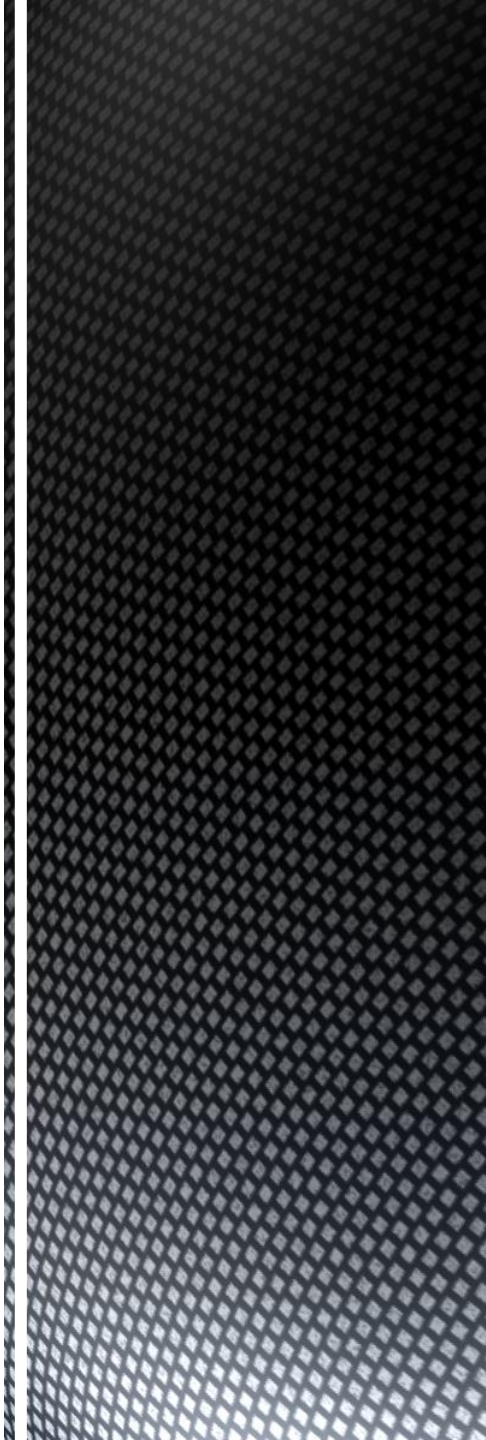
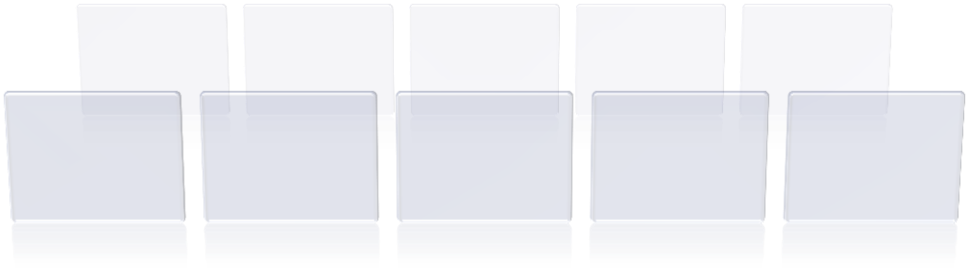
IT Risk Management



Topics

- Benefits of IT risk management
- Components of IT risk management
- High-level approach risk management
- Identifying /Understanding vulnerability
- Implementing cost effective strategies

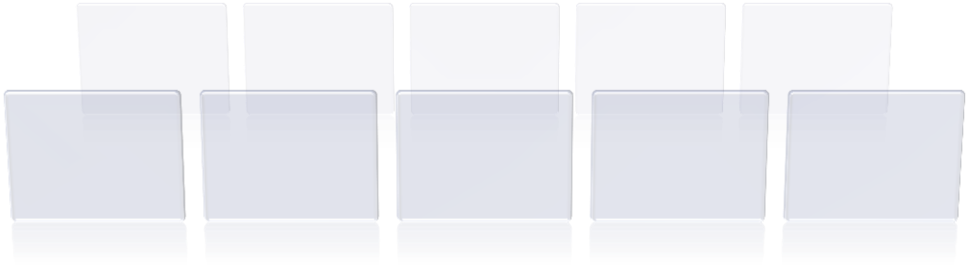


What is Risk ?

