Computer Security: Principles and Practice

Chapter 14 – IT Security Management and Risk Assessment

Overview

- security requirements means asking
  - what assets do we need to protect?
  - how are those assets threatened?
  - what can we do to counter those threats?
- IT security management answers these
  - determining security objectives and risk profile
  - perform security risk assessment of assets
  - select, implement, monitor controls

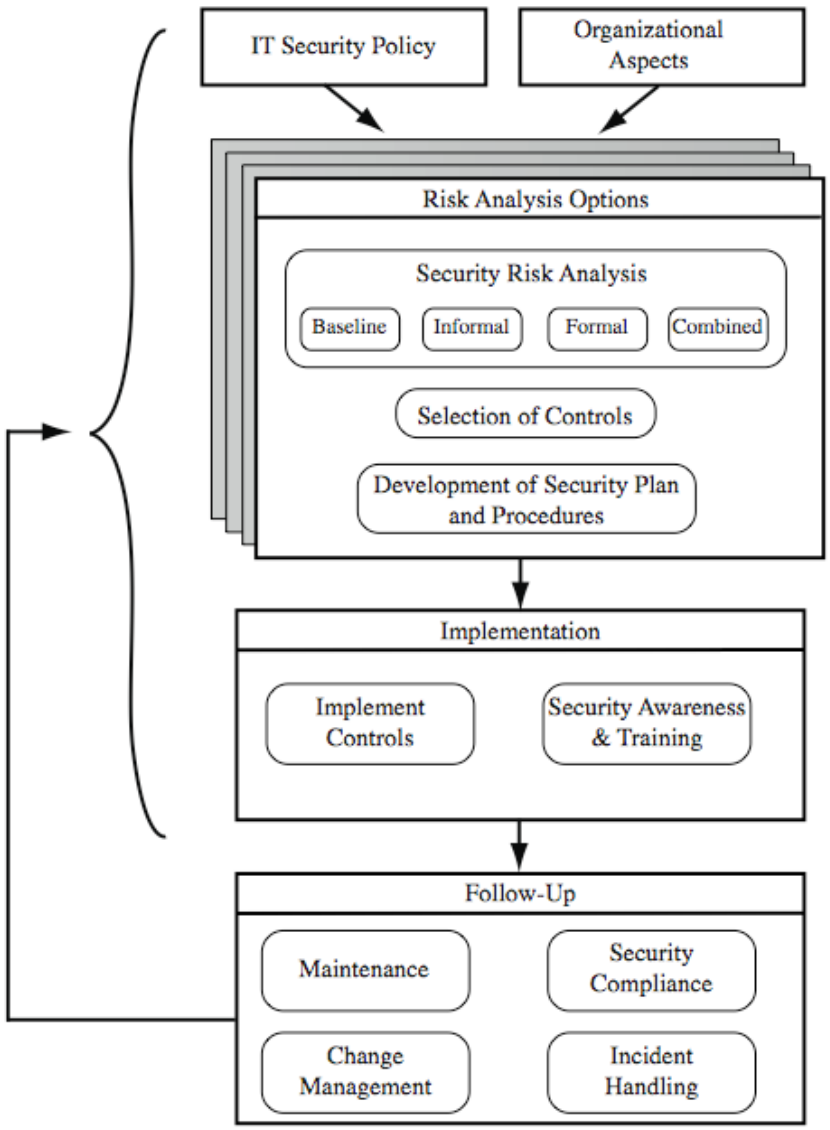
IT Security Management

- **IT Security Management:** a process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:
  - organizational IT security objectives, strategies and policies
  - determining organizational IT security requirements
  - identifying and analyzing security threats to IT assets
  - identifying and analyzing risks
  - specifying appropriate safeguards
  - monitoring the implementation and operation of safeguards
  - developing and implement a security awareness program
  - detecting and reacting to incidents

