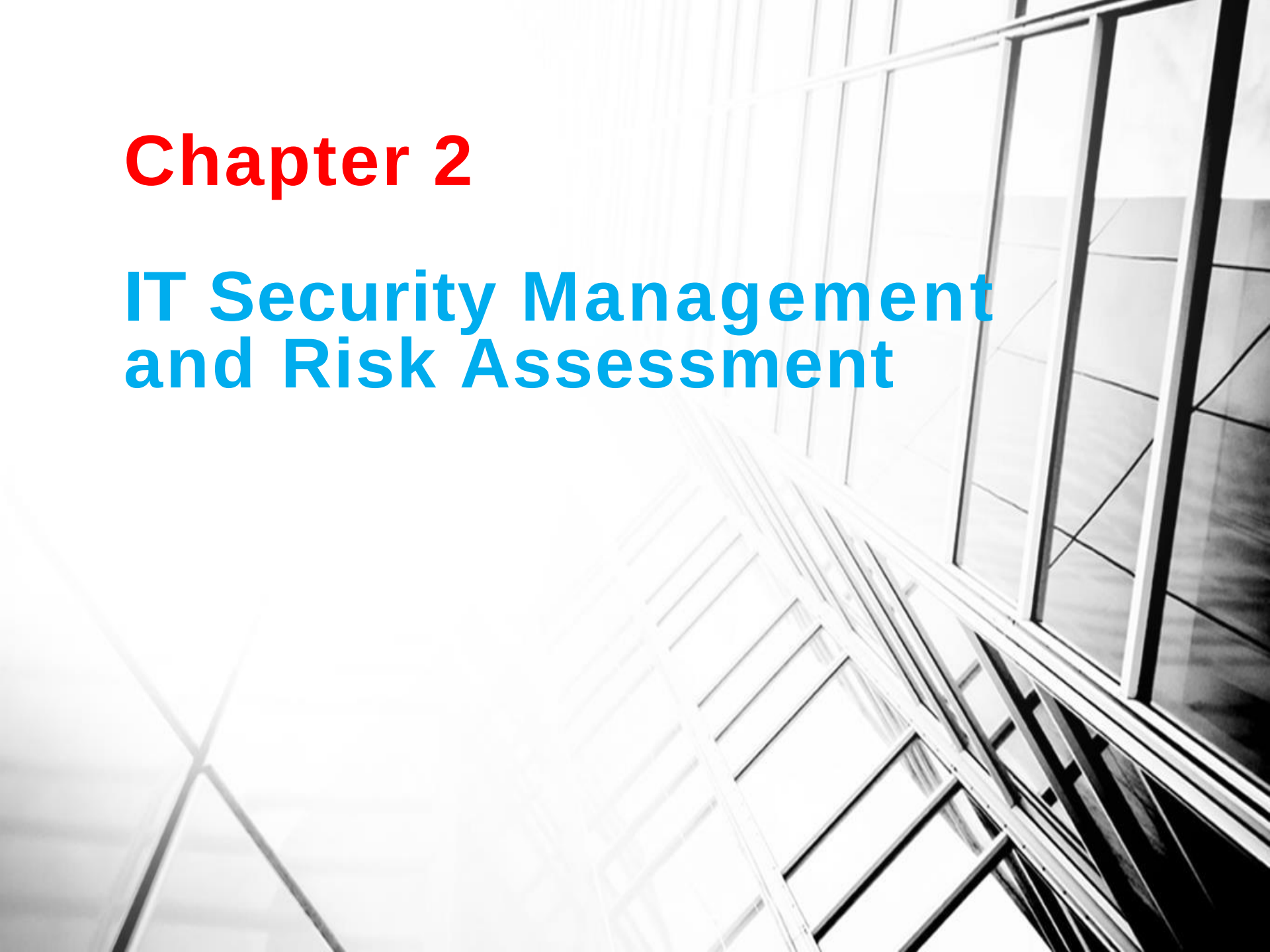


Chapter 2

IT Security Management and Risk Assessment

Overview

- IT security management
  - determining security objectives and risk profile
  - perform security risk assessment of assets
  - select, implement, monitor controls

