Enabling an IT Risk Management Culture

Interesting Perspectives, Harsh Realities & Seldom Unspoken Rules

Learning Outcomes/Agenda

- A brief review of
  - The general nature of risk and IT-related risk in particular.
  - Common approaches to managing IT-related risk via Frameworks & Standards
  - The ISO 31000 Risk Management Process
- A closer look at concepts which may impact a risk management culture, including:
  - The impact of the way risk is commonly perceived or mis-perceived.
  - Avoiding the danger of “moral hazards” and “group polarization” through engagement and involvement.
  - Transitioning from compliant behaviour to committed behaviour via behaviour modification.
  - Understanding “Target Fixation” and how it can particularly derail the risk treatment phase.

Basic Risk Management Concepts

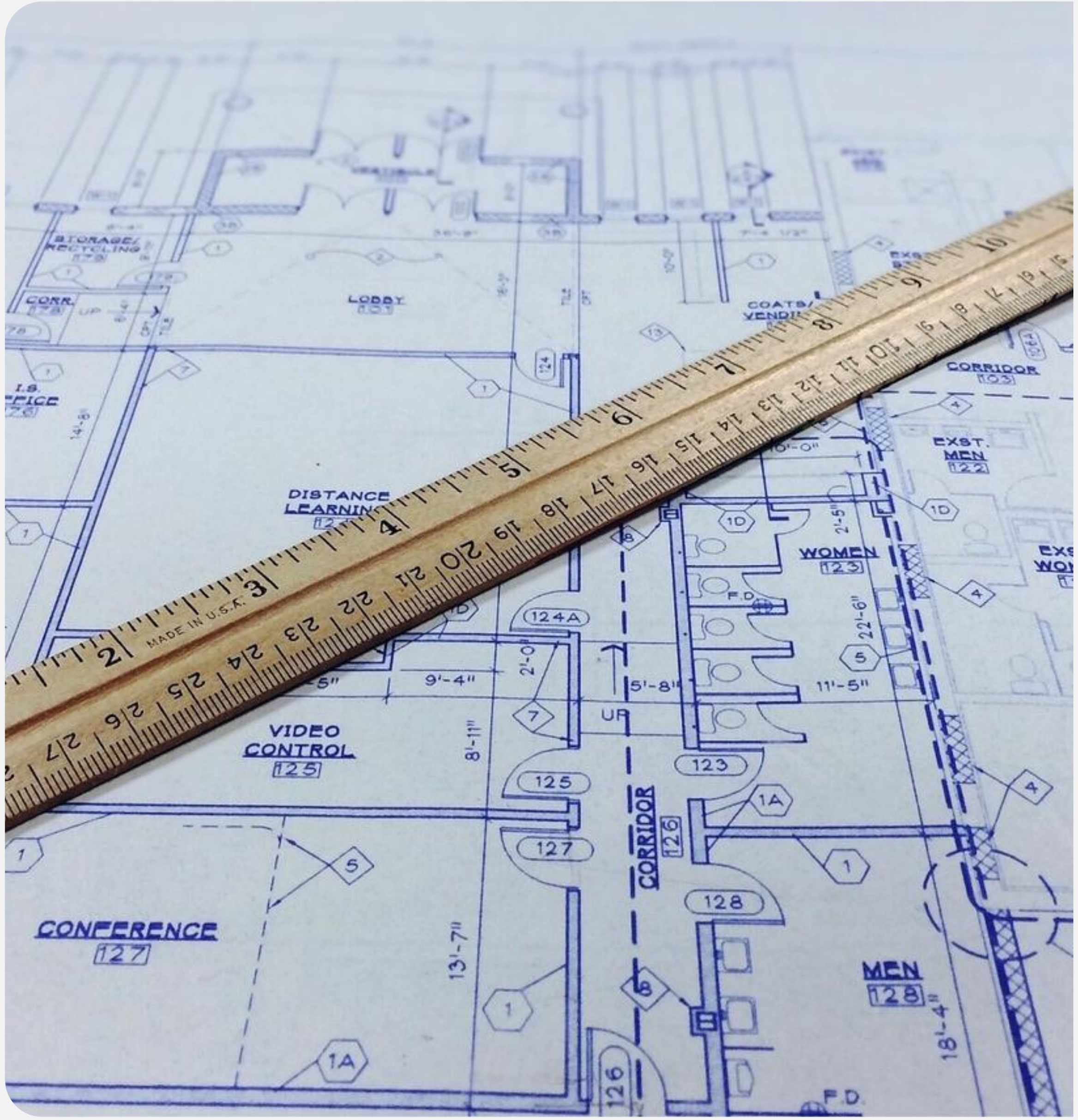
What is Risk?

- The effect of uncertainty on objectives [ISO31000]

- IT risk is business or mission risk [Risk IT Framework]
  - Specifically, the risk associated with the use, ownership, operation, involvement, influence and adoption of IT, within an enterprise.
  - Consisting of IT-related events, including cyber events, that could potentially impact the business or mission.
  - It can occur with both uncertain frequency and magnitude, and it creates challenges in meeting strategic goals and objectives

(IT) Risk Frameworks

- Framework:
  - A supporting structure around which something can be built
  - A system of rules, ideas, or beliefs that is used to plan or decide something
- Common frameworks/standards/guidelines
  - NIST Cybersecurity Framework
  - NIST Cloud Computing Framework
  - FAIR Cyber Risk Framework
  - COBIT 2019
  - ISO 27000 Series (ISO27005)
  - AICPA SOC 2 Framework
  - SANS Critical Security Controls
  - FFIEC IT Handbooks