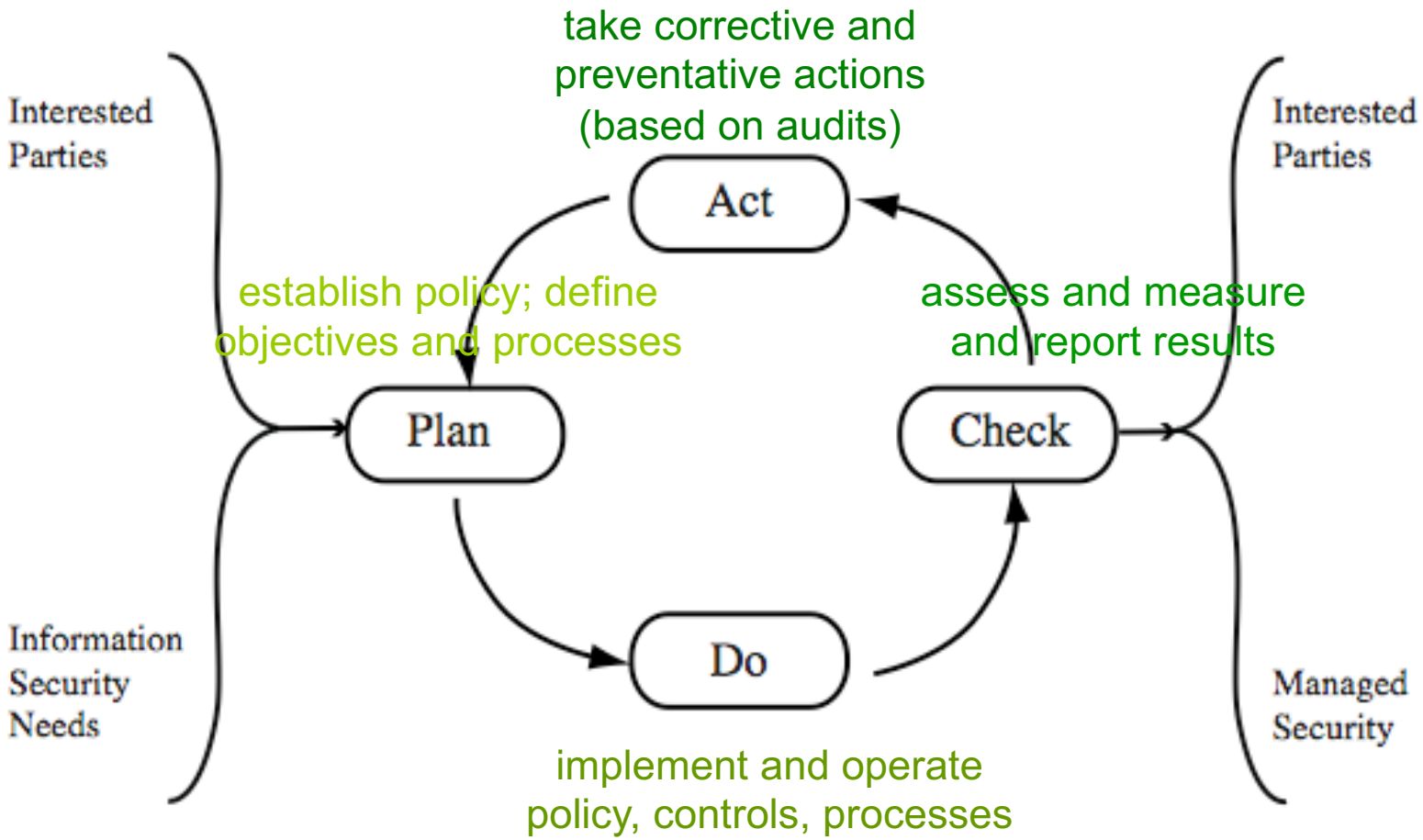
ISO 27000 Security Standards

ISO27000	a proposed standard which will define the vocabulary and definitions used in the 27000 family of standards.
ISO27001	defines the information security management system specification and requirements against which organizations are formally certified. It replaces the older Australian and British national standards AS7799.2 and BS7799.2.
ISO27002 (ISO17799)	currently published and better known as ISO17799, this standard specifies a code of practice detailing a comprehensive set of information security control objectives and a menu of best-practice security controls. It replaces the older Australian and British national standards AS7799.1 and BS7799.1.
ISO27003	a proposed standard containing ***implementation guidance*** on the use of the 27000 series of standards following the "Plan-Do-Check-Act" process quality cycle. Publication is proposed for late 2008.
ISO27004	a draft standard on information security ***management measurement*** to help organizations measure and report the effectiveness of their information security management systems. It will address both the security management processes and controls. Publication is proposed for 2007.
ISO27005	a proposed standard on information ***security risk management***. It will replace the recently released British national standard BS7799.3. Publication is proposed for 2008/9.
ISO13335	provides guidance on the ***management of IT security***. This standard comprises a number of parts. Part 1 defines concepts and models for information and communications technology security management. Part 2, currently in draft, will provide operational guidance on ICT security. These replace the older series of 5 technical reports ISO/IEC TR 13335 parts 1-5.

IT Security Management Process



Plan - Do - Check - Act (Deming Cycle)



Organizational Context and Security Policy

- first examine organization's IT security:
  - objectives - wanted IT security outcomes
  - strategies - how to meet objectives
