operation explains how to manage the IT services. ITIL Continual Service Improvement helps adopters evaluate and plan large and small improvements to IT services.

ISO/IEC 27005: 2011

- Published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC)
- Provides a framework of a standard for information security management
- It defines 133 security controls strategies, under 11 major headings
    - Measures based on legal requirements include:
        - Protection and non-disclosure of personal data
        - Protection of internal information
        - Protection of intellectual property rights
    - Best practices mentioned in the standard include:
        - Information security policy
        - Assignment of responsibility for information security
        - Problem escalation
        - Business continuity management

The standard stresses the importance of risk management and makes it clear that it is not necessary to implement every stated guideline, only those that are relevant.

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. CobiT can be used at the highest level, providing an overall control framework based on an IT process model that should suit every organisation generically. Specific practices and standards such as ITIL and ISO/IEC 27002 cover discrete areas and can be mapped to the CobiT framework, thus providing a hierarchy of guidance materials.

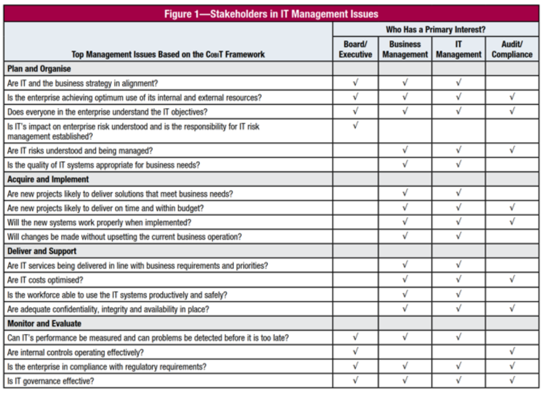


Figure 1—Stakeholders in IT Management Issues

Top Management Issues Based on the CobiT Framework	Who Has a Primary Interest?			
	Board/ Executive	Business Management	IT Management	Audit/ Compliance
Plan and Organise				
Are IT and the business strategy in alignment?	√	√	√	
Is the enterprise achieving optimum use of its internal and external resources?	√	√	√	√
Does everyone in the enterprise understand the IT objectives?	√	√	√	√
Is IT's impact on enterprise risk understood and is the responsibility for IT risk management established?	√			
Are IT risks understood and being managed?		√	√	√
Is the quality of IT systems appropriate for business needs?		√	√	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		√	√	
Are new projects likely to deliver on time and within budget?		√	√	√
Will the new systems work properly when implemented?		√	√	√
Will changes be made without upsetting the current business operation?		√	√	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities?		√	√	
Are IT costs optimised?		√	√	√
Is the workforce able to use the IT systems productively and safely?		√	√	
Are adequate confidentiality, integrity and availability in place?		√	√	√
Monitor and Evaluate				
Can IT's performance be measured and can problems be detected before it is too late?	√	√	√	
Are internal controls operating effectively?	√			√
Is the enterprise in compliance with regulatory requirements?	√	√	√	√
Is IT governance effective?	√	√	√	√

Heeft hij geskipt

This figure summarizes who has an interest in how IT standards and best practices can help address IT management issue

Due to their technical nature, IT standards and best practices are known mostly to the experts—IT professionals, managers and advisors—who may adopt and use them with good intent but potentially without a business focus or the customer's involvement and support.

Even in organizations where practices such as CobiT and ITIL have been implemented, some business managers understand little about their real purpose and are unable to influence their use.
To realize the full business value of best practices, the customers of IT services need to be involved, as the effective use of IT should be a collaborative experience between the customer and service providers (internal and external), with the customer setting the requirements. Other interested stakeholders, such as the board, senior executives, auditors and regulators, also have a vested interest in either receiving or providing assurance that the IT investment is protected properly and delivering value.

Due to their technical nature, IT standards and best practices are known mostly to the experts—IT professionals, managers and advisors—who may adopt and use them with good intent but potentially without a business focus or the customer's involvement and support.

To avoid costly and unfocused implementations of standards and best practices, enterprises need to priorities where and how to use standards and practices. The enterprise needs an effective action plan that suits its particular circumstances and needs.

<u>Successful implementation</u> requires the board to take ownership of IT governance and set the direction that management should follow:

- Make sure IT is on the board agenda
- Challenge management's activities with regard to IT to make sure that IT issues are uncovered
- Guide management by helping align IT initiatives with real business needs and ensure that management appreciates the potential impact on the business of IT-related risks
- Insist that IT performance be measured and reported to the board
- Establish an IT steering group or IT governing council with responsibility for communicating IT issues between the board and management
- Insist that there be a management framework for IT governance based on a common approach (e.g., CobiT) and a best practice framework for IT service management and security based on a global, de facto standard (e.g., ITIL and ISO/IEC 27002

Part VI: What is fraud?

The definition of fraud

= A representation about a material point which is false and intentionally or recklessly, so which is believed and acted upon by the victim to the victim's damage

⇨ **Fraud is…**
  - intentional
  - to trick or deceive someone out of his/her assets
  - theft
  - a crime

⇨ **Fraud is not…**
  - taken by physical force
  - a mistake or error
  - victimless
  - insignificant because no one is hurt
  - acceptable or justifiable

If you withdraw value from a company, any value, willing fully than you are committing fraud.
If you willing fully fool around with the figures in order to have better results, than you are not withdrawing value from the company but you are misinforming your financial associated and that is fraud as well.

Some statistics

- *U.S. organizations lose about 5 percent of annual revenues to fraud*
- *Median occupational fraud loss:*
  $145,000
- *Median Financial statement Fraud loss:*
  $1,000,0000
- *Median length before detection:*
  18 months
- *Most commonly victimized industries:*
  - *Banking and financial services*
  - *Government and public administration*
  - *Manufacturing sectors*
- *Most occupational fraudsters*
  First-time offenders (87%)

Recent Fraud Scandals

- *AIG: US American International Group – insurance provider that helped a client overstate earnings with a bogus insurance policy – backdated an insurance policy.*
- *Ahold: Koninklijke Ahold N.V. Dutch supermarket. Inflated profits – overstated earnings - and CFO was charged for insider trading.*
- *Bernie Madoff: Ponzi scheme with investors in funds. 150 years in prison.*
- *Lehman Brothers: Repo 150. Sold liabilities and entered and agreement to repurchase them later. Liabilities disappeared from the balance sheet. Created the impression Lehman had $50 billion more cash and $50 billion less in toxic assets than it really did.*
- *Enron: Traded energy and other commodities and derivatives. Artificially inflated stock prices – more during the first workshop.*
- *Worldcom is the largest US bankruptcy ever. Almost twice the size of Enron. They capitalized expenses, i.e. they said the expenses were investments which artificially inflated the balance sheet.*

Important components of fraud

- **Deception/ concealment**: every Fraud scheme involved deception.
- **Greed**: It also involved greed by the perpetrator and—this is important—greed by the investors, who wanted higher-than-sensible returns.
- **Confidence/ trust**: Fraud scheme involved the element of confidence. If he had not paid returns to original investors, no one would have invested additional money. By paying early "returns," Ponzi gained investors' confidence and convinced them that he had a legitimate business. In fact, confidence is the single most critical element for fraud to be successful.

Who commits Fraud

Who commits fraud and why?

Researchers have compared the psychological and demographic characteristics of three groups of people:

- White-collar criminals (fraud perpetrators)
- Violent criminals
- College students

What do you think they found?

- Significant differences between violent and white-collar criminals.
- Few differences between white-collar criminals and the general public.

→ This basically means that anyone is in the danger zone of committing fraud. So, we can't say that because someone has a clean criminal record, they won't manipulate financial statements. So, where do we look next?

Fraud Perpetrators

vs. violent criminals

Fraud perpetrators are:

- Older
- More likely female
- Better educated
- Less likely to have abused alcohol and drugs
- Better psychological health
- More optimism, self-esteem, achievement, motivation, family harmony, empathy,…

vs. college students

Fraud perpetrators are:

- More dishonest
- More independent
- More empathetic

→ *generally much more similar! There are no big differences: so anyone can do it !*

⇨ Fraudsters look like you and me, or your parents, grandparents.

The most common reaction of people is: I can't believe that this happened. He was the most trustworthy employee, friend, whatever.

Makes it almost impossible to know who is committing fraud.

Types of fraud

1. Management Fraud
2. Fraud where an organization is the victim
   a) Employee embezzlement
   b) Vendor fraud
   c) Customer fraud
3. Investment scams – victims are individuals
4. Miscellaneous frauds

⇨ Fraud can be classified in many ways, by victim, by perpetrator, or by scheme.

Most common way of doing this is by dividing frauds into those that are **committed against organizations,** and those that are **committed on behalf of organizations.**

Miscellaneous frauds: do not fall in the previous 3 categories, can be of reasons other than financial gains.

Management fraud

- Also known as financial statement fraud
- Victim: Shareholders, lenders, and others who rely on financial statements
- Perpetrator: Top management
    - They have the power/ the authority to do it

→ Management presents the results and affairs of the organization in a better light than the reality

- E.g., overstating assets or understating liabilities
- In order to:
    - Obtain financing
    - Increase bonuses
    - Increase the share price
    - Attract customers & investors

  → Personal gain

Employee Embezzlement

- Victim: Employers
- Perpetrator: employees
- Explanation:
    - Employees take or divert assets belonging to the employer
    - Most common type of fraud
- Direct fraud:
    - Theft of cash, inventory, tools, supplies, or other assets
- Indirect fraud:
    - Bribes or kickbacks from vendors, customers, or others for lower sales prices, higher purchase prices, non-delivery of goods, or the delivery of inferior goods

Vendor Fraud

- Victim: Organization/clients to which the vendors sell goods or services
- Perpetrator: Vendors
- Explanation:
    - Overbilling or provision of lower quality or fewer goods than agreed
    - Two main varieties:
        - Vendors alone
        - Collusion between buyers and vendors

⇨ Collusion between buyers and vendors: Agent of a company makes a deal for contracted work of 100.000 dollar. Actually it should only have cost 50.000 dollar. The customers pays the agent 20.000 dollar for the great deal. → if you look at it from a risk perspective, collusion is very difficult to detect. Covering it up is very easy for collusion.

Customer Fraud

- Victim: The organization which sells to the customers
- Perpetrator: Customers of the organization who
    - Do not pay for goods
    - Deceive organizations into giving them something they should not have
        - e.g. “identify fraud”: Act that you are a person of an organization / rich person.
- Examples:
    - Payment/credit card fraud – stolen cards
    - Credit fraud – obtain credit, purchase, and then disappear
    - Refund fraud – steal goods and return for refund

Investment Scams

- Victim: Investors
- Perpetrator: Individuals tricking investors into putting money into fraudulent investments
- Examples:

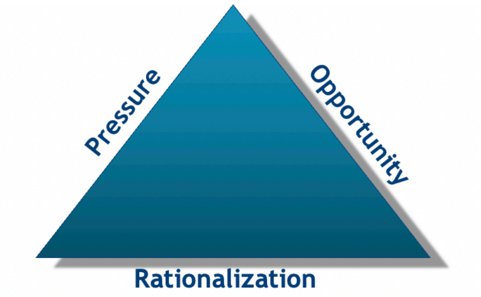
- Ponzi schemes
    - Lure investment funds from victims and then pay those victims a premium or interest from money that is paid by subsequent investors.
- Pump & dump
    - Encouraging investors to buy shares in a company in order to inflate the price artificially, and then selling one's own shares while the price is high.
- Short & distort
    - Investors who short-sell a stock and then spread unsubstantiated rumors and other kinds of unverified bad news in an attempt to drive down the equity's price and realize a profit.
- Off-shore investing
    - Capitalizing on the advantages offered ourside an investor's home country, e.g. tax reduction; asset protection, confidentiality

Other Types of Fraud

- Telemarketing fraud
    - Obtain victim's credit card information or identity and then use this information to make unauthorized purchases elsewhere
      → Try to get personal or financial information from you
- Identity theft
    - Assume someone else's identity e.g., to obtain credit
- Health insurance frauds
    - E.g., customers or providers bill insurers for services never rendered
- Mortgage fraud
- Many more

The fraud triangle

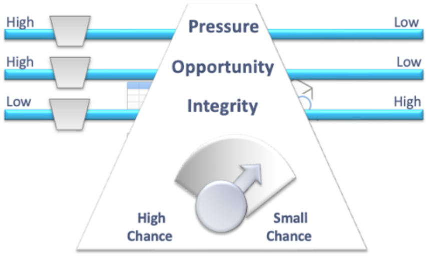
The fraud triangle by Donald Cressey (Important!)



Criminologist Donald Cressey, interviewed 200+ convicted white-collar criminals in an attempt to determine the common threads in their crimes. As a result of his research, he determined that three factors were present in the commission of each crime. These three factors have come to be known as the fraud triangle.

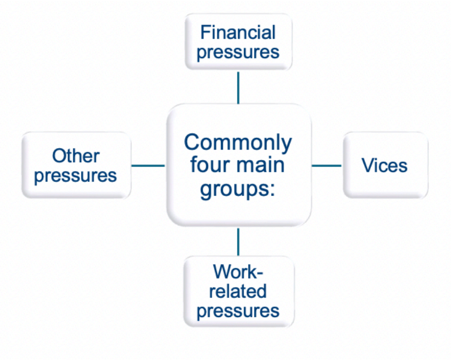
Pressure: Perceived or real pressure (financial needs / don't want to disappoint somebody)
Opportunity: A smart way to deceive people / conceal the fraud e.g. lack of internal control systems in a company
Rationalization: Believe that you are not doing something illegal, and believing that you will be able to pay back in time.

The fraud scale



If pressure goes up and opportunity up and low integrity: high chance of fraud

Pressure


Financial pressures

Other pressures

Commonly four main groups:

Vices

Work-related pressures

1. Financial Pressures

Common Financial Pressures:

1. Greed
   Excessive desire to possess wealth or goods. In other people’s eyes this may not count as a pressure, but what is important here is to consider what the person him/herself feels or perceives. In this case, being greedy will lead to a felt pressure of wanting more and more.
2. Living beyond one’s means
   In today’s world of credit cards and loans, many people simply don’t always understand until it is too late that they cannot afford that new computer, TV or even house. They live beyond their means and oftentimes don’t even notice it.
3. High bills or personal debt
   People end up with debts and bills too high to pay. Huge incentive to at least save on the tax payments…
4. Poor credit
   The poorer one’s credit the less one will be able to buy. Many companies – especially Internet companies – use credit information about customers to determine the payment method. If someone has exceeded their credit too often or not paid on outstanding bills, this person will end up on a black list, and companies won’t sell on credit anymore.
5. Personal financial losses
   Especially in the last few years, people lost tremendous amounts on the financial markets by investing in risky stocks.
6. Unexpected financial needs
   Major leakage in your house, illness in the family, not covered by the regular health insurance,…

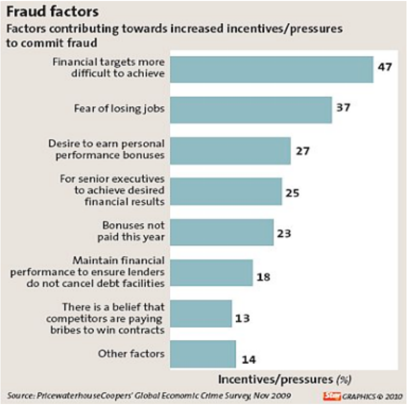
Includes real and perceived financial pressures

→ Not exhaustive

→ Not mutually exclusive

Financial Pressures Among Managers

- Financial targets difficult to achieve: Almost all organizations work with targets. Sales managers should make sure to sell this and that many products. Production managers should produce a certain number of products. Etc. Sometimes those targets become more difficult to achieve, due to bad economy, problems with the product, or other developments, resulting in potential pressure to e.g., make up sales or sell to customers with poor credit.
- Fear of losing jobs: You want to make a good impression with your boss, so you make your performance look better than it is.
- Desire to earn personal performance bonuses: Think about the huge discussion in the press lately related to excessive bonuses and the dysfunctional behavior those can lead to. Organizations now rethink very carefully how they compensate their (executive) employees, because we know that bonuses can lead to excessive risk taking, which in the short run result in bonuses for the individual, but in the long run may seriously harm the business.



Source: PricewaterhouseCoopers' Global Economic Crime Survey, Nov 2009

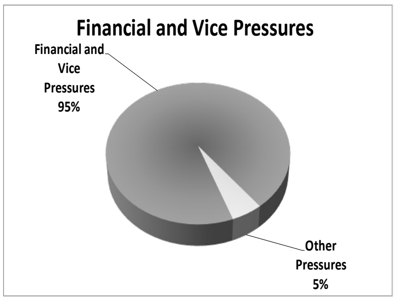
- Achieve desired financial results: At a higher level, it is extremely important for executives to meet the expectations by financial analysts. If the stock market expects a certain stock to rise to a certain level, executives might do anything in their power to make that happen, even if it means cooking the books somewhat.
- Bonuses not paid this year: Increases pressure to make sure next year's bonuses are paid!
- Maintain performance to meet debt covenants
- Competitors pay bribes, so should we – related to rationalization!

Positive pressures (incentives)
→ Wrong incentive system design encourages unethical behavior

2. Vice Pressures

Vice Pressures are the worst kind of pressures to commit fraud

- Examples include:
  - Gambling
  - Drugs
  - Alcohol
  - Expensive extramarital relationships



→ it is the most common fraud types

3. Work-Related Pressures

- Get even with the employer":
  "According to legend, a loyal bookkeeper for a company was denied a $100 monthly raise. The bookkeeper was incensed, so he methodically stole for the next 20 years, until he retired. His replacement discovered an amazing fact: The retired bookkeeper had pilfered exactly $100 a month—the precise sum of the raise he had requested."
- Motivated by these factors:
  - Getting little recognition
  - Feeling job dissatisfaction
  - Fear of losing one's job
- Being overlooked for a promotion
  - Feeling underpaid

4. Other Pressures

- Spouse Pressures
  - Spouse's lifestyle demands
  - Spouse loses job
- Life Pressures
  - Divorce
  - Medical pressures
- Social Pressures
  - "Being successful"
  - "Keep up with the Jones"

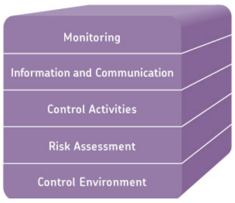
Opportunity

Five major factors that increase opportunity:

1. Lack of controls
2. Inability to judge performance quality: you should have evaluations in your performance as an employee, if that gets subjective than this is a major factor that increases that opportunity
3. Lack of access to information: if your work is not transparent, if it is not reviewed or monitored, than you can easily commit fraud
4. Failure to discipline fraudsters
5. Lack of audit trail: a system that traces the detailed transactions relating to any item in an accounting record
   → Not exhaustive

Five Interrelated Components of Internal Control

Committee of Sponsoring Organizations (COSO) Framework – Internal controls to prevent/detect fraud/opportunity



⇨ The COSO (Committee of Sponsoring Organizations) report discusses five interrelated components of internal control. The components are derived from the way management runs a business, and are integrated with the management process.

1. Control Environment

Control Environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across the organization

- Integrity and ethical values
  - Tone at the top, code of conduct
    - e.g. Employees realized top management was overstating revenues. In response, the employees began overstating expenses on their travel reimbursements

⇨ Having a code of conduct in place is not sufficient. This code has to be regularly updated, reviewed, and communicated throughout the organization. – changes or waivers of code of conduct need to be disclosed

- Management communication
  - Clear communication, e.g. orientation meetings, training, discussions, formal documents
    - E.g. communicate code of conduct (updates, yearly reminder)
- Organizational structure
  - Assignment of authority, responsibility and accountability
    - E.g. easier to track missing assets and harder to embezzle without being caught

⇨ Org. structure: Every organization needs an effective plan of organization. Manager needs good understanding of org structure and the resulting reporting relationships, whether functional, decentralized, or matrix org. structure. If org structure is poor this can lead to inefficiencies and especially if the org. grows to internal control problems.

- Policies and practices for HR management
  - Job descriptions, hiring/firing procedures, training and supervision, evaluation, promotion and compensation; disciplinary actions; vacations and rotations of duties
    - E.g. careful screen job applications / providing reasonable targets for promotions

⇨ Authority and responsibility: Defines lines of authority, responsibility, and reporting. E.g., internal audit dept. should have sufficient authority to check on senior officers' actions, while lower level employees should have no authority to access certain key files.

- Employees should

○ Be clearly assigned to authority/responsibility levels
○ Understand the entity's objectives
○ Be accountable for achieving them

- Internal audit committee
  - Independence from senior management
    - E.g. independent checks – deterrent effect

⇨ Philosphy and mgmt style: To what extent is mgmt willing to take risks? E.g., has an effect on accounting choices, rather aggressive or conservative. Investment decisions.

→ **Foundation for all other internal control components!**

2. Risk Assessment

= Risk assessment is the identification and analysis of relevant risks to achievement of the objectives

- Cost-benefit analyses of implementing Control Activities.

- Key risk management concepts
    - Type of risk (e.g. hiring new personnel /// new business activities)
        - Inherent risk: Outside the control of management and usually stems from external factors. For example, major retailer Wal-Mart is so large and dominant that it faces certain inherent risks due to its sheer size.
        - Residual risk: Risk that remains after mgmt responses to threats have been applied. There will always be some level of resicual risk.
    - Likelihood
        - Probability that the risk will occur. E.g., high, medium, low or percentage. Very difficult to estimate!
    - Impact
        - Easier to estimate. E.g., what if the data server crashes? Which equipment will need to be replaced? What data will be lost?

  → Basic idea is to assess all identified risk and rank them in terms of likelihood and impact, e.g., on a scale of 1 to 10.

- Four basic risk responses:
    a. Acceptance
    b. Avoidance
    c. Sharing
    d. **Reduction by control activities (prevention, detection, correction)**

3. Control Activities

- Segregation of duties
- if you give one person the role to look at the aging of accounts payable and someone else to look at the payment list than there will be no collusion in one function and you segregate those functions. But of course, having two employees costs money.
- System of authorizations
- Independent checks
- Access controls
- Documents and records
- Accounting records: Make sure there is always an audit trail; so record all valid transactions accurately and completely in source documents, journals, and ledgers. First, this is needed to conduct day-to-day operations (e.g., respond to customer inquiries). Second, firms have a legal obligation to report their transactions at least to the tax authorities and (publically listed firms) to their shareholders. Third, managerial reasons.