- **Risk – Possibility of an event occurring that will have an impact on the achievement of objectives**

- **Measured in terms of Impact & Likelihood**

Risk Management?



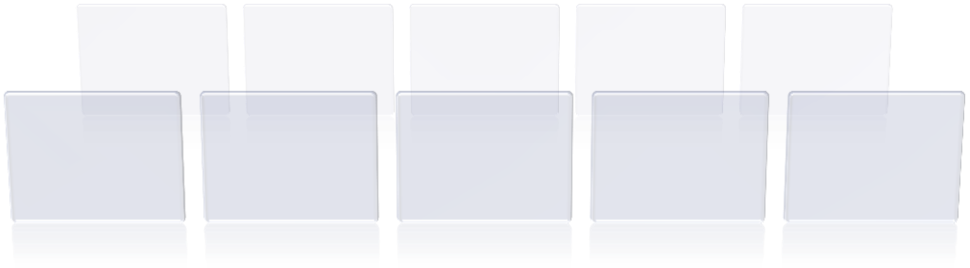
Process of

*Identifying **vulnerabilities** and **threats** to the information resources used by an organization in achieving business objectives,*

and

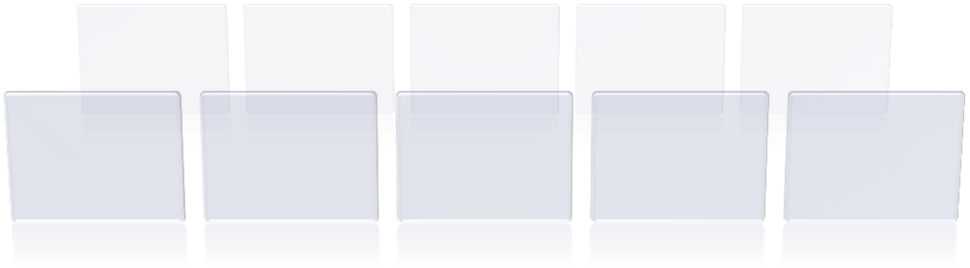
*Deciding what **countermeasures**, if any, to take in **reducing risk to an acceptable level**,*

Based on the value of the information resource to the organization."



Goal

- **As per NIST, the principal goal of enterprise risk management process should be to protect the enterprise and its ability to perform its mission, not just its IT assets.**



Risk Management - Facts

- Firstly, Risk management is an ongoing iterative process
- Second, the choice of countermeasure (computer)s (controls) used to manage risks must strike a balance between productivity, cost, effectiveness of the countermeasure, and the value of the informational asset being protected

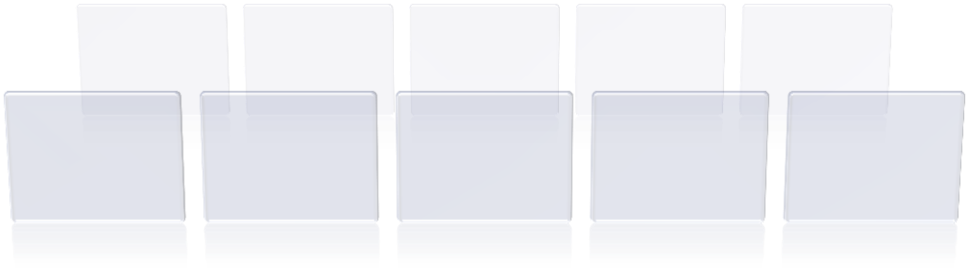
Facts!