  - policies - identify what needs to be done
- maintained and updated regularly
  - using periodic security reviews
  - reflect changing technical/risk environments

Security Policy: Topics to Cover

- needs to address:
  - scope and purpose including relation of objectives to business, legal, regulatory requirements
  - IT security requirements
  - assignment of responsibilities
  - risk management approach
  - security awareness and training
  - general personnel issues and any legal sanctions
  - integration of security into systems development
  - information classification scheme
  - contingency and business continuity planning
  - incident detection and handling processes
  - how when policy reviewed, and change control to it

Management Support

- IT security policy must be supported by senior management
- need IT security officer
  - to provide consistent overall supervision
  - manage process
  - handle incidents
- large organizations needs IT security officers on major projects/teams
  - manage process within their areas

Security Risk Assessment

- critical component of process
  - else may have vulnerabilities or waste money
- ideally examine every asset vs risk
  - not feasible in practice
- choose one of possible alternatives based on organization's resources and risk profile
  - baseline
  - informal
  - formal
  - combined

Baseline Approach

- use “industry best practice”
  - easy, cheap, can be replicated
  - but gives no special consideration to org
  - may give too much or too little security
- implement safeguards against most common threats
- baseline recommendations and checklist documents available from various bodies
- alone only suitable for small organizations

Informal Approach

- conduct informal, pragmatic risk analysis on organization's IT systems
- exploits knowledge and expertise of analyst
- fairly quick and cheap
- does address some org specific issues
- some risks may be incorrectly assessed
- skewed by analysts views, varies over time
- suitable for small to medium sized orgs

