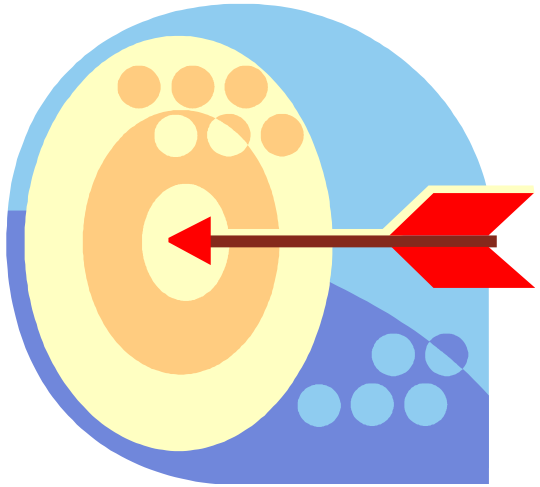
Governance, Risk & Compliance

TOPIC 5 : RISK OPTIMIZATION

Objectives

- Risk Management
- Risk Frameworks
- Risk Appetite vs Risk Tolerance
- Business Continuity & Risk
- Communication of Risk

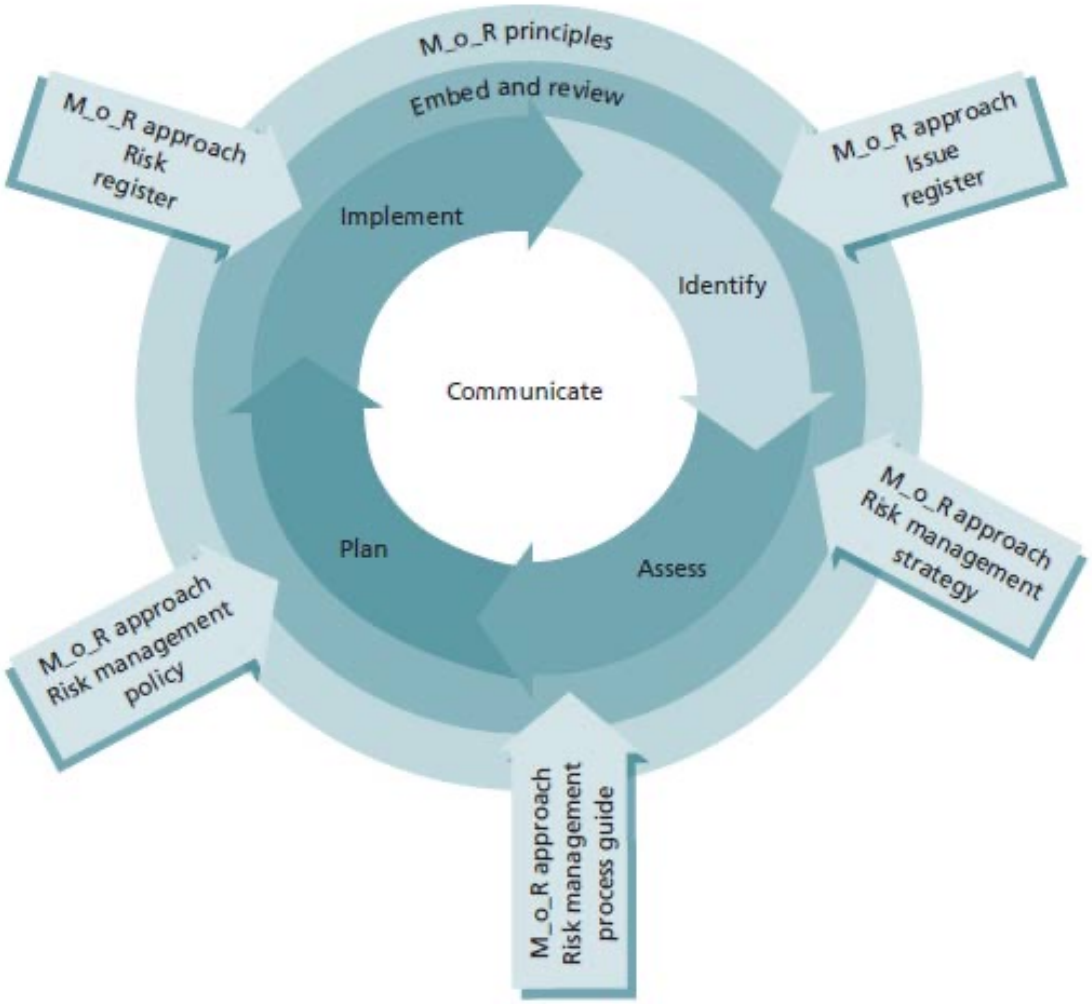


Risk & Risk Management

- Risk is the possibility of an event occurring that will have an impact on the achievement of objectives, and it is typically measured in terms of **likelihood** and **impact**.
- Risk in IT governance is essential due to the fact that today, IT failures can have devastating consequences.
- Good IT governance is a driver for risk management.
- At the higher level, risk management provides guidance to the governance function on its strategic planning while managing the level of risk – Risk Governance.

Risk Frameworks

- The M_o_R (Management of Risk) framework defines four levels of risk.
- Strategic-level risk
  - Risk to IT achieving its objectives
- Program-level risk
  - Risk involving procurement or acquisition, funding, organizational, projects, security, safety and business continuity.



Risk Framework

- Project-level risk
  - Risk concerning people, technical aspects, cost, schedule, resources, operational support, quality, provider failure and security.
- Operational-level risk
  - Risk regarding people, technical aspects, cost, schedule, resources, operational support, quality, provider failure, security, infrastructure failure, business continuity and customer relations.

8 Principles of M_o_R:

- Aligns with objectives
- Fits the context
- Engages stakeholders
- Provides clear guidance
- Informs decision-making
- Facilitates continual improvement
- Creates a supportive culture
- Achieves measurable value.

Risk Framework

- Strategic risk is long-term, in relation to business strategy.
- Program and project levels are on medium-term goals.
- Operational level focus on short-term goals to ensure business services are available.

Risk IT Framework

- ISACA's Risk IT framework helps to implement IT governance and enhance IT-related risk management.
- Aligned closely with COBIT, it consists of 5 domains – risk governance, risk management, risk assessment, risk awareness, reporting & communication and risk response.
- Risk governance
  - Ensure that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted returns.