- Risk Management addresses the safeguarding of IT assets, disaster recovery and continuity of operations
- About failing to grasp an opportunity to use IT –for example, to improve competitive advantage or operating efficiency- as it is about doing something badly or incorrectly.
- Appropriate frameworks exist and are aligned with relevant standards to identify, assess, mitigate, manage, communicate and monitor IT related business risks

- An element of managerial science concerned with the identification, measurement, control, and minimization of uncertain events. An effective risk management program encompasses the following four phases:

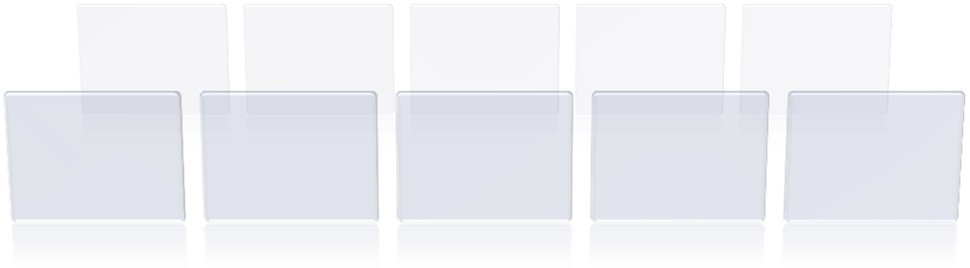
Another Angle!

  - a Risk assessment, as derived from an evaluation of threats and vulnerabilities.
  - Management decision.
  - Control implementation.
  - Effectiveness review.



Types of Risk Management

- Financial
- Operational & Systemic – IT, Information security etc.

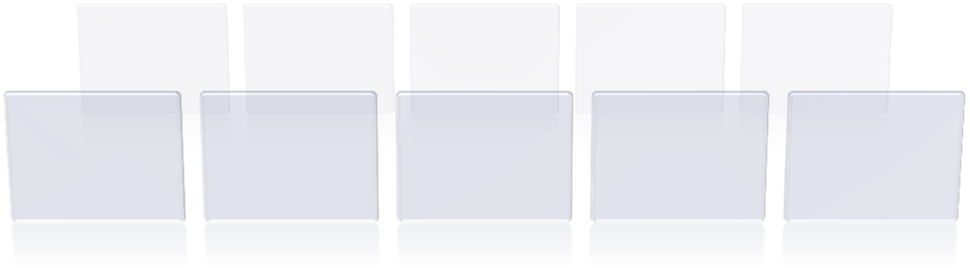


Risk Management Frameworks

- COSO ERM
- MoR
- OCTAVE
- ISO 31000
- AS/NZ 4360:2004

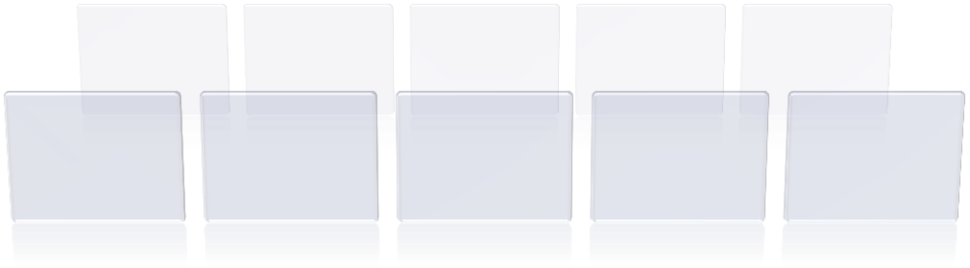
OGC Frameworks

- As per OGC in its Management of Risk (M_o_R) framework, four levels of IT risks
  - Strategic - Objectives
  - Program – Procurement, acquisition, etc
  - Project – People, technical, cost, schedule
  - Operational – People, technical, resources, support, quality etc.