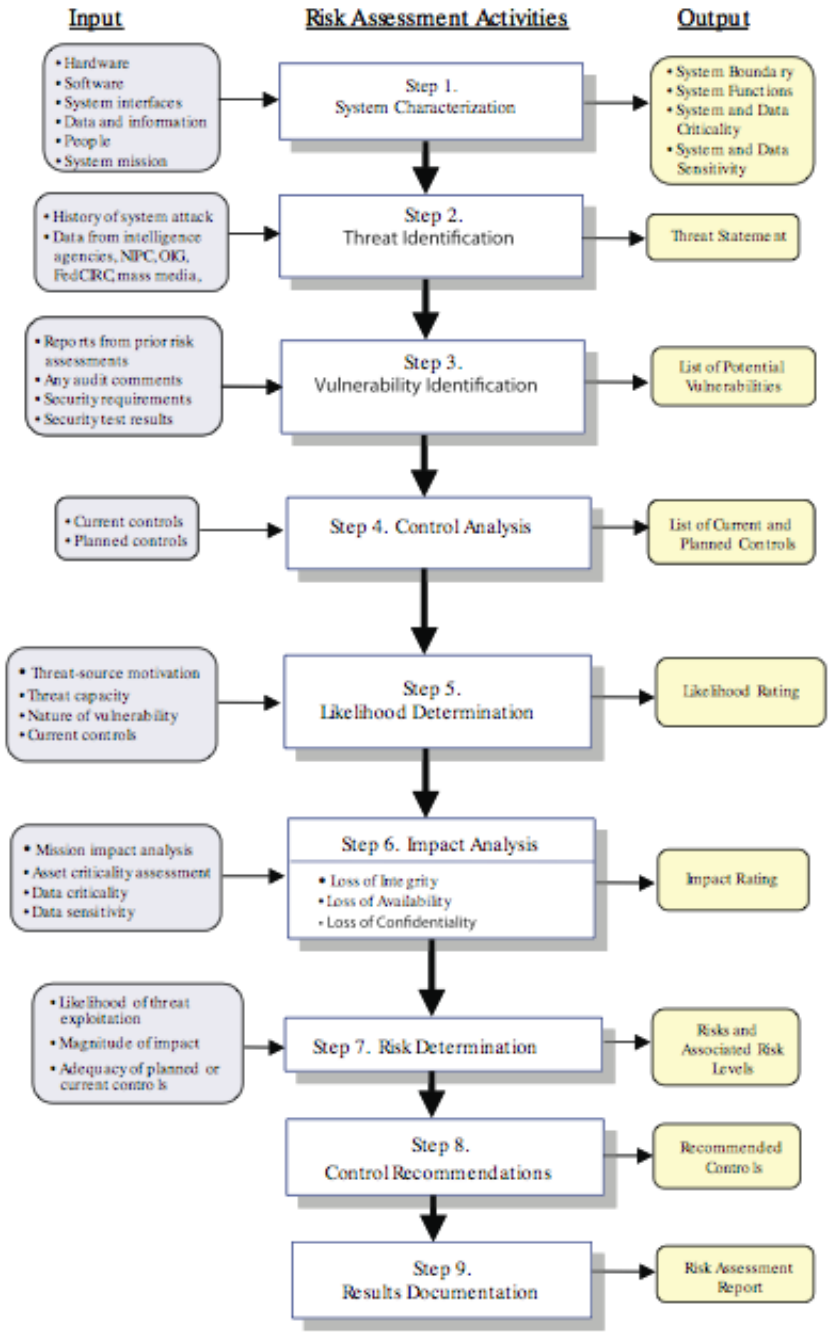
Detailed Risk Analysis

- most comprehensive alternative
- assess using formal structured process
  - with a number of stages
  - identify likelihood of risk and consequences
  - hence have confidence controls appropriate
- costly and slow, requires expert analysts
- may be a legal requirement to use
- suitable for large organizations with IT systems critical to their business objectives

Combined Approach

- combines elements of other approaches
  - initial baseline on all systems
  - informal analysis to identify critical risks
  - formal assessment on these systems
  - iterated and extended over time
- better use of time and money resources
- better security earlier that evolves
- may miss some risks early
- recommended alternative for most orgs

Detailed Risk Analysis Process



Establish Context

- determine broad risk exposure of org
  - related to wider political/social environment
  - legal and regulatory constraints
- specify organization's risk *appetite*
- set boundaries of risk assessment
  - partly on risk assessment approach used
- decide on risk assessment criteria used

Asset Identification

- identify assets
  - "anything which needs to be protected"
  - of value to organization to meet its objectives
  - tangible or intangible
  - in practice try to identify significant assets
- draw on expertise of people in relevant areas of organization to identify key assets
  - identify and interview such personnel
  - see checklists in various standards

Terminology

asset: anything that has value to the organization

threat: a potential cause of an unwanted incident which may result in harm to a system or organization

vulnerability: a weakness in an asset or group of assets which can be exploited by a threat

risk: the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Threat Identification

- to identify threats or risks to assets asK
  - who or what could cause it harm?
  - how could this occur?
- threats are anything that hinders or prevents an asset providing appropriate levels of the key security services:
  - confidentiality, integrity, availability, accountability, authenticity and reliability
- assets may have multiple threats

Threat Sources

- threats may be
  - natural “acts of god”
  - man-made and either accidental or deliberate
- should consider human attackers
  - motivation
  - capability
  - resources
  - probability of attack
  - deterrence
- any previous history of attack on org

Threat Identification

- depends on risk assessors experience
- uses variety of sources
  - natural threat chance from insurance stats
  - lists of potential threats in standards, IT security surveys, info from governments
  - tailored to organization's environment
  - and any vulnerabilities in its IT systems