- Supervision
- Supervision: compensating control for small companies. However, supervision becomes extremely inefficient if employees are not trustworthy or incompetent. Therefore, it should be coupled with an effective control over hiring procedures etc.

<u>Segregation of Duties</u>

- Dividing tasks into parts so that one person does not have complete control of the task
    - Credit Sales example:. Sales Agent vs Authorization of Sales
- Key parts are custody, authorization, recordkeeping and reconsolidation
    - Ideal system: different employees would perform each of the four major functions
    - **Authorization**:
        - e.g. verifiying cash collections / approving purchase orders / approving time sheets → approving transactions and decisions. Previous example: authorize that a machine is beyond repair.
    - **Custody**:
        - e.g. access to funds (transfer funds, checks, safes, lock boxes, assets) / receiving any goods or services / handling paychecks
          → Handling cash, maintaining an inventory storeroom, receiving incoming customer checks, writing checks on the organization's bank account.

    - **Record-Keeping**:
        - e.g. preparing documentation / billing information / posting payments in system / maintaining inventory records
          → Preparing source documents; maintaining journals, ledgers, or other files; preparing reconciliations; and preparing performance reports.
    - **Reconciliation or audit**:
        - e.g. inventory counts, inventory charges to amounts purchased, comparing funds collected to account receivables posting, etc.

If any two of the preceding functions are the responsibility of one person, then problems can arise.

Custodial/recording: A cashier (warehouse) can steal cash (inventory) and record it as an expense or not record it at all. Assets can also be lost and the person responsible doesn't want to take the blame.

Custodial/authorization: shop within a shop
ALSO: Preparing (authorizing) payroll checks and distributing (custodial) them

Recording/authorization: Authorize a fictitious sale and record it as completed (money received).

→ Those four roles need always to be segregated. If you include it in one person you increase the chances of collusion and fraud.

- **Limitations:** Costly, Company size, Collusion

Some examples where we mix these duties:

- Authorization/custody: The person who receives goods from suppliers in the warehouse cannot sign checks to pay the suppliers for those goods.
    - Otherwise, you could collude with the supplier (kickbacks – pay for inferior goods for a bribe)
- Record-keeping/custody: The person who maintains inventory records may not have physical possession of the inventory.
    - Otherwise, one could steal inventory and record that the inventory have become obsolete
- Authorization/record keeping: The person who sells a fixed asset to a third party cannot record the sale or take custody of the payment from the third party.
    - Otherwise, you could put the money in your own pocket without that it is ever recorded.

System of Authorizations

- Management lacks the time and resources to supervise each employee activity and decision. → establish policies and empower employees to perform activities within policy.
- System of Authorizations: Ensure that all decisions and transactions are approved by responsible personnel in accordance with their authority
    - General authorization
        - Allows an individual to execute all tasks or transactions that meet certain criteria.
        - E.g., sales clerk is allowed to accept customer's payment for up to $500 upon presentation of an ID. E.g., fixed reorder points for inventory purchasing to maintain inventory levels.
    - Specific authorization
        - E.g. payment in access of $500 needs approval by store manager

Examples

- Authorization of credit sales - needs to be separated from sales agents who might live under the pressure of sales targets or bonuses

Access Controls

- Logical access controls
  - Authentication
  - Authorization
- Physical access controls
  - Locks
  - Alarm systems
  - Security guards
  - Restricted access
  - Monitoring
  - Etc.

→ Again, redundancy! Guards make sure people authenticate themselves. Combination with authentication and authorization controls!

You can have segregation of duties but what you often see is that when you look behind the screens of the IT systems there are no segregation of duties anymore. So, in your day to day work, the duties are segregated, but when you access your computer system these two different people could do exactly the same thing. If you think about segregation of duties do not only think about the people doing it but also about the segregation within the computer systems.

Independent Checks

→ People know they will be monitored and are thus less likely to commit fraud

- Top-level reviews:
  - Management at all levels should monitor company results and periodically compare actual performance to:
  - E.g. Monitor results (planned performance / prior-period performance / performance of competitors)
- Comparison of actual quantities with recorded amounts
  - E.g. Periodically count significant assets and reconcile the count to company records.
  - Independent verification
  - E.g. after one person processes a transaction, another reviews their work.
- Independent verification
  - After one person processes a transaction, another reviews their work. E.g., shipments are examined to make sure they match the items ordered. Independent checks can also be done by a computer. Imagine that a customer number is entered by a clerk. The company has a system by which the last two digits are so-called check digits: The sum of the preceding digits. This way, the computer can verify that this is an actual customer number.
  - E.g. after one person processes a transaction, another reviews their work.

Documents & Records

- Creation of an audit trail
- Provide detective/accountability controls
- Example: a typical credit sale
  - Customer order
  - Sales order – multiple copies
    - Billing
    - Accounts receivable
    - Warehouse
    - Shipping
  - Matching documents to prevent fraud

→ EXAMPLE: filling out receiving reports days after shipments have arrived. Records will not be up to date, so errors and also fraud are more likely to occur.

Supervision

- Think of foreman in factory/warehouse
- Guard at jewelry store
- Management supervision of day-to-day operations

4. **Information and communication and monitoring**

- Captured information about transactions must be
    - Valid
    - Complete
    - Accurate
    - Timely

  Examples:
    - Control Environonment; Communicating Code of Conduct
    - Control Activities; Documents & Records
- Information flows and Monitoring across COSO components

5. **Monitoring**

- Do all COSO components work effectively?
- Monitoring mechanisms:
    - Tests of controls
    - Risk-related alerts, e.g., excessive sales/expenses by one individual

Limitation of internal control:

- Inability to judge the quality of performance
    - E.g., an auto repair shop. Customers typically won't know what parts and work is needed to repair their car, providing ample opportunity to overcharge customer.
- Failure to discipline fraud perpetrators
    - If you know you won't be prosecuted or sanctioning is very soft, you are more likely to commit fraud. – Humiliation is the best remedy.
- Lack of access to information
    - Particularly applicable to mgmt fraud: Many mgrs have access to confidential financial information and they know that the victim won't be able to look into this.
- Management override
- Ignorance, apathy and incapacity
    - If you know your victim is ignorant of the risk of fraud, or doesn't care…
- Collusion
- Lack of an audit trail: goes back to concealment issue on previous slide.

Rationalizations

- Most people have some level of integrity or morale that we want to satisfy
- Very few fraud perpetrators, if any, do NOT rationalize
- Some examples:
    - "I was just borrowing the money."
    - "It wasn't really hurting anyone."
    - "Everybody does it."
    - "I was only taking what was owed to me."
    - "I didn't take it for myself."
    - "I proved that it is possible to fool the system."

Some Real-Life Examples:

Al Capone

- "I am just a businessman, giving the people what they want."
- "All I do is satisfy a public demand."
- "I have spent the best years of my life giving people the lighter pleasures, helping them have a good time, and all I get is abuse, the existence of a hunted man."

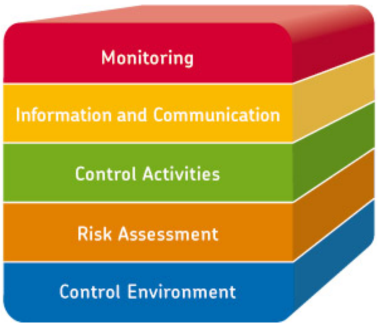
Enron

- Arthur Andersen: "We turned a blind eye because we feared losing Enron's consulting contracts."
- Enron's lawyers: "One of the investigators of the Powers Report recalls that when Enron's lawyers were explaining the details of the elaborate 'special purpose entity' deals that siphoned millions of dollars into Andrew Fastow's (Enron's CFO) pockets, they weren't ashamed or embarrassed. **They were proud of their handiwork, and eager to explain how they did it.**" (Luban 2006)

A Closer Look at Fraud Prevention & Detection

Control activities: COSO

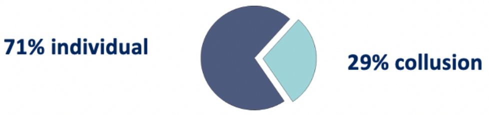
- Detecting Fraud: First three are more preventive measures, last two are detective measures



1. Segregation of duties
2. System of authorizations
3. Access controls
4. Independent checks
5. Documents and records

- none of them are perfect:
  - **Collusion**
  - passwords can be stolen/shared
  - …
- Often they are also not implemented correctly
  - Allow for (management) overrides

Collusion



- Most common form of collusion: indirect Vendor fraud – bribes

How to deal with it:

- Periodic letter to vendors (code of conduct / gifts are not acceptable)
- right-to-audit clause
- rotations of jobs / monitoring

Prosecution and Punishment

- **Fear of punishment is an effective remedy against fraud**
- Admitting the fraud to family members and friends is humiliating
- Mere termination of employment relationship not sufficient
- Strong policy of punishment eliminates rationalizations

But: costly, time consuming, reputational concerns

- Not doing so is only beneficial on the short term. In the long term sends a wrong signal to other employees that fraud is tolerated.
  "I can only lose my job"

Conducting proactive auditing & Whistleblower-systems

- Only very few firms actively audit for fraud. They only examine fraud when there are symptoms that fraud occurred.
- Proactive auditing increases the likelihood that auditors will detect fraud
- Also, actively searching for fraud at any point in time increases a fear of getting caught.

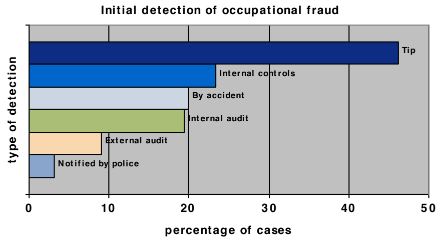
Whistleblower-systems

  - “Others are watching”
  - Detection and prevention
- Employees who know that fraud is happening may
  - Be afraid to come forward with that information
  - Don’t know how to reveal this information

Effective Whistle-Blowing Systems

- Anonymity
  - Employees are assured that they stay anonymous
- Independence
  - The fraud is reported to a party independent of the misconduct
- Accessibility
  - Several different channels through which misconduct can be reported (telephone, email, online, etc.)
- Follow up
  - Incidents must be followed up and corrective action must be taken

Why a Hotline?



Fraud symptoms

Common symptoms (red flags)

  - document may be missing
  - Transaction may not balance in the bookkeeping (e.g. excessive payment)
  - someone may act suspiciously
  - tip of fraud
- None of these are proof of fraud (unlike videos of robberies or bodies in a murder)
- Managers, auditors, employees must recognize symptoms and must check if it resulted from actual fraud or were caused by other factors.
  - Many go unnoticed
  - Or not pursued
- Symptoms can be classified **in 6 groups (see next page)**
  - **Accounting oddities**
  - **Internal control weaknesses**
  - **Analytical fraud symptoms**
  - **Extravagant lifestyles**
  - **Unusual behavior**
  - **Tips and complaints**

Accounting oddities

Unusual processes or procedures in the accounting system

- Irregularity in source documents
  - Missing documents
  - Common names or addresses of payees or customers
  - Duplicate payments
  - Non logical document sequence
  - Questionable handwriting on documents
- Faulty journal entries
  - Unexplained adjustments to receivables, payables, revenues or expenses
  - Unusual entries at the end of the period / and restating at beginning of next period
    - (temporarily boost earnings)
  - By people who usually do not make such entries
- Inaccuracies in Ledgers
  - Summary of all journal entries
  - Non-balancing (assets are not equal to equity and debt)

→ Example: fictitious businesses who send fictitious bills and cash them in – addresses of the businesses all the same P.O. box

Internal Control Weaknesses

- Lack of
  - segregation of duties
  - physical safeguards
  - independent checks
  - proper authorization
  - proper documents and records

Analytical Fraud Symptoms

- Procedures or relationships that are unusual or too unrealistic to be believable
  - Very large / small transactions or weird recurring transactions
- Unexplained inventory shortages or adjustments
- Excess purchases
- Cash shortages or overages
- Late charges
- Unreasonable expenses
- Inconsistency with industry performance
  - Unusual high return on investment, current ratio, days in inventory, cost of good sold ratio, …
- Abnormal inventory tags
  - Total weight of goods exceeds the maximum that your machines can carry.
- Many more..

Remaining Fraud Symptoms

- **Extravagant Lifestyles**
  - Toys, vacations, homes
  - Very few white-collar criminals save the money they steal
- **Unusual behavior**
  - Fear and guilt → stress
  - Changes in behavior
    - Insomnia
    - Alcoholism
    - Inability to relax
    - …
- **Tips and complaints**
  - From co-workers, friends and/or management
  - Customer/vendor complaints

Guest lecture

Guest lecture: definition of audit → has allot to do with the bias of your own opinion. As a human being you are always biased, this is inherent. As an auditor you must limit the biases as much as you can. We saw the three lines of defense. But what is the risk appetite of KUL? He never said something about that. He said that it was difficult to describe what the risk appetite was. It is important to have a clear idea about the risk appetite. The internal audit department of KUL is struggling with this. We would think a low risk appetite:

- The core business is giving a decent education.
- They use public money → publicly funded, you cannot speculate with that money.

He also talked about PCDA circle: the check step is most difficult. People are not always aware of this step.
He also talked about controls. He looks at adequacy and effectiveness of controls. → what's the difference?
Adequacy: we have a risk; do we think that that control is doing enough in theory to mitigate that control. The second step is looking for whether the control is doing its job and that is effectiveness.

Chapter 1: Data analytics in Accounting and Business

So first, what is data analytics and why is it important?
→ In recent years, data has become increasingly important. 59 zettabytes of data has been created, captured, copied and consumed worldwide in 2020. (And just to let you know, a zettabyte is 1 billion terabytes. And if you don't know what a terabyte is, a terabyte is 1000 gigabytes. So, a huge amount of data.) So, 59 zettabytes of data have been created in 2020. And this is compared to just two zettabytes in 2010. So, this growth is phenomenal in 10 years.

- ⇨ More data has been created in the last two years than in the entire previous history of humans. And with so much data available, there is a lot of potential for analyzing this data in a way that can answer fundamental business questions. And this is with the idea actually to create a value for the company.
  And this is exactly what we will be focused on this course.
- ⇨ So learn towards business questions with data, with the idea to make more informed decisions.

<u>Data analytics</u> as a process of evaluating data with the purpose of drawing conclusions to address business questions. So effective data analytics provides us a way to search through large, structured data and structured data to discover unknown patterns or relationship.

→ With structured data, it basically means data that is actually in a predefined data model in a tabular format. For example, data in an SQL database. With unstructured data, we mean basically any data that is not in a predefined data format. Think for example, about a PDF file or a text file with text data.
→ So that being said, format does not really matter actually. So, we can get our data in any form, structured or unstructured, and examine if relationship exists.

So data analytics involves using various technologies, system practices, methodologies, databases, statistics and applications to analyze diverse business data.

And the **<u>goal</u>** is to transform raw data into valuable knowledge that can inform sound and timely business decisions.
→*Although sometimes used interchangeably, we will focus on data analytics and not big data.*

And **big data** refers actually to data sets that are too large and complex for traditional systems to handle. In other words, big data goes beyond the capabilities of business existing systems to capture store data, manage and analyze data sets.

Another way to describe any available data source, as well as big data actually, is by using **<u>the four V's</u>**.

- ⇨ And four V's are basically volume, velocity, variety and velocity.
  - Volume stands for the sheer size of the data set.
  - Velocity, we capture the speed of data processing.
  - Variety is the number of types of data
  - Veracity is the underlying quality of the data.

So data analytics is important!
It's undeniable that data and data analytics have had tremendous impact on business.
According to PWC's 18 annual global CEO survey:

- 86% of CEOs believe that it's essential to champion digital technologies and have a clear vision of how technology can provide a competitive advantage.
- 85% of CEOs believe that high value on data analytics.
  - This is also confirmed basically in PWC's sixth annual digital IQ survey, which was done by more than 1,400 leaders from digital businesses.
- They reveal basically that business analytics is high on the CEO's list of priorities for investments. It's among the top priorities for CEOs to invest in.
  - And this is not only confirmed in PWC's surveys. For example, another survey from Mackenzie Global Institute also underscores this idea.
- They find that data analytics and technology have the potential to generate up to 2 trillion in value per year in a subset of industries alone.

So as a result, data analytics has the power to transform the way companies conduct their business in the near future as its true value lies actually in the insights that it provides. And it's not simply having tons of data around. It's really about using the data in the best way possible to answer business questions.

Data is being set, so most companies have vast amount of data at their disposal. And companies can actually now use and leverage that data analytics to uncover various patterns such as customer buying behavior, identifying unforeseen anomalies, predicting future trends, and many more trends.
→ So this valuable information can provide actually organizations with a competitive advantage and help them make data-driven decisions for the success of their business.

And in addition to these external benefits, data analytics has been found to impact as well internal processes leading to improved productivity and growth. So research actually suggests that data analytics is really forced to have a significant impact on, for example, auditing, financial reporting, tax managerial accounting, and others in the really near future.

How does data analytics affect auditing?

And according to, again, a recent report by the ForBus Insight and KPMG titled the Audi 2020, a focus in change, most survey respondents believe that audits need to basically to better their technology and that technology will enhance the quality and transparency, accuracy of the audits. So, data analytics is expected to become increasingly crucial in the future of audits. And this is because businesses are becoming more complex.

- ⇨ Organizations are looking to leverage advanced business analytics techniques to better identify and manage risks and gain deeper insights into their operations. Audits must do better in the race technology and this technology will enhance quality, transparency, and accuracy of the audit. And many auditors believe that audit data analytics will lead to deeper insights that will enhance the audit quality.
- ⇨ And this sentiment of the impact of data analytics on the audit has been growing for several years now and has given many public accounting firms incentives to invest in technology and personnel to capture and organize and analyze financial statement data to provide enhanced audits, expanded services, and added value to their clients.
- ⇨ So data analytics will does enable auditors to analyze the complete data set rather than sampling financial data which is normally done in the more traditional audit.

And the audit process is transitioning from a conventional approach to a more automated one. And this shift enables audit professionals to devote more attention to the reasoning and logic behind data queries and less on the collection of the raw data itself.

→ Overall, it should enable auditors to improve its risk assessment in both its substantive and detailed testing.

Auditors are thus no longer simply checking for errors, misstatements, fraud, and risk analysis of financial statements. They are now also able to provide deeper insights and more value-added services to their clients by analyzing vast amounts of data to identify patterns and trends and detect anomalies that may have gone unnoticed in the past. And it's expected that this trend will continue and that audit professionals will now be collecting and analyzing the company's data like a way a business analyst would do to help basically management to make better business decisions. And this means that in many cases external auditors will stay engaged with clients beyond the audit which is a significant bearing taking shift.

How does data analytics affect management accounting?
→ Next data analytics is also expected to have a huge impact on management accounting.
One could argue that of all the fields of accounting, the objective of data analytics aligns most closely with those of management accounting.

Management accountants are asked questions by management, find data to address those questions, analyze the data, and report the results back to management to aid in their decision making. The description of the management accountant's tasks and that of the task of the data analyst appear to be quite similar if not identical in many respects.

- It enhances them to do better cost analyzers, improve decision making, or to do better forecasting of budgeting, production, and sales. In all these respects, data analytics can enhance these processes.

⇨ And as information providers of the firm, management accountants must thus understand the capabilities of data and data analytics to effectively address management questions.

<u>How does data analytics affect financial reporting?</u>

According to auditing and management accounting, data analytics also has its impact on financial reporting. With the use of so many estimates and valuations in financial accounting, some believe that employing data analytics may substantially improve the quality of the estimations and valuations. Data from within an enterprise system as well as data from external to the company and system might be used to address many of the questions that face financial reporting.

Many financial statement accountants are just estimates and so accountants often ask themselves the following question to evaluate those estimates:

- How much of the accounts receivable bills will ultimately be collected?
- What should the allowance for loan losses look like?
- Is any of our inventory obsolete?
- Should our inventory be valued at market or at cost value?
- When will it be out of date?
- Do we need to offer a discount on it now to get it sold?
- Et cetera.

→ So there are many of these questions and I think it's actually clear that it can help us to, that data analytics and data in general can help us to answer a variety of these questions.

In addition, it allows an accountant or an auditor to assess the probability of a goodwill write on or a warranty claim or the collectability of bad debts or whatever based basically on information and data of what customers, investors and other stakeholders are saying about the company.

For example, we can collect such data in blogs and in social media. And this information might help the firm to determine both its optimal response to the situation and an appropriate adjustment to its financial reporting.

In addition, it may be possible to use data analytics to scan the environment.

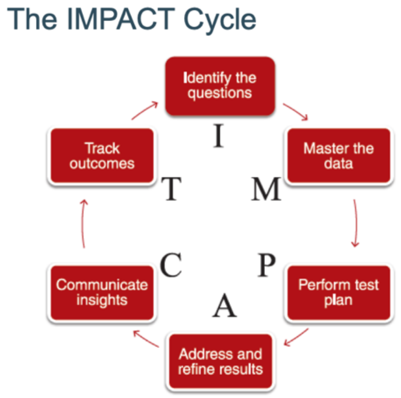
That is, for example, scan Google searchers or social media to identify potential risks or potential opportunities for the firm. For example, in a data analytics sense, it may allow a firm to monitor its competitor and its customers to better understand opportunities and threats around it. For example, our competitors and customers or suppliers facing financial difficulties that might affect the company's interaction with them and or opens potential new opportunities that otherwise would not have been considered.

A lot of these things are just possible to understand how external parties might react to the company and data analytics is ideal to understand these relationships.

Overall, I hope it's clear that data analytics will have a huge impact on how audits, management accounting and financial reporting are done. And the changes in these professions are already occurring now.

And it's important that you learn the necessary skills to really stay relevant in these fields.