- Define a Framework
- Identify the Risks
- Identify probably risk owners
- Evaluate the risks
- Set acceptable level of risk
- Identify suitable response to risk
- Implement response
- Gain assurance about effectiveness
- Embed and review

RM process - OGC

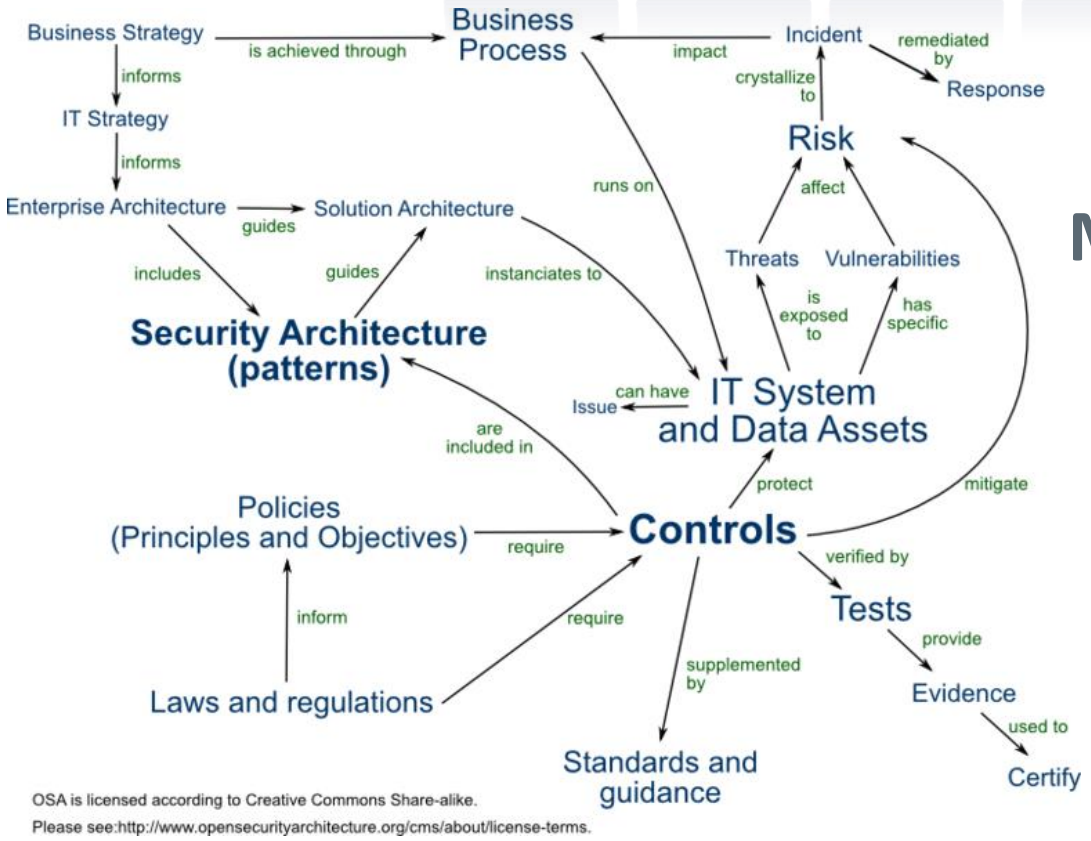


Response

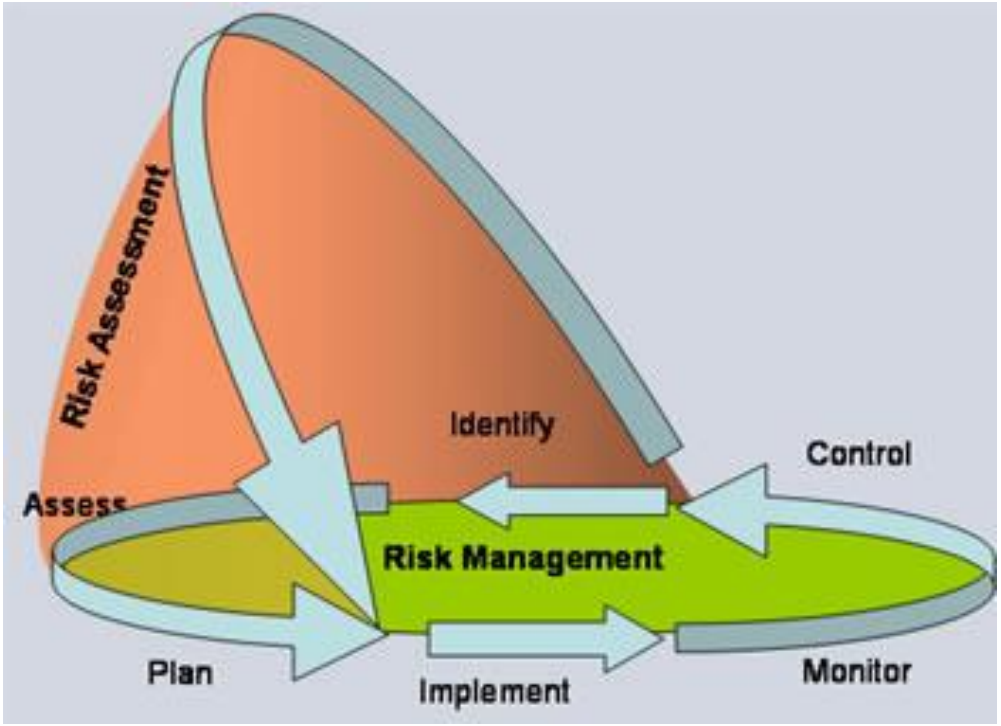
- Mitigate the risk
- Transfer the Risk
- Accept Risk
- Do Nothing

Risk Management process

A Continuous Interlocked Process—Not an Event



Risk Management & Enterprise environment



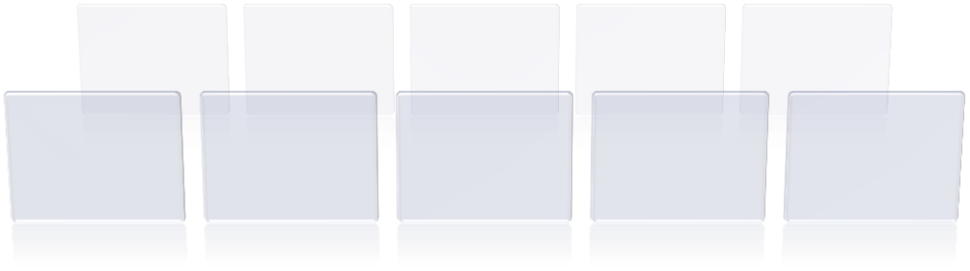
Risk Management & Assessment

- Cornerstone of IT Governance
- Strategic Objectives of the Business will be maintained
- To grasp the opportunity
- Demonstrate good enterprise governance to shareholders and customers