Vulnerability Identification

- identify exploitable flaws or weaknesses in organization's IT systems or processes
- hence determine applicability and significance of threat to organization
- need combination of threat and vulnerability to create a risk to an asset
- again can use lists of potential vulnerabilities in standards etc

Analyze Risks

- specify likelihood of occurrence of each identified threat to asset given existing controls
  - management, operational, technical processes and procedures to reduce exposure of org to some risks
- specify consequence should threat occur
- hence derive overall risk rating for each threat

  risk = probability threat occurs x cost to organization
- in practice very hard to determine exactly
- use qualitative not quantitative, ratings for each
- aim to order resulting risks in order to treat them

Determine Likelihood

Rating	Likelihood Description	Expanded Definition
1	**Rare**	May occur only in exceptional circumstances and may deemed as “unlucky” or very unlikely.
2	**Unlikely**	Could occur at some time but not expected given current controls, circumstances, and recent events.
3	**Possible**	Might occur at some time, but just as likely as not. It may be difficult to control its occurrence due to external influences.
4	**Likely**	Will probably occur in some circumstance and one should not be surprised if it occurred.
5	**Almost Certain**	Is expected to occur in most circumstances and certainly sooner or later.

Determine Consequence

Rating	Consequence	Expanded Definition
1	**Insignificant**	Generally a result of a minor security breach in a single area. Impact is likely to last less than several days and requires only minor expenditure to rectify.
2	**Minor**	Result of a security breach in one or two areas. Impact is likely to last less than a week, but can be dealt with at the segment or project level without management intervention. Can generally be rectified within project or team resources.
3	**Moderate**	Limited systemic (and possibly ongoing) security breaches. Impact is likely to last ***up to 2 weeks*** and generally requires management intervention. Will have ongoing compliance costs to overcome.
4	**Major**	Ongoing systemic security breach. Impact will likely last ***4-8 weeks*** and require significant management intervention and resources to overcome, and compliance costs are expected to be substantial. Loss of business or organizational outcomes is possible, but not expected, especially if this is a once off.
5	**Catastrophic**	Major systemic security breach. Impact will last for ***3 months or more*** and senior management will be required to intervene for the duration of the event to overcome shortcomings. Compliance costs are expected to be very substantial. Substantial public or political debate about, and loss of confidence in, the organization is likely. Possible criminal or disciplinary action is likely.
6	**Doomsday**	Multiple instances of major systemic security breaches. Impact duration cannot be determined and senior management will be required to place the company under voluntary administration or other form of major restructuring. Criminal proceedings against senior management is expected, and substantial loss of business and failure to meet organizational objectives is unavoidable.

Determine Resultant Risk

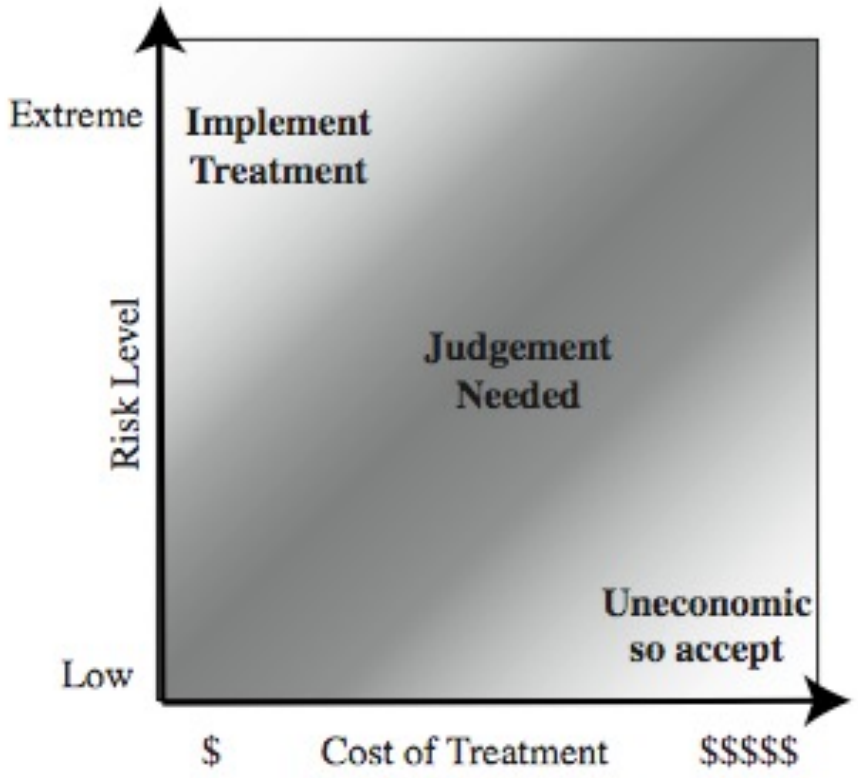
	Consequences					
Likelihood	Doomsday	Catastrophic	Major	Moderate	Minor	Insignificant
Almost Certain	E	E	E	E	H	H
Likely	E	E	E	H	H	M
Possible	E	E	E	H	M	L
Unlikely	E	E	H	M	L	L
Rare	E	H	H	M	L	L

