UPPSALA UNIVERSITET

Lecture 12

Risk Management, ERM & Cybersecurity

8th of February 2023
H 425
Kl. 15.15 – 17.00

What is ERM ?

Defintion

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**" (COSO, 2004)

UPPSALA UNIVERSITET

The Framework itself is a set of principles organized into five interrelated components:

1. **Governance and Culture**: Governance sets the organization's tone, reinforcing the importance of, and establishing oversight responsibilities for, enterprise risk management. Culture pertains to ethical values, desired behaviors, and understanding of risk in the entity.
2. **Strategy and Objective-Setting**: Enterprise risk management, strategy, and objective-setting work together in the strategic-planning process. A risk appetite is established and aligned with strategy; business objectives put strategy into practice while serving as a basis for identifying, assessing, and responding to risk.
3. **Performance**: Risks that may impact the achievement of strategy and business objectives need to be identified and assessed. Risks are prioritized by severity in the context of risk appetite. The organization then selects risk responses and takes a portfolio view of the amount of risk it has assumed. The results of this process are reported to key risk stakeholders.
4. **Review and Revision**: By reviewing entity performance, an organization can consider how well the enterprise risk management components are functioning over time and in light of substantial changes, and what revisions are needed.
5. **Information, Communication, and Reporting**: Enterprise risk management requires a continual process of obtaining and sharing necessary information, from both internal and external sources, which flows up, down, and across the organization.

Source: COSO ERM Executive Summary 2017

Important demarcations

Risk	⟷	Uncertainty
Siloed	⟷	Integrated
Compliance	⟷	Business Partnering
Measurement	⟷	Envisionment
Socio-technical	⟷	Socio-cognitive

In practice ERM is about: technologies, processes and people…

Picture Credit: FERMA FORUM 2022

ERM at Sandvik – The CRO Explains

"Risk management **takes place in many different processes** and operations throughout the group. The Group's risk management approach follows our decentralized structure. The Company Board of Directors is ultimately responsible for **the governance of risk** management. The Group Executive Management ensures there is a common and efficient process in place. All management teams in our different businesses are responsible for their own risk management."

"Swedish companies are focused on **the benefits of the process**, so yes comply with the codes, but the main focus should be to look at the benefits for the organization […] We conduct ERM in order to **create competitive advantage**, secure business objectives and **add value** to the business […]"

Source: Crawford & Nilsson (2021)

ERM at Svenska Kraftnät – The CFO Explains

"We try to **integrate the process** of planning – financial planning, the operational planning and risk management **into one process**. That is why risk management, risk analysis, and the risk workshop are part of the planning process which includes both operational activities and financial planning".

"Some people see risk management as an add on […] they don't see the connection between risk activities and a potentially stable P&L, for some people that is a huge distance. I guess some financial people can find that and top management can find it, but risk management to some people is an unknown area".

Source: Crawford & Nilsson, 2021

UPPSALA UNIVERSITET

ERM at Skandia – The CFO Explains

"A lot of those regulations, particularly those on the insurance side and even on the banking side, **integrate all the risks** and set a capital requirement for them (aggregated risks). Earlier, asset management worked on their own in managing market risks. The actuary function managed insurance risks. But now everything is much more connected"

"We really work together with **different scenarios** that we bring forward. You have certain scenarios (referring to finance), we have other scenarios (referring to risk management), but it is the same mode that we use".

Source: Crawford & Nilsson, 2021

ERM at Atlas Copco – The CFO Explains

The group's risk management approach follows the decentralized structure of Atlas Copco. Local companies are responsible for their own risk management, which is monitored and followed up regularly e.g., at local business board meetings (Extract from AR 2018).

"We want each manager, whatever they are responsible for, to feel that 'I am a risk manager', integrated in her job as a senior purchaser or an assembly team leader or general manager for a whole production site"

Source: Crawford & Nilsson, 2021

Is ERM still fit for purpose?

