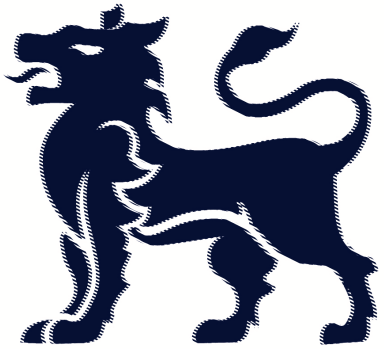


BIRMINGHAM CITY University

MSC CYBER SECURITY

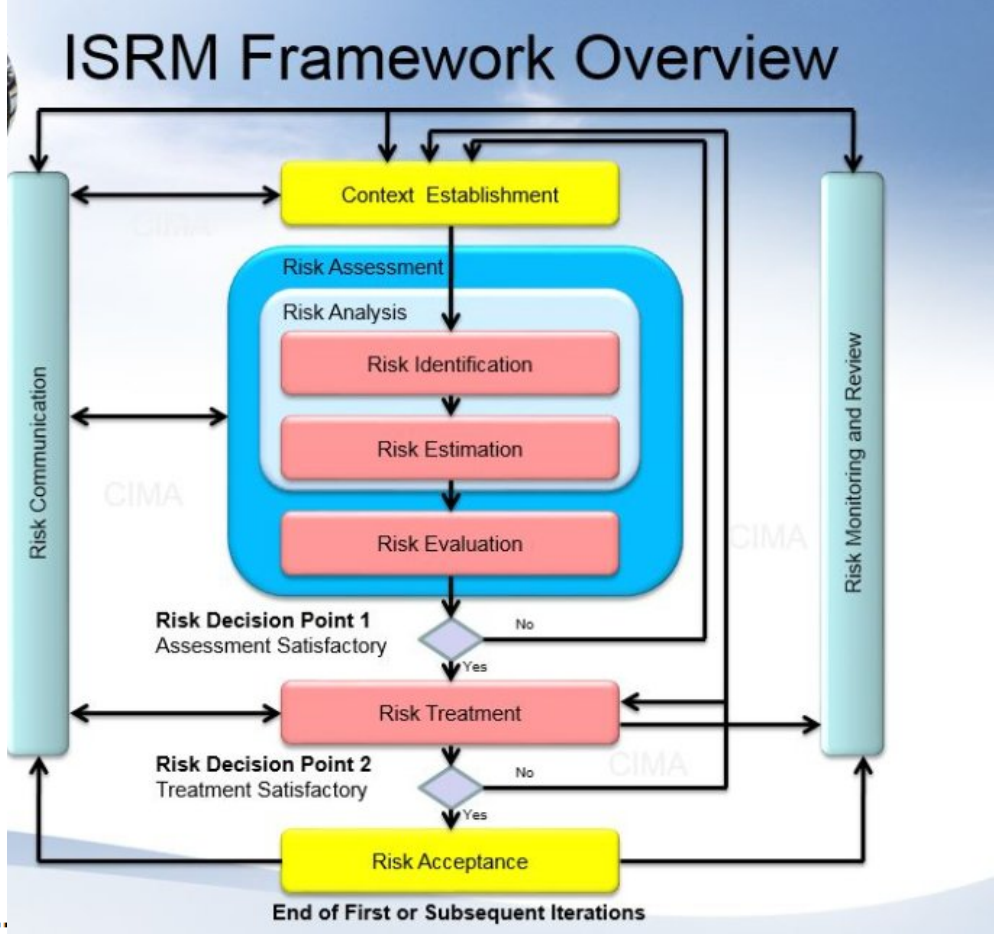
CMP7062 Information Risk Management

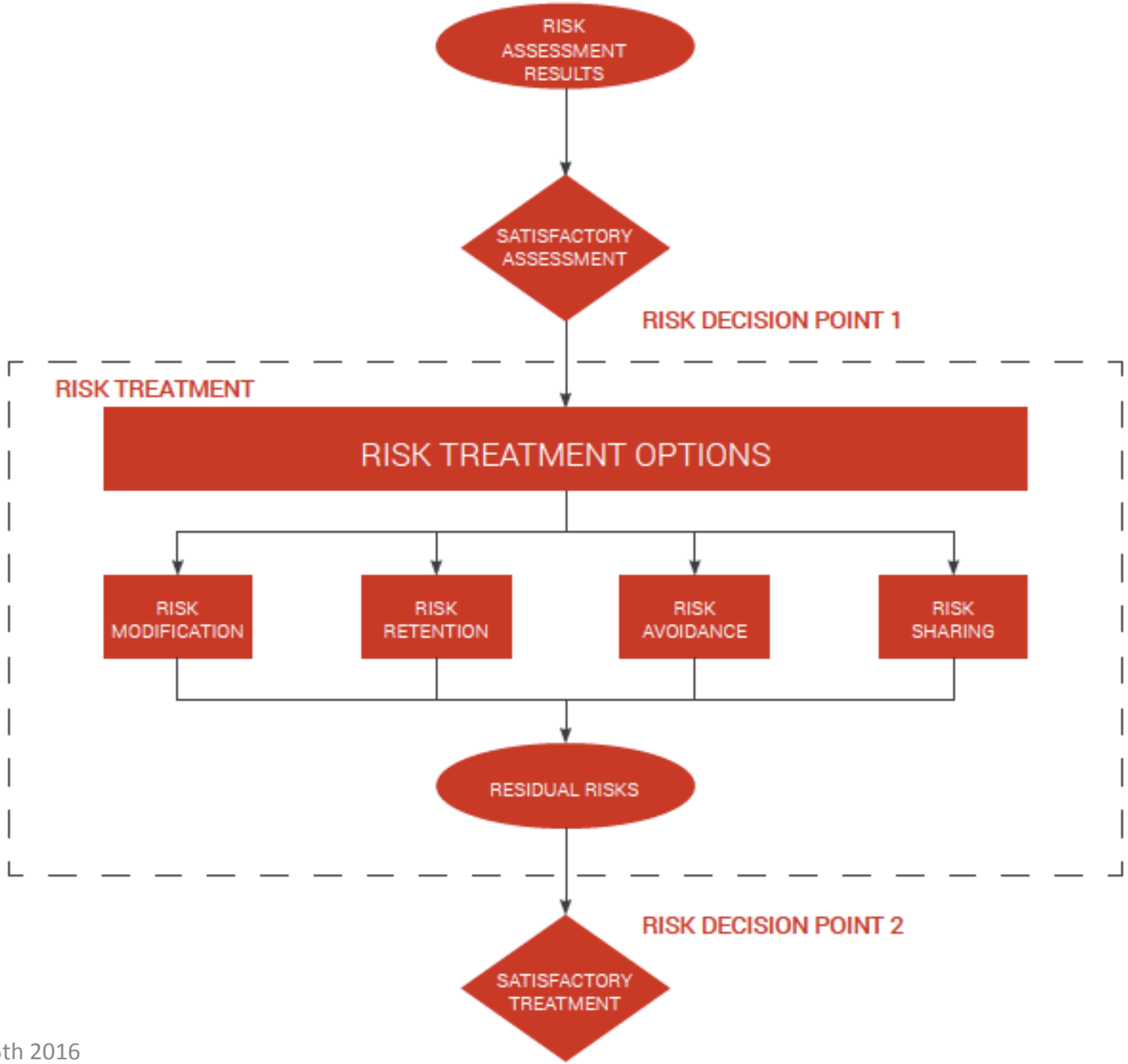
2015/16

Esther Palomar

Week 7 – Risk Treatment Plan

ISO/IEC 27005




RISK ASSESSMENT RESULTS
SATISFACTORY ASSESSMENT
RISK DECISION POINT 1
RISK TREATMENT
RISK TREATMENT OPTIONS
RISK MODIFICATION
RISK RETENTION
RISK AVOIDANCE
RISK SHARING
RESIDUAL RISKS
RISK DECISION POINT 2
SATISFACTORY TREATMENT