<u>How does data analytics make an impact ?</u>



→ the data analytics process concept in more general terms using the impact cycle.

So the basic scheme displayed here is the impact cycle that we will use. And we will use this throughout the course. And I want to re-emphasize that data analytics is a process to identify business questions and problems that can be addressed with data.

But very important here, it's with a real goal to create value for the company. So, it's not simply working with data. The key is analyzing questions with data to answer real business questions with the goal to create value for the company. *So, we start basically our journey in data analytics by using an established data analytics model called impact cycle developed by Eisen and Harriet.*

And we explain the full impact cycle briefly here in general terms. But in the next chapter and labs, we focus on each of these elements separately in more detail. And we just use this methodology to break down everything in smaller steps.

⇨ We start from carefully Identifying the business questions, assessing and analyzing the data, to communicating insights and tracking outcomes.

The impact model stands basically for the following steps:

- Identify the questions
- Master the data
- Perform the test plan
- Address and refining results
- Communicating insights
- Track outcomes.

<u>Step 1: Identify the questions</u>

The first step in our impact model is thus **identifying the questions.**

→ And here it all begins with understanding a business problem that needs addressing.

Identify a specific question that can potentially be answered by data analytics is a crucial initial step as questions may arise from various sources such as improving customer attraction, product pricing, cost reduction or identifying errors and frauds. Having a concrete specific question that is potentially answerable by data analytics is an important first step. And this is a very important skill to learn. And it's already now already relevant as well because you're now writing, asking this as well, you must write basically a question, a research question, which you need to be able to answer with data as well.

So you need to answer the right question, which is which you're able to answer with data. And indeed, accountants actually often possess this unique skillset, right, so to improve an organization's data analytics, because they're actually able to ask the right questions, right, especially since they often understand the company's financial data.

→ So in essence, we could ask any questions in the world. But if we don't ultimately <u>have the right data</u> to address a question, there really isn't much use of data analytics for those questions.

So next to understanding the business problem and obtaining the right data to answer those questions, we also need to consider a couple of other elements.

- And an important one is the audience: <u>who is the audience that will use the results of the analyzers</u>? Is this the initial, the internal auditor or the external auditor? Is this a CFO? Is this the financial analyst? Is this the tax professional, etc. So depending on the audience, you might focus on different questions, different data or different level of detail.
- And the scope of the question is also important: <u>So, is the question too narrow or too broad?</u>
- And important also to use: <u>how will the results be used?</u> Is this to identify risks or is this to make data-driven business decisions? All these things are important to take into account when formulating your questions.

List of potential questions accountants might address using data analytics.

- Are employees circumventing internal controls of payments.

One could go into, for example, more detail and ask specific questions such as

- Are there any suspicious travel and entertainment expenses?
- What is the level of travel and entertainment expenses that we need to check considering various costs for searching for such a, what frauds that might exist?

So, the costs and benefits, doing a trade-off there. And all these things, so all these things on how to formulate the question will depend basically on your audience.

Other questions that one could ask are, for example

- Are our customers paying us in a timely manner?
- How can we predict the allowance for loan losses for a bank loan?
- How can we find transactions that are risky in terms of accounting issues?

- Who authorized checks above $100,000? And how can errors in journal entries be identified?

These are just a couple of examples, but there are tons of things that we can basically analyze and answer real-life business questions with data.

<u>Step 2: Master the data</u>

Once we know which questions we want to solve, we need to understand where we have available data on. And it's important to **master the data**. And to excel in data analytics, it's crucial to have a comprehensive understanding of the available data and to evaluate if they can assist in solving the business problems at hand.

- ⇨ So to effectively work with the data, we must have a comprehensive understanding of its characteristics, such as accessibility, availability, reliability, update frequencies, time periods covered, and all the relevant factors that ensure the data aligns with our business questions.

To provide you some guidance for formulating data-related questions, it may be helpful to consider the following.

- For example, review data availability in firms' internal systems, like, for example, their internal financial reporting system or enterprise systems that might occur in its accounting processes.
  - For example, financials procured to pay production processes or to cash, human resources, etc. On all these levels, we will have tons of data which we might be able to use to solve our business questions.
- Next, one we would also want to review data availability in a firm external network, including those that might already be housed in an existing data warehouse.
- Next one could also examine data dictionaries and other contextual data basically to better understand the data and provide some details about the data so we can basically have a better understanding of what is available.
- Importantly, we also want to evaluate and perform the ETL, so in other words, extraction, transformation, and loading. And the ETL process, and we need to better understand the ETL process, and it assesses basically the time required to basically complete the job.
- Next to these things, a couple of things are also important, such as assess the data validation and completeness to provide a sense of the reliability of the data, evaluate and perform data normalization to reduce data redundancy and improve data integrity
- Evaluate and perform data preparation and scrubbing, so in other words, data cleaning. And it's important to note that this last element, so the process of cleaning the data, is crucial and time-consuming element in this whole process of mastering the data.

So according to data analytics professionals, it can take up to 50 to 90 percent of their time to ensure that the data is actually in a suitable format for analysis.

<u>Step 3: Perform the test plan</u>

So, after that we formulated the questions and mastered the data. This basically means that the data is now ready to use, and we can now perform a test plan.

→ And so we need to think of the right approach to the data to be able to answer the questions. And in the field of data analytics, our goal is to basically to extract insights and solutions from available data to tackle questions and challenges. And this involves examining all available data to identify potential relationships between the response variable, also known as the dependent variable, and the factors that influence them. And they are also often known as the predictor, the explanatory, or the independent variables. Typically, we develop a model, a simplified representation of reality, to help us achieve this aim.

> *And in the upcoming videos, we will formally discuss the most relevant approaches to accounting and highlight the accounting questions that each approach can address.*

These are the eight different approaches that we will discuss, which include:

- Classification
- Regression
- Similarity matching
- Clustering
- Co-current scoping
- Profiling

- Link prediction
- Data reduction

Step 4: Address and Refine Results

So once the data analysis is completed in step three of the impact cycle, the fourth step involves basically **addressing and refining the results**.

⇨ So the process of data analytics is iterative and involves slicing, dicing and manipulating the data, testing hypotheses, finding correlations and asking further and hopefully better questions.

So, we also seek feedback, for example, from colleagues and revise and rerun the analyzers multiple times. So, once we have completed this process, we have the results ready to be communicated to the interested stakeholders, which should directly address basically the questions.

Step 5 and Step 6: Communicate Insight and Track Outcomes

Step five and step six is communicating insights and track outcomes. So once the results have been determined, so the step four of the impact cycle, we go basically, create insights for the decision makers that we need to communicate to them.

And that's basically the C in the impact cycle. Of course, afterwards, some outcomes will be needed to be continuously tracked. So, and that's then the last element, the D in the impact cycle.
→ So in the following session, we will explore various methods for presenting results, such as executive summaries, static reports, digital test boards and data visualizations.

So, in data analytics, the goal is to deliver the results that enable decision makers to view data from a new perspective and gain insights that address business questions. But we need to acknowledge that different users may interpret deliverables in a different way. So as a result, digital dashboards and data visualizations are becoming increasingly useful in conveying insights and monitoring outcomes.

And as the impact cycle is basically continuous process, the gained insights and tracked outcomes lead to the emergency of no more refined questions that may require the use of the same or different data sources and different analyzers.

> So therefore, the impact cycle starts again. So, we get from these results that we generated and that we communicated to the CEO, the CFO, for example, we might again gain new insights and then again, new business questions arise. And then the impact cycle starts again to address these new questions and to gain further insights. And that's basically the last thing we need to start the process again.

What data analytic skills do accountants need?

So let me make clear that the accountants are not expected to become data scientists. They may never need to be able to build a database from scratch or perform the real hardcore data analytics. But professionals who work with data must possess several key skills. And these include basically the following:

- So, they should be able to clearly articulate the business problem that the company is facing.
- Effective communication with data scientists to understand the specific data needs and assets and assess basically the quality of the data.
- They need to draw accurate conclusions from the data and address the business problem and provide timely recommendations.
- They need to be able to present results in an accessible manner to various members of the management such as the CEO, the auditors, the CFOs, etc.
- And they really need to develop a development analytical mindset and think critically about the data and the insights.

Develop Analytical Mindset

So having an analytical mindset these days is really crucial. And to develop an analytical mindset is important to have proficiency basically in the following seven areas.

- So, for example knowing when and how data analytics can address business questions,

- Understand data scrubbing and data preparation processes necessary basically to clean and prepare the data before the analysis can start
- Recognize data quality and understanding what is meant by completeness, reliability, or validity
- perform descriptive data analysis to gain insights into the quality of the underlying data and its ability to answer the business question
- Demonstrating the ability to manipulate data to sorting, rearranging, merging, and reconfiguring it in a manner that allows for enhanced analysis. And this may include diagnostic predictive or prescriptive analytics to appropriately analyze the data.
- Next one also need to be able to basically identify and implement an approach to statistical data analyzes that allows for timely conclusions and recommendations.
- And finally reporting the results of analyzes in an accessible way to each decision maker and for their specific needs. So you can actually only learn these skills really by doing it.

Microsoft Data Analytics Tools

So instead of giving you only theory we will also do some exercises. So these labs that are available on Toledo. And we will do these exercises with Microsoft tools. But I do want to highlight that there are actually many other providers that provide solutions to analyze data. For example, other tools that are popular in different industries are for example Tableau, Qleak, Tipcore, etc.

But I want to say that Microsoft tools are the ones you will most likely encounter because of their positions as leader in the data analytics space. So for this reason each of the exercises throughout these sessions will use Microsoft tools and will help you to become proficient in those tools. But you must mainly see that developing analytical mindsets.

So, the skills you learn as you work through the workshop and the labs are easily transferable to other tools as well. It's simply a software package that you're using and all other packages are basically very similar. But the main idea of the workshop is to make you to make it a bit more practical and visual for you as well.

> → So Excel is a widely used spreadsheet software that is often utilized for basic data analyzers.
>
> → PowerQuery is a powerful data connectivity and preparation tool that is actually integrated in both Excel and Power BI.
>
> → And Power BI is a powerful analytical platform that allows users to create both basic and complex data models and visualizations which can be combined basically to create test boards for easy sharing with relevant stake rulers. All these data are basically in the basic office package and Power BI is a free tool that any Windows user can also use basically and freely download on the web. All the information is normally also added in, is added on Valdido, whether it's a page how you can basically download Power BI on your Windows computer.

Hands- on example of the impact model

→ A complete and hands-on example of the impact model to show you how it could be implemented for a specific situation.

Suppose that I need to secure a loan to pay off some credit card debt and a friend of mine has informed me about a known traditional funding source that doesn't require to go to a bank.

→ Peer-to-peer lending. And this has gained a lot of popularity in recent years with the help of the internet, and it allows basically individuals to lend and borrowing money from each other.

- And there are various peer-to-peer lenders exist, but we will focus specifically on lending club a

Hands On Example Step 1: Identify the question

We will share some data as well from this institution. *So the key question at hand is whether actually I would be able to qualify for a loan based on my credit score, prior loan history and some other relevant factors.*

So to be a bit more specific, the key question that we're actually asking is *what are the common characteristics of loans that have been rejected?*

Hands On Example Step 2: Master the data - LendingClub

→ We need to master the data first.

We ideally would want to have data just from lending club, the organization itself. And lending club is basically headquartered in San Francisco, California and is a peer-to-peer lending company operating in the United States. And it facilitates basically borrowing and lending, specifically offering unsecured personal loans ranging from $1,000 to $35,000 with a loan period of approximately three to five years. And investors who are interested in investing in loans on lending club platform can basically access information about loan listings, power information, loan amount, loan gates, and the purpose of the loan. So, by investing in these loans, investors can earn interest while lending club basically generates revenues by charging powers, organization fee, and investors' service fee. And since 2007, lending club has facilitated over $60 billion in loans for hundreds of thousands of borrowers.

So where can we find the data?

- Some basic lending statistics are included in the lending club statistics website. And each borrow represents basically the volume of loans each quarter during its respective years.
- Next, we also observe some data that borrowers borrow money from a variety of reasons, including and paying off credit cards, as well as borrowing for other purposes.

⇨ The great news is that lending club also provides some data sets. They have data on the loans it's approved and funded, as well as data for the loans that were declined. And to address our question, right, so what are the characteristics of rejected loans, we will basically mainly focus on the data set of rejected loans.

The data that is available:

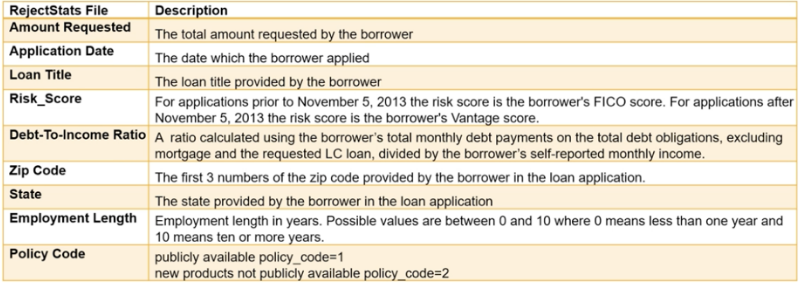
- Approved loans (LoanStats)
- Rejected loan stats (RejectStats)

⇨ So in this specific case, we're less interested in the loans that got approved because of our research questions. So we focus basically on the question, on the data set for rejected loans, because it just contains less relevant information for our purposes.

So, we just gather to correct data and check it in detail. Right, so to effectively analyze the data, it is crucial to understand what if information is at our disposal.

→ So, for this purpose, we can, for example, report to the data dictionary, which offers basically detailed explanations of each data attributed and included in the data set. And the subset of the data dictionary specifically for the rejected loan database is provided here in this account. For example, the variable application date would give a description of the date which the borrower applies.

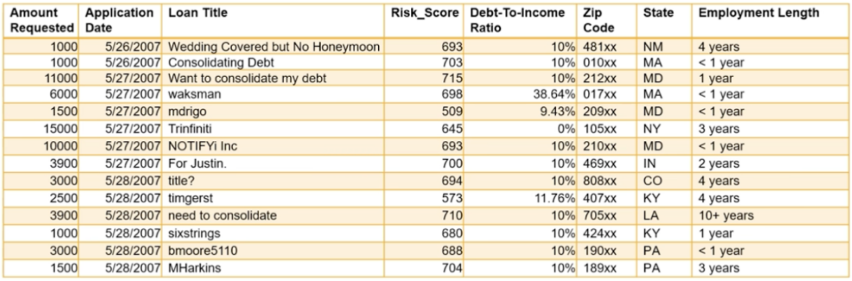
And all these variables are basically in our database. And next to it is a nice description of what each variable means.



RejectStats File	Description
Amount Requested	The total amount requested by the borrower
Application Date	The date which the borrower applied
Loan Title	The loan title provided by the borrower
Risk_Score	For applications prior to November 5, 2013 the risk score is the borrower's FICO score. For applications after November 5, 2013 the risk score is the borrower's Vantage score.
Debt-To-Income Ratio	A ratio calculated using the borrower's total monthly debt payments on the total debt obligations, excluding mortgage and the requested LC loan, divided by the borrower's self-reported monthly income.
Zip Code	The first 3 numbers of the zip code provided by the borrower in the loan application.
State	The state provided by the borrower in the loan application
Employment Length	Employment length in years. Possible values are between 0 and 10 where 0 means less than one year and 10 means ten or more years.
Policy Code	publicly available policy_code=1 new products not publicly available policy_code=2

Then we can also deep dive into the data itself, now that we know what each variable needs and we already saw some interesting variables there. And here I present basically a snapshot of the data of the rejected loan data file. And exploring the available data is important for basically answering your question about the characteristics of the rejected loan, right.

→ "What are the characteristics of the rejected loans"



Amount Requested	Application Date	Loan Title	Risk_Score	Debt-To-Income Ratio	Zip Code	State	Employment Length
1000	5/26/2007	Wedding Covered but No Honeymoon	693	10%	481xx	NM	4 years
1000	5/26/2007	Consolidating Debt	703	10%	010xx	MA	< 1 year
11000	5/27/2007	Want to consolidate my debt	715	10%	212xx	MD	1 year
6000	5/27/2007	waksman	698	38.64%	017xx	MA	< 1 year
1500	5/27/2007	mdrigo	509	9.43%	209xx	MD	< 1 year
15000	5/27/2007	Trinfiniti	645	0%	105xx	NY	3 years
10000	5/27/2007	NOTIFYi Inc	693	10%	210xx	MD	< 1 year
3900	5/27/2007	For Justin.	700	10%	469xx	IN	2 years
3000	5/28/2007	title?	694	10%	808xx	CO	4 years
2500	5/28/2007	timgerst	573	11.76%	407xx	KY	4 years
3900	5/28/2007	need to consolidate	710	10%	705xx	LA	10+ years
1000	5/28/2007	sixstrings	680	10%	424xx	KY	1 year
3000	5/28/2007	bmoore5110	688	10%	190xx	PA	< 1 year
1500	5/28/2007	MHarkins	704	10%	189xx	PA	3 years

And this file, we might for example find some interesting variables that can give us some descriptive reasons why this might be the case. Note that in this file we already have basically a clean and transform data set, right, making basically immediately available for use.

In the next chapters, we will dig deeper into this. I will not talk too much about data scrubbing and data preparation and cleaning. This is something for the next chapter, but normally this would be the first step that we perform. Now we're quite lucky. We already have a clean data set, and we can immediately start our analysis.

Hands On Example Step 3: Perform the Test Plan - Analyses

So we had a look at our data and there were some interesting variables in there.
And so giving this file, we were thinking about doing three different analysis to assess what is considered to reject a loan.

- The debt-to-income (DTI) ratio and the number of rejected loans. (So how are these two related?
- The length of employment and the number of rejected loans
- The credit or risk score and again related to the number of rejected loans.

And we expect that these three loan characteristics, which are also collected by landing club, will allow us to evaluate the borrower's ability to repay the loan and provide insight into the likelihood of a loan approval or injection.

Hands On Example Step 3: Perform the Test Plan – Pivot

Okay, so the initial evaluation we conduct focuses on the potential borrower's debt to income ratio. So, in other words, we assess the proportion of the potential borrowers existing debt to their annual income. And this is all prior to adding the proposed loan, of course. So, in order to incorporate the debt-to-income ratio into our analysis, we now create basically three distinct categories, and we refer to that as the DDI pockets.

→ And for each, and we classify them depending on the range from the DDI, so the debt-to-income ratios. And the three pockets are classified as follows:

- High is, for example, greater than 20% of income.
- Medium can be debt between 10 and 20% of income
- Low is basically debt is less than 10% of income.

So, this is basically simply creating three buckets out of this debt-to-income ratio that we have available. And in the labs, I will also show you how to do this yourself. And then we can immediately see basically what is going on here. And an ideal way how to do that is with Excel, for example, with a pivot table.

And this provides a convenient method for comparing the various levels of DDI. So, by conducting a pivot table analysis, we can emphasize the loan counts, which represent the number of loan applications that were submitted and subsequently rejected, as well as the DDI buckets. So, the pivot table tells us the number of loan applications in each of the three DDI buckets: high, medium, and low.

And this implies that since the high DDI bucket exhibits the greatest number of loan applications, it is plausible that the applicants requested a loan that exceeded their income level. So landing clock may have regarded this as too risky and decided not to approve a loan based on the depth of income ratio as a deterrent effector.

Hands On Example Step 3: Perform the Test Plan – Buckets

The second panelizes examines the duration of employment and its correlation with declined loans. One could argue that the longer an individual has been employed, the more stable their job and income would be, thus increasing their likelihood of repaying the loan. And the nice thing is again, landing club records, the length of the employment for each of the declined loan application. And the pivot table analyzers represent here the number of loans categorized by employment duration. So, these are all the categories that are available in our database.

So this time we don't basically classify the data in smaller group, we just use all the data that is available and then see what is the count for each of those employment levels.

And what do we see?
→ Approximately 77 percent, so basically the 459,000 over 645,000 is a 70 percent right of the overall rejected loans feature individuals who have been employed for less than one year. And this suggests that this could be a significant reason for the loan inadequate. So, it's plausible that some applicants had only been employed for a week or a month, yet still they were looking for a large loan. And of course, these guys then got rejected, which is confirmed by our analyzers here.

Hands On Example Step 3: Perform the Test Plan – Scores

Our third analyzers and tales basically assessing the credit or risk of the loan applicant. So as stated risk scores are typically categorized based on credit scores, which those failing within the excellent and very good range receiving the most favorable terms and lowest interest rates. So, this is a credit score here with above 750.
In contrast individuals with a very bad score, so credit rates below 600 are the opposite of the spectrum and they're most likely to either not get a loan or at very high interest rates.

You all also have already a credit score and there are companies, credit rating agencies, who are basically specialized in creating these scores for individuals. So, they work together for example with companies such as electricity providers, telephone and internet providers, and these type of service providers basically provide information to the credit rating agency how you are basically paying your bills/ your payment behavior. So, if you do not pay in time your bills or do not pay off your credit card debt or something like that, this will in the end have a negative impact on your credit score right and this credit score is then used by other parties for example banks, which then will basically decide should you get a loan or not right. So, and in the end that this might all have an impact on your later owners, on your impact on how much interest rates you pay etc.

In any case here, like the debt-to-income ratio, we will basically classify again the credit ratings in these categories as well right. So, we will classify them in an excellent, very good, a good, fair, poor or very poor credit rating and then again see how these loans, what is basically the count of the rejected loans. And in every valuation of credit scores and the client loans, we once again employ basically a five-table analysis. So, by counting basically the number of rejected loan applicants by credit score, we see basically that almost 82% of the applicants either held a very bad or poor or fair credit score. Again, indicated that this can have a significant, could be a significant reason for the loan denies. And furthermore, what we also observe here is that only 0.3% or the 2494 divided by the 645,000 in grand total, so the 0.3 of the rejected loans were basically only if you have an excellent credit score. So, it's not 0 but a very, very low amount.