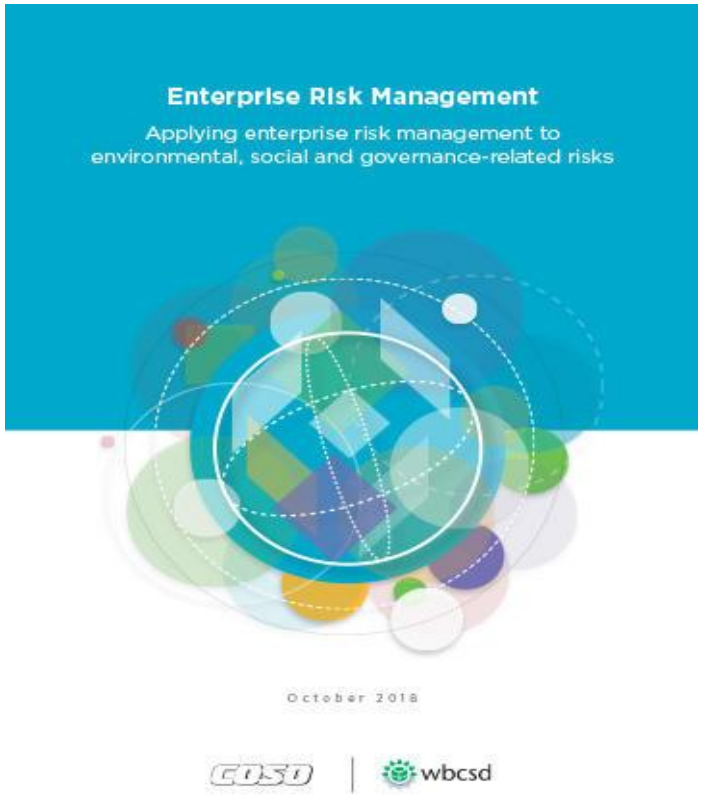
2008 Focus Short Term Financial Risks

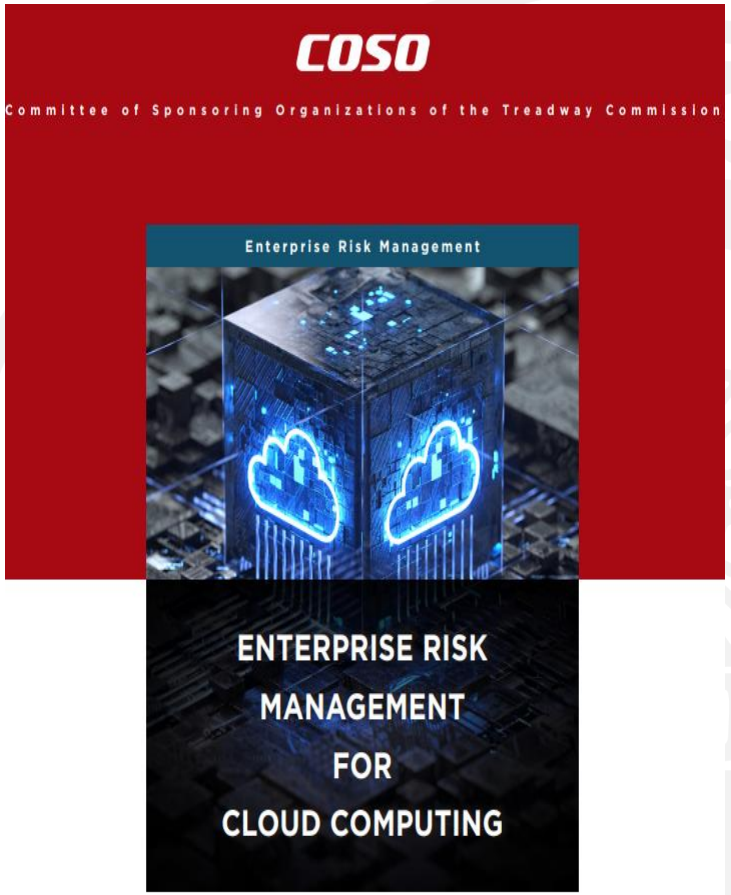
2022 Focus Long-Term Environmental Uncertainty

Many frameworks to choose from…

- COSO's ERM Integrated Framework (204/2017)
- Joint Australia/New Zealand 4360-2004 Standards
- ISO 31000 (2009/2017)
- The International Association of Insurance Supervisors Framework
- Basel Accords
- Organisational specific frameworks (a mix of the above)