IT Security Management

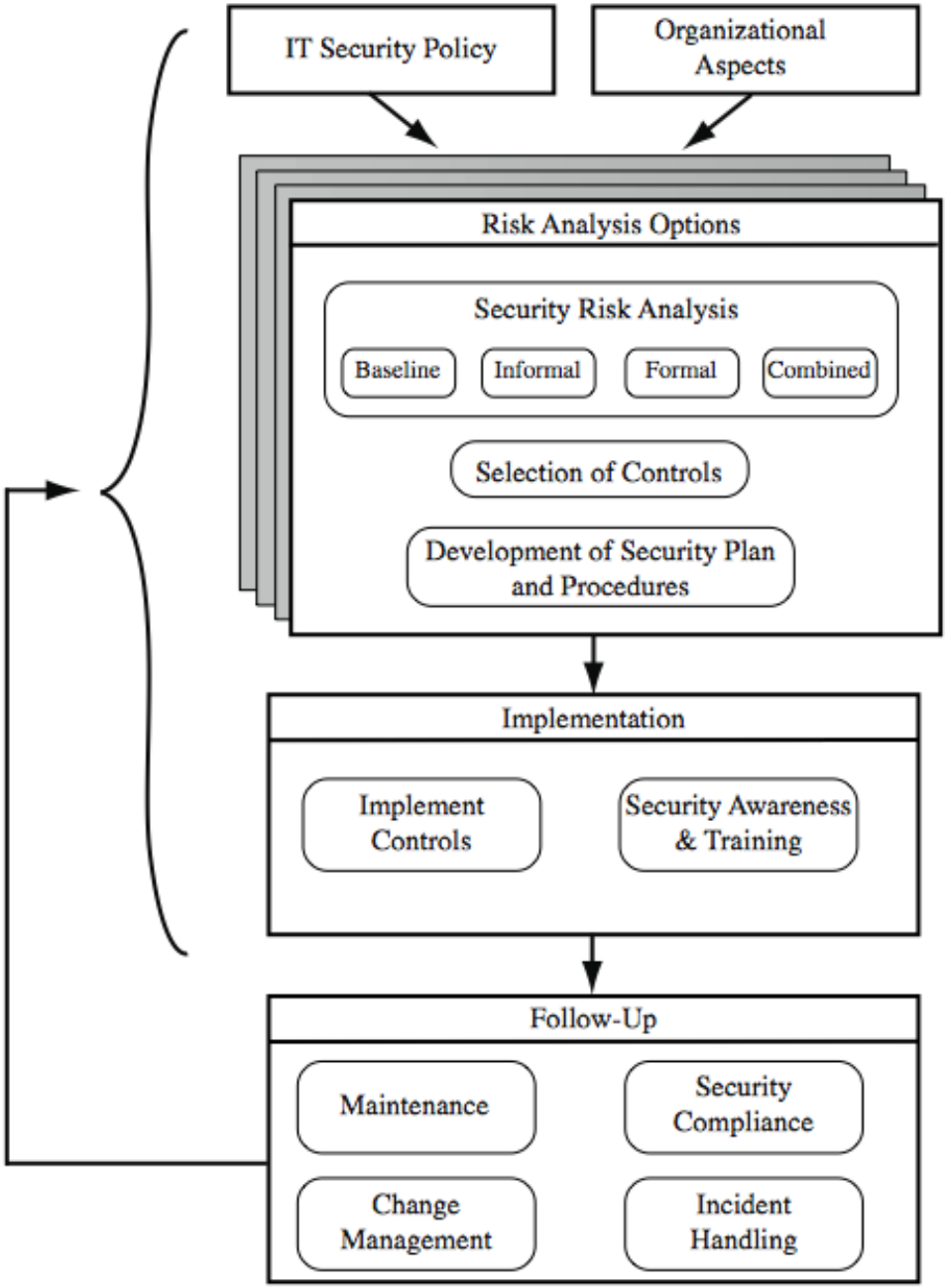
- A process used to achieve and maintain appropriate levels of confidentiality, integrity, availability, accountability, authenticity and reliability. IT security management functions include:

  - 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

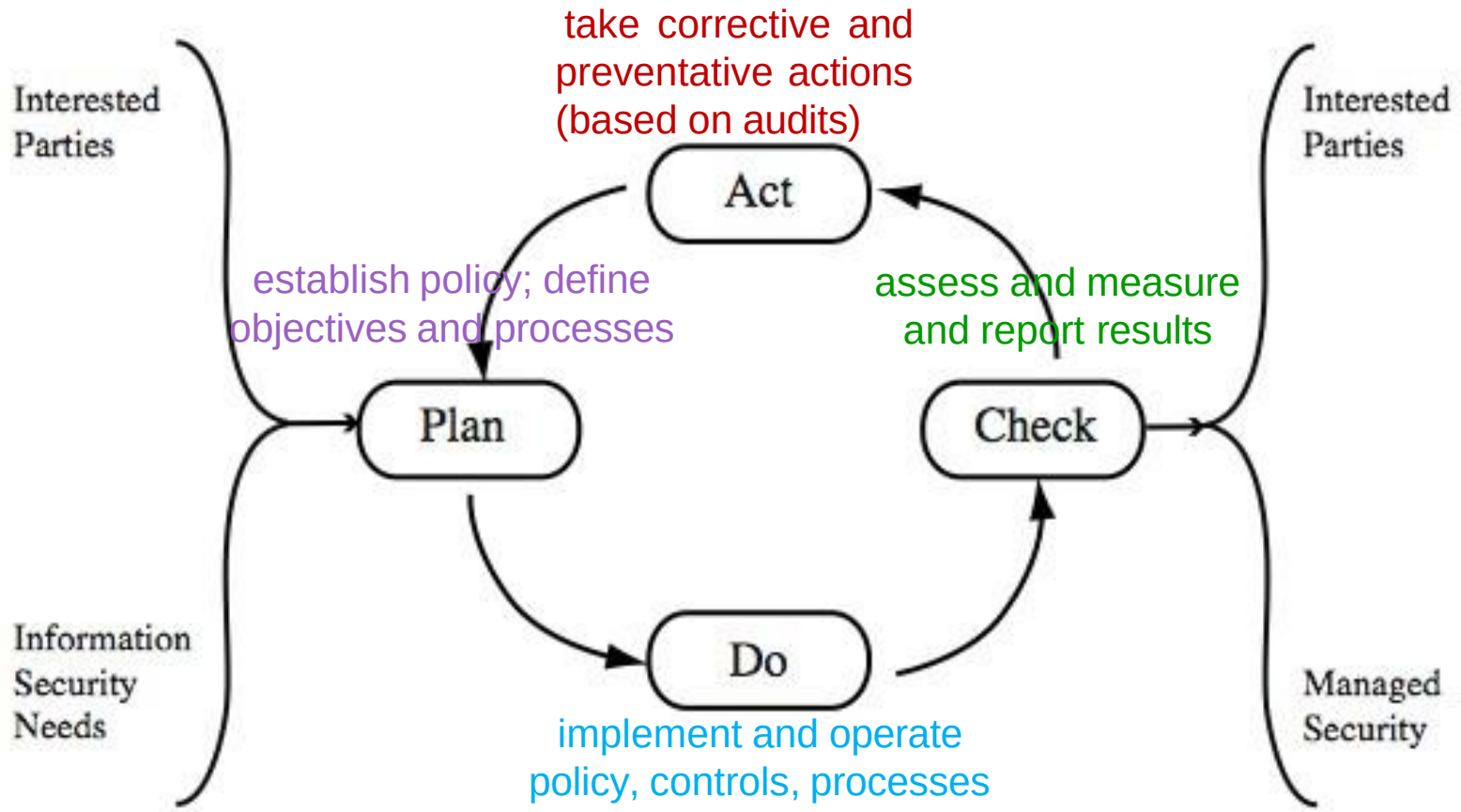
ISO 27000 Security Standards

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

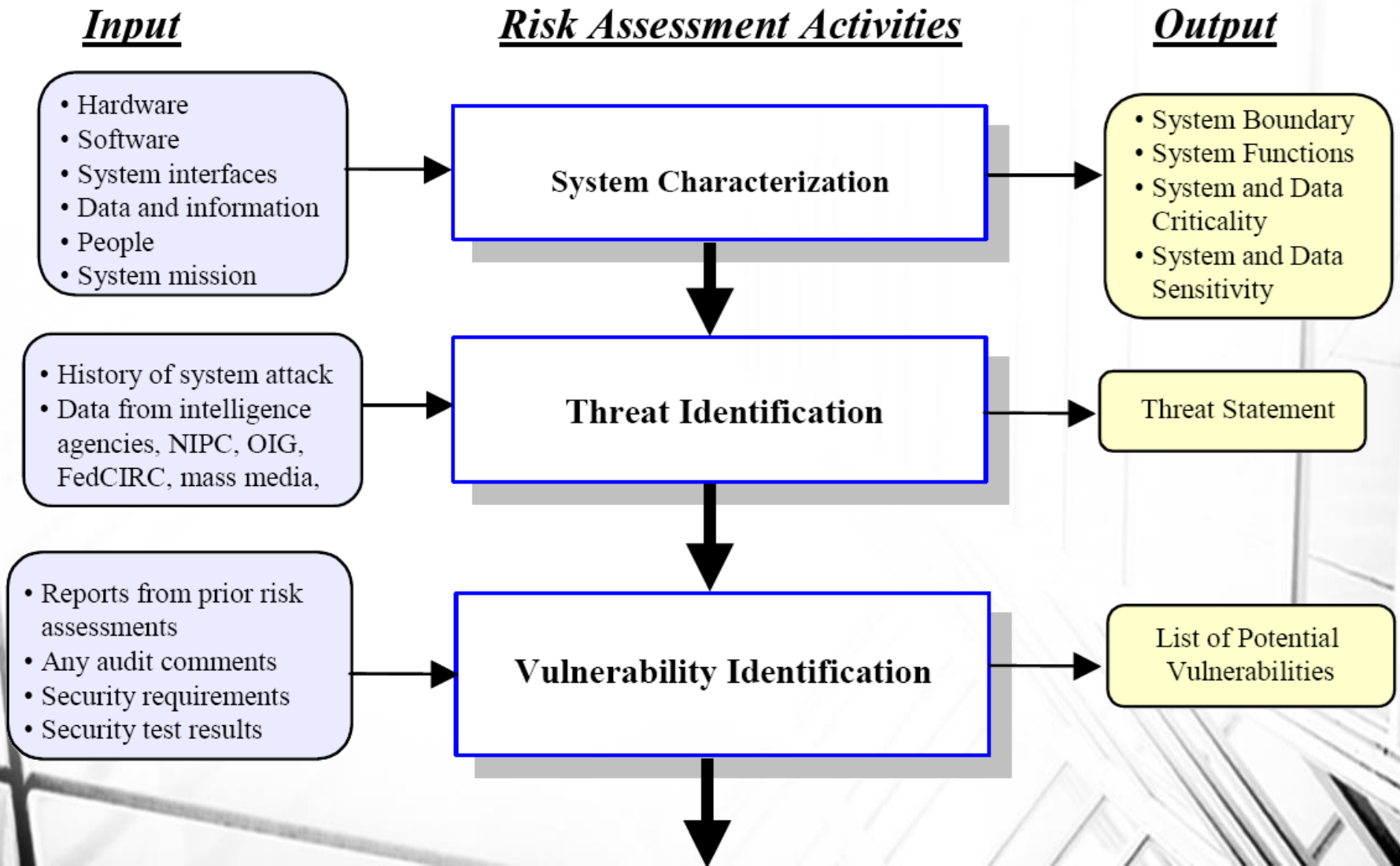
Detailed Risk Analysis

- 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

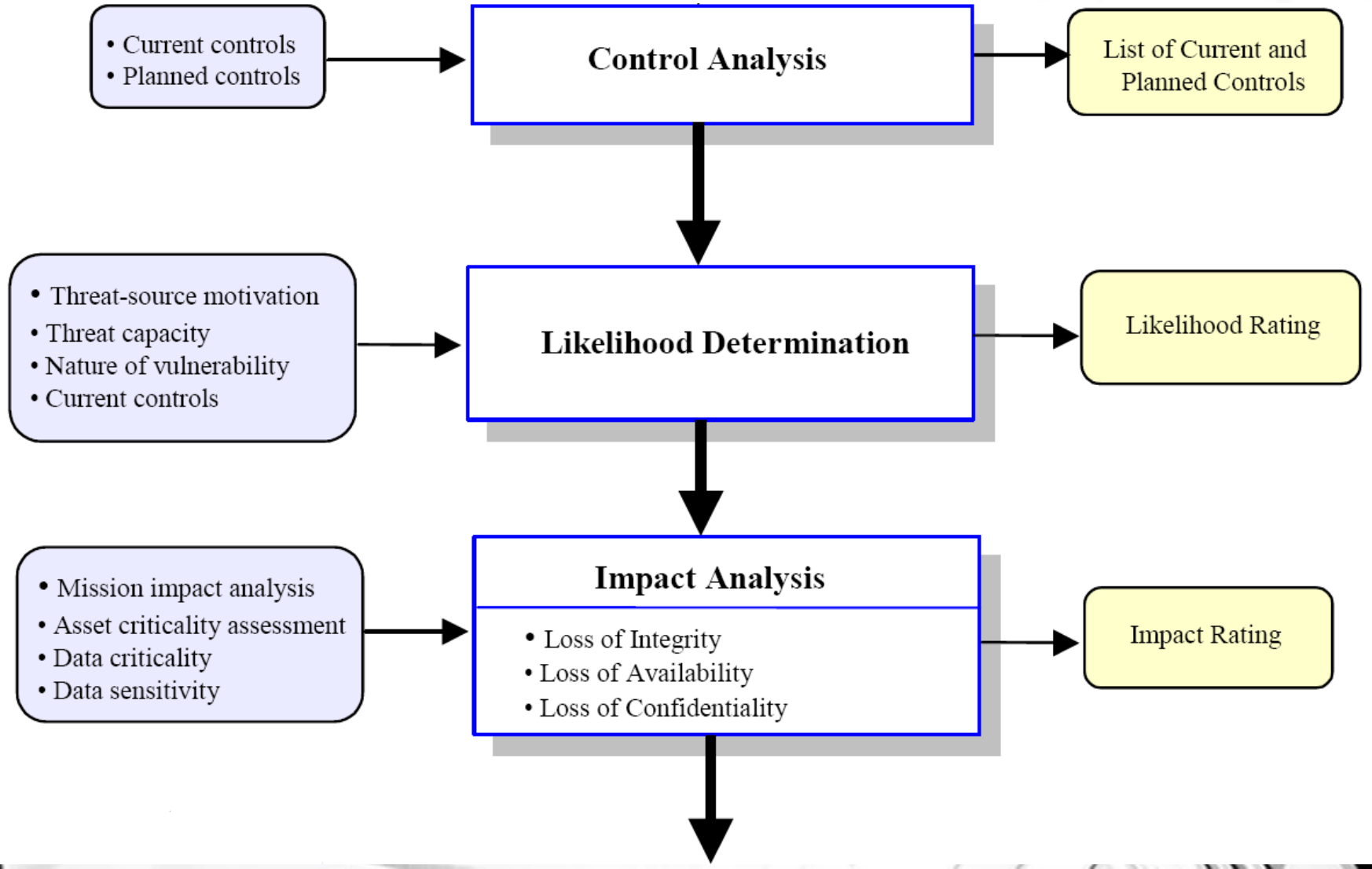
Combined Approach

- 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

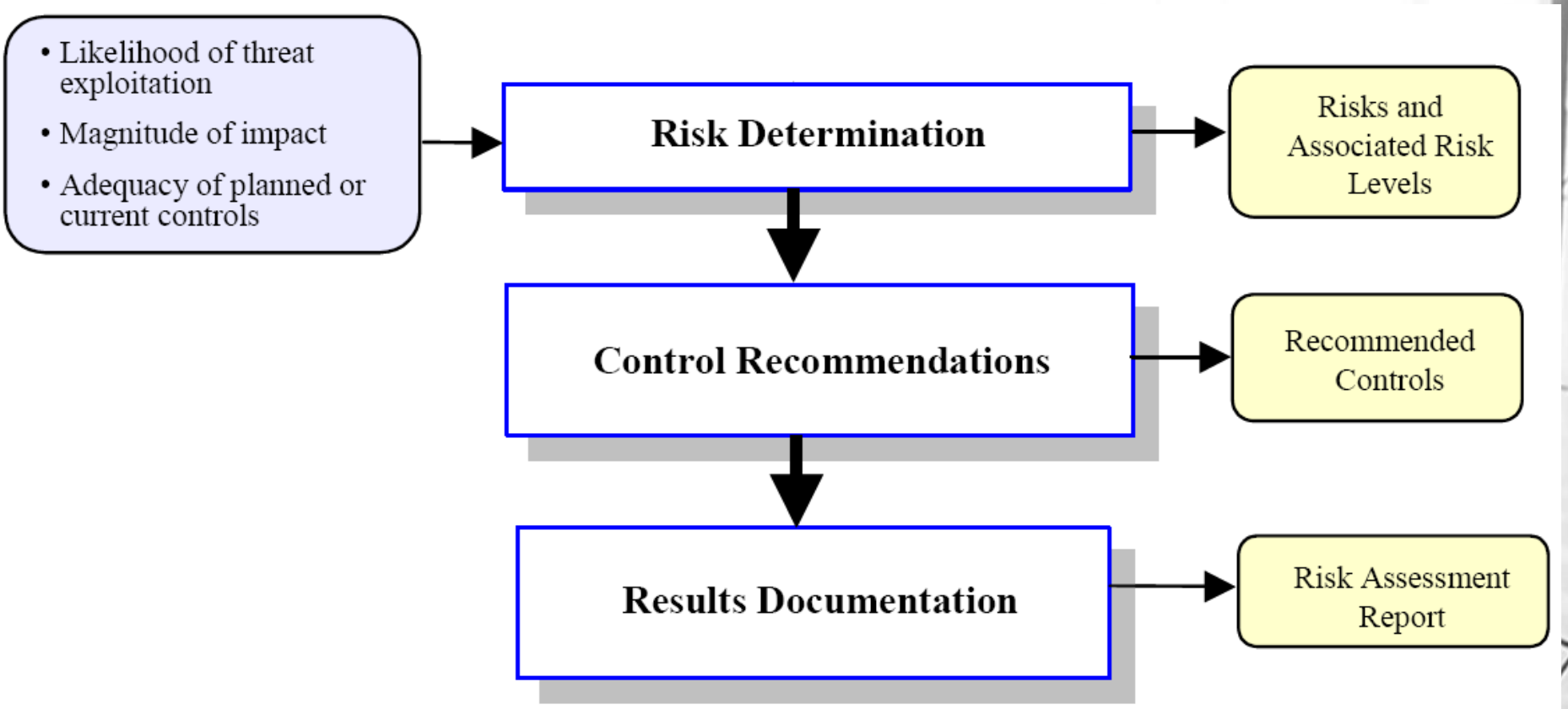
Risk assessment (1/3)



Risk assessment (2/3)



Risk assessment (3/3)



Establish Context