Risk IT Framework

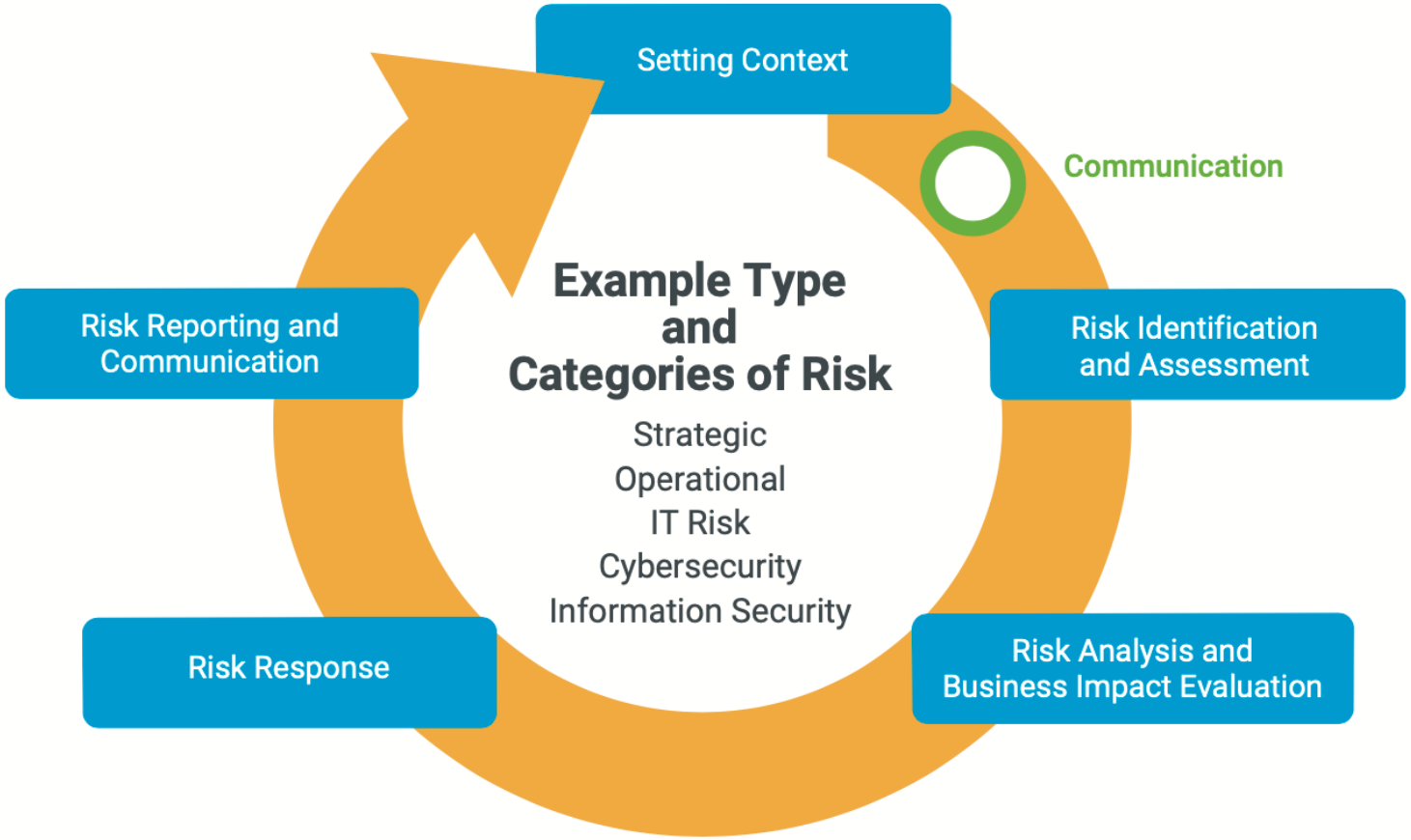
- Risk management
  - Ensures that an effective risk management process is implemented, with the appropriate context and scope applied.
- Risk assessment
  - Ensure that IT-related risks and opportunities are identified, analysed and presented in business terms.
- Risk awareness, reporting & communication
  - Ensure that risk stakeholders are kept aware of timely risk information to be able to act based on these information.

Risk IT Framework

- Risk response
  - Ensure that the appropriate response is applied to the identified risk through one or more of the following:
    - Risk avoidance
    - Risk mitigation
    - Risk sharing or transfer
    - Risk acceptance

Principles of Risk Management

Risk Management Workflow



Risk Appetite vs Tolerance

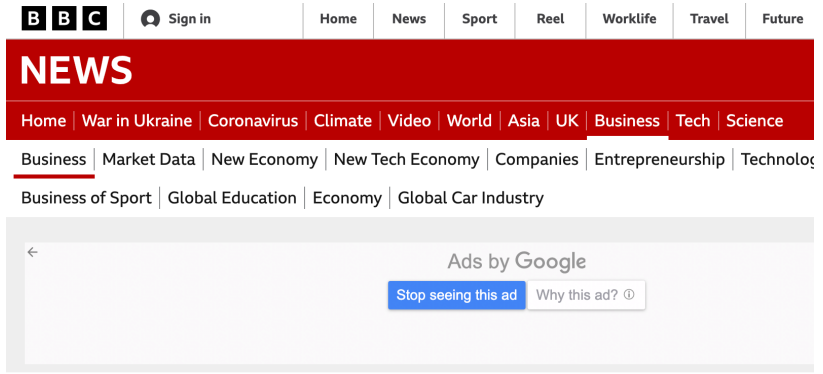
- Risk appetite and risk tolerance are 2 aspects that need to be defined by the Governance function, that is, the Board.
- Risk appetite and tolerance are defined at enterprise level and is reflected in policies set by senior management.
- Risk appetite
  - The broad-based amount of risk a company or other entity is willing to accept in pursuit of its mission.
- Risk tolerance
  - The acceptable variation relative to the achievement of an objective.