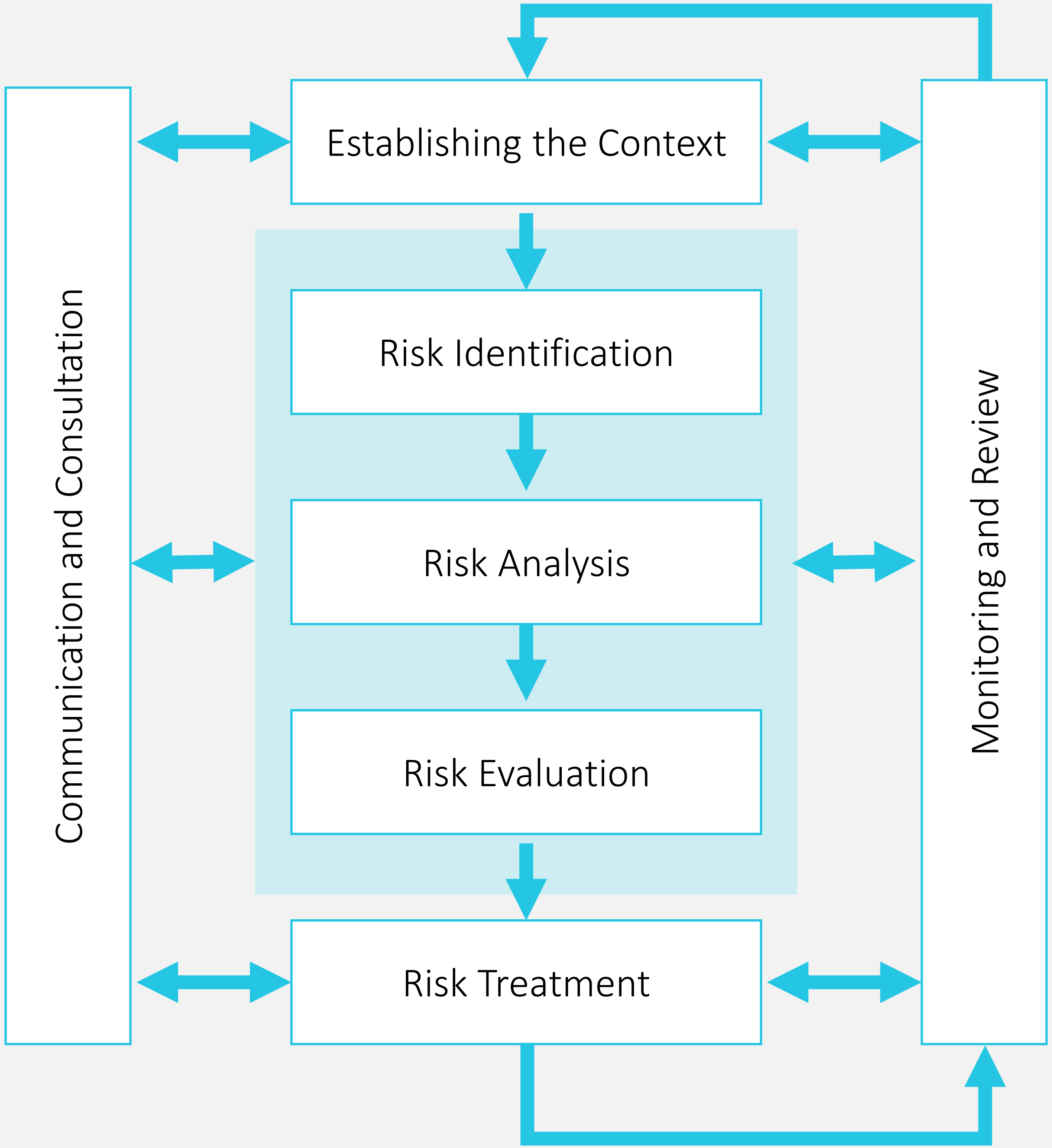
ISO 31000

- Provides principles, a framework and a process for managing risk.
- Can be used by any organization regardless of its size, activity or sector.
- Provides guidelines, not requirements, and is therefore not intended for certification purposes.
- Places a greater focus on creating value as the key driver of risk management
- Aims to develop a risk management culture where employees and stakeholders are aware of the importance of monitoring and managing risk.

COBIT 2019

- Culture, ethics and behaviour of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
- COBIT EDM03 – Ensured Risk Optimization
  - Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.
- COBIT APO12 – Managed Risk
  - Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.