Risk Level	Description
Extreme (E)	Will require detailed r esearch and management planning at an executive/director level. Ongoing planning and monitoring will be required with regular reviews. Substantial adjustment of controls to manage the risk are expected, with costs possibly exceeding original forecasts.
High (H)	Requires management attention, but management and planning can be left to senior project or team leaders. Ongoing planning and monitoring with regular reviews are likely, though adjustment of controls are likely to be met from within existing resources
Medium (M)	Can be managed by existing specific monitoring and response procedures. Management by employees is suitable with appropriate monitoring and reviews.
Low (L)	Can be managed through routine procedures.

Document in Risk Register and Evaluate Risks

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Internet Router	Outside Hacker attack	Admin password only	Possible	Moderate	High	1
Destruction of Data Center	Accidental Fire or Flood	None (no disaster recovery plan)	Unlikely	Major	High	2

Risk Treatment



Risk Treatment Alternatives

- **risk acceptance**: *accept risk (perhaps because of excessive cost of risk treatment)*
- **risk avoidance**: *do not proceed with the activity that causes the risk (loss of convenience)*
- **risk transfer**: buy insurance; outsource
- **reduce consequence**: *modify the uses of an asset to reduce risk impact (e.g., offsite backup)*
- **reduce likelihood**: *implement suitable controls*

Case Study: Silver Star Mines

- fictional operation of global mining company
- large IT infrastructure
  - both common and specific software
  - some directly relates to health & safety
  - formerly isolated systems now networked
- decided on combined approach
- mining industry less risky end of spectrum
- management accepts moderate or low risk

Assets

- reliability and integrity of SCADA nodes and net
- integrity of stored file and database information
- availability, integrity of financial system
- availability, integrity of procurement system
- availability, integrity of maintenance/production system
- availability, integrity and confidentiality of mail services

Threats & Vulnerabilities

- unauthorized modification of control system
- corruption, theft, loss of info
- attacks/errors affecting procurement system
- attacks/errors affecting financial system
- attacks/errors affecting mail system
- attacks/errors maintenance/production affecting system

Risk Register

Asset	Threat/ Vulnerability	Existing Controls	Likelihood	Consequence	Level of Risk	Risk Priority
Reliability and integrity of the SCADA nodes and network	Unauthorized modification of control system	layered firewalls & servers	Rare	Major	High	1
Integrity of stored file and database information	Corruption, theft, loss of info	firewall, policies	Possible	Major	Extreme	2
Availability and integrity of Financial System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	3
Availability and integrity of Procurement System	Attacks/errors affecting system	firewall, policies	Possible	Moderate	High	4
Availability and integrity of Maintenance/ Production System	Attacks/errors affecting system	firewall, policies	Possible	Minor	Medium	5
Availability, integrity and confidentiality of mail services	Attacks/errors affecting system	firewall, ext mail gateway	Almost Certain	Minor	High	6

Summary

- detailed need to perform risk assessment as part of IT security management process
- relevant security standards
- presented risk assessment alternatives
- detailed risk assessment process involves
  - context including asset identification
  - identify threats, vulnerabilities, risks
  - analyse and evaluate risks
- Silver Star Mines case study