Risk Appetite

- The amount of risk an entity is prepared to accept when trying to achieve its objectives.
- Two main factors when considering the enterprise's risk appetite levels:
  - The enterprise's objective to absorb loss, e.g., financial loss, reputation damage.
  - The (management) culture or predisposition towards risk taking – cautious or aggressive.
    - What is the amount of loss the enterprise wants to accept to pursue a return?

Risk Tolerance

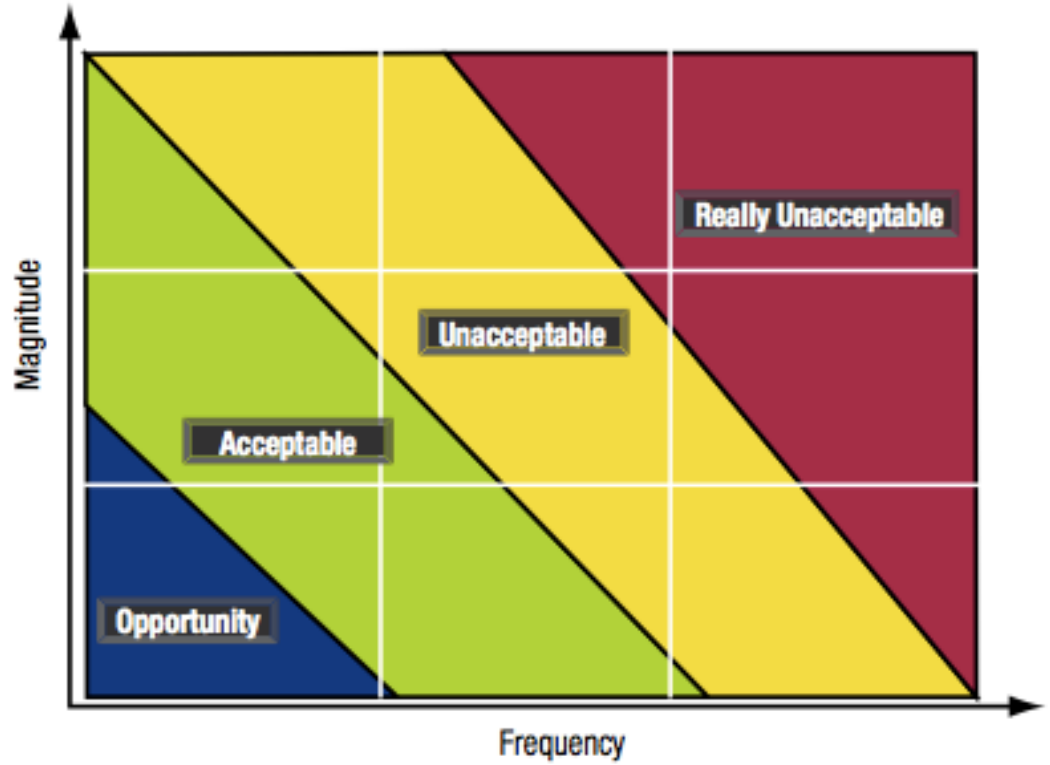
- Tolerable deviation from the level set by the risk appetite and business objectives.
- E.g., projects can tolerate overruns of 10% or 20% overtime.
- Risk tolerance is defined at enterprise level and is reflected in policies set by senior management.
- Explains why some companies chose to terminate some projects after embarking on them – the risk has evolved and change to the state where it exceeds the risk tolerance.



