If you know the enemy and know yourself, you need not fear the result of a hundred battles.

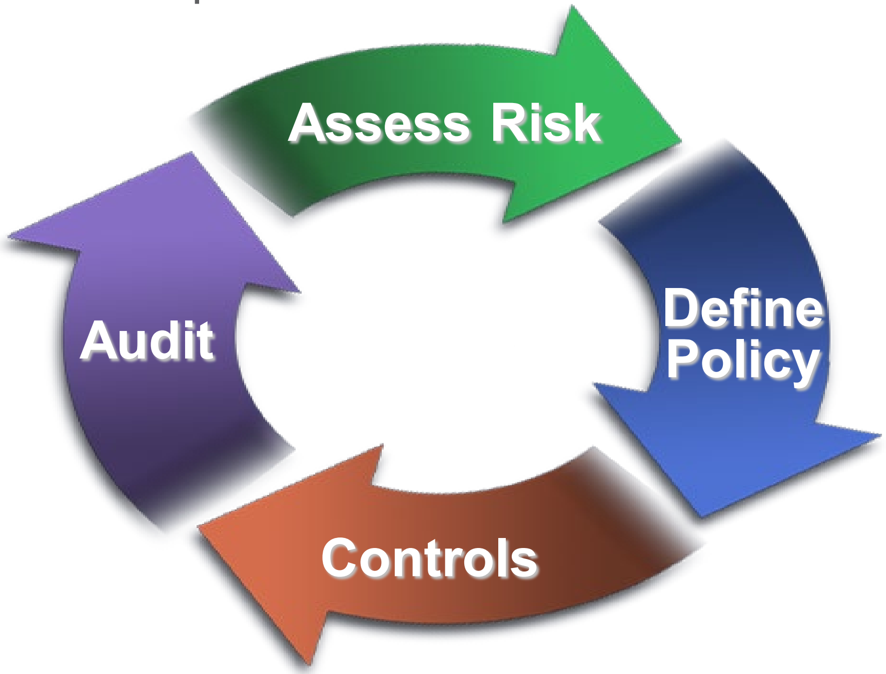
If you know yourself but not the enemy, for every victory gained you will also suffer a defeat.

If you know neither the enemy nor yourself, you will succumb in every battle

General Sun Tzu

Risk Planning - What is a Risk Management Plan?

- Summarises the proposed risk management approach for the business.
- Usually included as a section in the Business Plan or maintained as a separate document.
- It is dependent on the establishment of a *Risk Register*.



Minimum Risk Planning Components

- Identify, analyse, evaluate and treat risks both initially including estimated costings (where practical);
- Transferring approved risk costings into the budget;
- Transferring risk mitigation strategies into Systems (application, network)
- *Reviewing Risk Register* – how often and who will be involved;
- Responsibility for each aspects of risk management;
- Reporting Risk Status
- Snapshot of the major risks, current gradings/score, planned mitigation strategies and costings and who will be responsible for implementing them

Why develop Risk Plan?

- Ensure levels of risk and uncertainty are properly managed
- Strategies of containing the risk and the likely cost of mitigation strategies.
- document risk mitigation strategies being pursued in response to the identified risks and their grading in terms of likelihood and seriousness;
- Risk status can be reported upon;
- Communication of risk management issues to key stakeholders;
- Feedback mechanism
- Identify the mitigation actions required for implementation of the plan and associated costings.

When to Develop a Risk Plan?

- Initial risks must be identified and graded according to likelihood and seriousness
- A *Risk Management Plan* is developed in an iterative manner

Benefits

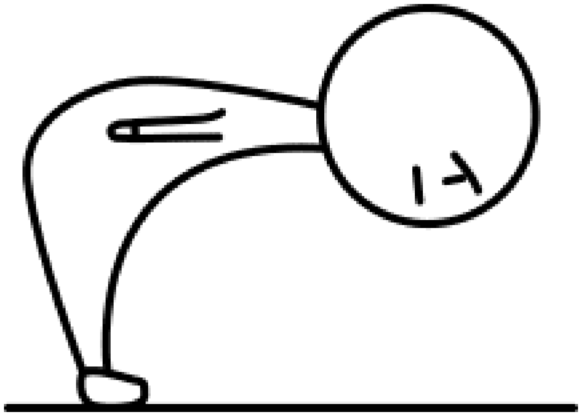
- Management Commitment
  - Manage risk according to business objectives
  - Define organizational roles and responsibilities
- Users and Data
  - Manage to practice of Least Privilege
  - Privacy strictly enforced
- Application and System Development
  - Security built into development lifecycle
  - Layered defense and reduced attack surface
- Operations and Maintenance
  - Security integrated into Operations Framework
  - Monitor, audit, and response functions aligned to operational functions

Sources

www.egovernment.tas.gov.au

Management of information security, Fourth edition 2014, Michael E Whitman

Microsoft Tech Net



Thanks for your attention