ERM Framework Extensions -



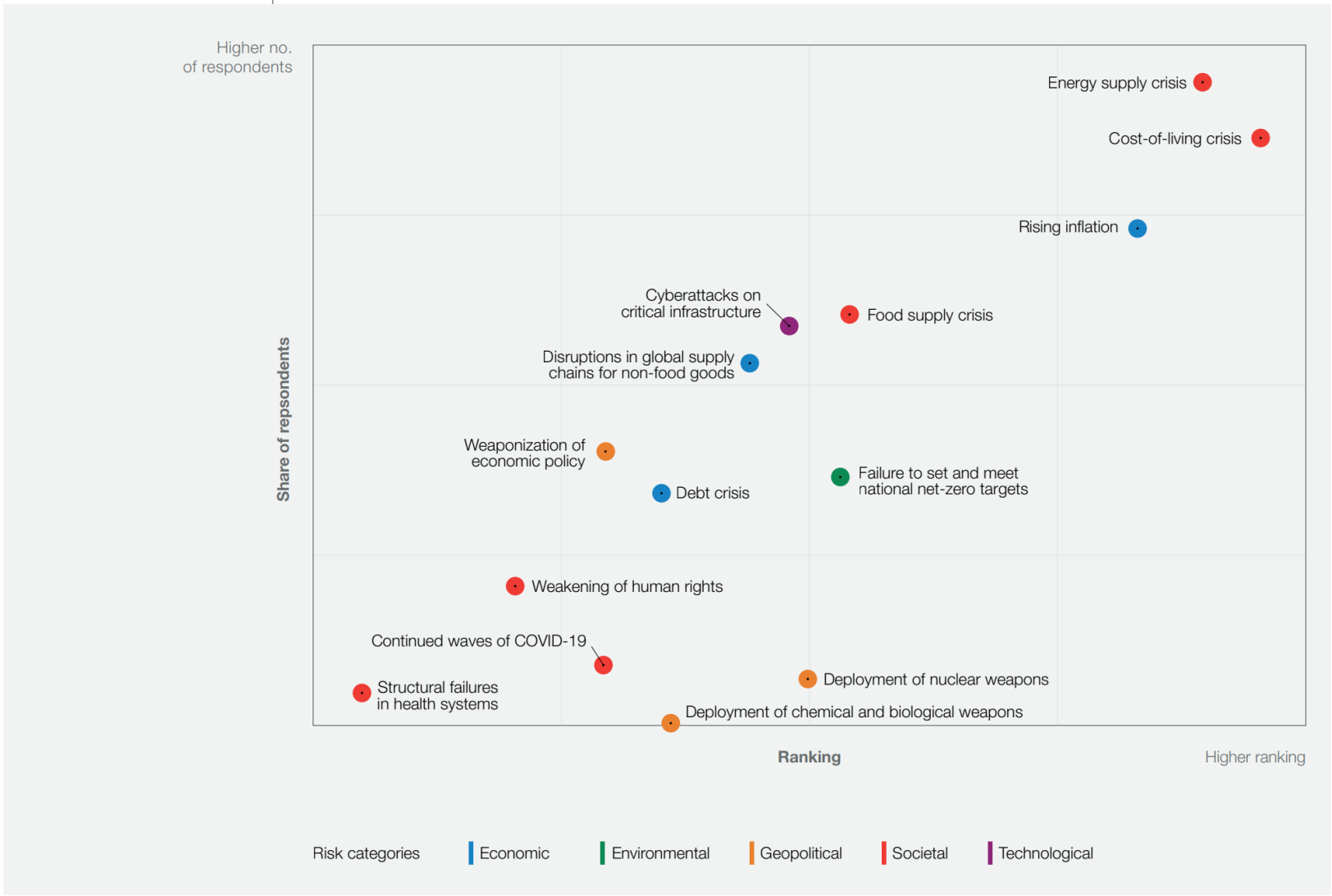


Risk: Real World Manifestations (Global)

FIGURE 1.1

Currently manifesting risks

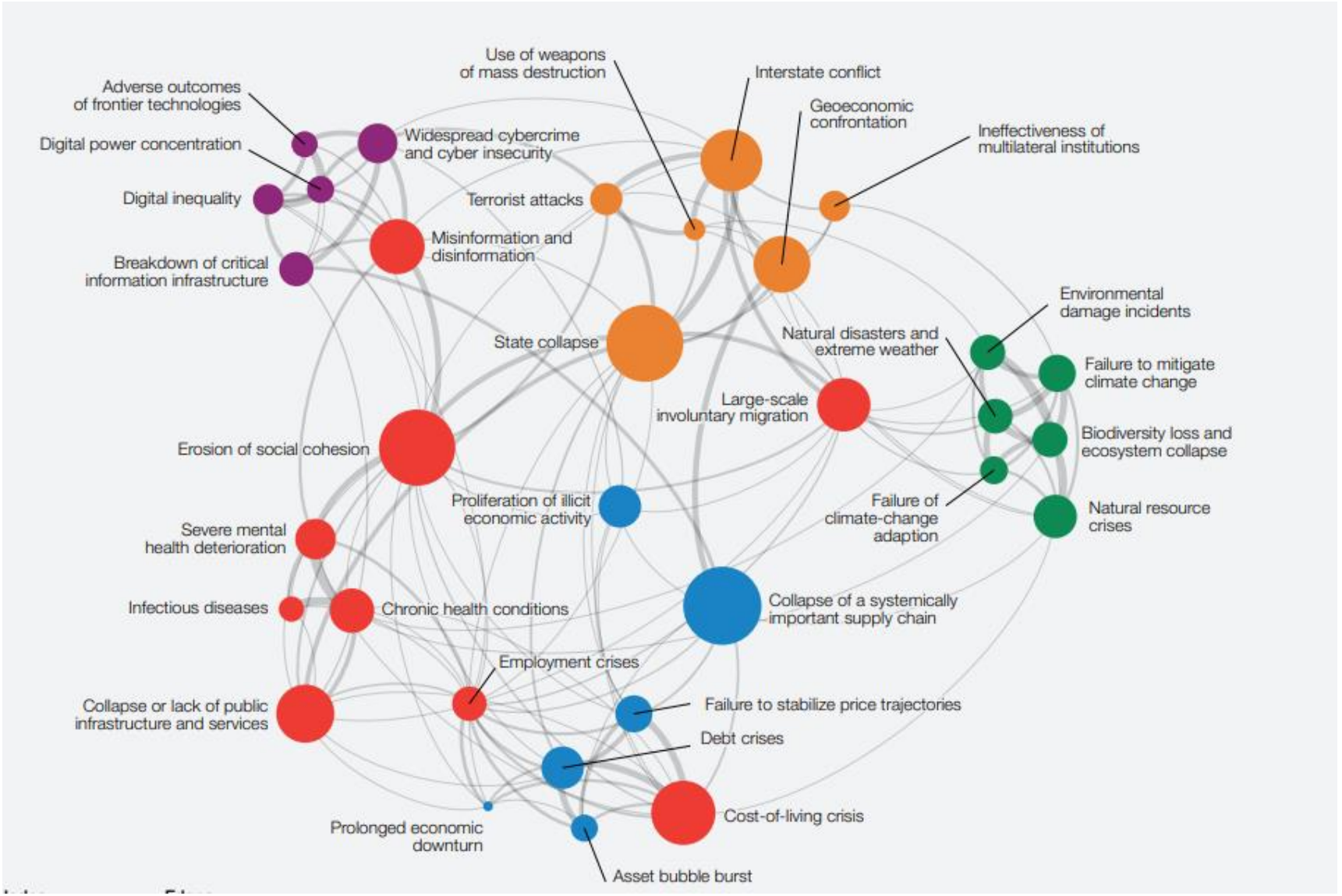
"Please rank the top 5 currently manifesting risks in order of how severe you believe their impact will be on a global level in 2023"