Dyson has scrapped its electric car project

11 October 2019

Risk Map



Risk Map showing the bands of risk based on frequency of possible loss.

Other Risk Management Frameworks

- Other Enterprise Risk Management (ERM) frameworks exist.
  - COSO ERM Framework
  - ISO 32000
  - M_o_R
  - OCTAVE
- Other risk-related frameworks.
  - ISO 27000 series
  - ISO 20000

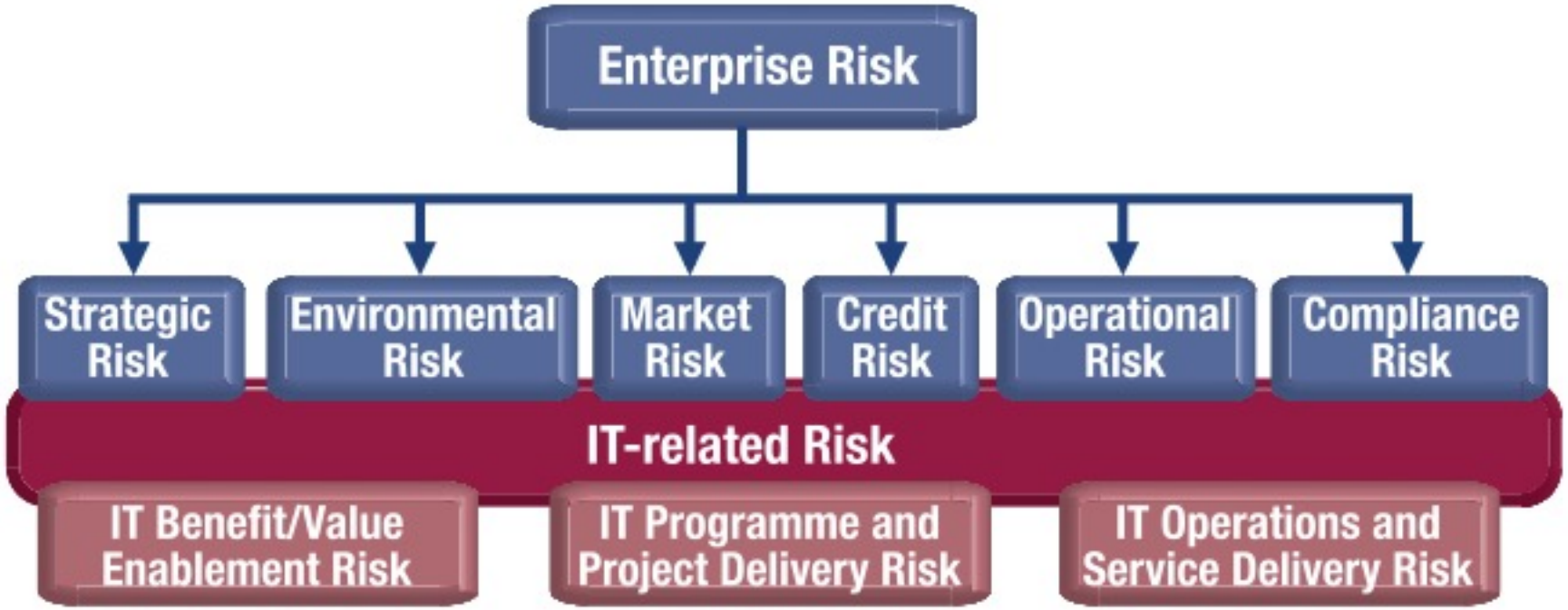
IT Risk Management

- IT risk is a component of the overall risk of the enterprise.
- IT risk must be aligned with enterprise risk management.
- Due to use of IT, IT risk is business risk.
- IT risk can be categorized as :
  - IT benefit realization risk : Associated with missed opportunities to use technology to reap benefits such as improving efficiency or enabler for new initiatives.