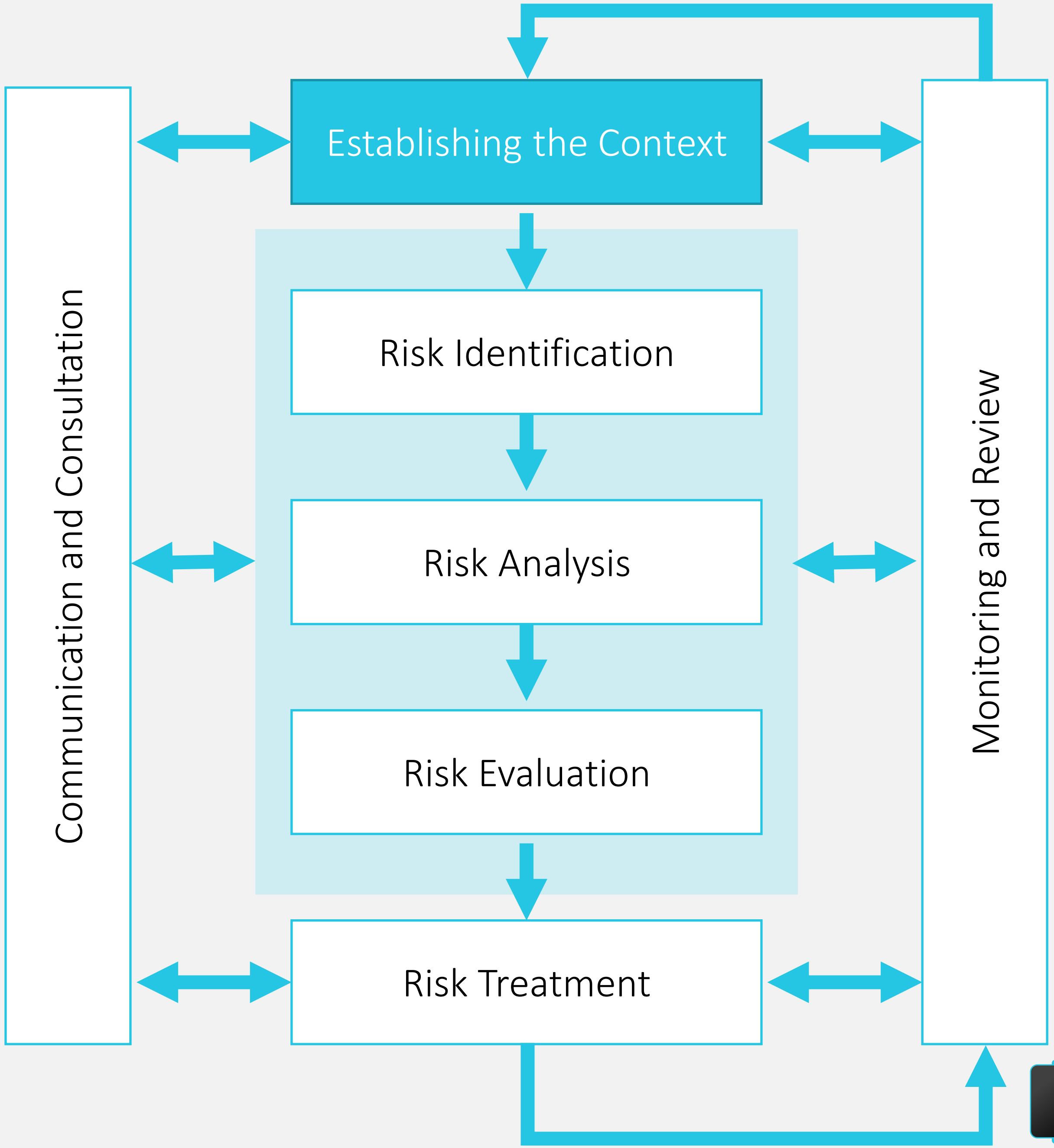
ISO 31000 Risk Management Process



Establishing the Context

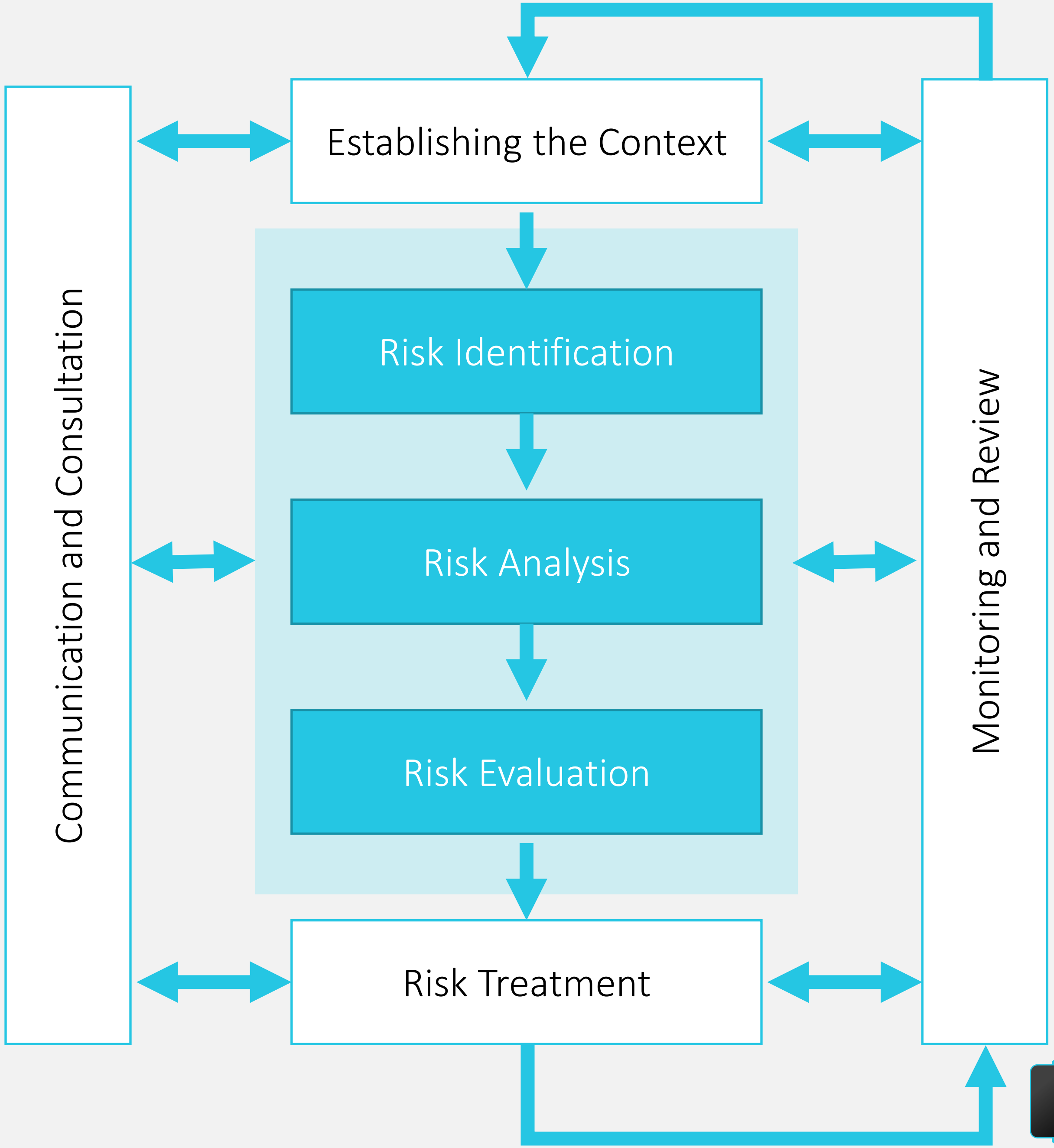
- Goal: Customize the risk management process, enabling effective risk assessment and appropriate risk treatment.

- Define the scope of risk management activities.
- Understand the external and internal context (the environment in which the organization seeks to define and achieve its objectives).
- Specify the amount and type of risk that may or may not be taken, relative to objectives.
- Define criteria to evaluate the significance of risk and to support the decision-making processes.



Risk Assessment

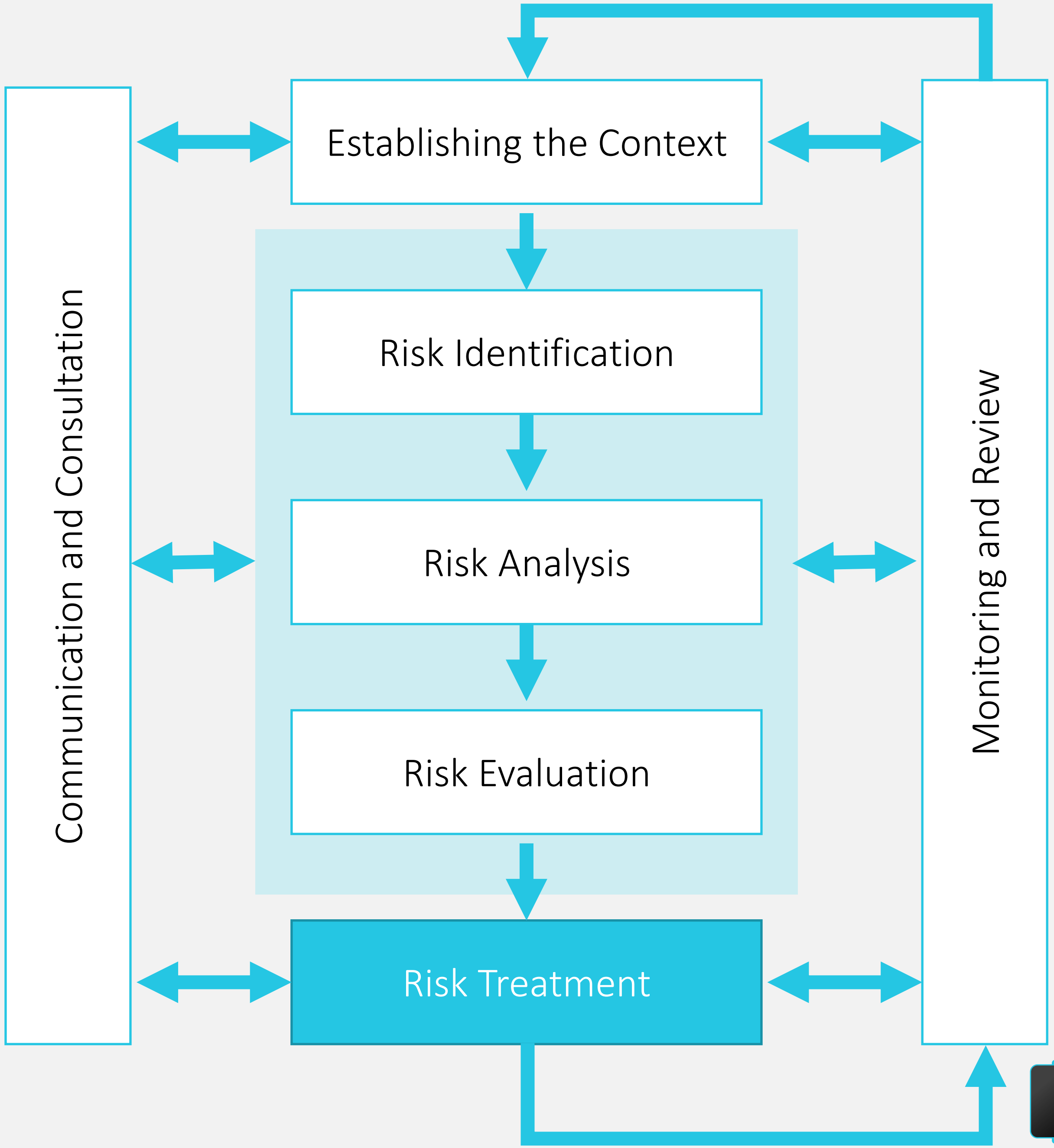
- Should be conducted systematically, iteratively and collaboratively, drawing on the knowledge and views of stakeholders.
- Should use the best available information, supplemented by further enquiry as necessary.
- <u>Identification:</u> find, recognize and describe risks that might help or prevent an organization achieving its objectives.
- <u>Analysis:</u> comprehend the nature of risk and its characteristics including, where appropriate, the level of risk.
- <u>Evaluation:</u> Support decisions by comparing the results of the risk analysis with the established risk criteria to determine where additional action is required.