- Regulations

Benefits of IT Risk Management

Important Factors

- Knowledge of the
  - context of risk management
  - Frameworks
  - business objectives
  - enterprises risk management framework
  - external business environment
  - internal environment



Knowledge of

- how the enterprise defines and executes business strategies to achieve its goals and objectives
- how to map business process down to IT process to understand dependencies and root cause
- Enterprise's risk appetite & risk sensitivity
- Enterprise's IT Resources (applications, information, infrastructure, and people)

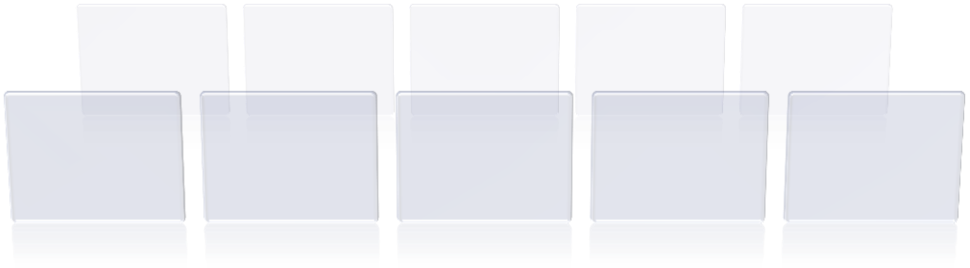
Important Factors

- Ensure the risk management strategies are adopted to mitigate risk and to manage to acceptable residual risk levels