Source: WEF Global Risks Perception Survey 2022-2023

UPPSALA UNIVERSITET

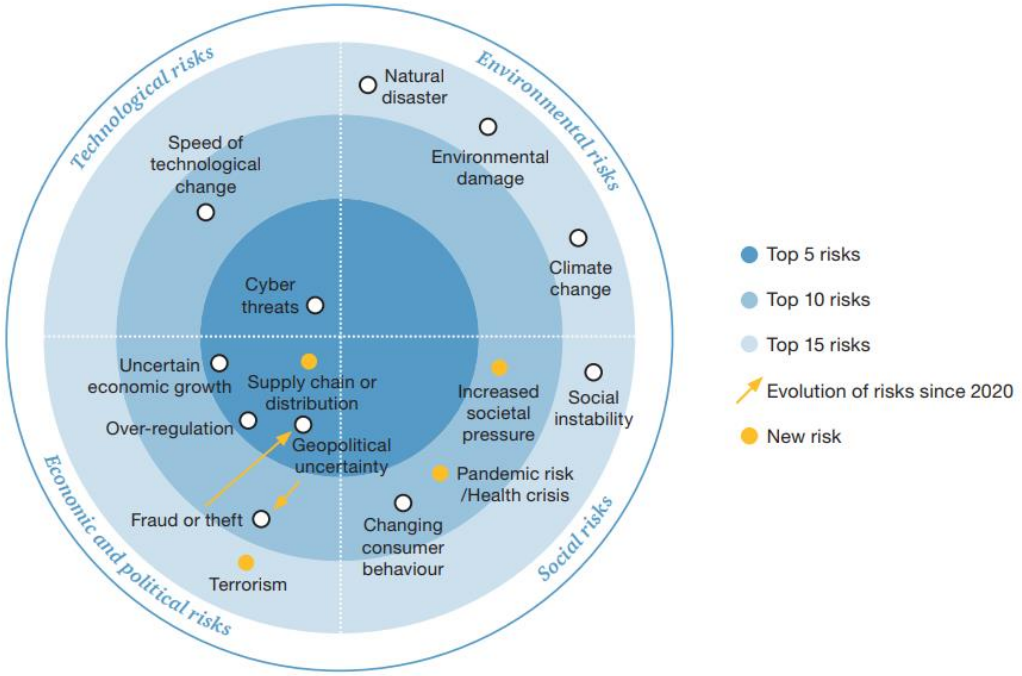
An increasingly connected global risk landscape



Source: WEF Global Risks Perception Survey 2022-2023

Risk: Real World Manifestations (Firm-General)

Top 15 critical threats to the organisation's growth prospects within the next 12 months



This radar highlights 4 new risks in the Top 15 in 2022:

- Supply chain or distribution failure
- Pandemic risk
- Increasing societal pressure
- Terrorism

5 other risks have disappeared from the 15 most critical threats:

- Extreme weather events
- Asset bubbles in a major economy
- Brexit
- Exchange rate volatility
- Availability of key skills

Source: FERMA European Risk Manager Survey Report 2022

UPPSALA UNIVERSITET

Extending ERM to Include ESG Risks

Benefits of integrating ESG-related risks into ERM

Applying this guidance along with the ERM principles and processes detailed in COSO's ERM framework (or other frameworks) can provide a starting point for effectively understanding, managing and disclosing the full spectrum of risks. By doing so, a company can achieve:

- **Enhanced company resilience**
  A company's medium- and long-term viability and resilience will depend on the ability to anticipate and respond to risks that threaten its strategy and business objectives.
- **A common language for articulating risks**
  ERM identifies and assesses risks for potential impact to the business strategy and objectives. Articulating ESG-related risks in these terms enables ESG issues to be brought into mainstream processes and evaluations.
- **Improved resource deployment**
  Obtaining robust information on ESG-related risks allows management to assess overall resource needs and helps optimize resource allocation.
- **Enhanced pursuit of opportunity**
  By considering both positive and negative aspects of ESG-related risks, management can identify ESG trends that lead to new business opportunities.
- **Efficiencies of scale**
  Managing ESG-related risks centrally and alongside other entity-level risks helps to eliminate redundancies and better allocate resources to address the company's top risks.
- **Improved disclosure**
  Improving management's understanding of ESG-related risks can provide the transparency and disclosure investors expect and ensure consistency with jurisdictional reporting requirements.