Risk Treatment

- Goal: Select and implement options for addressing risk.

- Involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation.
- Justification for treatment is broader than solely economic considerations and should take into account all obligations, voluntary commitments and stakeholder views
- Options are not necessarily mutually exclusive or appropriate in all circumstances



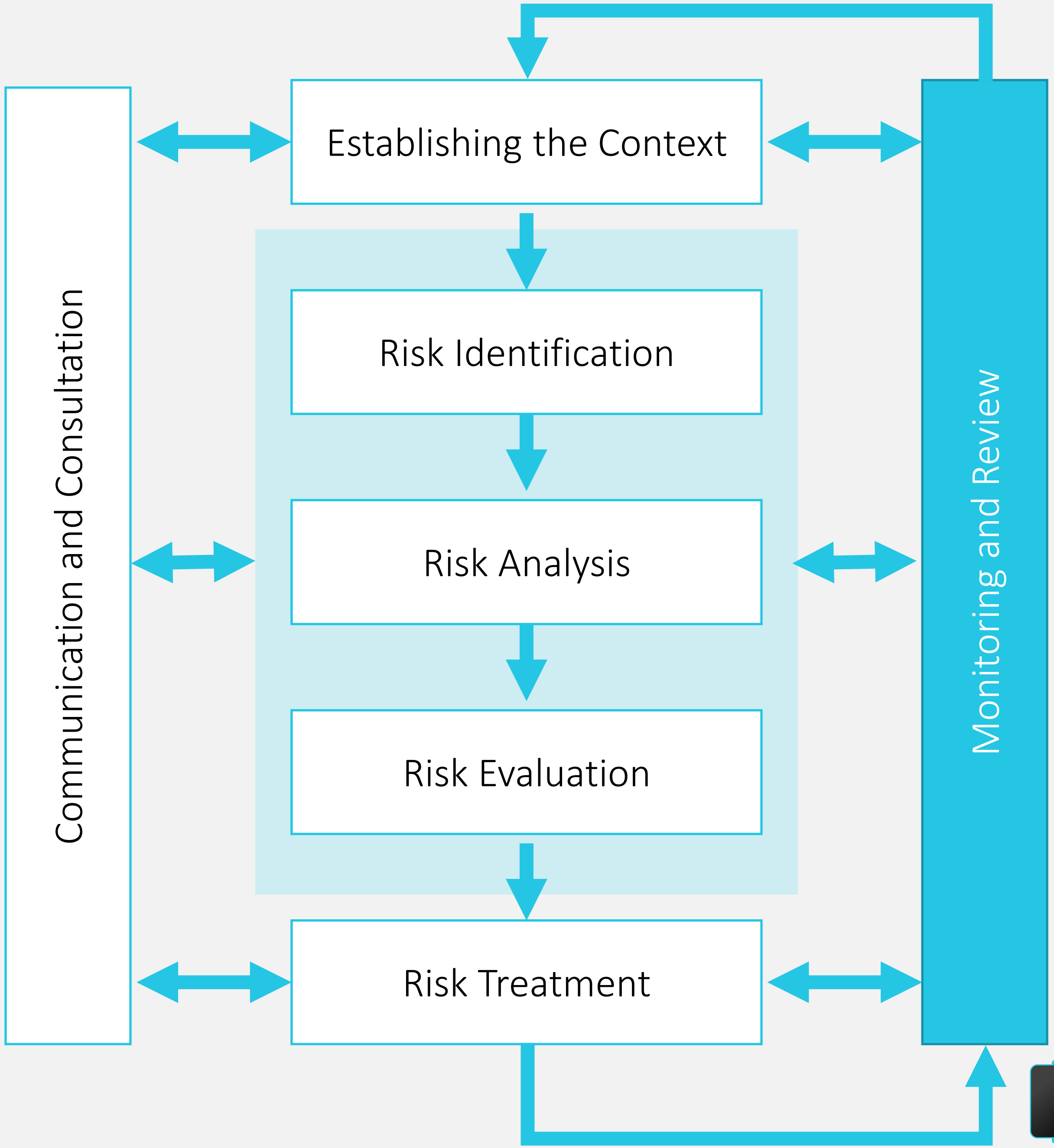
Monitoring & Review

- Goal: To assure and improve the quality and effectiveness of process design, implementation and outcomes.