Information Risk Treatment Plan

Inputs	Actions – ISO	Outputs
9.0 Information security risk treatment		
9.1 General description of risk treatment		
I1,J1 List of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks	Select controls to reduce, retain, avoid, or transfer the risks Prepare a risk treatment plan	K1 Risk treatment plan K2 Residual risks subject to the acceptance decision of the organization's managers
9.2 Risk Reduction	Reduce risk by selecting controls so that the residual risk can be reassessed as being acceptable	
9.3 Risk Retention	Decide to retain the risk without further action, based on risk evaluation	
9.4 Risk Avoidance	Avoid the activity or condition that gives rise to the particular risk	
9.5 Risk Transfer	Transfer the risk to another party that can most effectively manage the particular risk, based on risk evaluation	

Risk treatment options: Risk Reduction/Modification

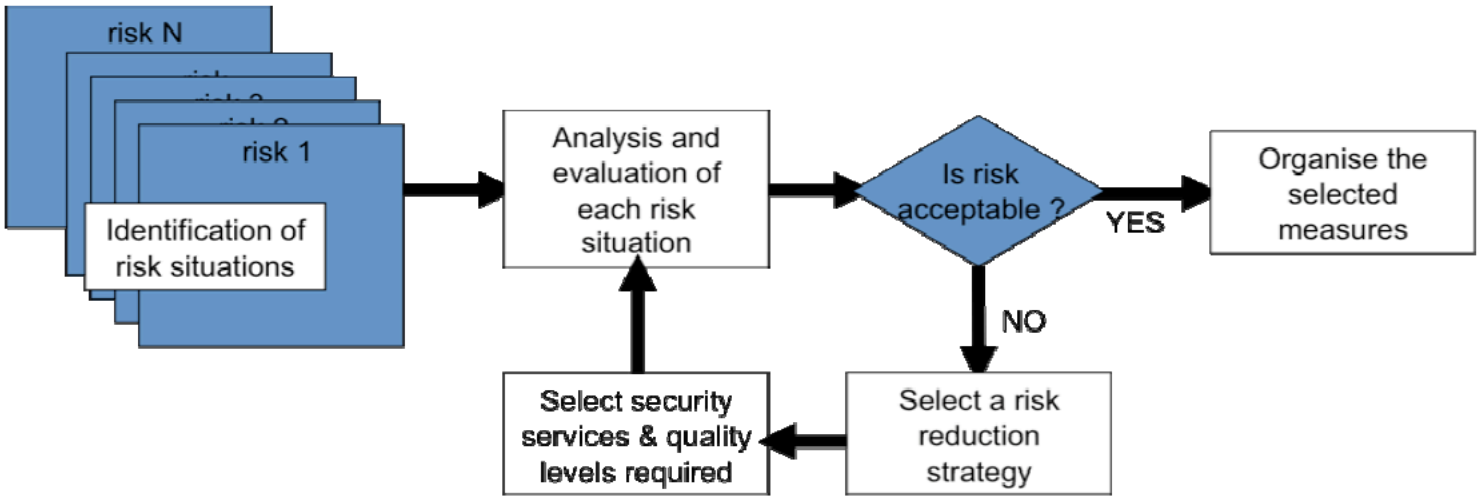
- Controls (measures, e.g., usually the introduction of a technology, process, procedure or employee training) are implemented to reduce the risk.
- It generally affects the vulnerability.
- ISO/IEC 27002 proposes a set of controls.
- Constraints for risk reduction exist
  - Time, financial, technical, etc…

A non-exhaustive list suggested in the ISO/IEC 27002

- Labelling of all media based on how they are classified.
- Access restrictions.
- A continually updated list of those authorised to receive information.
- Data entry and output validation controls.
- Data protection prior to publication or transmission.
- Media storage and periodical review of publication and distribution lists.
- Etc…

Directly reducing risk using a knowledge base

- Risk scenario knowledge base in which pertinent security measures are referenced for each scenario.



Direct risk reduction by the activity/ project/process manager

- When circumstances in which risk may occur are completely defined.
- Directly manage the solution to be implemented.
- Economical.
- Decision could be to simply modify the process.

Indirect treatment of critical risks

- When risks are defined based on threats and vulnerabilities.
  - Reduce vulnerabilities.
- Two-ways links to global/theme-based security policies, or security operational manual.