Source: COSO & WBCSD (2018)

Applying ERM to ESG risk – evidence from practice

Länsförsäkringar:

”Sustainability issues have a tendency to end up detached, instead of being integrated with other processes and risks” […] ” We have therefore extended the tasks of the risk management function and the types of risks that are mapped” (CEO LFGB)

Handelsbanken:

”The low tolerance for risk, including sustainability risk, is a cultural matter. They [employees] are not encouraged to take on certain risks even if they could be priced favorably” (Head of Sustainability)

Source: Crawford and Nilsson, 2023

Applying ERM to ESG risk –
evidence from practice

Scania:

> ”The strength of Scania is that we always try and bring things into the normal processes and then we work with it thoughout the whole organisation. A centralised team in the sustainability department needs to support that work and everything needs to be integrated. An if it needs to be integrated it really needs to be understood and usable”
>
> (Head of Group Risk Management)

Source: Crawford and Nilsson, 2023

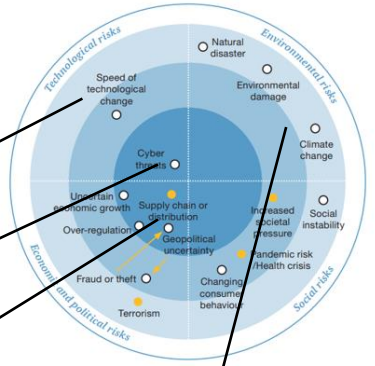
A look to the future

Global Risks: Fractured Future

"Among the highest likelihood risks of the next ten years are **extreme weather**, **climate action failure** and human-led **environmental damage**; as well as digital power concentration, **digital inequality** and **cybersecurity failure**. Among the highest impact risks of the next decade, **infectious diseases** are in the top spot, followed by climate action failure and other environmental risks; as well as **weapons of mass destruction**, **livelihood crises**, debt crises and **IT infrastructure breakdown**"

Source: The Global Risk Report 2021

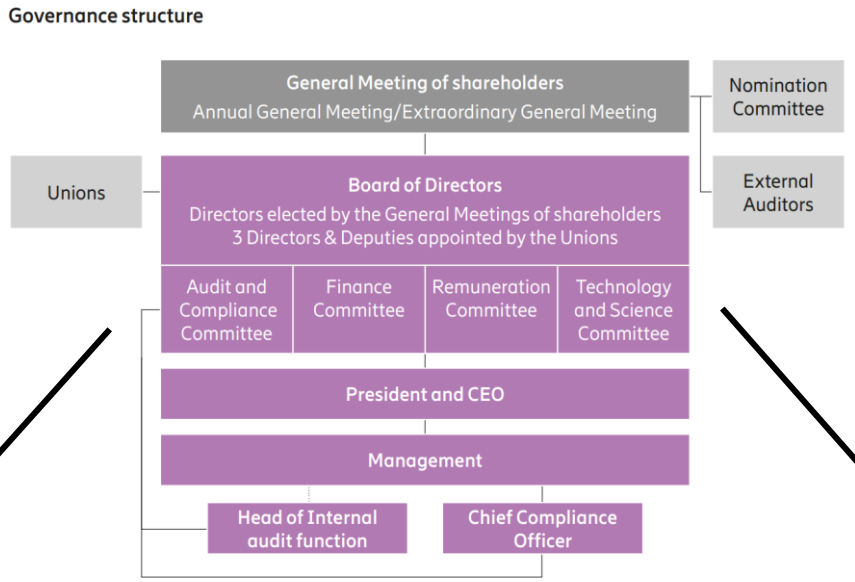
Risk: Real World Manifestations (Firm-Specific)



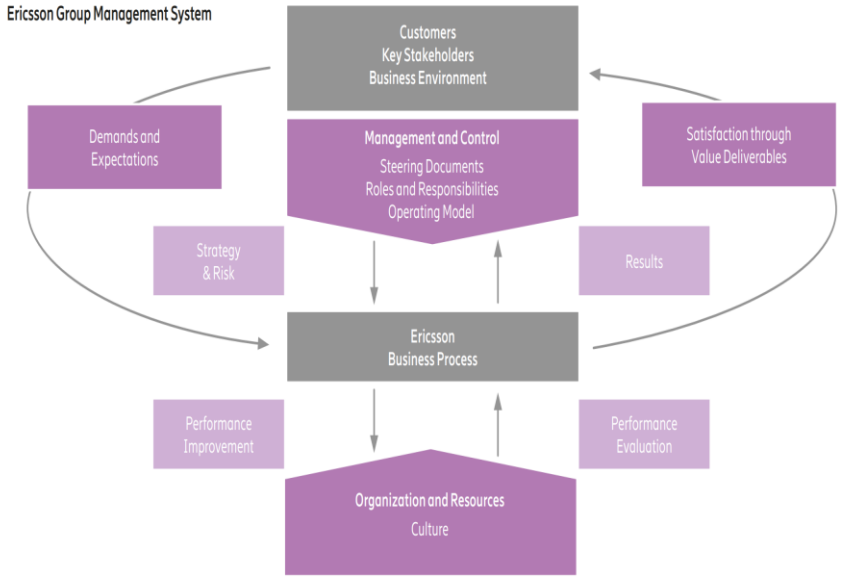
Risk Universe

Intellectual Property Rights	Competition	M&A	Cyber and information security	Security, safety and continuity	People
Governance, risk and control	Laws and regulations	Communication and marketing	Geopolitical	Customer	Accounting
Treasury	Technology	Supply and sourcing	Product and service	Project execution	Environment and climate

UPPSALA UNIVERSITET



The relationship between the GS, EGMS, and ERM??