- Plan and clearly define responsibilities for ongoing monitoring and periodic review of the risk management process and its outcomes

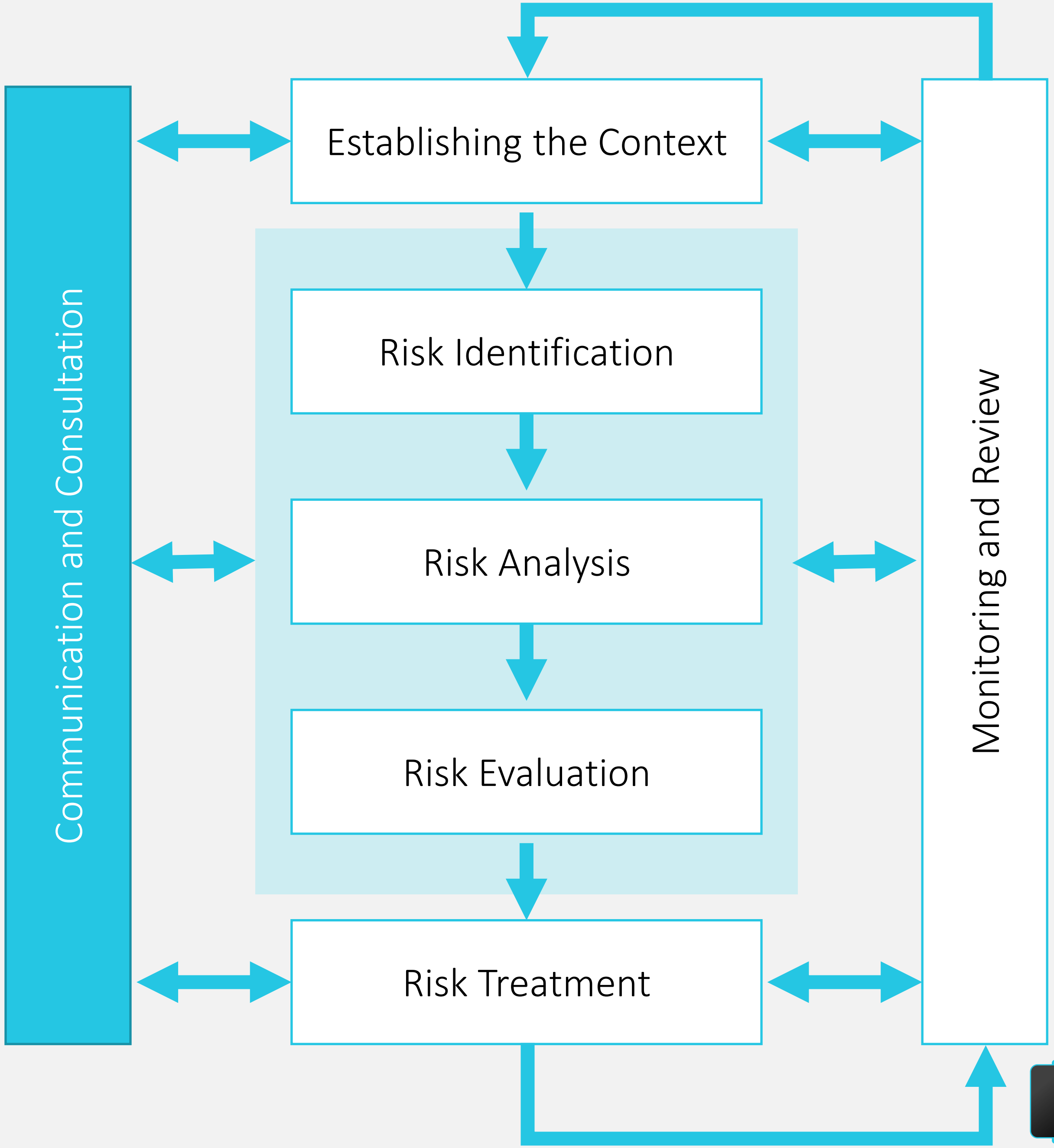
- Monitoring includes planning, gathering and analysing information, recording results and providing feedback.

- The results of monitoring and review should be incorporated throughout the organization's performance management, measurement and reporting activities.



Communication and Consultation

- Goal: to assist relevant stakeholders in understanding risk, the basis on which decisions are made and the reasons why particular actions are required.
- Communication seeks to promote awareness and understanding of risk.
- Consultation involves obtaining feedback and information to support decision-making.
- Close coordination between the two should facilitate factual, timely, relevant, accurate and understandable exchange of information, taking into account the confidentiality and integrity of information as well as the privacy rights of individuals.

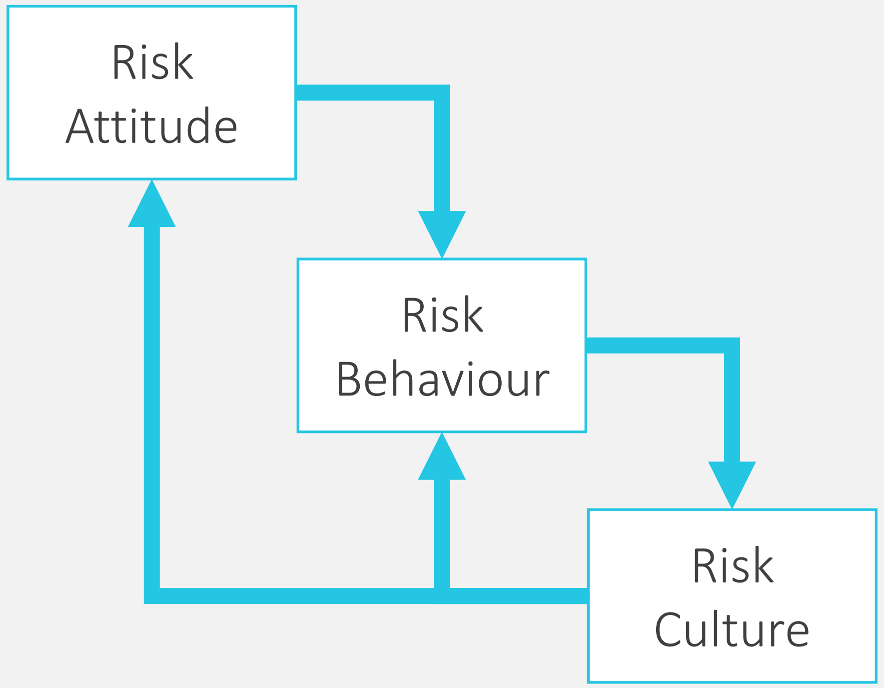


Risk Culture

What is Risk Culture?

- The norms, attitudes and behaviours related to risk awareness, risk taking and risk management.

- Risk attitude is “the chosen position adopted by an individual or group towards risk, influenced by risk perception”
- Risk behaviour comprises external observable risk-related actions, including risk-based decision-making, risk processes, risk communications etc.
- Risk culture is “the values, beliefs, knowledge and understanding about risk, shared by a group of people with a common purpose”.



Risk Culture – Desired Behaviours

- **Committed**
  - Showing a desire to be more risk aware gain more risk management knowledge
  - Demonstrating a positive attitude to risk management.
- **Proactive** - Always considering risk in any decision that is made, prior to the decision being made
- **Transparent & Honest**
  - Strong and open communication. Escalate as soon as a problem or issue arises
  - Telling the truth and taking ownership of problems
- **Responsible** - Taking responsibility for risk and controls. Be willing to stand up and claim ownership
- **Mindful** - Being concerned about the impact of their risk management on others – appreciating what is downstream when something goes wrong
- **Supportive** - Encouraging and educating others in risk and risk management

Risk Culture – Organizational Principles

- There should exist a commitment to ethical principles and practice
- Risk and risk management must be understood by all.
- The risk management process must be efficient and not cumbersome.
- Desirable behaviour and actions should be recognised and rewarded. Undesirable behaviour should have consequences.
- There should be avoidance of a blame culture, and encouragement of active learning from impacted risks and near-misses.
- The correct culture must be set at the Board and Senior Management level (tone at the top) and must be demonstrated to staff through “walk the talk” not “talk the talk”.