Hands On Example Step 4: Address and Refine Results – Summary
So we now did a couple of basic analyzes, right, so the fundamental analyzes, but we can now also enhance our analyzes for getting basically deeper insight. So more refined analyzes may for example evolve an in-debt examination of the rejected loans. For instance, for the set of declined application, we could now investigate how many of these applicants possess not only excellent credit but also held 10 or more years of employment and applied for a loan amounting to less than 10% of their incomes.
So, in other words, we can combine these measures together to get a bit of deeper insights, what are the extreme values where we find the strongest or the weakest effects.

From the PivotTable analysis, we find that of the rejected loans:

- 82% have either very bad, poor, or fair credit
- 48% have a high D T I ratio
- 76% had a work history of one year or less

Hands On Example Step 4: Address and Refine Results – Interactions
Now we can examine a three-way interaction and determine that the answer is 365 out of the 645,000 representing a 0.057% of the total. So, this finding actually shows that only a very, very small amount of people was basically rejected the loan in case they, for example, have an excellent credit rating at 10 or more years of employment and the loan requested accounted to less than 10% of their income. And it's such a small, small, small percentage of the loan term that this also makes a lot of sense.

Hands On Example Step 4: Address and Refine Results – Predictions

Now, it's possible that those with those excellent credits were denied because they requested a loan amount that was way too large in relation to their existing debt. So, we dig into this, and the analysis indicates that the individuals with excellent credits requested a loan amount equaling 60.2% of their income, which was larger than any one of the other credit categories. And this might explain why even borrowers with excellent credits were rejected. So, all these results are now produced basically with pivot tables. In other words, we merged several data bases together and produced some descriptive statistics. And this gives us immediately some important insights on the questions that we raised.

Hands On Example Step 5: Communicate Insights

Further, even more advanced analysis could be conducted, but for now, we have a good understanding of the factors that Lenni Club uses to determine loan applications or injections. The question now is how to effectively communicate those insights to decision makers, for example, would it be the best to show the pivot tables, or should we create the graph of the results or simply present the names of the three determinants?

The answer to this question will depend a bit on the company's communication standards and preferences of the decision makers. So, understanding these preferences will help the analysts to determine the most effective way to present the results. And in the following sections, we will also provide some additional examples of how to effectively present your insights using several kinds of visualizations.

Hands On Example Step 6: Track Outcomes
The final step involves tracking outcomes, which can take many forms. However, predicting future outcomes based on past data may be the most effective approach. For instance, we can use the data analyzed from 2007 to 2012 to make predictions for subsequent years and adjust our prediction model as new insights and data become available. And this process can help us improve the accuracy of our predictions and identify areas for improvements*. More examples of the impact models are also available on Toledo as well.* So, this was basically a high-level summary of the impact model.

Summary

So in this chapter, we basically discuss how businesses and accountants derive value from data analytics. We gave some specific examples how data analytics is used in businesses, accounting, managerial accounting, and financial accounting. We introduced the impact model and explained how it's used to address accounting questions. And then we talked specifically about the importance of identifying the questions. We walked through the first few steps of the impact model and introduced eight data approaches that might be used to address different accounting questions. And we also discussed basically the data analytics skills needed by analytical mind and accountants.

We followed the user up by using a hand-on example of the impact model, namely what are the characteristics of rejected loans at lending clubs. We performed this analyzing using Fedris filtering and PivotTable Toss. And in the next set of labs, you will basically learn some of this and you will basically do this yourself as well with some real examples. Overall, with all the data around us, businesses and accountants are looking at data analytics to extract the value that the data might possess. And data analytics is changing the auditors and the way that accountants look for risk. So now auditors can consider 100% of the transactions in their auditing testing. It is also helpful in finding anomalies and unusual transactions.Data analytics is also changing the way financial accounting, managerial accounting and taxes are done at the company.

The impact cycle is a mean of performing data analytics that goes all the way from identifying the questions to mastering the data, to performing data analyzers and communicating and tracking results. It is recursive in nature, suggesting that as questions are addressed, new, more redefined questions may emerge that can be addressed in a similar way. A data approach addresses different ways of testing the data. We will discuss those more in detail later onwards, such as classification, recognition, matching, etc. And data analytics skills are needed by two accountants to create an analytical mindset. And they are basically consistent with the impact cycle and they include the following, which is basically develop an analytical mindset, data scrubbing and data preparation, data quality, descriptive data analyzers, data analyzers through data manipulations, statistical data analyzers competency and data visualization and data reporting.

Chapter 2: Mastering the data

And in this chapter, I'll give you a quick run-down of different types of data used in accounting and what you can typically find in a relational database. So, the second step of the impact cycle is all about mastering the data, which is also known as the ETL. And this stands for extracting, transforming and loading the data.

→ *We'll talk about how to get the data you need to answer questions related to any specific business. And we'll also cover how to prepare, validate and clean the data to make it easier to work with.*
Finally, we'll explain how to load this data into the right tool so you can analyze it and make smart decisions.

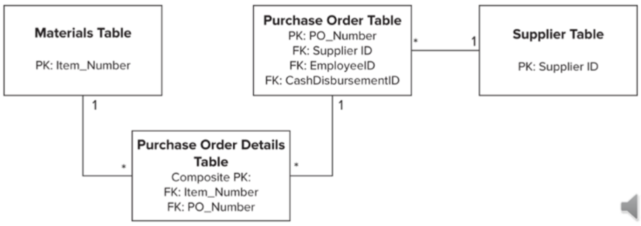
How are data used and stored in the accounting cycle?

So first things first, so before you can get the data that you need, you need to know what kind of data is available and where it's stored.

- Data can come from a bunch of different places, so both from inside or outside the organization.
    - Inside the organization, you might find data, for example, in the accounting system, a supply chain management system, customer relationship management system, or a human resource management system. There's also sometimes called an enterprise resource planning system that combines all these different systems into one big system, so one big data warehouse.
    - So next to that, so inside the organization, we can have data, but we can also collect data from outside the organization. And so you can basically find external data from different sources, like data about the economy, financial institutions, from the government, or other places.

  → So, all these different sources can be helpful when you're trying to answer questions related to accounting and business.

- So you should basically, with data that either comes from inside or outside the organization, have an idea of what tables and attributes hold the data that you need.
    - But you need to have a basic understanding of the accounting processes and how the data are organized, so it can basically help you to ask for the right data and also to find where it's basically stored.
- There are basically different ways that data can be stored. So both, but most commonly they're basically stored into flat files or databases. *(We'll be focusing on databases throughout this course, but we'll also be transforming the data into flat files for some of our activities.)*
    - Flat file is just a simple spreadsheet basically, like for example with Excel, where all the data is all in one table available. So, to put simply, a flat file is just a simple way of keeping all your data into one place. You can use Excel to do some really cool analyzers and calculations.
    - But when it comes basically to storing a lot of data for the business, it's not a very efficient way to do this. So, it's the best thing is not to keep all the data in one huge, big spreadsheet. It's better to store that basically in a relational database. A relational database is like a special kind of software that is good at keeping a lot of data organized and making sure that it's accurate. You can use it to store all kind of data for the business. It helps make sure that everybody's looking at the same correct version of the data across different processes. And there are basically a lot of different software calculations that support relations databases. And one way of naming those are these **RDBMs**. So, it's basically the **relations in database management system.**
        - A good example of this is for example, Microsoft SQL Server. But there are many different database management systems that you could use. So like Amazon RDS, Teradata, MySQL, Oracle, RTBMs and many more. And even though there are different software options that you could use, they all follow very similar principles for how to organize the data. And these principles are basically called a relational database, because they make sure that all the different pieces of data are connected to each other. And they relate each other in a very logical way.



And this relational database, as you could actually see that a little bit has a lot of flat files, for example Excel files. A lot of flat files that are connected to each other in various ways. And we can draw a diagram out of that: how they are all related to each other.
And we could, for example, write down a **unified modeling language** class diagram. And it's a diagram that shows how all these different tables in a database are related to each other and give you immediately a quick overview on how the data is organized.
→ but in a real life, this diagram scheme becomes much more complicated if you're really dealing with like a big enterprise system that's combined data from a lot of different places like manufacturing, accounting, human resources, etc.

<u>How are data used and stored in relational databases?</u>

So when we want to analyze the data, we want to actually make sure that everything is organized in a way that makes a lot of sense. Preferably we just work basically what we call basically a normalized relational database to store all the structure of data.

- And this really helps us to keep things organized and makes it easier to work with the data.
    - But sometimes we also might need to work with the data directly in the database
        - But we can also basically export some of the data to more user-friendly formats so that we can really do some analyzes on this.
    - To write reports to find an answer on your business question, sometimes it just makes sense to export some of the data to write an important about it. But the raw data we basically keep stored in those rational databases.
    - And even though exporting that data can take some extra time, it's worth it because the benefit of having it then organized in a flat file outweighs some of the time sites as well.

  - But storing data in a rational database that is organized and free from redundant information really helps you to ensure that the data are complete and consistent.
  - It also makes it easier to enforce, for example, business rules and internal controls and facilitate communication and integration across different business processes.

There are actually a lot of benefits:

- make sure that the data is complete and that all the necessary data for the business processors are included in the data set.
- Next, it's also important to import storing redundant data because this takes up space. And in case of processes time and raises the risks of errors.
  - So instead of having one relational database, you could have a lot of flat files, but these can cause a lot of redundancy. And these known large relational databases don't because they require only one version of the truth, and each element of the data is stored only in one specific place.
- Next, it's also very handy that we can set up a lot of business rules and internal controls to help us ensure that everything runs smooth as well. So, we can put some controls there to see that the data is stored correctly as well. And this is something that flat files actually cannot do as well.
- A last point is basically about communication and integration of the business processes and relational databases are actually designed to help different parts of a company to communicate and work together more smoothly.

⇨ So, by using these normalize relational databases, data is basically stored in a way that is efficient, accurate and consistent, which helps to break down skills silos and improve collaborations between departments. This can result in a better integration of business processes and improve communication across different areas of the organization. And it's basically important to appreciate the advantages of using a relational relational database to store data because it can be challenging to create a database structure and understand how it works.

⇨ It might seem easier to have like a dump of data in one single spreadsheet, but it's actually way more beneficial to have an institutional relational database, but it does take some time basically to set it up.

There are four types of attributes

So, it's very important to know so how this table in a relational database are related. You need to understand how these tables are structured. And here I provide a quick guide to understand the different types of attributes which are typically in a table in a relational database. And I'll try to explain how they basically are connected to other tables as well. So, this guide may not cover everything, but it will help you to make, for example, later on with data requests when you're working in a company and you need certain data, how you can optimally request such kind of data.

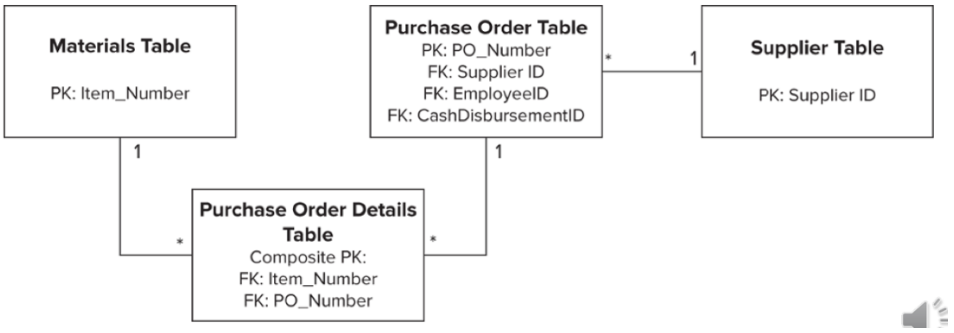
Each table within a relational database, each column in that table should have a specific purpose. You should not have repeated information already presented in another column within that table.
And there are basically three types of different columns. So, the **primary keys, the foreign keys and the descriptive attributes.** We also have the **composite key**, which is actually a special case of this form. But we do have basically three main ones:

- A primary key: this is basically a unique identifier for each role within that table. Primary keys usually made up of one column and it's not typically descriptive in nature. So, it's actually usually a collection of letters or numbers that are assigned in a sequential manner.
  - For example, as a student, you will have a unique identifier as well, your student ID. And this uniquely identifies you as a person within the organization of the KUL. But there are tons of other examples of these unique identifiers, right?
  - for example, as Amazon. You there have unique order numbers or invoice numbers or account numbers. You can have social security numbers, et cetera. So there are already always primary keys that within a certain table of can be editing

  → So instead set of persons, firms, organizations, et cetera, they will have a primary key to be identified that specific object or person
- Foreign keys: are basically attributes that actually point to a primary key in another table. So these foreign keys are also unique identifiers, which can help us to link this specific table to another table within a relational database as well.

- Composite keys: that's basically a similar as a foreign key, but it's basically a combination of two foreign keys used for the line item.
- Descriptive attributes (a lot of these): which includes everything else
    - For example, if you would have a database about a person. You as a student at the KUL, we might have a table there. So, there is a full list of all the students that are enrolled, and we have the primary key, your student number, which then may contain some other information next to this: Did they, for example, pass for certain courses, et cetera, which would then be all descriptive attributes within that specific table.

<u>Examples of tables, attributes, and data.</u>
Notice the PK-FK relationship



→ the main difference between a flat file and a relational database is the number of tables that the data is stored in. In a flat file, you get one big table with a lot of repeated information, but in a relational database, each group of information is stored in a separate table. And to show how these tables are related to each other, a foreign key is placed in one of the tables. So, the foreign key is another type of attribute and it's used to create a relationship between two tables. And whenever two tables are related, one of them must contain these foreign keys. So, in a table, the other columns that are not primary or foreign keys are called basically descriptive attributes. So, these columns contain important information about the business process, such as the name of the supplier, the number of sales, et cetera, but they're not used to build the data model.

The primary and foreign keys are essential for the structure of the database, while the descriptive attributes contain the actual business data. So again, here is basically an example of how a database is set up to handle a common purchasing process.

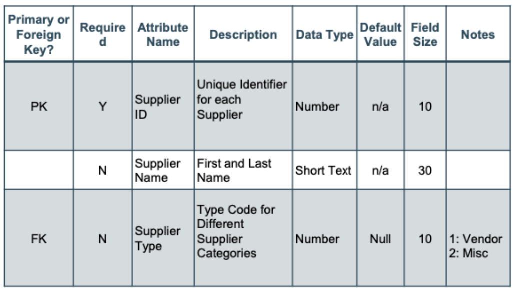
> Each table in the database has a unique identifier called the primary key represented here by the letters pk. For example, the primary key for the materials table is item number, and for the purchase order table it is p o number. Additionally, some tables also have foreign keys represented by the letters fk, which connects them to other tables. For example, here the supplier table and the purchasing order table are connected to each other by the key called suppliers ID. So, it's basically the primary key in the suppliers table, then you can find back the suppliers ID, and it's a foreign key in the purchasing order table. By combining, we can now merge these two tables with each other by this unique identifier, so those lines are connected to each other. I hope this makes it clear that this helps you basically to organize and manage data. And in this specific example, it helps us basically to organize the purchasing process within an organization.

<u>Data dictionaries define what data are acceptable</u>

Looking at each process and scheme by itself can help us understand it better, but it can also be misleading. So, these schemes usually don't stand alone as separate databases, but instead each scheme for a specific process is part of a bigger database that includes all the schemes together. When all these processes are combined in one database, there can be a lot of data to handle. Even if you understand how the data is stored, it can be hard to remember where every piece of information is or what it exactly means.
So, it's important to create and use, for example, a data dictionary, and especially for database administrators who need to maintain the databases and also for analysts who need to find the data. These data dictionaries are a very useful tool as well.

And in chapter one, we already introduced a data dictionary. For example, when we discussed the landing club data for the rejected loads. And in that example, it was simple. Because the landing club data is a flat file. So, the only thing needed to describe it are the attributes name and the description. The description is an important thing because it helps us basically to ensure that each attribute is used and analyzed correctly. Computers only do what they're told. So, it's necessary to really understand the data completely to avoid making bad decisions. So therefore, before doing any analyzes, it's important to thoroughly review the database schemes and the data dictionaries: to understand how the database is structured, but also to know for each single attribute what they exactly measure.

And here I provide basically an example of a data dictionary for a supplier table within a relational database. In the previous example, we just had a flat file. Then we didn't serve any form and case or primary case, etc. But this is a typical dictionary for a table within a relational database.



Primary or Foreign Key?	Require d	Attribute Name	Description	Data Type	Default Value	Field Size	Notes
PK	Y	Supplier ID	Unique Identifier for each Supplier	Number	n/a	10	
	N	Supplier Name	First and Last Name	Short Text	n/a	30	
FK	N	Supplier Type	Type Code for Different Supplier Categories	Number	Null	10	1: Vendor 2: Misc

We have a data dictionary which basically lists the attributes of the tables, such as, for example, here, the supplier ID, the name, the type, etc. For each attribute, there is a description of what it represents and how it should be used in data analytics. And it also lists, for example, if certain items are then primary case or form case, which then helps us to link these tables to other tables.

It's important to keep a data dictionary to ensure and to understand basically what is in the data. But also to ensure that we can basically use the data correctly and analyze the data also in a proper way. And it avoids basically incorrect assumptions, which then again lead to mistakes or poor decision making, etc. So, each time when you look at the database, right, look at the schemes!

So, the schemes basically describe how databases are related to each other, how these tables within a relational database are related to each other. The schemes are therefore very important.
Next to that, the data dictionaries are also important because it really tells us, what does every single attribute within that table exactly measure?

<u>What does it mean to extract, transform, and load?</u>

Once you have familiarized yourself with the data via data dictionaries or the schemes, you are basically prepared to request the data from a database manager or extract the data yourself. The ETL process then begins with identifying which data you need and is complete when the clean data are loaded in the appropriate formats in the tool that is used for the data analyzers.

This process basically involves five steps

1. Determine the purpose and scope of the data request
2. Obtaining the data
3. Validating the data for completeness and integrity
4. Cleaning the data
5. Loading the data for analyzers.

<u>Step 1: Determine the purpose and scope of the data request</u>

Before you start with analyzing the data, you need to figure out exactly what data you need to answer your question. Asking for data from a database is usually a process that involves several rounds of communication. However, the more you're prepared before you're asking the data, the less time you'll spend going back and forth to be the database team. So, the process of requesting data involves the first two steps of the ETL process.

Each step has its own questions that you basically need to try to need to answer to make the process as smooth as possible. Several questions just need to be asked.

- What is, for example, the purpose of the data request?
- What do you need the data to solve?
- What business problems will they address?
- What risk is this in the data integrity?
- Etc.

Once you have a clear understanding of why you need the data and have identified any potential risk assumptions, the next step is basically to figure out who to ask for the data and what exactly you need from them. And then you should also think about already about the specific required formats for the data that you need. For example, do you want to have it in Excel, a PDF or a database format? And what is that deadline by which you need the data? And it's important to be clear and specific in your request really to save time for yourself, but also for the database team.

Step 2: Obtain the data – questions

Step two is obtaining the data. Again, several questions are related to these steps that you need to answer before you do this step or during the process of obtaining data.

- So how will the data be requested and how will you obtain them?
- Do you have access to the data yourself or do you need to request a database administrator or the information systems department to provide the data for you ?
- If you need to request a data, is there a standard data request form?
- Where are the data located in the financial or related systems?
- Etc.

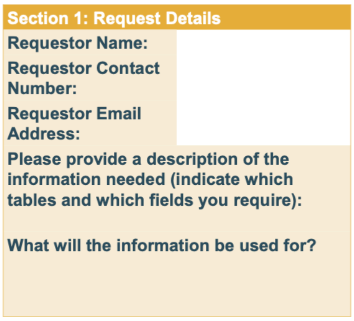
→ So these are all questions to ask yourself.

Step 2: Obtain the data – Methods

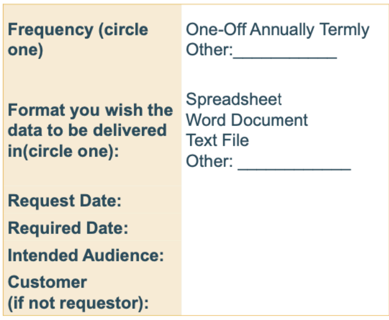
To obtain the data, you have basically two options, right?

- Obtain the data yourself: If you have access to the database, you can write some queries to basically extract the data.
- If not, and there is basically a data management team where you need to obtain the data. After you need to work with the standard data request forms.

Example Standard Data Request Form – Header



Section 1: Request Details	
Requestor Name:	
Requestor Contact Number:	
Requestor Email Address:	
Please provide a description of the information needed (indicate which tables and which fields you require): What will the information be used for?	



Frequency (circle one)	One-Off Annually Termly Other:___________
Format you wish the data to be delivered in(circle one):	Spreadsheet Word Document Text File Other: ____________
Request Date:	
Required Date:	
Intended Audience:	
Customer (if not requestor):	

Here's an example of a data request form. You always must give some contact details, but also provide the scripture or the information that you need. And you can be very specific here.

For example, you could ask for a flat file. And then be specific that the first row should contain the headings and each subsequent row should contain basically the corresponding data. You could also mention that you want to avoid including like subtotals or breaks of subheadings as they can really complicate the data cleaning process as well.

Once you receive the data, check each column basically to really understand the data that you receive. And if there is data dictionary, make sure to read that of course. But if it's not a range available, also arrange a meeting with the database users or the database team to really gain some clarity here.

Obtain the data yourself

You could also try to obtain the data yourself. And if you have access to the database or an information system that has basically the data that you need, you can extract the data yourself instead of going through that more formal process of data request.

Start with identifying the goal of the data analyzers and the project that we basically identified in the first step of the impact cycle. When you have identified the data that you need, again, by using data dictionaries, relationship models, examine the necessary attributes and tables, et cetera, you can basically start gathering the information from this database. And there are a variety of methods on how to do this that you can basically think that you can use to retrieve the data. For example, when you plan to perform your analyzers in Excel or Power BI, each tool basically also has an SQL option where you can basically directly connect to a database and pull basically the data out of this database, out of these relational databases.

➔ So, understand the data dictionaries and the relationship between all these databases before you can basically start this process as well.