ERM Framework at Ericsson

- **Governance and culture:**
  - Clear allocation of responsibility and accountability to risk owners. Attitudes and behaviours reflect upside and downside risk knowledge that influences decision-making.
- **Strategy:**
  - Risk management is linked to strategic objectives, and influences business and functional level strategy formulation and implementation
- **Assessment and Treatment:**
  - Risks are connected to strategic objectives (see risk description and treatment plan tools, :19)
- **Communication & Reporting**:
  - Group Risk Council: faciliates ”cross-group alignment”
- **Monitoring:**

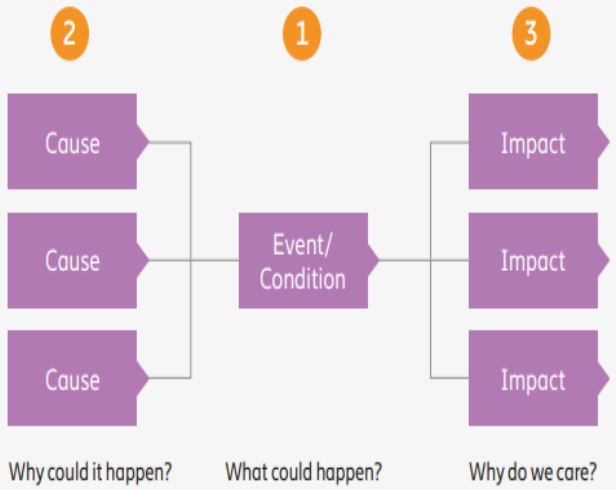
  Self and internal assessment process (ISO9001)

Examples of ERM artefacts

Assessment and Treatment:

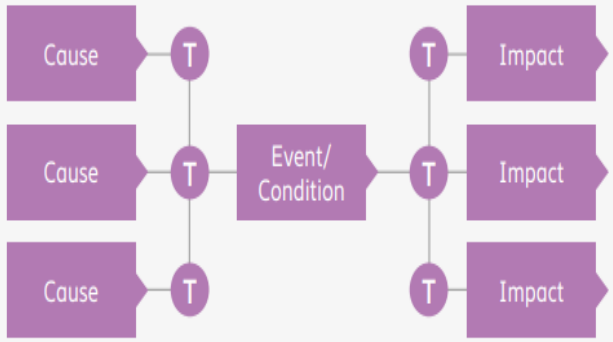
Risk Description

Risk Descriptions are created by answering the following questions:

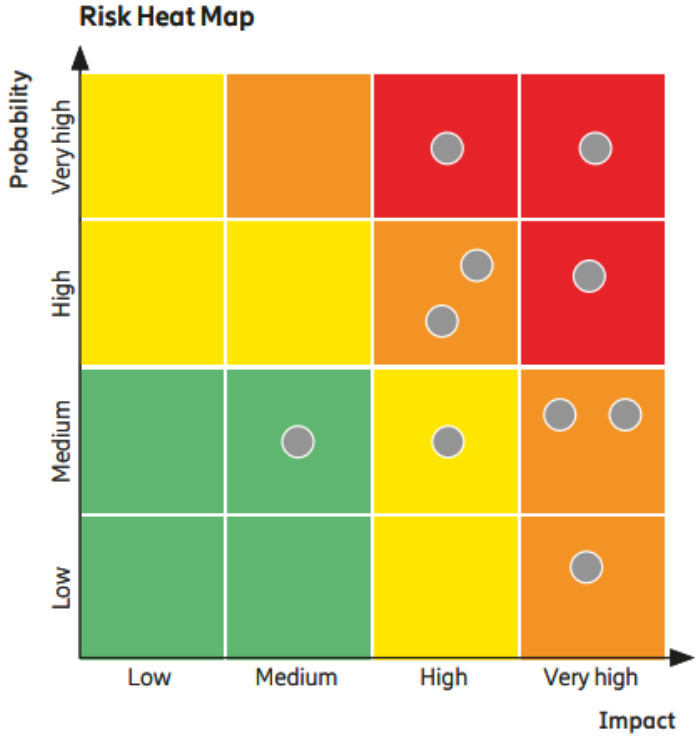


Treatment plan

T Treatment plans for the risk are defined by looking at different treatment options to reduce the probability of the cause and impact of the event.



Communication & Reporting:



What about risk treatment?

Risk Treatment

For identified risks of relevance, treatment options are chosen, i.e. avoid or accept the risk, mitigate the probability or impact of the risk, or increase the risk in order to pursue an opportunity. Based on the selected treatment option(s), a treatment plan for getting the probability and impact within the risk appetite is defined and described, including references to current or planned internal controls (illustrated below). Once the treatment plan is implemented, its effectiveness shall be assessed on an ongoing basis, and decisions shall be made where corrective actions are needed.

1. How does an organization know what is at risk and why it is relevant?
2. How can risk probability and impact be affected?
3. Why is the risk appetite so important?