- Implement timely reporting on risk events and responses to appropriate levels of management (including the use of key risk indicators, as appropriate)

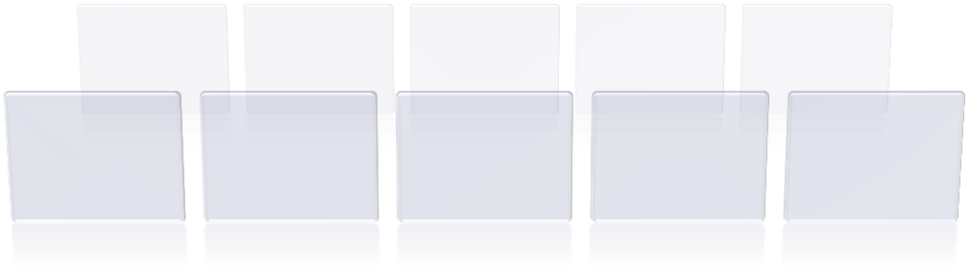
- Establish the monitoring processes and practices to ensure the completeness and effectiveness of established risk management processes

Important Factors



Important Factors

- Threats, vulnerabilities and opportunities inherent in the enterprise's use of IT
- Types of business risks, exposures and threats that can be mitigated with IT
- Quantitative and qualitative methods to determine sensitivity, criticality and maturity of IT related contribution to business success.
- Quantitative and qualitative methods to assess IT risks

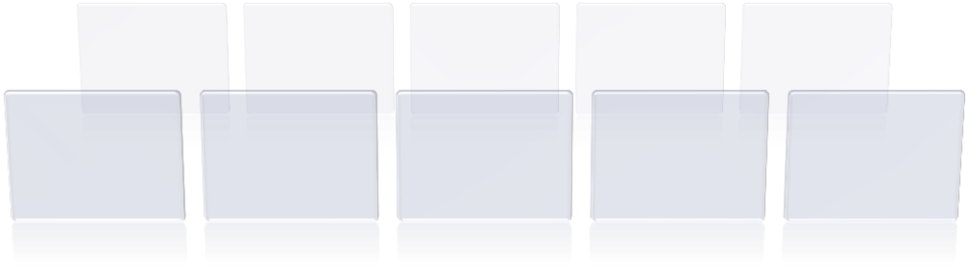


- Methods to discover more rare, but high impact risk types
- Risk mitigation strategies in relation to the use of IT in the enterprise
- Risk management techniques that can be applied to affect enterprise risk management
- Methods to effectively manage and report the status of identified risks

Important Factors

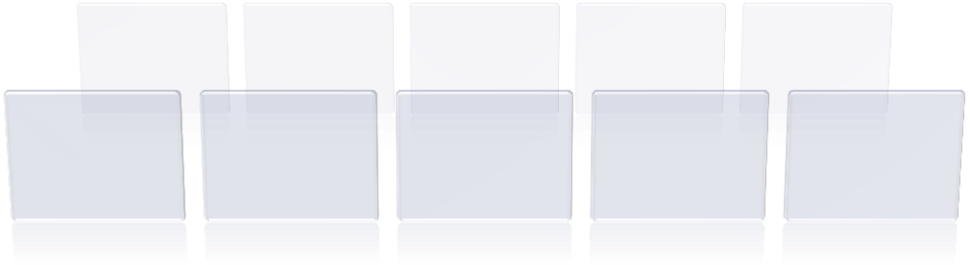
Final words

- Ensure that IT Risk Management is integrated into business strategic and tactical planning process
- Align the IT Risk Management process with the enterprise business risk management framework
- Ensure a consistent application of the risk management framework across the enterprise IT environment
- Ensure that the risk assessment and management is included through out the information life cycle
- Define risk management strategies and prioritize responses to identified risks to maintain risk levels with in the appetite of the enterprise.



Conclusion

- Questions ?



Thanks!