IT Risk Management

- IT solution delivery/benefit realization risk : Associated with the contribution of IT to new or improved business solutions.
- IT service delivery risk : Associated with the performance and availability of IT services, which can bring destruction or reduction of value to the enterprise.

IT Risk in Risk Hierarchy



Business Continuity & Risk Management

- The presence of business continuity processes have a positive impact on the impact of business outage.
- By doing so, it can also affect the risk appetite of the enterprise as a whole.
- Generally, an organization with an effective BCM practice may undertake greater risk with the expectation of more gains.
- Reduction of impact is generally a good thing for risk management.

Risk Categories

- Risk can be classified into the following categories:
  - Inherent risk
  - Control risk
  - Detection risk
  - Residual risk

Quantitative and Qualitative Risk Assessment

- Qualitative uses expert opinions to estimate the likelihood and business impact of adverse events.
- Usually used when limited or low quality information is available.
- Has a high level of subjectivity due to variance in human judgment.
- But it is less complex and also less expensive.

Quantitative and Qualitative Risk Assessment

- Quantitative calculates risk based on statistical methods and data, usually from historical records.
- More objective than quantitative, though in many cases, past performance do not necessarily determine future behaviour.
- More expensive to determine but preferred as it provides better input for judgment.

Qualitative Risk Assessment

No.	Asset	Threat	Threat Likelihood [TL]	Threat Impact [TI]	Risk Level TL x TI
1	Business transaction records	Application errors	High	High	High
		Unauthorized access	Low	High	Low
		Denial of Service	Low	Low	Low
		Hardware failures	Medium	High	Medium
		Malware	High	Low	Low
2	24/7 online processing of business transactions	Application errors	High	High	High
		Unauthorized access	Low	High	Low
		Denial of Service	Low	High	Low
		Hardware failures	Medium	High	Medium
		Malware	High	High	High

Quantitative Risk Assessment

No.	Asset	Threat	Threat Likelihood (no. of incidents) [TL]	Threat Impact (loss per incident) [TI]	Risk Level TL x TI
1	Business transaction records	Application errors	4	$ 50,000.00	$ 200,000.00
		Unauthorized access	0.1	$ 50,000.00	$ 5,000.00
		Denial of Service	1	$ 1,000.00	$ 1,000.00
		Hardware failures	2	$ 50,000.00	$ 100,000.00
		Malware	4	$ 1,000.00	$ 4,000.00
2	24/7 online processing of business transactions	Application errors	4	$ 30,000.00	$ 120,000.00
		Unauthorized access	0.1	$ 30,000.00	$ 3,000.00
		Denial of Service	1	$ 30,000.00	$ 30,000.00
		Hardware failures	2	$ 30,000.00	$ 60,000.00
		Malware	4	$ 30,000.00	$ 120,000.00

Probabilistic Risk Assessment

- Both qualitative and quantitative methods have advantages and otherwise.
- Probabilistic risk assessment attempts to use both methods to create a mathematical model to better determine (and predict) risk.
- Where missing data is present, innovative ways are used to realistically determine and fill in the gaps.

Risk Mitigation Strategies

- When risk is identified, various mitigation techniques are available:
  - Risk avoidance
  - Risk reduction/mitigation
  - Risk sharing/transfer
  - Risk acceptance
- Risk response selection & prioritization aims to assist in selecting the most appropriate technique