The significance of - risk technologies

ERM artefact design, reconfiguration, and use	Experts and technologies continually evolve together via circular dynamic interactions (Arena et al., 2010). Complex risk artefacts used to calculate and model risks are black-boxed and less malleable in their design and use when compared to risk artefacts used for risk envisionment (Jordan et al., 2013; Mikes, 2011). Information produced or represented by highly technical and quantitative risk artefacts tends not to generate organisational action (Christiansen & Thrane, 2014), unless it includes information and knowledge from other managers that is considered relevant for decision-making (Hall et al., 2015), and that risk artefacts are embedded into daily managerial activities (Nasteckienė, 2021). For strategic risks, artefacts that provide qualitative data increase the perceived relevance and reliability of that information (Stoel et al., 2017). Decision uncertainty can be increased or decreased by using risk measurement artefacts (Mikes, 2011), and certain risk artefacts can increase risk awareness amongst distributed actors (Braumann, 2018; Woods, 2009). Risk artefacts can also be used to enhance dialogue and define boundaries, facilitating coordination amongst distributed actors (Jordan et al., 2013).

Source:
Crawford & Jabbour, forthcoming

The significance of - risk cultures

Risk cultures	Risk cultures shape managerial preferences for ERM practices (Diab & Metwally, 2021), including risk measurement vs. risk envisionment. The value of human judgement varies depending on the risk culture (Mikes, 2009:2011). Differences between risk cultures may lead to tensions between risk and business managers concerning the usefulness of risk artefacts in forming judgements and making decisions about risk and uncertainty (Kallenberg, 2009, Wahlström, 2009). These tensions may serve as a catalyst for actors to exercise their agency to change how risk artefacts are designed and used in the future (Arena et al., 2010; Jabbour & Abdel-Kader, 2015). Risk culture also has a pervasive effect on shifting cognition and redefining identities so that they may be aligned with the risk management system (Diab & Metwally, 2021).

Source:
Crawford & Jabbour, forthcoming

Cybersecurity

The Global Risks Report 2023
18th Edition

"The **ever-increasing intertwining of technologies** with the critical functioning of societies is exposing populations to direct domestic threats, including those that seek to shatter societal functioning. Alongside a rise in cybercrime, attempts to disrupt critical technology-enabled resources and services will become more common, **with attacks anticipated against agriculture and water, financial systems, public security, transport, energy and domestic, space-based and undersea communication infrastructure**. Technological risks are not solely limited to rogue actors. Sophisticated analysis of larger data sets will enable **the misuse of personal information through legitimate legal mechanisms**, weakening individual digital sovereignty and the right to privacy, even in well-regulated, democratic regimes".

Cybersecurity

- A key consideration for many organisations considering recent advances in e.g., AI, quantum computing, IoT (costs/reputation/insurance).
- A top priority from a risk management perspective (i.e., identification and containment).
- Related to information (e.g., information security) and non-information assets (e.g., risk of harm to humans).
- Our understanding of the implications of cybersecurity breeches have moved beyond technical issues (e.g., the AI Act), to social, political, legal issues.
- Cybersecurity is now accommodated in COSOs ERM-Integrated Framework but is it working?

Source: Eling et al., 2021

Cybersecurity

Perpetrators and Motivations

- **Nation-states and spies:** Hostile foreign nations who seek intellectual property and trade secrets for military and competitive advantage (e.g., those that seek to steal national security secrets or intellectual property).
- **Organized criminals:** Perpetrators that use sophisticated tools to steal money or private and sensitive information about an entity's consumers (e.g., identity theft).
- **Terrorists:** Rogue groups or individuals who look to use the Internet to launch cyber attacks against critical infrastructure, including financial institutions.
- **Hacktivists:** Individuals or groups that want to make a social or political statement by stealing or publishing an organization's sensitive information.
- **Insiders:** Trusted individuals inside the organization who sell or share the organization's sensitive information.

Source COSO, 2019 Managing Cyber Risk in A Digital Age

Some recent examples…

- Lapsus group – targeted Ubisoft, Samsung, Microsoft
  - Data stolen and leaked.
- Lazarus group – targeted Ronin (blockchain bridge)
  - Ethereum and Stablecoin stolen.
- Ransomware gangs – targeted the NHS in the UK
  - Major outage of services across the UK
- Marriot hotels
  - Remote access breeches & stolen data