Step 3: Validate the data for completeness and integrity

Once you have the data, you need to validate the data for completeness and integrity. Whenever you move data from one place to another, there is a risk of losing some of the data during the extraction process. For example, by doing it on birch with one of the tables from a foreign key to a primary key, that something went wrong. So it is very important to make sure that the extracted data are complete and that have not been tampered with or duplicated during the extraction.

To do this, you need to have some technical skills, but also a good understanding of the data. If you know what to expect from the data, you can more easily identify errors or issues. Some questions that you could add to validate the data is basically to check that your data is valid. So how many records would we have expected that should be in this flat file and does this compare basically with what we have in the end? Or do some checks on some controls, etc.

The following four steps should be completed to validate the data after extraction:

- And the first important step is basically doing some data validation is to compare the number of records that were extracted. So, the number of records basically in the source database. And you can basically check those to quickly identify any missing or improperly extracted data due to errors or due to data type mismatches, etc. However, this only confirms that the record count matches and does not provide any information about actual data. The total records could be the same, but still the underlying data there can still be an issue there.

- Next to that you could do some descriptive statistics on numerical fields. For example, calculate the minimums and the maximums or the averages and the medians, to help basically ensure that the numeric data will be extracted completely.
    - So if you have, for example, a sales records where you see the maximum of certain value, does this compare with the maximum in the original database as well.

- Next you can validate the date and time fields in the same way as numeric fields by converting the data type to numeric and running also descriptive statistics there to compare. So then you basically see is the maximum of our data field the same in the maximum of the original database.

- Next, we can also compare string limits for text fields. So when validating the data it is important to check for any limits on the number of characters in the text fields. Excel does allow quite large number of characters per cell, but there is also a limit. So if you extract data into a tool with a smaller limit, for example, a certain database that you use for each cell, there is, for example, a limit of one million characters that you can enter in a specific cell, but let's say that it's in Excel only 255. Then there is an issue: each cell will then be cut off. So you need to basically check what is the maximum number of characters that you have there to see if there is any differences and to avoid losing information within yourself.

Whenever you then would encounter an error, it's important to identify the missing or the incorrect data and do that in a timely manner, right before you do the analysis. For a small data set might be possible to just do a visual scan. Right. So just check the data by doing that. However, for a large database, this is basically impossible. If you have millions and millions of rows, it's a very complex database. It may be necessary to do all these scans. Right. So, comparing descriptive statistics for all your cells and attributes to see if something is going wrong. And if that's the case it's necessary then to revisit the extraction process and examine the code that you use. For example, SQL code to extract the data and see if this led to any errors. So once the issues have been addressed, right, so you can rerun then the extraction and proceed basically with the validation process again to ensure that the data is now accurate and complete.

Step 4: Clean the data

Once you basically got the data and you check that everything is accurate and complete, it's now very important to basically to clean it up as needed to make sure that it's actually that the data is of good quality for your data analysis that you want to do. And here are four common ways that you might need to clean up the data to do a proper analysis.

- So first of all, you need to remove headings or subtotals. Depending on the extraction techniques used and the file types of the extraction is possible that your data could contain some headings or some subtotals that are not useful for your analysis. In the ideal case, you just have a flat file where the top row is basically heading all other information who are just data items related to those columns.But it should not include again subtitles or subtotals, etc. Each column should contain one attribute in your database.
  - Of course, it might be some things that you can overcome in the extraction process, so in the ideal process and then go back to the previous step to try to extract the data in a way that they are not in there. If that is not possible, you basically need to do probably manually that and remove all these headings and subtotals.
  - If this is the only way possible to get the data, you will need to remove those headings and subtotals within the data.

- Next, we also want to make sure that the cells that we have for each column that they have clean data, right, and we want to basically clean the leading zeros or non-printable characters at the set. So sometimes this data may have extra characters, for example, leading by a zero or non-printable character like a space or something like that, and they need to be removed for accurate analyzers. I'm leading zeros are those zeros that appear before the actual number and non-printable characters are characters that you can't see such as spaces, page, page, line breaks and tabs, etc. These characters can really cause issues during the data analysis, especially when you're joining data or comparing strings, etc. It's very important because a machine will only merge observation when they are the same right and one small difference (for example, a space that you do not observe, but there is a space there in that cell) it will not merge those two databases to each other right so those two variables will not be merged because the cell will be different because of a non-printable character space for example. So, it's important to make them identical and to remove all these inconsistencies.

- Another thing that we also want to check is for example negative numbering. It's important to ensure that the formatting of negative numbers in your database is basically appropriate for your analyzers. So, for instance, if you have data including negative number formats in parenthesis right but you would prefer to have them displayed with the negative sign instead of having positive number in parent thesis, you will need to make sure that this is the case right. The most important thing is that it's consistent right it doesn't really matter how you format them, but it should have a consistent format across your different tables right so across your different columns.

- Next you want to correct for inconsistencies across data in general right so for example if the database source did not have consistent rules for data entries, you may find variations in the way the data is recalled. To give an example: imagine that you have a country field, and you have a cell where we would observe for example Belgium: it could be formatted many ways it could be written completely just Belgium, or it could be written as Be or it could be written as bel etcetera. So if you have variations in that that's not a deal we want to have one consistent way across the data that we want to observe, similar like with the format of the negative numbers right so either you have the negative sign and then your number or you put your number within parenthesis right that's also a typical example but in any case we want to have it consistent across the database. And it's important basically to clean this up by replacing these inconsistent values with a common value. For example, with Belgium and we have several ways out to write it down either Belgium, be or BEL, we just choose one doesn't really matter which one, but we choose one and we keep that consistent. this will help us later to group and analyze the data base on this specific criterion.

Watch out for bad data quality.

Great invalid data can really distort the results and lead to incorrect conclusions. So low quality data may include various areas obsolete or incorrect information or invalid entries in general, and it can really negative impact the analyzes.

So therefore, you really need to check and validate the quality of the data to ensure that your analyze procedures really produce meaningful and reliable insights and to validate the data sets and it's under a line data quality. Here are basically five main data quality issues to consider when you evaluate data for the first time.

- Dates: dates can be a common issue in data preparation due to the variety of formats which you are presented in.
    - For instance, July 6th 2023 can be expressed in various ways so you need to format the date basically to match the acceptable format for your tool. There is an ISO standard right that indicates the format that you could use right so and that's basically the year one pay format so 2024 0706 and most professional query tools except this format. So you highlight your dates and go to home then number then format cells and choose the appropriate version on how the format should be.
- Numbers: so often with this database will look at sales or whatever right but it's important to be aware that the numbers can easily be integrated especially if there are some manual data entered in this line.
    - So, for instance the number one can for example be mistaken for the letter I and the system kept the letter I. Over zero can for example sometimes be an O. This can lead to basically to errors in terms of sorting or analyzing the data. It is important to watch for this invalid number formats and then to also to correct them right so.
    - For example, it's common to see accounting simple such as dollar signs commas or parentheses in spreadsheet data. For example, if you have 12 million dollars right. Then the dollar sign should be removed usually remove the commas for the thousand separators etc. To clean the data remove all these extra accounting characters: the commas, the dots etc. So that's important and the dollar signs so that you just have a number there which is consistently formatted.
- International characters and encoding: dealing with special characters can actually be a challenge when working with data from different countries for example. So, you can have like special characters like exit marks not invisible characters used in programming language languages etc. And these can all cause issues, so to address this you can find basically replace the function or put the characters in quotes so that they can basically be known by the programming languages right. Also older databases may use still an older standard right ASCI inside of the Unicode for text encoding. So if you encounter issues with your data set international characters and symbols may actually be the cause, so always check these special characters.
- Languages and measures: sometimes data elements can have multiple words or measures that mean actually the same thing. For instance, from March and cheese right so these two things mean exactly the same thing but they are then you they're using a different word for basically measuring the same thing. So to correctly analyze the data you should choose one standard words and replace all equivalent words with it. Additionally you need to ensure that the measures being used does not change the meaning right for example the total value in US dollars is not the same as the total value in euros so it's also important to compare the same measure to ensure accurate analysis.

- human errors : when people manually enter data mistakes really can happen such as typos or entering data in the wrong place. And this can result really in bad data so the best way to deal with this input errors is to stay alert right and correct them when they happen. For example by using a final replace function.

Step 5: Load the data for data analysis

If you have extracted and transformed your data properly actually loading should be the easiest step of the ETL process. In fact, if you plan to analyze your data in Excel and have already cleaned and transformed it in Excel then you're done basically right there is no further need for loading steps right.
So, while Excel may be sufficient for some data analyzers test, it may not actually be the best tool for all scenarios, so the choice of analyzing tool will depend really on factors such as the data analyzing techniques that you will use, or the specific business questions that are asked or the desired format for presenting it etc. It's important to consider all these factors when selecting an appropriate tool for your analyzers.

What ethical issues do we encounter in data collection and use?

And as a last note so mastering the data involves a little bit more than just the ETL processes, so it will also enforce that ensuring the data collection is secure. And the ethics of data collection and use have been carefully considered. In the past digital risks only focused on cybersecurity threats to really protect the data security. But now there is an increase in concern about ethical data practices. So, it's important to ensure that the data collected from traditional and non-traditional sources are used ethically and for their intended purposes. Assuring the ethical use of data involves addressing potential privacy concerns and providing guarantees that the data will not be misused. It's important to consider whether individuals have the right to limit access to their personal information and control how it's shared or used with others. For instance, if somebody shares their credit card information for an online purpose purchase you should be assured that the card number will not be used for any under and authorized activities.

To ensure ethical data practices the Institute for Business Ethics recommends that companies consider these elements listed here.

1. How does the company use data, and to what extent are they integrated into firm strategy
2. Does the company send a privacy notice to individuals when their personal data are collected?
3. Does the company assess the risks linked to the specific type of data the company uses?
4. Does the company have safeguards in place to mitigate the risks of data misuse?
5. Does the company have the appropriate tools to manage the risks of data misuse?
6. Does our company conduct appropriate due diligence when sharing with or acquiring data from third parties?

Chapter 2: Summay

The first step in the impact cycle is basically to identify the questions that you intend to answer to your data analyzing project. So once a data analyzes problem or question has been identified the next steps of the impacts cycle is mastering the data which includes obtaining the data needed and preparing it for analyzes. And we often call the processes associated with mastering the data the EDL process which stands for extract transform and load.

And to obtain the right data it's important to have a firm grasp of what data are available to you and how the information is stored.

> Data are often stored in a relational database which helps you to ensure that the organization's data are complete and to avoid redundancy. Relational databases are made up of tables which rows of data that represent records and each record is uniquely identified with a primary key. Tables related to other tables can basically be linked by using the primary key for one table as a foreign key in another table.

Then we have basically the extract process right and that is to obtain your data. So, you will either have access to extract the data yourself or you will need to request the data from a database administrator or the information system team. If the latter is the case you will complete the data request form indicating exactly which data you need and why. Then we will transform the data.

Once you have the data you will need to basically to validate it for completeness and integrity. You will basically ensure that all the data you need were extracted and that all the data are correct. Sometimes when data are extracted some formatting or sometimes even entire records might get lost and this results basically in occurrences. So, correcting these errors and cleaning the data is an integral part in the mastering the data process and a very important part as well.

Next, we will load the data and just after that when everything is cleaned this is basically the very last step of mastering the data. We will load them into the tool that will be used for analyzers. But often this cleaning and correcting the data can for example occur in Excel and the analyzers can potentially also be Excel. So, if that is the case there is basically no loading step necessary anymore. However, if you for example clean everything Excel but then you want to use another software program for example PowerBi-I then this loading step still occurs. This can for example occur if you want to do more rigorous statistical analyzers to do more robust data visualizations etc. Mastering the data does goes beyond just the EDL process right. So those who collect and use data also have the responsibility of being good stewards providing some assurance that the data collection is not only secure but also that the ethics of data collection and data has been used and data use have been considered.

Chapter 3: Performing the Test Plan and Analyzing the Results

In this chapter we will focus on performing the test plan and analyzing the results.
But let us start this session again with a short recap of last session. in the last session we talked about how we get data ready to use for business questions. We explain how we clean it up, get it organized and make sure it's accurate. We also talked about how we follow rules to exchange data between people. And lastly, we also talked about how it's important to protect people's privacy when we collect and use data

In this chapter we will thus focus on the test plan and analyzing the results. Data analytics means using different methods and tools to figure out what's going on, compare things, predict what might happen and decide on what to do next. So, in this part we talk about different ways to do this and when to use it. We also gave some examples related to accounting to show how to use these methods and what to expect from the results. We focus on following elements:

- Describe some descriptive analytics approaches including summary statistics and data reduction.
- Explain the diagnostic approach to data analytics including profiling and clustering.
- Understand predictive analytics including any questions.
- Describe the use of prescriptive analytics including machine learning and artificial intelligence.

<u>What are the four categories of Data Analytics</u>
The third step of the impact cycle is thus called performing the test plan. And that's the focus of this chapter. And here we will discuss thus different data analytics methods to analyze what happened, why it happened, what we can expect to happen in the future and what actions we should take based on our predictions. And these methods that we will discuss here will help us answer business questions and support accounting and management decisions.

And there are basically four big types of data analytics tools that we can use, and they include these four mentioned here.

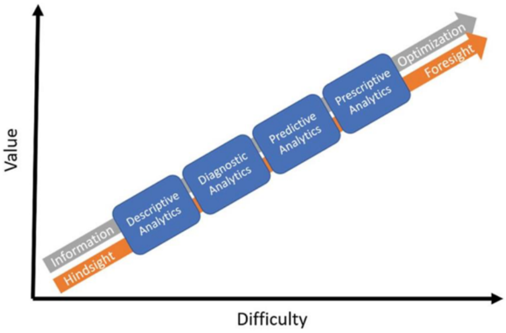
- Descriptive analytics: these are basically procedures that summarize existing data to determine what has happened in the past.
    - So, some examples of these descriptive analytics include summary statistics, think about creating accounts, a minimum or a maximum, the average, the median, etc. Or to look at distribution and proportions.
- Diagnostic analytics: and these are procedures that explore the current data to determine why something has happened the way it has. Typically comparing the data to a benchmark. And as an

example, diagnostic analytics allow us users to drill down in the data and see how they compare to a budget competitor or a trend.

- Predictive analytics: these are procedures used to generate the model that can be used to determine what is likely to happen in the future. So some examples of predictive analytics include, for example, a regression analysis forecasting classifications or other modeling tools. We will mainly focus in our course on regression analysis.
- Prescriptive analytics: these are procedures that work to identify the best possible option, giving certain constraints or changing conditions. And this typically include developing more advanced machine learning and artificial intelligence models to recommend a course of actions or optimize based on constraints and or some changing conditions.

Each stage takes additional effort but provides additional value

Each of these elements can be seen as different stages in the data analytics process. Some stages require more effort, but they also provide more value. We usually start with descriptive analytics, which involves describing what happened in the past. Then we might move on to diagnostic analytics, which help us understand why things happened. After that we can do predictive analytics, which help us predict what might happen in the future. And lastly, we have prescriptive analytics, which suggests what we should do based on our predictions.



- ⇨ So, depending on the question we're trying to answer, we might want to use some or all of these stages in the data analytics process. So choosing the right data analytics model really depends on the type of question you're trying to answer. And of course, also the data you have available to answer.
- ⇨ Descriptive and diagnostic analytics often go together when you want to describe past data and compare them to a benchmark to understand why the results turned out the way they did.
- ⇨ On the other hand, we basically have these predictive and prescriptive analytics, and they are often used together when you want to predict what will happen and then make recommendations on what actions should take.

So as you move actually from one data analytics approach to the next, you shift from looking at what's already happened to predict basically what might happen in the future. So that's basically the flow that you might want to work with. But most of the time we basically just start with these descriptive analytics

Descriptive analytics examples:
Two main examples of the most typical ones that we think about when we're talking about descriptive analytics.

- Summary statistics: can really just be the starting point to answer a certain business question or it might even be the end point. For some basic questions that one might have, just looking at the summary statistics might already give you an answer. And the summary statistics, they basically describe a set of data in terms of their location. And this can for example be the mean or the medium. Could also be the range, the standard deviations, the minimums and the maximums or the shape and the size. With all these things we can already have a very good idea on how the data looks like by just looking at the summary statistics.
- Data reduction or filtering: this is used to reduce the number of observations to focus on the most relevant observations. For example, the highest cost, the highest risks, the largest impact, etc. And it does this actually by taking a large set of data, potentially the full population, and reduce it to a smaller set that has the vast majority of the critical information of the largest set. For instance, in auditing, data reduction can actually be used to narrow down transactions based on the relevance or their size. So while auditing is traditionally used to handle stratified sampling techniques, data analytics offers actually no ways to identify which transactions do not require the same level of scrutiny.

Diagnostic analytics examples:

- Profiling: identifies basically the typical behavior of an individual, a group or a population, by compiling some very statistics about the data and comparing individuals to the population. So profiling does the technique used in data analytics to identify patterns of typical behavior so that any deviation from that behavior can be easily identified as abnormal. And in accounting, profiling can be used to identify transactions that may require additional investigations such as outlier travel expenses or potential fraud. And by using profiling techniques, we can actually quickly and efficiently identify anomalies and take appropriate action to investigate them.
- Clustering: his helps us to identify groups or basically clusters of individuals such as customers for example, that share common underlying characteristics. So in other words, identifying groups of similar data elements and the underlying drivers of those groups. For example in a customer analyzes, clustering can be used to segment customers into a small number of groups for example for additional analyzes and risk assessments. Similarly, transactions can also be grouped into clusters based on their characteristics or attributes to better understand the underlying relationship between them. So by using these clustering techniques, we can identify patterns and relationships that may not be immediately being parent from the data, but which allows us actually then to make more informed decisions.

Next we have two more diagnostic analytics examples:

- Similarity matching: and that's a group technique used to identify similar individuals based on data that we know about them.
    - For example, companies can use this technique to find out if a seller or a customer is committing fraud by comparing their characteristics to those of no fraud cases. And then they can take actions if they find any similarities.
- Co-occurrence grouping is something similar again, so this discovers associations between individuals based on a common event such as transactions they are involved in.
    - And a good example is here at Amazon, so they use this technique to suggest other products to customers based on what other people have bought alongside the product that they are looking at. So, for example, if you're looking at a book on Amazon, they might suggest other books that customers bought, that also bought this book as well. This is called Co-occurrence grouping.

Predictive analytics examples:

- Regressions: estimates or predicts a numerical value over dependent variable based on the slope and intersect of a line and the value of an independent variable.

Prescriptive analytics examples:
We will mainly discuss machine learning and artificial intelligence. And these learning goals or intelligent agents can adapt to new external data to recommend a course of action

So, we have these four types. We have descriptive diagnostic predictive and prescriptive analytics. And we will now go through each of these four elements in a little bit more detail. And I've already highlighted here a couple of examples that we will discuss, but there are many, many more different techniques that one can use. However, we do not have sufficient time to discuss really everything. But in the next couple of slides, we will just limit our discussion to the most common models, including summary statistics, data reduction, profile, enclosing, regression, and artificial intelligence. This means also that these different data approaches can be used to answer certain business questions, but they can also be used together. They are not completely separate from each other as well. And sometimes it's necessary to use a combination of these techniques to get the best results as well. And maybe also the last final point, as I mentioned before, we have here the impact cycle model that we discussed, the third action, performing the test plan, so the P in the impact model, the third phase. But it's these elements that we discussed here are equally important in the fourth step, so the A of the impact model, addressing refining results. So as a model, you will basically learn from all these tests that you will do, and by doing it, you will also refine your approaches as well. So basically, we're focusing here now on the step three and the step four of the impact cycle, where we will basically learn from these methods as well. And from one method, you can go through the other methods to get more detailed results.

<u>What are some descriptive analytics approaches including summary statistics and data reduction?</u>

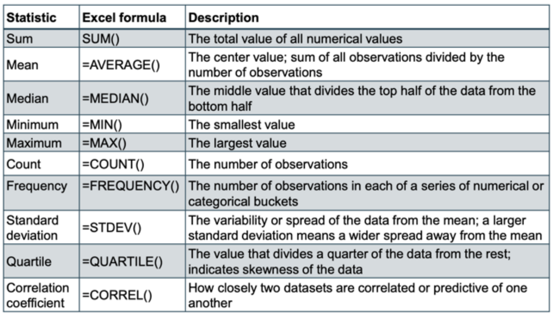
And descriptive analytics is a way to summarize what has happened in the past.

- So, a financial encounter would add up all the sales transaction within a period to calculate the value for sales revenues that appears on the income statement.

- And analysts would, for example, also count the number of records in the data extract to ensure that the data are complete before running a more complex analysis.

- An auditor would filter data to limit the scope to transactions that represent the highest risk. All these cases use basic analysis to help decision makers understand what happened in the past and make good decisions going forward.

<u>Summary statistics</u>
Summary statistics are a set of numbers that help us describe a group of measurements, or variable. They tell you things like the highs and the lows value, the average, how much the value value from one variable to another. Other summary statistics include, for example, the middle value, how much the value are spread out, and how often each value occurs.



Statistic	Excel formula	Description
Sum	SUM()	The total value of all numerical values
Mean	=AVERAGE()	The center value; sum of all observations divided by the number of observations
Median	=MEDIAN()	The middle value that divides the top half of the data from the bottom half
Minimum	=MIN()	The smallest value
Maximum	=MAX()	The largest value
Count	=COUNT()	The number of observations
Frequency	=FREQUENCY()	The number of observations in each of a series of numerical or categorical buckets
Standard deviation	=STDEV()	The variability or spread of the data from the mean; a larger standard deviation means a wider spread away from the mean
Quartile	=QUARTILE()	The value that divides a quarter of the data from the rest; indicates skewness of the data
Correlation coefficient	=CORREL()	How closely two datasets are correlated or predictive of one another

And using summary statistics can help you understand the data better. For instance, you can use the sum function to calculate the total amount of money in the count. You can use the mean and the median to group transactions by employee, location, or division. And the standard deviation and frequency can help you detect patterns and see what is normal in the data. So, a lot of things are possible here, and it really helps you to see the difference across different groups. So, it can also help you to better understand the data set. For example, the minimum and the maximum might help you to check for outliers or abnormal values. And this can already be part of mastering the data, right? So, the second step in the impact model. But one could also answer basically already some basic business questions as well by just looking at these statistics and comparing differences across, looked in a descriptive way.