Risk treatment options: Risk retention

- Risk is accepted.
  - Nothing is done to reduce it.
- Generally when risk level is less than risk acceptance value.

Risk treatment options: Risk avoidance

- Risk is refused:
  - "business" function cancelled.
- Generally if the risk is too high and that no "cost-effective" solution is found.

Risk treatment options: Risk transfer/ sharing

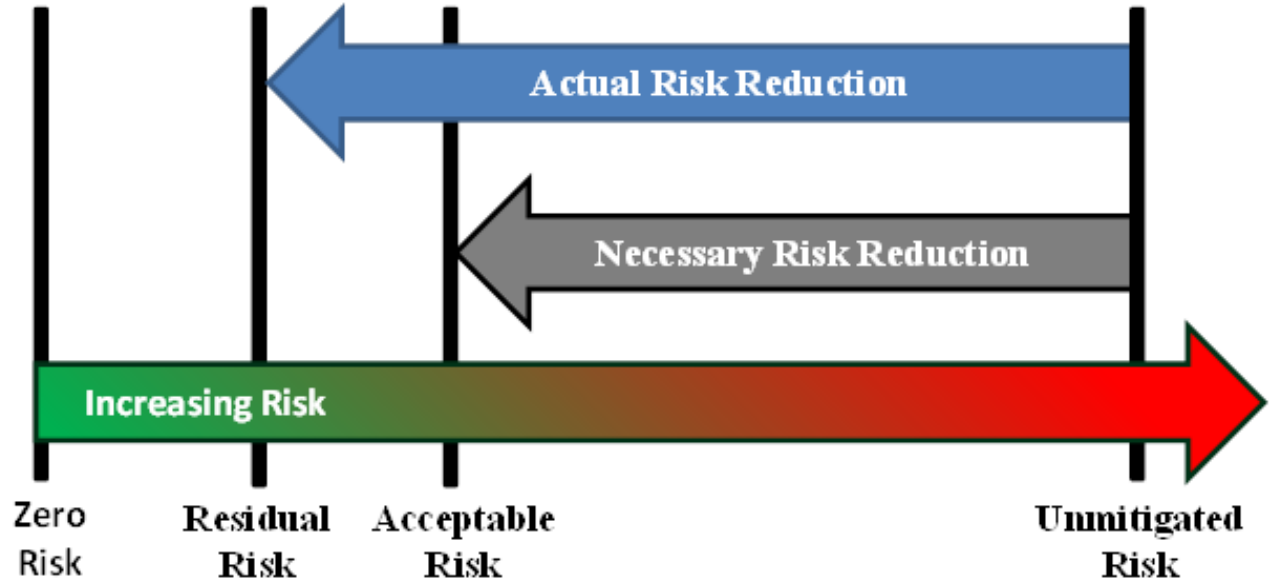
- Risk is transferred or shared with third party:
  - Outsourcing.
  - Acquisition of insurance.
- Generally for high impact risks with low occurrence.
- Can create other risks or modify existing risks.
- Transfer the responsibility to manage the risk but not the liability of an impact.

Risk treatment plan

- The idea of the Risk Treatment Plan is essentially to document how your organization intends to "treat" identified risks, where "treatment" means reduce, avoid, accept or transfer.
- You could set this up as a table or matrix, since many risks will require some combination of treatments and, in virtually all cases, "accept residual risk" is a necessary evil:

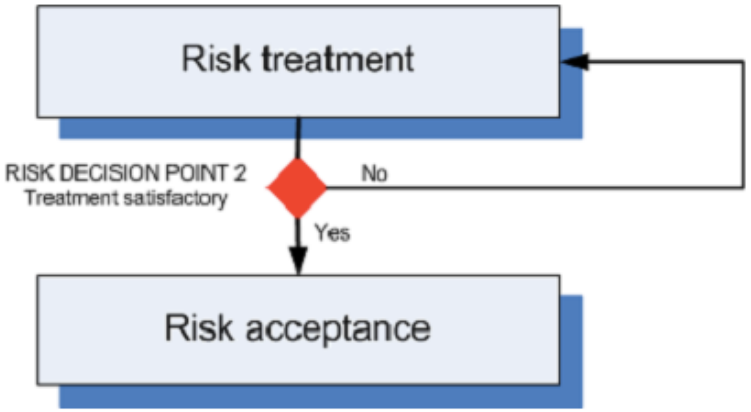
Risk	Treatment			
	Reduce	**Avoid**	**Accept**	**Transfer**
1. Name or describe an information security risk here (with reference to the output of your risk analysis and prioritization process)	Say how you plan to reduce or mitigate the risk through the implementation of suitable information security controls selected from ISO/IEC 27002 or elsewhere	Can you avoid the situation that creates the risk in some way e.g. by good design and pre-planning, or by not doing risky business processes?	If it is not cost effective to completely mitigate a risk, management should openly acknowledge the residual risk	Can you transfer some or all of the risk to a third party, for example an insurer or business partner?
2. Next risk				

An organization generally has a responsibility to assure that risks are within acceptable limits. This first requires defining acceptance limits and then applying mitigation until remaining (or 'residual') risk is within those acceptance limits. The mitigations can take many forms.



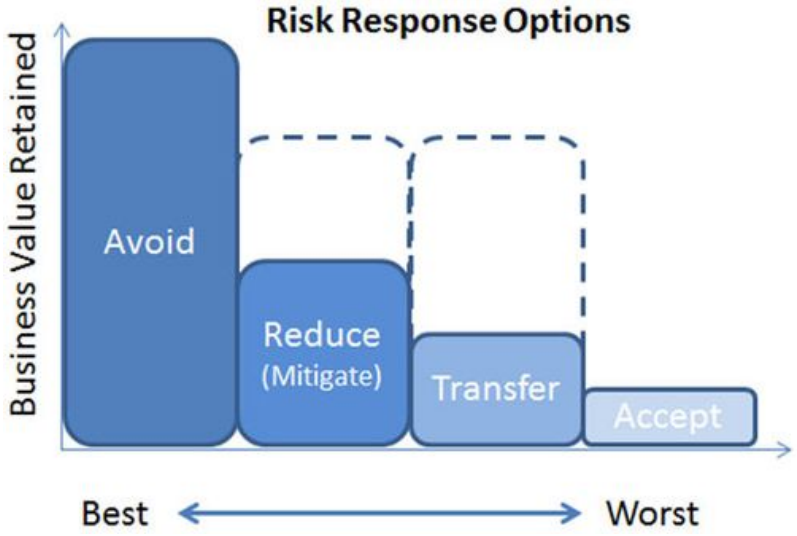
Risk acceptance

- Risks effectively treated.
  - Review of the risk treatment.
  - Validation of selected solutions.
  - Selection of residual risks.



- Residual risks:
  - Accepting a number of risks that can consider itself unable to deal, or are acceptable to the organization.
  - ***Residual risk*** **is the risk left over after you've implemented a risk treatment decision. It's the risk remaining after you've done one of the following: accepted the risk, avoided the risk, transferred the risk, or reduced the risk.**

Residual risks



- The purpose of residual risks is to find out whether the planned treatment is sufficient – the question is, how would you know what is sufficient? This is where the concept of acceptable level of risks comes into play – it is nothing else but deciding how much 'risk appetite' an organization has – each organization has to decide what is appropriate for its circumstances (and for its budget).
- Top management needs to know which risks their company will face even after various mitigation methods have been applied.

Apply any changes to residual risk status

- Once you find out what residual risks are, what do you do with them? Three options:
  - If the level of risks is below the acceptable level of risk, then you do nothing – the management needs to formally accept those risks.
  - If the level of risks is above the acceptable level of risk, then you need to find out some new (and better) ways to mitigate those risks – that also means you'll need to reassess the residual risks.
  - If the level of risks is above the acceptable level of risk, and the costs of decreasing such risks would be higher than the impact itself, than you need to propose to the management to accept these high risks.
- Updating an organization's risk assessment to reflect changes if upgrades to security controls, hardware and software are major due to residual risk.