The proliferation of technology and new cyber threats…

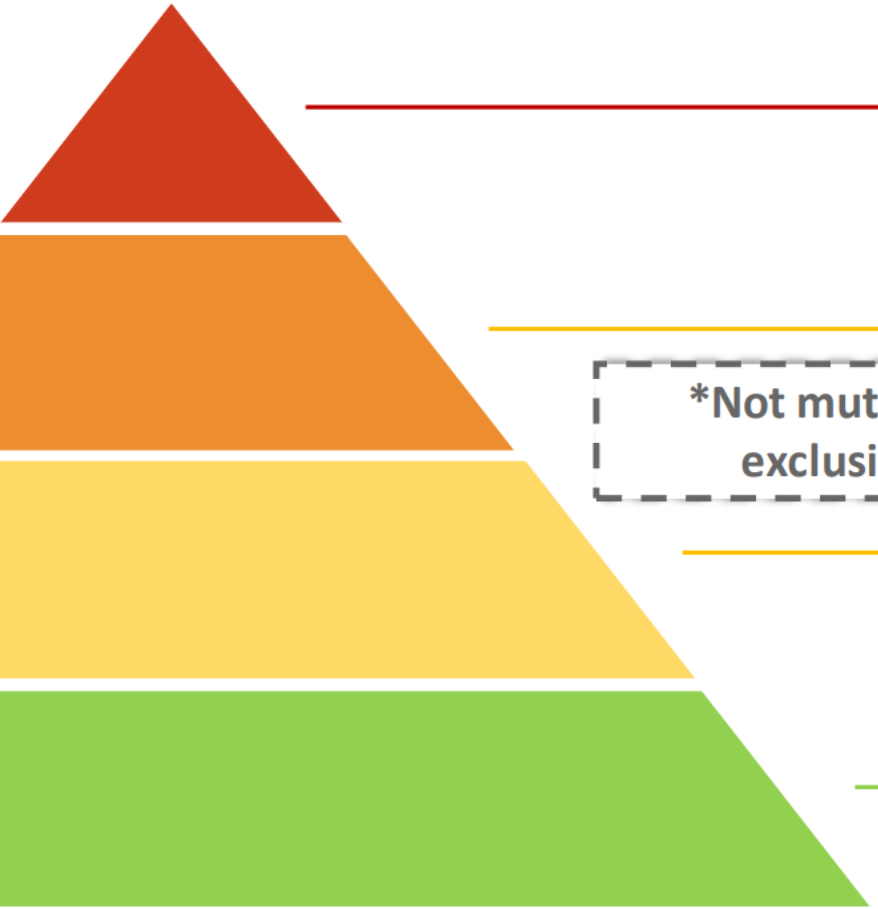
"A lot of folks think this is something we have to worry about in the future … the bottom line is that there are threat actors out there that are collecting encrypted data today … data that [using classical computing technology] would take thousands of years to decrypt. And they're collecting it for a reason."

The reason is that its quickly becoming apparent that quantum technology will be available in the not-too-distant future that will make short work of many of the industry-standard encryption techniques that are used to secure data today.

"This data has a long shelf-life … we're racking up a tab that we're eventually going to have to pay for."

Equifax CISO Jamil Farshch

A risk-based approach to regulation



*Not mutually exclusive

Unacceptable risk
e.g. social scoring

Prohibited

High risk
e.g. recruitment, medical devices

Permitted subject to compliance with AI requirements and ex-ante conformity assessment

AI with specific transparency obligations
'Impersonation' (bots)

Permitted but subject to information/transparency Obligations

Minimal or no risk

Permitted with no restrictions

European Commission

Cybersecurity & ERM

- Strategies for cybersecurity risk management
  - Avoidance; not a realistic approach, i.e., considerations for product development
  - Transfer; via insurance. Capacity affected by data for pricing, risk of insured risks in a portfolio exposed to the same incident, insurance perceived as a substitute for good risk management.
  - Retention; deciding optimal mix of risk retention and risk transfer.
- Emerging issues:
  - The majority of corporate data is in the cloud – the risk of attack is significant (oracle, 2020).
  - Managerial overconfidence and lack of expertise at board and senior management levels an issue.
  - New challenges for risk governance (as a subset of corporate governance), executive decision-making.

Source: Eling et al., 2021

Cybersecurity & ERM

- Integrating cybersecurity into ERM is very difficult. Cybersecurity is often siloed.
- Many boards are not equipped to deal with cybersecurity, from a risk governance perspective this is a serious issue.
- At the organisational level, the CRO and the CIO have a difficultly understanding each other because they use different terminology.
- The ERM framework contests that risks have downsides and upsides, but cybersecurity risk do not have risk that can be exploited to generate positive benefits for the organization.
- There is a lack of data, therefore it is difficult for managers to identify and recognize patterns for the purposes of mitigating reoccurring risks.
- Its very difficult to estimate likelihood in CRM (due to extreme unpredictability), instead it is argued that there is a need to reduce uncertainty through knowledge acquisition and create “cyber resilence”

Source: Eling et al., 2021

Increasing attacks on critical infastructure

pwc | Sverige

Sverige drabbas oftare av cyberattacker än de nordiska grannländerna

2020-02-12

När PwC har undersökt cybersäkerheten i Sverige, Norge och Danmark visar resultaten att svenska företag oftare uppger att de drabbas av cyberattacker. Åtta av tio svenska bolag menar att de har varit utsatta för incidenter under det senaste året, vilket kan jämföras med att bara hälften av de danska bolagen säger sig ha råkat ut för attacker. Undersökningen visar även att den organiserade brottsligheten nu tar allt större kliv in i cybervärlden.

SVENSKA DAGBLADET Nyheter Näringsliv Kultur Ledare Debatt Tidningen

Cyberattackerna mot Sverige

Allvarliga cyberattacker har gjorts mot svenska IT-företag rapporterar MSB. Här har vi samlat artiklar i ämnet.

Source: https://www.pwc.se/sv/cyber-security/cyberattack.html

UPPSALA UNIVERSITET

Thank you for listening! &

Good luck with the rest of the course!