Interesting Perspectives, Harsh Realities & Seldom Unspoken Rules

Everyone manages risk!

- The management of risk is an inherent and often intuitive part of human nature.
- Everyone has a perspective as to what they consider risky and what they consider not.
  - Even though not everyone may agree on the likelihood and impact of the risk, or manage it on equal terms.
- Management of well understood (personal) risks tends to become instinctive and habitual.
- This has clear implications for a culture of commitment and proactivity

Most people tend to underestimate risks for which they are responsible

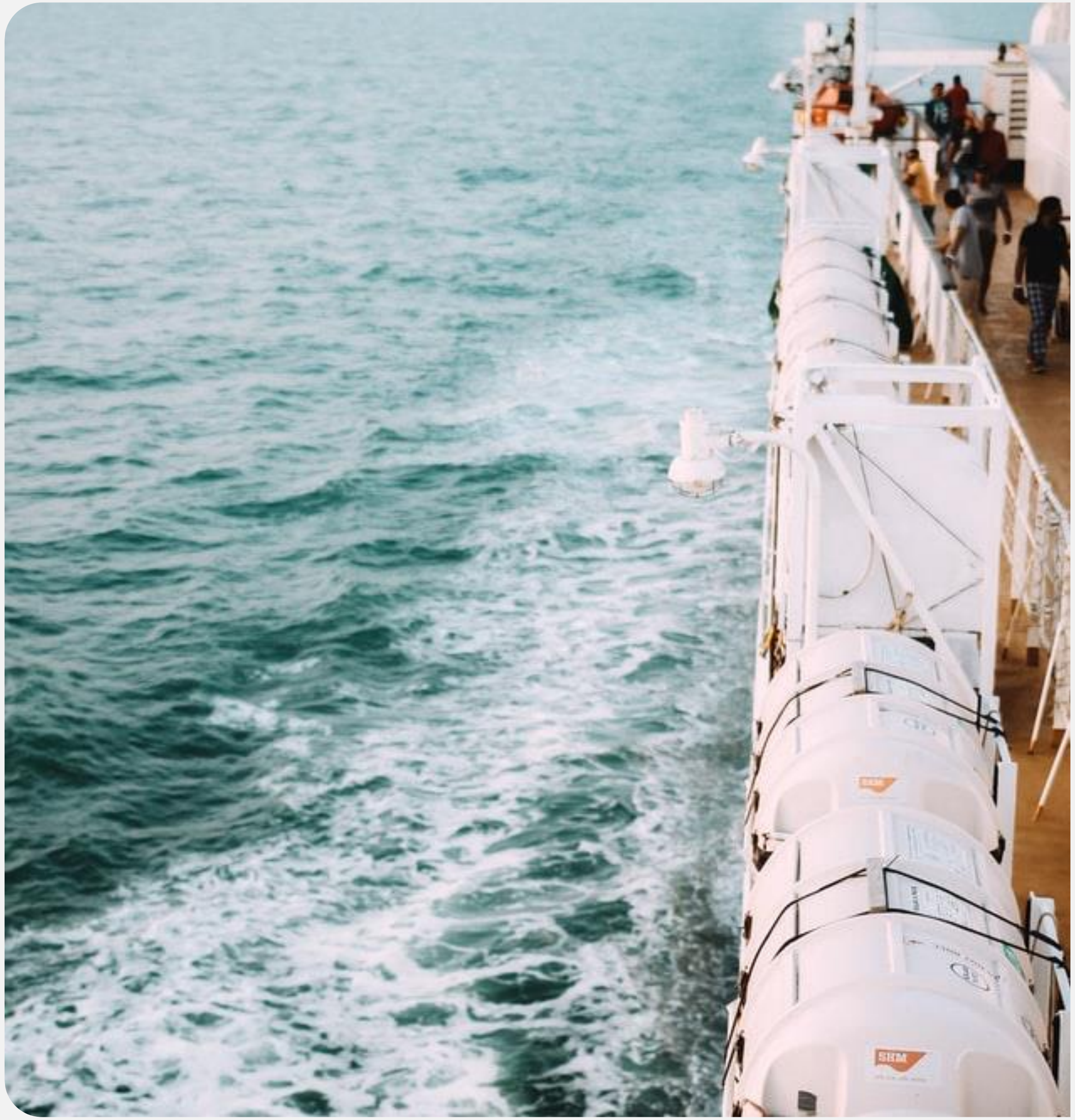
- “Ransomware – It’s not likely to happen to us!”
- “Mail server – It will be offline for an hour at most!”

- Our perception of risk is often subjective and influenced by our biases, in particular our confidence and our mindfulness of how our analysis and response to the risk in question may impact our professional reputation.

Most people tend to overestimate their capability to treat with risks for which they are responsible