<u>Data reduction involves the following steps:</u>
→ The second step in the impact model.

But one could also answer basically already some basic business questions as well by just looking at these statistics and comparing differences across, looked in a descriptive way. Next to the summary statistics, data reduction is also a very important tool that one can use. It's a way to simplify a lot of information and focus on the most important or unusual items. It filters through a big set of data to create a smaller set that has the most important information. So, this approach is usually used for data distorting structure way, like in a database or spreadsheet.

And data reduction involves the following steps:

- So first of all, you need to identify the attribute that you would like to reduce or that you want to focus on.
    - For instance here, in this example, this might be a case where an auditor decides that he wants to focus on whole numbers. Because most transactions are actually not a whole number. Normally we have a lot of decimals. But a fraudster, somebody is committing fraud and trying to embezzle money, might implement a couple of transactions in there to steal money from the organization. But we also know that this fraudster is much more likely to

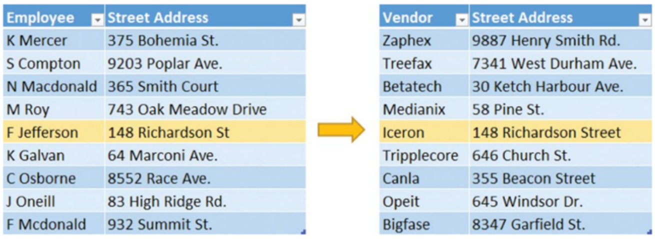
    basically embezzle a whole number instead of like a number with some decimals there. So this might stand out and we want to have a closer look. And to do so, therefore we decide, we identify the attribute, we want to focus on the amount with the whole number.

- Next, we then need to filter the result. This could be as simple as using a filter in Excel. But it may also involve a more complicated calculation.
    - For example, an auditor might want to use a fuzzy matching technique, which uses basically the probability to find how similar certain cases are. *We'll focus on this fuzzy matching in a later section as well.*
- But once we filter the results, we want to interpret the results.
    - So, you want to see, for example, if you have eliminated all irrelevant data, and you want to take a look, take a moment to see if the results actually made sense. For example, you can again calculate some similar statistics and if you eliminated any obvious entry. Or other some amounts that come back very often, etc. So you can learn a lot already by looking at some statistics after that you did that data reduction.
- But of course, once you interpret the results, you need to also follow up on the results. At this point, you will continue to build them all or use the results as a target sample for follow-up. So the auditor should then, for example, give you the company policy, and for example, check if certain transactions are indeed correct in this example. It might be the case that certain transactions are indeed whole numbers, and this makes a lot of sense. So, these are again some things to do.

<u>Fuzzy matching locates approximate matches</u>

As an alternative example, as mentioned above, like filtering one could also use just more complicated measures, which could be, for example: fuzzy matching.

Fuzzy matching: So, one might want to compare in this example here the addresses of a vendor and employees to ensure that the employees are not transferring funds to themselves. Can, for example, be the case that an employee creates a fake account, a fake vendor in the system, and the employee within the company is then actually just booking personal expenses on this vendor account. In other words, it's just actually putting fake expenses in the system on a fake vendor account. And here we could, for example, use fuzzy matching to see if the names, but especially then the addresses come back in the two databases. Because often a fraudster will not use the same name, right? But he might use his own address still because in the end, the goods or the money still need to come to his place as well. It's better to check these addresses. But of course, a fraudster might also be smart enough to not put the same address name into the system but create a small variation. In the example: Street is mentioned as SD. In the end, it's basically the same name. But for data, this is still a bit of a difference. You would not immediately find a match here. So, one could use fuzzy matching to see how similar all of these matches are. A simple exact match would just not match these two items because there is a difference in these characters between both cells. But with fuzzy matching, we looked at similarities between these cells. And then we can basically set a certain threshold, how similar should that be? We could say 99% similar, 70%. So, there is a bit of lean way that you can play around with that. So we will also look at this in one of the labs that we will do where you will implement basically fuzzy matching yourself. But this is just a way to basically reduce the sample. You want to focus on not all the vendors, but you only want to focus on the vendors which also an employee of the company. And there you then maybe want to see how there's some weird transactions going on as well. So, this is just another example of data reduction.



Employee	Street Address
K Mercer	375 Bohemia St.
S Compton	9203 Poplar Ave.
N Macdonald	365 Smith Court
M Roy	743 Oak Meadow Drive
F Jefferson	148 Richardson St
K Galvan	64 Marconi Ave.
C Osborne	8552 Race Ave.
J Oneill	83 High Ridge Rd.
F Mcdonald	932 Summit St.

Vendor	Street Address
Zaphex	9887 Henry Smith Rd.
Treefax	7341 West Durham Ave.
Betatech	30 Ketch Harbour Ave.
Medianix	58 Pine St.
Iceron	148 Richardson Street
Tripplecore	646 Church St.
Canla	355 Beacon Street
Opeit	645 Windsor Dr.
Bigfase	8347 Garfield St.

A Fuzzy Matching Shows a Likely Match of an Employees and Vendor

<u>How does the diagnostic approach to Data Analytics work, including profiling and clustering?</u>

Diagnostic analytics provide insights into why things happen or how individual data values relate to the general population. So after that you summarize the data using the skip-diff methods, you can investigate further to find out which numbers are causing the certain results. And benchmarks provide you context by giving you a point of comparison, like a reference line for the data. For instance, the average of a data set can give you a reference point for a particular value. And these benchmarks can be based on past performance or compared to competitors or the industry.

So diagnostic analytics has two common methods, which are called profiling and cluster analyzers. And these methods help you to compare a specific value to the rest of the group. And if a value is very different from the others, it can be important to investigate further. And this can help you to identify the risk or opportunities to learn more about your business process.

Hypothesis testing is another way to analyze the data and see if there are important differences between groups. So, by running a hypothesis test, you can compare the scatter statistics of two groups of variables, like for example the average or the data distribution, and see if the differences is more than what you expected by chance. And this helps us determine if there is a significant difference between the groups or the variables.

And these diagnostic analytics can be especially important, for example for internal and external auditors. It helps them to look for errors, outliers, and especially fraud, for example financial statements. So, some accounting researchers also suggest that companies that are investing in diagnostic analytics software are associated with the following benefits. So that's basically reduced external auditing phase, reduced audit delays, and lower material weaknesses.

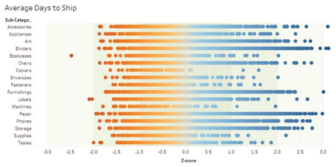
<u>Profiling compares an individual to the population</u>

So profiling is a way to understand the typical behavior of an individual group or the population. By using common summary statistics, analysts can describe the individual to group or the population, like for example finding the average, the spread and the total of those groups or individuals or groups.

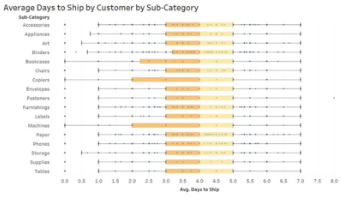
So profiling is basically usually done with data that is already ready available, and it's basically ready for the analyzers. And it helps us basically to find better unseen behavior. We can do this by using Z-score.

⇨ So, a Z-score is actually quite simple: for each value you deduct the average, and then you divide it by the standard deviation. And by doing that, so by setting the mean to zero, each data point value now represents a number of deviations from the mean. And this greatly helps us to identify actually extreme cases.

<u>Z-scores and box plots show spread and outliers</u>



Example of Profiling That Helps Identify Outliers



Box Plots Provide an Example of Profiling That Helps Identify Outliers

On the graph on the left, we can see there are certain products with a higher Z-score, meaning does they're farther away from the average. Because with the Z-scores for each individual, again we deduct the average, and we divide it by the standard deviation. So, we basically can see the higher the Z-score is, the further away from the average.

⇨ And then in this specific example, we see basically that certain products are more likely to have delayed shipments. So a Z-score of three means that the data point is three standard deviations away from the mean. And we can just use profiling to investigate the characteristics of products that might be causing shipping delays.

Another way how to do that is creating a box plot, and then we can get actually very similar insight. So instead of just looking at the mean and standard deviation, a box plot shows the median and the portals, like shown here on the graph on the right. And box plots are basically used to show how data are spread out in terms of their interquartile range, which is a way to understand the shape of the data set that focus on the middle values. And to find interquartile range, we divide basically the data set into four parts, so the quartiles, and the middle two quartiles that surround the median are the interquartile range. And everything that is outside there could be seen as more of an extreme value.

Profiling relies on gathering summary statistics and identifying outliers

Data profiling can thus be as easy as creating simple summary statistics for example, like finding the average time it takes to ship a product, or how much we usually pay for a product, or how long the purée usually works. This is basically just creating some simple statistics averages across quotes.

But it can also be much more complex, like building models to really predict fraud. For instance, we could make a profile for each employee that includes a salary, that hours, how they spend company money, etc. And even an employee that suddenly acts differently from their usual behavior, it could be risky and needs to be checked by the auditors.

Data profiling typically involves the following steps.

- First, you need to identify the objects or activity that you want to profile.
    - So what data do you want to evaluate? For example, sales transactions, customer data, credit limits, etc. So you need to identify basically the objects over the activity that you want to profile.
- Next, you need to determine the types of profiling that you want to perform.
    - So here, some questions would be, what is your goal? Do you want to set a benchmark for minimum activity?
- Next, you need to set some boundaries or thresholds for the activity.
    - So this is basically a benchmark that may be manually set, right? Such as a budget value, but it can also be automatically set, such as statistics. So like for example, passing a quarter or a specific person there, and that we would see this as an outline.
- Next, we could look at, we need to interpret the results and monitor the activity. And generate a list of exceptions.
    - So here is actually where the dashboard comes into play. So management can use digital dashboards to quickly see multiple sets of profile data and make decisions that would affect behavior. So as you evaluate the results, try to understand what the deviation from defined bound ABA represents. Is this, for example, a risk? Is it fraud? Or is this just something to keep an eye on?
- Lastly, we need to follow up on the exceptions.
    - So once a deviation has been identified, management should have a plan to take a course of action. So for example, to validate, correct or identify the cause of this abnormal behavior. So these are basically the steps that we need to take once you're using profile.

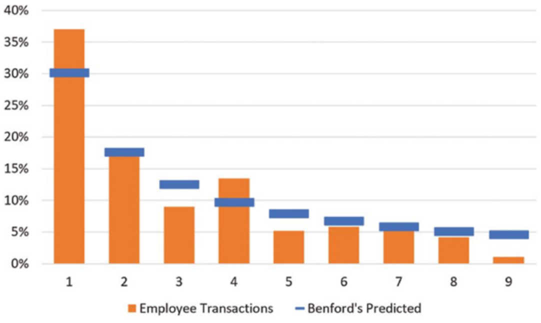
Benford's Law is diagnostic analytics that compares actual to expected values
→ use more advanced techniques like the Bamford's Law.

Bamford's Law is used to see if a certain set of transactions deviate from the know. And Bamford's Law is basically an observation about the frequency of leading digits in many real-life sets of numerical data. And Bamford's Law states that in many natural occurring collections of numbers, numbers to leading digits is likely to be small.

> So, if the distribution of transactions for an account like the Sales Revenue account is substantially different than Bamford's Law would predict, then we would investigate the Sales Revenue account further and see if we can explain why there are differences from Bamford's Law.

Bamford's Law basically states that of you look at all numbers and you take a first digit, it's much more likely that this number will start with a one compared to a nine. In fact, the chance is basically that any number would start with a one is 35%. Of course, this is not the case with all numbers. For example, if you think about human invented numbers, such as primary keys or foreign keys that we invented and basically attached to a data set for example, these will of course not follow Bamford's Law. But if you look at other types of numbers, for example, take all the numbers that you would observe within a financial statement/ within an annual report. And you would always take the first digit and then plot these on the graph. So what is the proportion of all these numbers? And then you will find back basically this distribution. And you can do that with many things. For example: all the transactions in sales accounts, etc. This is something that you will find back. And then you will basically see that a one will occur more often than the two, the two more often than three, etc.

And here I displayed here also an example of Bamford's Law using the first digit of employee transactions. So, we take basically all the transactions within that account of all the employee transactions that occur. And we only take the first number of that transaction to the first indicator here. And here in this specific example, we basically see an abnormal frequency of transactions beginning with the number four. And this may indicate that employees are attempting to circumventing internal controls such as an approval limit or something like that. Because normally we would see basically a distribution would look perfectly aligned with Bamford's Law as well.



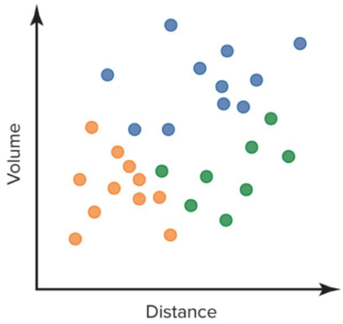
Benford's Law Applied to Large Numerical Data Sets (including Employee Transactions)

What you, for example, could do is you could analyze that for each single vendor. For each single vendor, you take, for example, all the sales and then you always take the first number and then for each single vendor, you basically create this graph. And then some vendors might follow this and there might be one or two that does not follow it, and this might be an indication. Is there something wrong? Is there something happening with that specific vendor? Is there some fraud going on, etc. Of course, there's an indication, right, so this is a red flag. This does not mean that fraud did occur, but it could be the case, right. It's just a profiling technique that the chances are higher that there is something wrong in this set of data. And then you can put more attention to that specific case. And this is actually a very interesting case, which is also used by all of us as well to see if somebody basically messed with the data. And the reason why basically we would see this deviation is because fraudsters are basically implementing certain numbers, right, creating fake transactions. They often do not follow this transaction. So human generated numbers do not follow this distribution, but a natural set of numbers does follow this prediction. And then we can basically use this as well to do some profiling as well.

Cluster analysis shows natural groupings of data

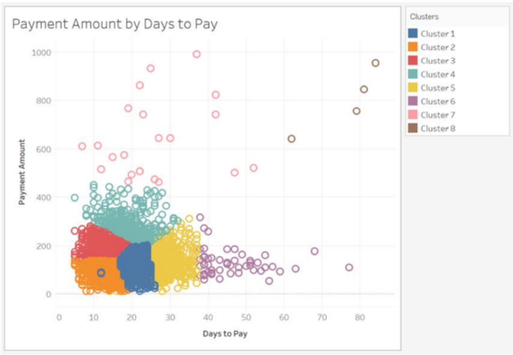
Next to profiling, clustering is another diagnostic tool that you can use. It's a way to group similar data together. It helps to identify patterns in data, but by looking at how close or far apart different data points are from each other. By grouping similar data together, analysts can better understand the characteristics of the data and draw meaningful insights. Clustering analyzers calculate the distance between each data point and the center of each group or cluster to determine which data point belongs together.

⇨ And the result is a set of clusters where data points within each cluster are more like each other than to data points in other clusters



What are some examples of clustering?

Example of clustering in a UCNR thing set. So clustering data can also be used to help arbiters to detect suspicious activities. For instance, when all the payments made to insurance, beneficiary or suppliers, transactions with similar characteristics can actually be grouped into clusters.
And the cluster that have only a few transactions of a small population are then investigated as they represent unusual groups of outliers. And these flagged clusters can contain transactions with unusually large payment amounts or along the laying processing payments. And by identifying these abnormal clusters, arbiters can have focused their attention on potential fraudulent activities. And the dimensions used in clustering may be simple correlations between variables, such as payment amounts and the time to pay, or more complex combinations of variables such as a ratio or weighted equations. And as they explore the data, arbiters develop attributes that they think will be relevant to intuition or data exploration.



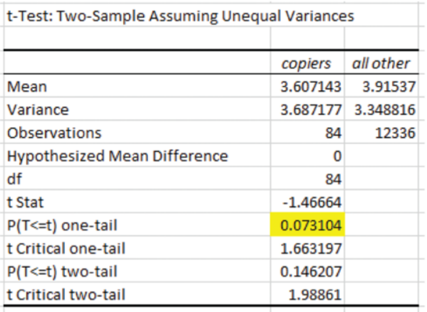
And here I display basically an illustration of clustering of insurance payments based on the following attributes. So, we have the :
-Payment amount, that's basically the value of the transaction paid
-Days to pay, that's the number of days from the original recorded transaction to the payment date.

And the data are normalized to reduce the distortion of the data and other outliers are basically already removed. And here they are all out with the number of days to pay on the y-axis and the payment amount on the x-axis. And of the eight clusters identified, three clusters highlight potential anomalies that may require further investigation as part of an internal or external audit. In cluster six is basically the purple one, they have a long duration between the processing to payment date. Cluster seven have high payment amounts and then we have cluster eight, they have high payment amounts and a long duration between the processing date and the payment date. And with this insight, arbiters may assess the risk associated with these specific payments and try to understand transaction behavior relative to acceptable behavior defined by internal controls.

Hypothesis testing is used to identify hoc different groups are

So in profiling by using any of these methods, right, so it might also be important to test if these differences that we observe are significantly different. And hypothesis testing is basically an ideal way to do that. One way of uncovering causal relationship is to form a hypothesis of what you would expect to will or will not occur. And a common test to identify differences in means is significant is to do **a two-sample t-test for equal means**. And two sample t-test for equal means is used to determine if the difference between the means of two different populations is significant or not.

And here is an example to illustrate an opportunity to run basically two sample t-test:
Imagine that we did some first test, so some of the statistics and some profiling tests to see if certain categories stand out. In this case, we have basically two groups that seems to have a quicker average shipping time. And after digging into the averages, we can basically find out that one of these subcategories mentioned here, the copiers, have the lowest average shipping time.
And we can drill down into this observation to discover if these copiers take significantly less time to ship on average than all the other categories.



t-Test: Two-Sample Assuming Unequal Variances

	copiers	*all other*
Mean	3.607143	3.91537
Variance	3.687177	3.348816
Observations	84	12336
Hypothesized Mean Difference	0	
df	84	
t Stat	-1.46664	
P(T<=t) one-tail	0.073104	
t Critical one-tail	1.663197	
P(T<=t) two-tail	0.146207	
t Critical two-tail	1.98861	

T-Test Assessing for Significant Differences in Average Shipping Times across Categories

So, we take the copiers out and we compare them with all the other categories. And then we want to see do they really have significant less shipping time.
→ And if that's the case, and the difference is not just simply due to chance, then perhaps there are efficiencies that can be gained in the other subcategories.

So, to run the hypothesis test, we first need to frame our hypotheses. And usually hypotheses are paired in two, right?

- **The null hypothesis** is the base case often called as the null hypothesis. And it assumes that the hypothesized relationship does not exist. So basically there is no significant difference between the two samples of populations. In this case, the null hypothesis would basically states as follows. So we have basically the average shipping time for the copiers category is not significantly different than the average shipping time of all the other categories.
- **The alternative hypothesis** would be the case that the analyst believes that this relationship is true. And basically the alternative hypothesis is the opposite of the null hypothesis. And basically this would state that the copiers category is significantly different from the average shipping time of all the other categories.

For the null hypothesis to hold, we would recognize that even though there is a difference in the average shipping time, the difference is not significant. In this case, there is no evidence that the difference in the average shipping time are not simply due to chance. So here basically the 3.60 would not be significantly different from the 3.91 in case the null hypothesis is true. So, we do not find a significant difference.

To do that, we basically describe our findings by interpreting, for stating if something is significant or not, we try to interpret the p-value of this statistical test. And the p-value is basically compared to the alpha threshold. And we have some common alpha thresholds that we use. That's basically the 1% level, the 5% or the 10% level. And the result is just statistically significant when the p-value is less than the alpha, which signifies a difference between the two means for detectors. So that basically means the default hypothesis can just be rejected.

So in our specific case, imagine that which state are alpha is 5%. We want to see if something is significant at a 5% level. We would have to fail to reject the null hypothesis in this case because the p-value is 0.073104. And this is greater than the alpha. Hence, we would not claim that these are significantly different from each other. But what if we have set our alpha at a 10% level instead of the 5%? Suddenly, our p-value of 0.073104 is less than the alpha, so 0.10. And we would have accepted that these are significantly different.

So, this points out as well so that it's critically deep to think in advance and make first a decision on what you believe is a significant level prior to running your statistical test. You basically need to state first what is the 1% level, the 5% level, the 10% level. You need to decide on your alpha. And this might depend on various things. So including the sample size as well as how large the cost would be in case you would need a run fully except to reject the hypothesis. It’s mainly important here that the p-value shouldn't dictate which alpha you select as anything that might be. But overall, this is just a powerful test to see if statistical differences exist between your groups And it can help you to guide you to examine certain groups in more detail.

When do you use predictive analytics, including regression and classification?

So next to these descriptive and diagnostic tools we can also make use of predictive analytics. And here we will discuss basically mainly regressions as a tool that you can use.

On this setting we often talk about a target or otherwise called a dependent variable. And the target of the dependent variable is an expected attribute or value that we want to evaluate.

For example, if you're trying to predict whether a transaction is fraudulent, the dependent variable might be then a specific fraud score, for example. Or if you're trying to predict an interest rate, the target would basically be the interest rate.

So you might use a regression to predict a specific value to answer a question such as “how many days do we predict it will take a new vendor to chip an order?” Or “what is the impact of my prior debt on the interest rate that I will receive?” Again, the prediction is based on the activity that we have observed from past observation. So old data.

And here in this example shown, it's based on data from vendors in the past.

As we use historical data to create a model, and we do have a dependent variable that we try to explain with several independent variables that might explain this relationship. And the goal of regression is to help you to predict an expected outcome based on past data.

So to do so, you need to think about a couple of things.