Evaluation of residual risk

- You should deem residual risks "high" if security controls for the initial risks are weak; "moderate" if security controls for "high" initial risks are adequate, or security controls for the low initial risks are weak; and "low" if security controls for the high, medium or low initial risks are strong, or if security controls for the medium- or low- rated initial risks are adequate.
- Your next step is to identify applied security controls and any resulting residual risk.
  - Replacing security controls that have become out-dated or are no longer available.

Security controls

- **Preventative** security controls, which are designed to avoid information disclosures or alteration of GRC-sensitive information. Examples of preventative security controls include multi-modal biometric authentication, clustered servers, encryption, nested firewalls to block unauthorized networks, and policies to prohibit unauthorized network connections.
- **Detective** security controls, which identify unauthorized or undesired activities after an event has occurred. Examples include intrusion detection systems, automated log monitoring, system audits, virus scanners and file-integrity checkers.

Security controls

- **Corrective** security controls, which respond to and recover from an incident, as well as prevent future occurrences. They also limit further damage from an attack. Corrective security controls include incident response systems, procedures to remove a virus from the infected system, and updated firewall rules to block an attacking IP address.

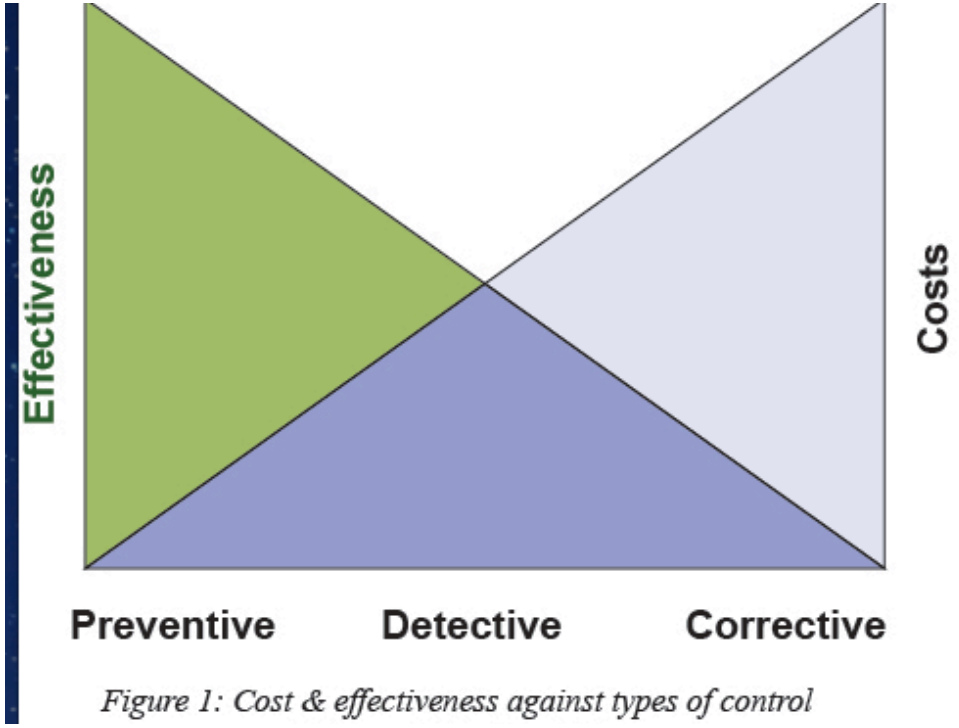


Figure 1: Cost & effectiveness against types of control

Security controls

- **Recovery-focused** security controls, which return the system to production mode after an incident. One example is using a backup tape to restore data after disk failure.
- **Directive** security controls, which outline actions that should be taken to protect sensitive information. Examples include policies, procedures and guidelines.
- **Deterrent** security controls, which discourage security violations. One example is a policy stating that access to servers is monitored in an attempt to discourage unauthorized access.

Next…

References

- BS ISO/IEC 27005:2008
- For more information about the risk management process read ISO 27001 risk assessment & treatment – 6 basic steps.
- ISO/IEC Guide 73:2002, Risk management – Vocabulary- Guidelines for use in standards