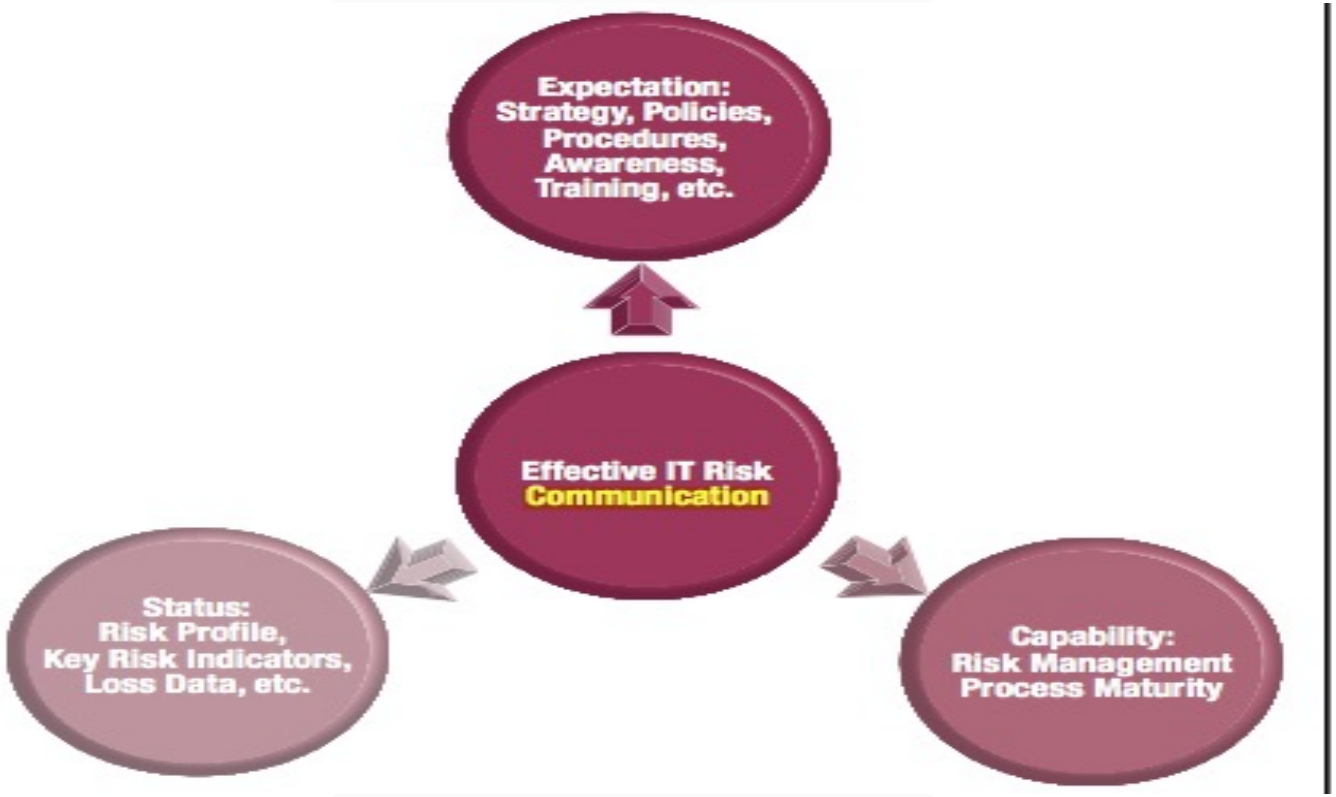
Communication of Risk

- Effective risk management requires effective communication of risk to stakeholders, in particular senior management.
- If done properly, benefits include:
  - Executive management understand the exposure to IT risk.
  - Awareness among all stakeholders and its importance.
  - Transparency to external stakeholders.

Communication of Risk

- Important IT risk communication topics :
  - Policies, procedures, awareness training, etc.
  - Risk management capability and performance information.
  - Operational risk management data such as :
    - Enterprise risk profile
    - Root cause of loss events
    - Threshold for risk

Risk Communication Components



Conclusion

- Risk optimization is not the absolute reduction of risk to its lowest levels.
- Risk optimization is keeping risk at levels which matches the risk appetite of the enterprise.
- Remaining risk is there due to enterprise’s interest in obtaining better returns through adoption of calculated risk.
- Risk has to be communicated to stakeholders

References

- *Everything you wanted to know about Management of Risk (M_o_R®) in less than 1000 words White Paper*, https://www.axelos.com/resource-hub/white-paper/everything-you-wanted-to-know-about-m-o-r-in-less-than-1000-words