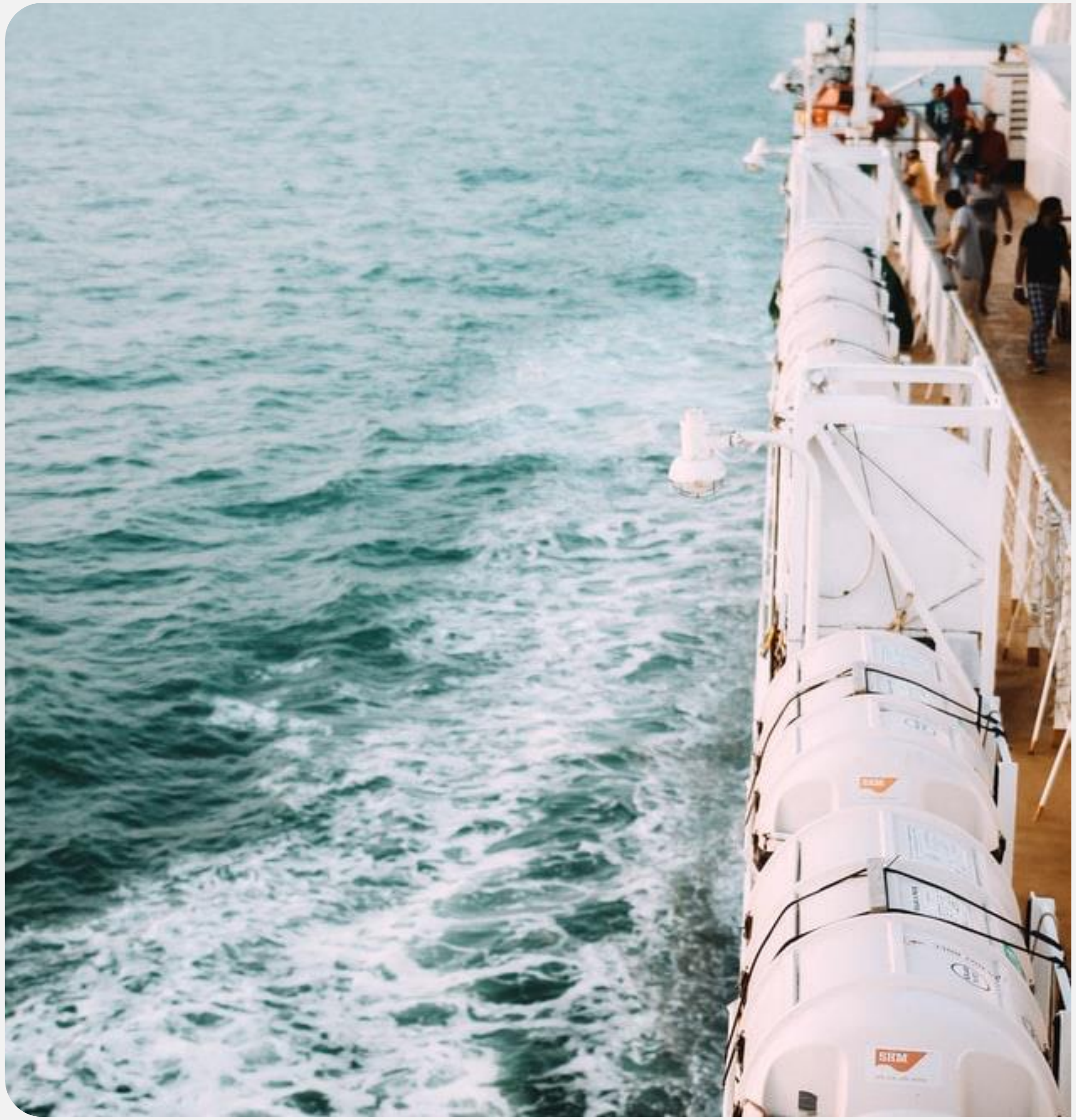
- "Ransomware – <u>IF</u> it does happen to us, we can probably manage it without outside help"
- "Mail server – It will be offline for an hour at most, but I can have it back up in 30 minutes, maybe 45"

- These factors also directly relate to a bias, by some, towards optimism in risk assessment, and can often run counter to the desirable behaviours related to mindfulness, transparency & honesty.



The misconception of risk is quite common

- Decisions in Risk Analysis, Evaluation & Treatment are sometimes made based on information, views or opinions that (sometimes) are incorrect due to faulty thinking and/or understanding.
- The common example: compliance vs. risk/security
- To address:
  - Include a diversity of viewpoints in decision making.
  - Probe with “High Contrast Questions”
  - Acknowledge and avoid “Target fixation”
    - Obsessive focus on the information risk associated with a specific threat or vulnerability.



Too much of Risk Management is focussed on compliance vs. commitment.

- Clearly the antithesis to commitment, and counter to proactivity, transparency, and responsibility.
- Compliant behaviour implies making the minimum effort necessary to achieve good performance to a predefined standard.
- Committed behaviour is intrinsically motivated and self-directed. Being committed implies that people are emotionally impelled to invest in risk management.
- Success in risk management often depends on the ability to modify behaviours across the organization.
- Compliance largely depends on supervision and policing while commitment depends on persons taking responsibility and ownership.

Too much of Risk Management is focussed on compliance vs. commitment.

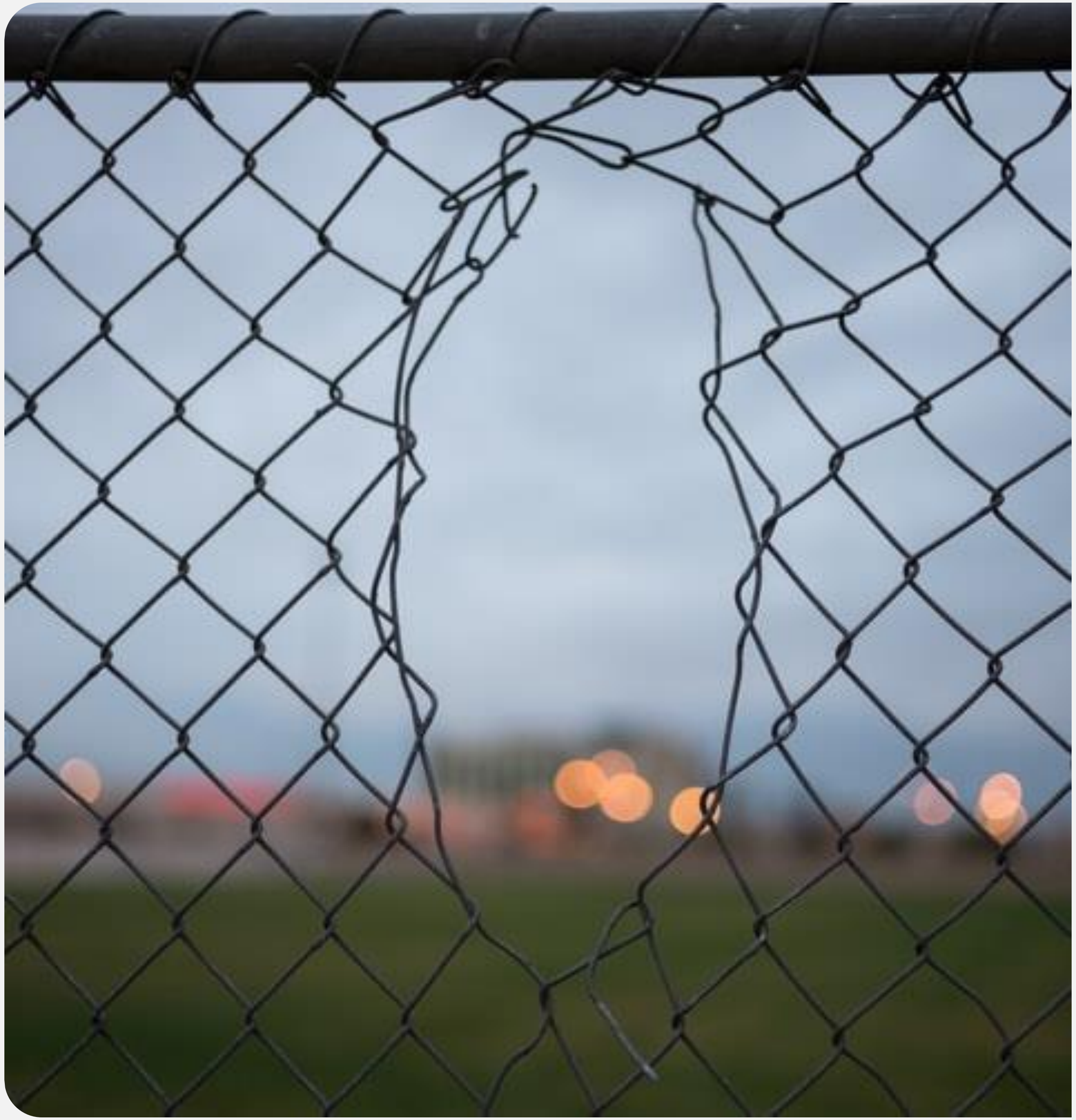
- To address: Target specific behaviour with well crafted (risk) awareness programs that focus on the root causes of risky behaviour and improve culture
- Five psychological factors influencing security (and risk) awareness and behaviour:
  - Encourage knowledge of policy
  - Encourage self-interest in risk management.
  - Improve perception of the risk to the organization
  - Heighten the emotional commitment to effective risk management.
  - Address the perception that secure behaviour imposes a high burden.