- First, you need to identify the variables that might predict an outcome or target or dependent variable. And the inputs or explanatory variables or the independent variables are basically the ones that you try to use to explain that outcome variable.
- Next to that, you also need to determine the form of the relationship. This is a linear relationship where each input plots to another in a linear way. Or is the relationship nonlinear? For most accounting question we basically utilize a linear relationship, but it's also possible to consider nonlinear relationships as well.
- Next, you also need to identify the parameters of the model. What are the relative weights of each independent variable on the dependent variable? And these are basically the coefficients that you will find. Each of these independent variables is basically what the regression will tell you, (so what the coefficients are)

- And then we have some statistical t-test that assess each regression coefficient at the time to basically determine if the weight is statistically significantly different from zero, which basically would mean that if it is significant for zero, it has an impact. If not, it basically has no weight at all. And particularly multiple regression, it can be useful to assess the p-value for each variable. You interpret the p-value for each variable the same way that you assess the p-value in a t-test as we did before in the prior example.
    - So if the p-value is less than your alpha, typically 0.05, so the 5% level, then you again inject the null hypothesis. And the regression this implies that the explanatory variable is statistically significant and helps you to explain basically your outcome variable.

<u>What are some examples of regression?</u>

Predictive and Heditisk in this facility is making full costs of the counting outcomes. It can basically help management with counters to predict future performance, for example, future sales, earnings and cash flows. And this then helps them to set basically budgets and plan production. It can also help auditor, for example, to predict financial statements that need to be stated, will help investors and financial analysts to predict future sales, earnings, cash flows, etc. And in each of these cases, you can just think about a specific model that you can destroy, a cash model. And to be a bit more specific, I have two examples here.

- An accounting firm that experience a great amount of employee turnover each year, between 50 and 25% each year. And especially in this company, it's just very important to be able to predict employee turnover. Each year they must predict how many new employees might be needed to accommodate growth, but also the replace the employees who have left.

    → So an accounting firm might basically predict employee turnover by predicting and running the following regression in this specific way. Right, so we would have employee turnover as a dependent variable, and then we can plug in there several independent variables that might basically explain this relationship. For example, current professional salaries, health of the economy, salaries offered by other accounting firms, etc. So using such a model, accounting firms could then begin actually to collect all the necessary data to test their model. And this helps them basically to protect basically the employee turnover that will occur in the next year.
- We could also think about an example with auditors: one of the key tasks for an auditor of a bank is to consider the number of allowances for loan losses. And this is important because these allowances are often subject to some manipulation to help basically manage the earnings in the company. And the financial accounting standards both, right, FACP requires basically that banks provide an estimate of expected credit losses by, for example, considering historical collection rates, current information, reasonable and supported forecasts, including estimates of pay payments. And using these historical and industry data, auditors may want to work to test the model to establish a loan loss reserve in this way. So they would, for example, have allowances for loan losses on the left hand side, right, so the dependent variable. And then a couple of explanatory variables such as current age, loans, loan type, customer loan history, etc. And this will then help them to basically establish what he allows for loan losses amount should actually be.

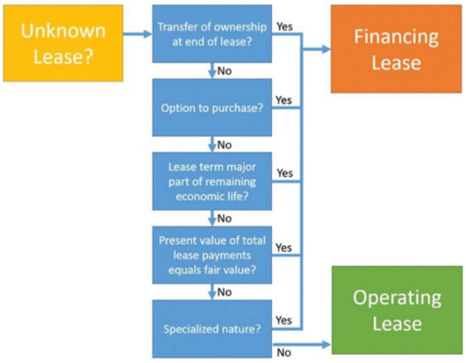
<u>What are prescriptive analytics, including machine learning and artificial intelligence?</u>

Prescriptive analytics answer this question, what do we do next?

We have collected the data, analyzed, and profiled the data, and in some cases developed predictive models to estimate the proper target value. Once those analyzes have been performed, the decision process can be aided by rule-based decision support systems, machine learning models, or added to an existing artificial intelligence model to improve future predictions. These analytics are the most complex and expensive because they rely on multiple variables and inputs, structure, and non-structure data, and in some cases the ability to understand and interpret natural language commands into data-driven queries.

Decision support systems use rules to guide the accountant.

So as an example: decision support systems, they are information systems that support decision-making activities within a business by combining data and expertise to solve problems and perform calculations.
They are designed to basically be interactive and adapted information collected by the user. In the accounting domain, they are typically built around a series of rules or something with an if-then relationship that basically guide the user through the process and then basically do the end results.


Unknown Lease?
Transfer of ownership at end of lease?
Yes
No
Option to purchase?
Yes
No
Lease term major part of remaining economic life?
Yes
No
Present value of total lease payments equals fair value?
Yes
No
Specialized nature?
Yes
No
Financing Lease
Operating Lease

The decision support systems can basically help applications based on accounting rules as well. For example, here, when a company classifies a lease as a financing or operating lease, it must consider whether the lease meets a number of criteria. And using a decision support system, a controller could evaluate a new lease and answer five basic questions to determine the proper classification as also displayed here on this graph.

Machine learning learns from past data to predict better outcomes.

And what all these models actually have in common is that the use of algorithms and statistical models are used to generate a previously unknown model that relies on patterns and inferences. And both unsupervised explanatory analyzers and supervised models provide insights and predictive foresight into the business and decisions made by the accountants and the auditors. They can also model judgment and decision making to recommend clouds or action based on new or unknown data. So artificial intelligence models work similarly in that they learn from the inputs and corrections to improve decision making.

> For example, image classification allows auditors to take a photograph of inventory or fixed assets, and this then automatically identifies the object within the photo, rather than having an auditor has to manually check each object.

And for most applications of artificial intelligence models, the computer power is such that most companies will outsource these underlying systems to companies like Microsoft, Amazon or Google rather than to develop itself. So these companies have actually large data sets to create more accurate predictions. And they also provide basically the algorithms and the code to do all this.

Chapter 3 Summary

In this chapter we address basically the third and fourth step of the impact cycle model. So that is basically how are we going to test or analyze the data to address a problem we're facing.

We identified descriptive analytics that help describe what happens with the data, including some statistics, data reduction and filtering.

We provide an example of diagnostic analytics that helps user identifies relationship in the data that uncover why certain events happen through for example, profiling, clustering, and similarity matching.

We also explained example of predictive analytics and introduce some data mining concepts related to recreations.

And we briefly discussed prescriptive analytics, including decision support systems and artificial intelligence. And that is basically it for this chapter.

Chapter 4: Communication Results And visualizations

In the last chapter, we talked about different ways to analyze data and when to use them. And we used examples related to accounting to explain which methods to use for each question we want to answer. We also discussed how to understand the results of each method. And in this chapter, we will discuss communicating results and visualizations. So, this chapter does wraps up basically the introduction to the impact model. We will discuss how to show the results of your data analyzes to others. It explains that making a chart is more than just putting data into a basic chart in Excel. It helps you to figure out why you want to make a chart and how to choose the best chart for your data. You'll also learn how to make your chart easy to understand. Here we will also talk a little bit how to write a report for different audiences who are interested in your data analyzing results.

Data are important and data analytics is effective, but they're only as important and effective as we can communicate and make the data understandable.

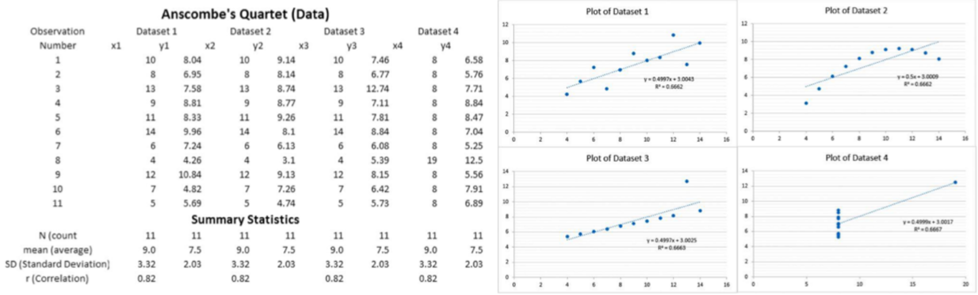
So as a simple example, what would you do if you just started your job and your boss asked you to supply information regarding in which countries all of the customers of your organization are located? Would you then simply point your boss to the customer's table in the sales database? Would you go further and isolate the attributes to the company name and the state? Perhaps you could go even further and run a quick query or pivot table to perform a count on the number of customers in each different state that the company serves. → Probably the best way is to give your boss a short-written summary of the answer to the research question as well as an organized chart to visualize the results.

- ⇨ So, data visualization isn't just only for people who are visual learners. When the results of data analyzers are visualized, the results are made easier and quicker to interpret for everybody. Whether the data you're analyzing are small data or big data, they still merit synthesis and visualization to help your stakeholders interpret the results with ease and efficiency.

<u>What is the difference between statistics and visualizations?</u>

So as discussed in the first lecture, as part of the impact model, the results of the analyzers need to be communicated to others. As with selecting and refining your analytical model, communicating results is more art than science. Once you're familiar with the tools that are available, your goal should always be to share critical information with stakeholders in a clear, concise manner. This communication could involve the use of a written report, a chart of a graph, or just displaying a few key statistics. Depending on the needs of the decision maker, different means of communication may be considered.

And to stress the point of how visualization might help, here is an example of a statistician named Francis Anscombe. And he illustrates the importance of visualization using four datasets that had nearly identical descriptive summary statistics. Yet they appear to be very different when a distribution was graphed and visualized. It came to be known as Anscombe's-quartet, and it emphasized the importance of visualizations together with underlying statistical properties.



Anscombe's Quartet (Data)

Observation	Dataset 1		Dataset 2		Dataset 3		Dataset 4	
Number	x1	y1	x2	y2	x3	y3	x4	y4
1	10	8.04	10	9.14	10	7.46	8	6.58
2	8	6.95	8	8.14	8	6.77	8	5.76
3	13	7.58	13	8.74	13	12.74	8	7.71
4	9	8.81	9	8.77	9	7.11	8	8.84
5	11	8.33	11	9.26	11	7.81	8	8.47
6	14	9.96	14	8.1	14	8.84	8	7.04
7	6	7.24	6	6.13	6	6.08	8	5.25
8	4	4.26	4	3.1	4	5.39	19	12.5
9	12	10.84	12	9.13	12	8.15	8	5.56
10	7	4.82	7	7.26	7	6.42	8	7.91
11	5	5.69	5	4.74	5	5.73	8	6.89
Summary Statistics								
N (count	11	11	11	11	11	11	11	11
mean (average)	9.0	7.5	9.0	7.5	9.0	7.5	9.0	7.5
SD (Standard Deviation)	3.32	2.03	3.32	2.03	3.32	2.03	3.32	2.03
r (Correlation)	0.82		0.82		0.82		0.82	

So this slide shows both detailed observations in the four datasets and their summary statistics, and you'll know that they are nearly identical, these summary statistics, for each of these four datasets. And it's only when the data points are visualized that you see that the datasets are quite different. Even the regression results are not able to differentiate between the various datasets, as shown by the straight lines here on the graph. While this is not always the case, the example of Anscombe's-quartet would be a case where visualization would more easily and readily communicate the results of the analyzers compared to these statistics.

Visualizations are preferred over text

Visualization is important, and increasingly visualization is also preferred to read the content to communicate results. So according to one study, 90% of people prefer visual content over reading content.

- ⇨ So why is that? So some argue basically that the brain processes images 60,000 times faster than text, and 90% of information transmitted to the brain is actually visual. As further evidence, so for example, take Facebook, photos have an interaction rate of more than 87%, compared to only 4% or less for other types of posts, such as links or texts. So, while some company executives may prefer text to visualization, recent experience suggests that visualizations are increasingly an effective way to communicate to management, and for management to communicate to from stakeholders. Overall, it can actually be a way for more creating summarizing basically complex information in a much easier way.

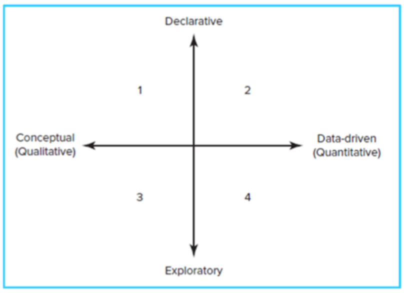
What is the purpose of your data visualization?

When you want to visualize data, you need to always first determine the purpose of your data visualization . And to help you out with that, you can basically try to answer these first two questions:

- What type of data are being visualized?
  - Is this more conceptual or data driven data? Or in other words, qualitative first quantitative data?
- Are you explaining the results, for example, of a privacy done analyzers, or are you exploring the data through visualization?
  - So, is the purpose declarative or exploratory?

And if you take that into account, basically, these two questions, this will interest you up in four different groups that you can identify any specific data. And this is also based on the senior editor of Harvard Business Review, so Scott Berglingato. And he summarizes basically these two possible, the possibilities basically on how you answer these questions in a chart where you have four different possibilities.

And the majority of the work that we will actually do will basically result for a data analyzers which will be projected in quadrant 2 here, so the declarative data-driven quadrant.



The four chart types

But we can also do a bit of work in quadrant 4, right? So, the data-driven exploratory quadrant. That's also some of the exercises that we will do. There isn't as much qualitative work to be done in our assignments, although we will work a little bit with categorical qualitative data occasionally. And when we do work with qualitative data, it will be more strictly, it will be visualized through the tools basically in quadrant 1, so the declarative conceptual quadrant.

In any case, once you know the answers to the two key questions mentioned here and have determined basically in which quadrant you're working, you can determine then the best tool for the job.

Is a written report with a simple chart sufficient? If so, worth or excel will likely suffice. With an interactive dashboard and repeatable reports, be required. If so, then likely power BI may be a better tool. So later in the chapter, we will discuss these two tools in more depth along with which each tool is better used.

Are you using qualitative and quantitative data?

An important question is, are you using qualitative versus quantitative data? `

→ So in other words, we're comparing quadrant 1 and 3 versus quadrant 2 and 4 in the graph displayed on the previous slide.

So qualitative data are categorical data. All you can do with the data is count them, group them, and in some cases, you can also hang them. Qualitative data can be further defined in two ways. We basically have nominal data and ordinal data. Nominal data are the simplest form of data. So, examples of nominal data are hair color, gender, ethnic groups, etc. If you have set of data on people with different hair colors, you can count the number of individuals who fit into the same hair color category, but you cannot rank it. So brown hair isn't better than red hair, for example. Nor can you basically take the average or do any other further calculations beyond counting. You can't take an average of blonde, for example.

So, increasing in complexity but still categorized as qualitative data are ordinal data. So ordinal data can also be counted as categorized like nominal data, but you can go a step further. So, the categories can also be ranked. And some examples of ordinal data include basically gold, silver, and bronze medals. Or for example, one to five rating skills on teacher evaluations, or for example letter grades for students. For example, if you have a set of data of students and then a letter grade, you can basically count the number of instances, for example, that the students received either A, B, C, and so on. But you can also of course categorize them just like with nominal data, but you can even go a step further. For example, you can sort them, right? So an A is, for example, better than a B. C is better than a B, etc. But that is as far as you can basically take your calculations. So if the creator remains a letter and aren't then, for example, transformed into a corresponding numerical grade for each individual, you cannot do calculations such as taking the average, the standard deviation, or any other more complex calculation. So beyond counting and possibly sorting, if you have ordinal data, the primary statistic used with quantitative data is proportions. So the proportion is calculated by counting the number of items in a particular category and then dividing that number by the total number of observations.

For example, if you have a data set of 150 people and you know, for example, for each one, their hair color, and for example, you have 25 people in your data set that have the red hair color. You could then calculate the proportion of red hair people in your data set by dividing 25, so the number of people with red hair, by 150, the total number of observations in your data set. And this will give you the proportion of red hair people. And this would be 16.7% in this specific case. So qualitative data, both nominal and ordinal, can also be referred to as conceptual data because such data are text driven and represent concepts instead of numbers.

Next to qualitative data, we of course also have quantitative data. And these are more complex than qualitative data because it's not only that you can count them and grow them just like qualitative data, but the difference between each data points are meaningful.

For example, when you subtract four from five, the difference is then a numerical measure that can be Interpreted and compared, for example, when you subtract three from five.

So quantitative data are made up of observations that are numerical and can be counted and ranked just like all the qualitative data, but they can also be average. And standard deviation can be calculated and then data sets can be easily compared when standardize if applicable, of course. So like qualitative data, quantitative data can be categorized into two different types. Here we have intervals and ratios. However, there is some dispute about this among the analytical community on whether the difference between these data sets is meaningful. And for the sake of the analytics and calculations, you will be referring to write as textbooks, the difference is not that important. But the simplest way to express the difference between an interval and ratio data is that ratio data have a meaningful zero and interval data do not. In other words, for ratio data, when a data set approaches zero, zero means the absence of.

Consider money as ratio data we can have $5 $27 $9000, etc. But as soon as we reach, for example, $0, we have the absence of money. Interval data do not have a meaningful zero. In other words, if the interval data is zero, there it would not mean the absence of but it's simply another number. An example of interval data is the Celsius degree of temperature. So, we can have 30 degrees, and this is hotter than 20 degrees, which is then again hotter than zero degrees. But zero degrees does not represent the absence of temperature. It's just another number on the scale.

And due to the meaningful zero, this difference between the interval and ratio data is basically makes the ratio data as the most sophisticated form of data. This is because the meaningful zero allow us to calculate fractions proportions and percentages. So, ratios reflecting the relationship between these values basically.
However, we can perform all other functions basically also put on interval and ratio data.

Next to ratio versus intervals, we can also further categorize quantitative data as either discrete or continuous data. Discrete data are data that are represented by whole numbers. An example of discrete data is, for example, the points in the in the basketball game. You can earn two points, three points or 175 points, etc. But you cannot earn 3.5 three and a half points. That's impossible. On the other side, for example, height, you can be 4.7 feet tall, 5 feet tall, 6.273 for 5 feet, etc. So the difference between this great and continuous data can be sometimes blurry. Because you can also express a discrete variable as a continuous, for example. But the number of children, for example, a person can have is a real discrete number. A woman and man could not have basically 2.7 children. But you could have either two or three children. However, if you're researching, for example, the average number of children that people can have between, for example, the age of 25 and 40, the average would again be a continuous variable.

⇨ So whether your data are discrete or continuous can basically help you determine the type of chart that you want to create. Because continuous data lends itself more to line charts, for example, than discrete data.

Is your visualization declarative or exploratory?

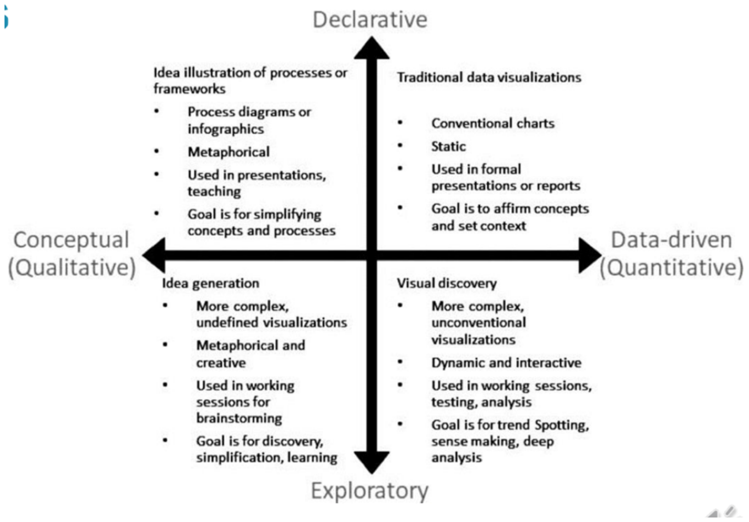
Basically, quadrant one and two versus quadrant three and four. And in the context of the labs and tools that I will provide, the majority of your data visualization created in step C of the impact model will be created with declarative purposes.

So declarative visualizations are the product of wanting to declare or present your findings to an audience. The data analyzers project begins with a question, proceed through with some analyzers, and in the end, you will basically communicate those finances. This means that while the visualization may prompt conversation and debate, the information provided in the short should be solid. Even if your analyzers, the previous step in the impact model, in your impact model was basically an explorative finding an explorative way of finding a first answer to your question. By the time that you basically arrive to the communication step of your results, you're basically declaring what you have thought. On the other hand, you will sometimes use data visualization to satisfy an exploratory visualization purpose. When this is done, the lines between step, the steps P so perform the test plan A address and refine the result and C communicate results: so, these three steps of the impact model are not really that clearly divided in this specific step if you're doing exploratory visualization.

So exploratory data visualization will help align you with performing the test plan within visualization software, for example, power BI, and you will gain some insights while you're interacting with the data. Often the presenting of explanatory data will be done in an interactive setting. And the answer to the question of step I, wont already has been answered before working with the data individualization software.

Chart Type Details

So, the chart here present on this slide is actually very similar to the first chart I presented earlier. So, but this one has a bit more detail to help you determine what to do once you've answered the first two questions.



Idea illustration of processes or frameworks

- Process diagrams or infographics
- Metaphorical
- Used in presentations, teaching
- Goal is for simplifying concepts and processes

Traditional data visualizations

- Conventional charts
- Static
- Used in formal presentations or reports
- Goal is to affirm concepts and set context

Idea generation

- More complex, undefined visualizations
- Metaphorical and creative
- Used in working sessions for brainstorming
- Goal is for discovery, simplification, learning

Visual discovery

- More complex, unconventional visualizations
- Dynamic and interactive
- Used in working sessions, testing, analysis
- Goal is for trend Spotting, sense making, deep analysis

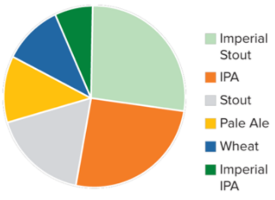
Remember that the quadrant represent two main questions right so what type of information is being visualized right so qualitative versus quantitative data. Or, and the second question is, are you explaining the results of the previous analysis, or are you just exploring the data through visualization. this is then basically declarative or exploratory. And one you have determined the answer to the first two questions you can be ready basically to begin determining which type of visualization will be the most appropriate for your purpose and your data set.