Risk doesn't always need to be reduced to the lowest level

- Risk **Management** should be the primary focus rather than risk elimination.
- Quite often there is an acceptable point, above the lowest rating at which the likelihood and/or impact of a risk can be accepted.
- "As low as reasonably possible" is a reasonable goal, however "as low as acceptable" is often worth consideration. In particular where the costs of controls may be prohibitive.
- To enable this approach we need:
  - Clear ownership of risk (Responsibility)
  - High quality information on which to make decisions (Mindfulness & Transparency)
  - A robust risk acceptance approach

Controls create friction and can also be sources of risk

- Security controls can slow users and business processes by impacting system performance or forcing them to use cumbersome processes.
- High-friction controls therefore impose a “drag coefficient” on business velocity.
- Users react to a high degree of control friction by circumventing the controls whenever possible; as a result, the controls can actually introduce new risks as business users go around IT to get their jobs done.
- Largely relates to the desirable behaviours of Mindfulness & Transparency

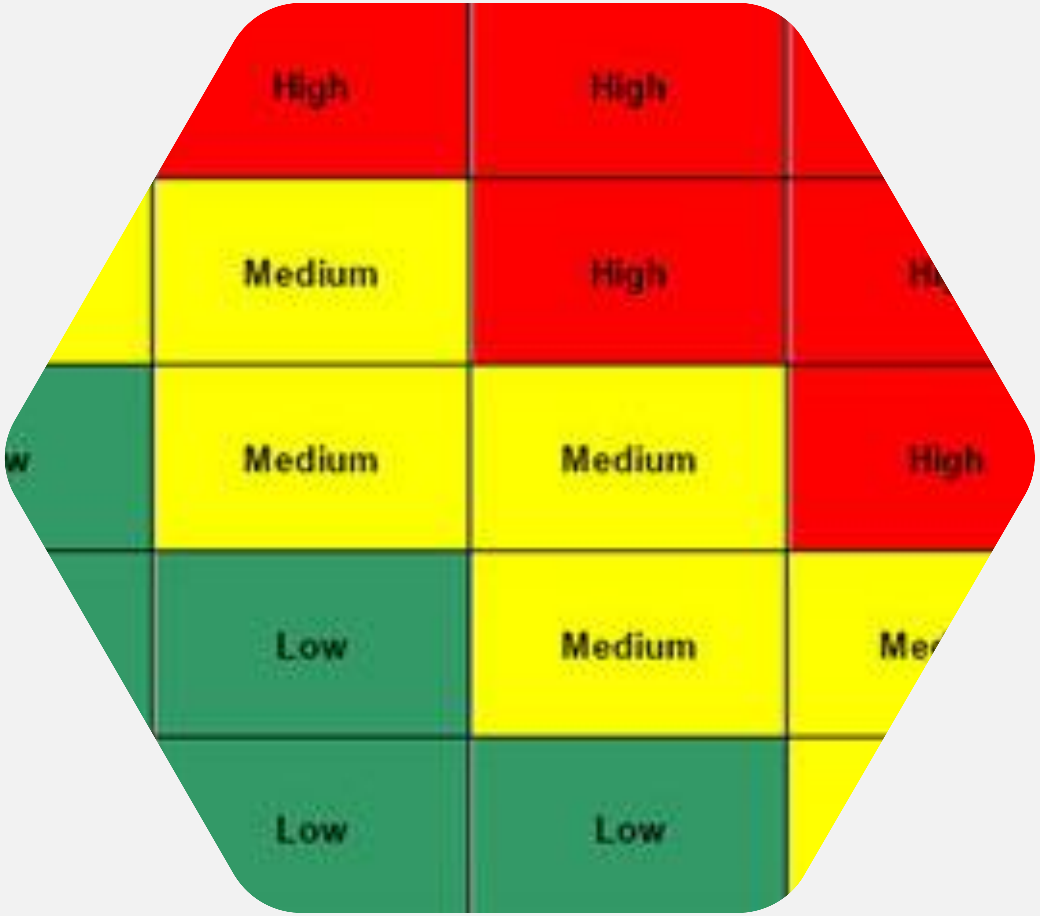


The efficacy of a control deteriorates with time

- Once put in place, security controls tend to remain static, but the environment in which they operate is dynamic.
- Organizations tend to “set and forget”: to install security controls and then fail to update them with security patches or to properly maintain access lists.
- As attackers find new ways to circumvent or compromise the controls, their effectiveness progressively degrades.
- To address:
  - Encourage and provide genuine support for the periodic review of control design effectiveness.

The inefficient use of Risk Matrices (and other tools) can be a source of risk

- Risk Matrices while providing a means to visually describe risks and their potential impact/likelihood, also create opportunities for misperception of risks.
- Consider the potential discussion around:
  - How bad is a yellow risk?
  - How many yellows are a red worth?
  - Is a thousand green risks acceptable?
  - How do multiple risks interact with each other?
- To address:
  - Don’t abandon risk matrices completely
  - Engage business owners, discuss risk in real terms.
  - Storyboard and Simulate
  - Allow for a graduated approach to more mature methods (e.g. quantitative approaches)



Questions?

References

- https://www.protechtgroup.com/blog/key-elements-to-creating-and-maintaining-a-good-risk-culture
- https://www.pmi.org/learning/library/understanding-risk-culture-management-5922
- https://www.ey.com/Publication/vwLUAssets/EY-understanding-risk-culture-and-its-challenges/$FILE/EY-understanding-risk-culture-and-its-challenges.pdf
- https://blog.blackswansecurity.com/wp-content/uploads/CISO_Mentor_Modern_Security_Risk.pdf
- https://www.researchgate.net/publication/310802191_What's_Wrong_with_Risk_Matrices_Decoding_a_Louis_Anthony_Cox_paper
- Harkins, Malcolm W.. Managing Risk and Information Security . Apress.