<u>Chart appropriate for qualitative data</u>

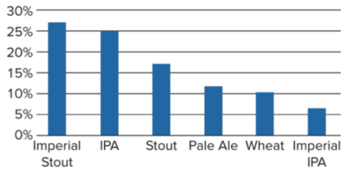
Once you have determined the type of data that you're working with and the purpose of your data visualization, the next questions must be basically about the design of the visualization. So, what color font graphics will you use, and most importantly, which type of chart graph will you use. And the visuals should basically speak for itself right so without needing too much explanation for what's being represented.

And because qualitative and quantitative data have such different levels of complexity and sophistication, there are some charts that are more appropriate for qualitative data, and that do not work too well for quantitative data. When it comes to visual representing qualitative data, the charts more friends were frequently used are basically pie charts, simple bar chart or stack bar charts, and sometimes some more fancy things such as word clouds.

- The pie chart is probably the most famous data visualization for qualitative data. It shows the part of the parts of the whole thing. In other words, it basically represents the proportion of each category as it corresponds to the whole data set.
- Similarly, a bar chart bar chart also shows the proportions of each category as compared to each of the others. So in most cases, basically bar chart is more easily interpreted and a pie chart, because our eyes are more skilled at comparing the heights of the columns or the lengths of the horizontal bars depending on the orientation of your chart then, for example, comparing the sizes of the pie, especially if the proportions are relatively similar.



Pie Chart Showing Proportion

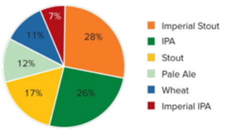


Example Bar Chart

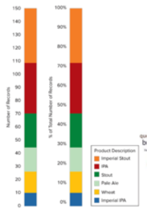
Consider the two different bar charts from the slain database. So, the second graph displayed here is a little bit easier. It compares basically the proportions of each beer type sold by the brewery. And the magnitude of the difference between the empirical start and the IPA is almost impossible to see in the pie chart. You don't really see a difference there. And it's much easier to digest basically in the bar chart presented on the right.

Of course, we could also improve the pie chart by adding the percentages associated with each portion. But it's much quicker for us to see the difference in proportion by glancing at the order and the length of the bars in the bar chart.

And the same set of data could also represent it in a stack bar chart or 100% stack bar chart like displayed here in the second graph here. In the first graph displayed here is basically we now added the percentages in the pie chart.
Compare the previous slide with this one here you will see the percentages, which already makes it a little bit clear. But now again, focusing on the second graph displayed here. This is a stack bar chart. And this basically shows the proportions of each



Pie Chart Showing Proportion



Example of Stacked Bar Chart

data
analysis
table
database
Sales
Excel

Word Cloud Example

type of beer sold, expressed in the numbers of beer sold for each product. It basically shows the proportion expressed in terms of a percentage of the whole in 100% stacked bar chart. What bar charts and pie charts are among the most common charts used for qualitative data.

There are also a couple of other different graphs and charts that you could use. And each of those has a bit of their own purpose. And I displayed one example here as well. So that's a word cloud. If you're working, for example, with text data instead of categorical data, you can represent them in a word cloud. And word clouds are formed by counting the frequency of each word mentioned in a data set and the higher the frequency. So again, the proportion of a given word, the larger and bolder the font will be of that word in your word cloud. Consider analyzing the results of an open-ended response question on a survey. A word cloud would be a great way to quickly spot the most used word to tell basically if there is a positive or a negative feeling towards what has been surveyed. There are also some settings that you can put into place when creating the word cloud to leave out the most used English words. For example, you can remove the and e, etc., like this typical stop words as well. So you can over move them so that it doesn't get too skewed as well. And the graph displayed here on the right is an example of such a word cloud based on the text that we have used in chapter two.

Which charts are appropriate for different data ?

A quick summary of what you can use for qualitative data. I already mentioned here as well on the slide what you could use for quantitative data.

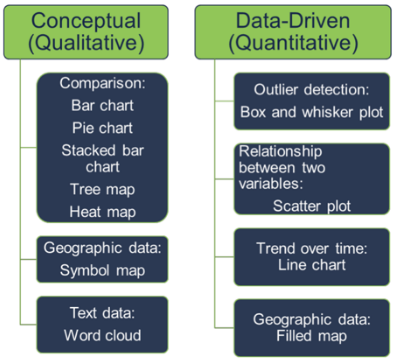
The data visualizations and short possibilities for qualitative data, right, so bar chart, pie charts, etc. Those can also be used for quantitative data. So you can use pie charts as well bar charts, etc., for quantitative data, but you can just do a lot more with quantitative data. And there are many different methods for visualizing quantitative data. But except for the word cloud, all the methods mentioned in the previous section for qualitative data can basically work for quantitative data as well.

But we have a couple of additional things that we can do there as well. For example, we can use line charts, so they show similar information to what a bar chart would show. But line charts are good for showing data changes or trends over time. So line charts are useful for continuous data while bar charts are often used for discrete data. For that reason, line charts are not really recommended for qualitative data, which by nature being categorical can never really be continuous as well.

So next to that, we basically also have box and whisker plots. And these are basically useful for when quotas, mediums and outliers are required for analyzing and for getting certain insights into the data. And scatter plots can also be useful for identifying, for example, the correlation between two variables or for identifying a trend line or the best fit, etc.

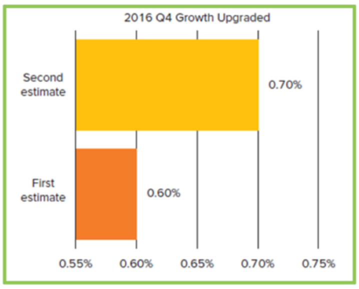
Types of charts ?

Communicating results is more art and science. So once you're familiar with the tools that are available, your goal should always be to share critically information with stakeholders in a clear and concise manner.
 And while visualization can be incredibly impactful, right, they can also become a distraction if you're not careful. So, for example, bar charts can be manipulated to show bias and while novel 3D graphics are incredible, this can be incredibly subjective because they may distort basically the scale and even the numbers.


Conceptual (Qualitative)
Comparison: Bar chart Pie chart Stacked bar chart Tree map Heat map
Geographic data: Symbol map
Text data: Word cloud
Data-Driven (Quantitative)
Outlier detection: Box and whisker plot
Relationship between two variables: Scatter plot
Trend over time: Line chart
Geographic data: Filled map

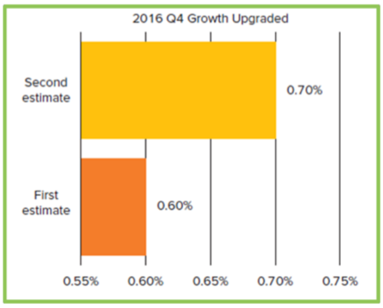
Bad example: How does this chart illustrate bias?

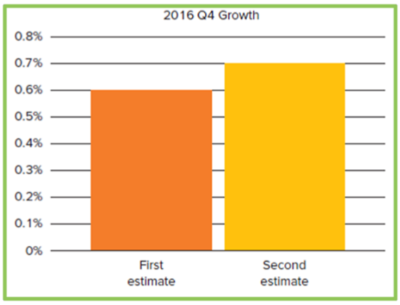
You should sometimes be careful with using some of these charts as well. To explain this a little bit in a more detail and also to explain you how to create a good visualization, it can sometimes basically help you to look at problematic cases.



In this chart displayed here, so about the Daily Mail, so you keep this newspaper. This is actually a very good graph of problematic graph.So here they tried basically to emphasize an upgrade in the estimated growth of the British economy and the estimate from the official of national statistics indicated that Q4 would grow by 0.7% instead of the 0.6%. So a relatively small increase of 0.15%. Yet the visualization makes it appear as if this is a 200% increase because of the scaling used by the specific newspaper. Another issue is that some time has passed between those two estimates, and we don't really see that here mentioned here. So, in the way how basically this graph is created.

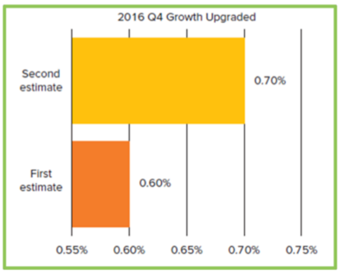
A more appropriate scale is a good start

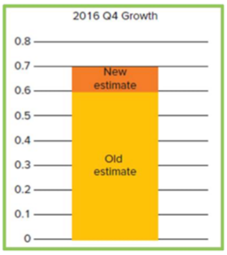




So, if we rework this a little bit to basically to correct scale. We start basically at zero instead of the 0.55 as previously used. And we make use of a change over time almost right so by basically plotting the data along the horizontal axis instead of the first circle axis. We basically see something like you would be displayed here. So this is already a better version of the graph. Now we have the time dimension, and we also don't. It doesn't seem that we have like a 200% increase as well. And this already helps right so just turn in the graph around and using proper scale.

Staking can reveal the real increase

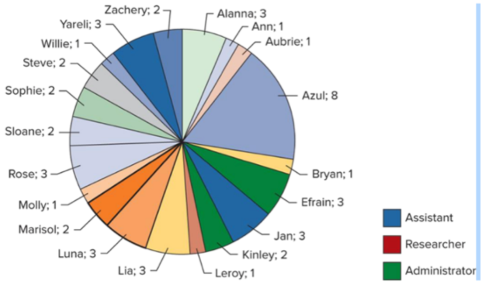




This is another way how to do this, so this is very similar and a better way how to present the graph that we first did right so but here you're basically emphasizing the growth here. In any case, but what should be basically clear is that both these two types of grass basically show an increase but it's much less dramatic and confusing as was done in the very first graph that we saw.

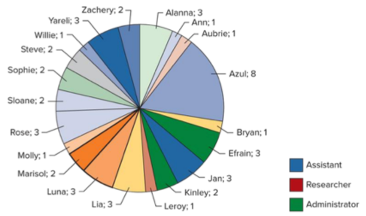
Bad example: What is this chart trying to tell the reader about whose computer is attacked more?

And this is another problematic case here out of a bad visualization. The data represented here come basically from a study assessing cybersecurity attacks. And this chart attempted to describe the number of cybersecurity attacks employees fell victim to, and as well what the role was in the organization. You should basically assess this chart and think about the question if this pie chart really the best way is to represent the data.

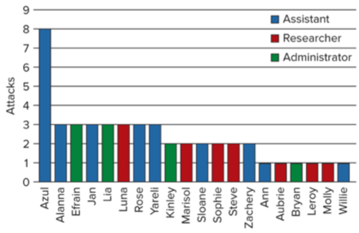


The main problem here is basically that there are simply way too many slices of the pie and that the key referencing so the job for each user is basically unclear. There are a couple of ways that we can basically improve upon this chart.

The first way how we can do this is basically by considering a hand order bar chart like this play here. And this really emphasizes the users.

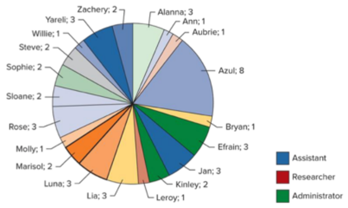


Difficult to Interpret Pie Chart

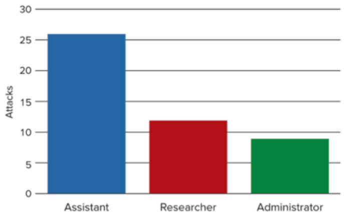


More Clear Rank-Ordered Bar Chart

Another way of doing this you could again use a range order bar chart. But here you're basically not emphasizing the users but here you're emphasizing the category. And here you can make a nice comparison as well by using this range order bar chart.

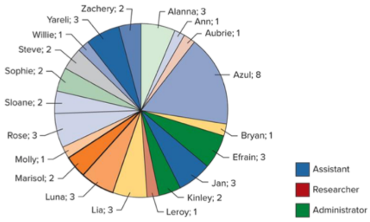


Difficult to Interpret Pie Chart

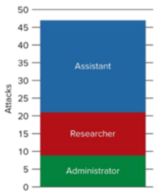


Bar Chart Emphasizing Attacks by Job Function

Alternatively, if you're for example interested in the proportions, a stack bar chart might be more useful. So again, everything depends a bit on what you want to emphasize. So, we provided here a couple of changes that you could implement and there's not a merely a right or wrong here. It really depends on what you want to emphasize. For example, the individuals, the groups, or the proportions. So, a few of these represent the presentation are slightly better over the others, but we already made a huge improvement instead of the first class displayed here compared to this pie chart.



Difficult to Interpret Pie Chart



Stacked Bar Chart Emphasizing Proportion of Attacks by Job Function

<u>How can you refine your charts ?</u>

So after identifying the purpose of your visualization and which type of visual will be most effective in communicating results, you will need to further refine your chart to pick the right data scale, the color and the format.

That being said, Excel already has a lot of power and intuition here and they automatically give you already a standard data scale and with the right increments, etc. Already a lot is automated in this sense. But of course, you might disagree with the standard that is provided and might may want to make small changes here as well.

Consider scale and increments:

I listed four questions basically that you need to think about when you're basically deciding on on the scale and the increments that you want to use.

- So first question, how much data do you need to share in the visual to avoid being misleading yet also avoid being distracting?
    - So for example, do you need to display the past four years or will the past two quarters suffice. Or when you consider leaving out some data, is this to show only the insight that are meaningful or is it an attempt to skew the data or to hide all performance. So be careful not to hide data that are meaningful just because they just don't align with your expectations. - -
- What do you do with outliers?
    - So if your data contains outliers, should they be displayed or will they distort your scale to the extent that you can leave them out. So if the purpose of your chart is to call attention to the outlier, they need to remain and you need to ensure that they are not errors. So basically, this step right that they're not errors should already have been done in step two of the impact model when you master the data. But of course, if the purpose of your chart is to display the middle back of the data, these outliers may not be relevant to the insights and then you might need to leave them out. Depending on a little bit on what you want to show, this is something that you need to decide on.
- What is the baseline?
    - Other than determining how much data that you need to share; you need to think about what scale that you should place on the data. So typical shows begin with the baseline of, for example, zero. But if zero is meaningless to your data set, you could find a different baseline that makes sense. So be careful to not exaggerate the height of the baseline so that your trend line or bar chart is over or under emphasize. So, your trend line should take up two thirds of the chart. Once you decided on a data scale, the increments for your data should also be natural. Right, so, for example, splits in ones, twos, fives of hundreds and so on. But you should take not unnatural versions like for example splits of three or splits of zero point two, something like that. Right, so better to take a natural split.
- Would context of reference lines make the scale more meaningful?
    - So for example, if you were provided with the stock price of $100. Would you immediately be able to tell if that's a high number or a low number. And that's, that's not necessarily the case. Without context of the stock price of time, the companies or the companies industry or its competitors stock prices.This is sometimes some relevant information that you need to include as well. And certain numbers are sometimes meaningless without some reference lines as well.

Think about your use of color:

Excel is quite good at picking basically already an appropriate data scale and increments. And similarly, Excel also provide you with some default color teams when you will begin to create your data visualizations. So immediately you will have some colors in there as well. But of course, you might choose to customize the team. However, if you do so, right, here are a couple of points to consider.

- So one thing is, for example, should you use multiple colors. So using multiple colors to differentiate different types of data can be very effective.
    - So for example, using a different color to highlight like a certain focal point can be very effective. However, don't use, for example, multiple colors to represent the same type of data. It's better to use the same color for that specific for a group of items together. So don't differentiate there. But in general, it does important to take care of the colors.
- It's important not to use multiple colors just to make your chart look pretty. The point of the visualization is to showcase insights from your data, not to make art or something like that.
- Try to keep in mind with some of the meanings that some colors represent. So we're quite trained to understand the difference among red, yellow and green.
    - Red meaning something negative that we would want to stop something and green being something positive that we would like to continue just like with traffic lights. For that reason, use red and green only for those purposes. Use red to show something positive or green to

    - show something negative would really be counterintuitive. And it will just make it harder to your job harder to understand.
- You also want to consider a color blind audience.
    - So if you're concerned that someone reading your visuals may be color blind, avoid the red, green scale and consider using orange and blue. So once your chart has been created, convert it to a gray scale to ensure that the contrast still exists. This is both to ensure your color-blind audience can interpret your visuals. And also, it's to ensure that the contrast in general is stark enough with the color palette you have chosen.

How can the use of words provide insight?

We also need to communicate our results in a reader report. And this can sometimes be as small as a couple of words. But you must write something to make the graph more interpretable as well. So short reader report.

And as a student, most of the writing you do is basically for your professors, right? So you likely have written emails to your professors, which you should carry a respectful tool. But you might even have the opportunity also to write a business report or report for your business professors, an essay, et cetera. All the while though, you were aware that you were writing for a professor when you did that. So when you enter the professional world, however, your writing will need to take on a different tool. If you're accustomed to writing with an academic tool, transitioning to writing to your colleagues in a business sector requires some practice. Same for example, when you're writing a master thesis, right? This is also an academic science tool, right? So, writing to your colleagues or to the CEO, CEO, CFO, et cetera, all requires a little bit of a different tool.

A good style is ultimately nothing more than writing that is easy to understand. So it should be clear, unambiguous, correct, interesting, and direct.

Remember to use plain language throughout the IMPACT model

The main point that I want to make is basically that you use plain language. For communicating your results for a data analysis project, you need to write directly to your audience with only the necessary points included and as little as descriptive style as possible. The point is to get to the point. And each step of the impact model should be communicated in your write-up as noted here.

- So, for the I: explain what has been researched, even if your audience is the people who requested the project, right?
    - You still need to restate the purpose of the project. So include any relevant history as well. If your project is part of a larger program or if it's a continuous effort to explain an issue or help a decision come to an end, so then include this as the background.

- The M part: depending on your audience, you may not cover too much of what your process was in the master, the data step of the impact model, but just give an overview of the data source and which pieces of data are included in the analyzers is something that you could include.
    - But if your audience is, for example, more technical and interested, you may go into detail on your ETL process. But it's more likely that you will leave this part out. It depends really on the audience.

- The P and A: So similar on how you write about mastering the data, you may not need to include thorough description of your test plan or your process for refining your results, depending again on what the interest is of your audience and what they exactly need to know. But including an overview of the type of analyzers performed and any limitations that you encounter might be important to include here.

- The C: so if you're including a data visualization within your write-up. So, you need to explain how to use the visuals. If there are certain aspects that you expect to stand out from the analyzers and the accompanying visual, you should describe what those components are. The visuals should speak for itself, but the write-up can provide confirmation about the important pieces that are displayed in your visuals.

- The D, discuss what's next in your analyzers. Will the visuals or the reports result in a weekly or quarterly report? What trends or outliers should be paid attention to over time? These are all details to take into account.

Consider your audience and tone

So, for example, if you have several different people to communicate results to, you may consider crafting several different versions. For example, one that contains all the extraction, transformation and loading details, so the ETL process, you could include that, for example, for the programmers and the database and administrators. But next to that, so if you want to communicate your results to the managers, you might just heavily want to rely on the interpretation of the visuals. So, it really depends on the audience. So really consider the knowledge and skill of your audience. Don't talk down to them, but don't overwhelm a non-technical crowd with technical jargon. So, explain the basics when you should and don't when you shouldn't.

An additional piece of communication to consider is also the vehicle for communication. So, we have a variety of options available to us for communicating. Email, phone calls, Skype, instant messaging, printed reports, face-to-face conversation, etc. And this can all be either informal or formal presentation that you can provide there. When crafting your communication, consider really the best way to provide the information to your intended audience. Also, if the concept is quite difficult to understand, a written report will probably not suffice. Plan to supplement your written material with a sit-down conversation or a phone call to explain the details and answer some questions. But then again, if the topic is quite easy to understand, it's a simple topic. So, an email response summarizing the visualization results will likely already be enough.

Next to that, you should also consider the professional culture of your organization. It may be commonplace to communicate casually using abbreviations and jargon in your workplace. But if that's not the way your workplace operates, or even if it's not the way that the recipient of your message communicates, take the time to refine your message and mirror the norms of the organization and recipients. So is the report going to be updated and send out to regular intervals, for example daily, weekly or monthly? If so, keep a consistent template so that it's easy for the recipients to identify the information they seek on a regular basis.

There are of course many more concepts to consider that will be unique to each message that you crafted, right? So take the time to always consider your audience, their communication style and what they need from the communication. And then try to provide it via the right message, the right tool and the right vehicle.

Writing and Revising

Just as you are at the presently refining results in the four steps of the impact model, you should also refine your riding. Until you get plenty of practice, and even once you consider yourself an expert, you should ask other people to read through your riding to make sure that you're communicating clearly. So, revising your riding requires you to be ego-less: Ready to dislike anything you have previously written. So, if someone dislikes something you have written, remember that it's the leader you need to please, not yourself.
So always placing your audience as the focus of your riding will help you maintain a proper tone, providing the right context and avoid too much detail.

Summary Chapter 5

To summarize, so this chapter focuses on the fifth step of the impact model, or the C, to discuss how to communicate the results of your data analyzers project. Communicating can be done through a variety of data visualizations and in-ear reports, depending on your audience and the data you're using.

In order to select the right chart, you must first determine the purpose of your data visualization.
And this can be done by answering two key questions.

- Are you explaining the results of a previously done analytics, or are you exploring the data through the visualization? So in other words, is your purpose declarative or exploratory?
- A second question is what type of data is being visualized? Qualitative data or quantitative data?

And the difference between each type of data, declarative and exploratory, or qualitative and quantitative, are explained, as well as how each data type impacts both the tool you're likely to use and the chart you should create.

After selecting the right chart based on your purpose and data type, your chart will need to be further refined. Selecting the appropriate data scale, scale interference, and color for your visualization is explained through the answers to the following questions.

- How much data do you need to share in the visuals to avoid being misleading, yet also being distracting?
- If your data contains outliers, should they be displayed, or will they distort your scale to the extent that you can leave them out?
- Other than how much data you need to share, what scale should you place the data on?
- Do you need to provide context or reference point to make the scale meaningful?
- And when should you use multiple colors?

Finally, this chapter discusses how to provide a written report to describe your data analysis project, and each step of the impact model should be communicated in your write-up, and the report should be tailored to the specific audience to whom it is being delivered.