- determine broad risk exposure of the organization
  - 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

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 the organization

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
- aim to order resulting risks in order to treat them
- Two kinds of methods could be used: Qualitative, Quantitative.

Qualitative Risk Analysis

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.

Qualitative Risk Analysis

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.

Qualitative Risk Analysis

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.

Qualitative Risk Analysis

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

Quantitative Risk Analysis

Computing ALE

- Single Loss Expectancy: Loss to an asset if event occurs
  - Value of the lost asset = Ci
  - Impact on the Asset (if event occurs) = Pi
  - SLE = Ci * Pi

- Annualized Rate of Occurrence (ARO) characterizes, on an annualized basis, the frequency with which a threat is expected to occur.

- Annualized Loss Expectancy (ALE) computes risk using the probability of an event occurring over one year.

- Formulation

$$ALE = (SLE)(ARO)$$

Quantitative Risk Analysis

Example #1: Hard Drive Failure

- The chance of your hard drive failing is once every three years
  - **Probability** = 1/3
- Intrinsic Cost
  - $300 to buy new disk
- Hours of effort to reload OS and software
  - 10 hours
- Hours to re-key assignments from last backup
  - 4 hours
- Pay per hour of effort
  - $10.00 per hour
- **Total loss** (risk impact)
  - $300 + 10 x (10+4) = $440
- **Annual Loss Expectancy** (pa = per annum)
  - (440 x 1/3)$pa = $147 pa

Quantitative Risk Analysis

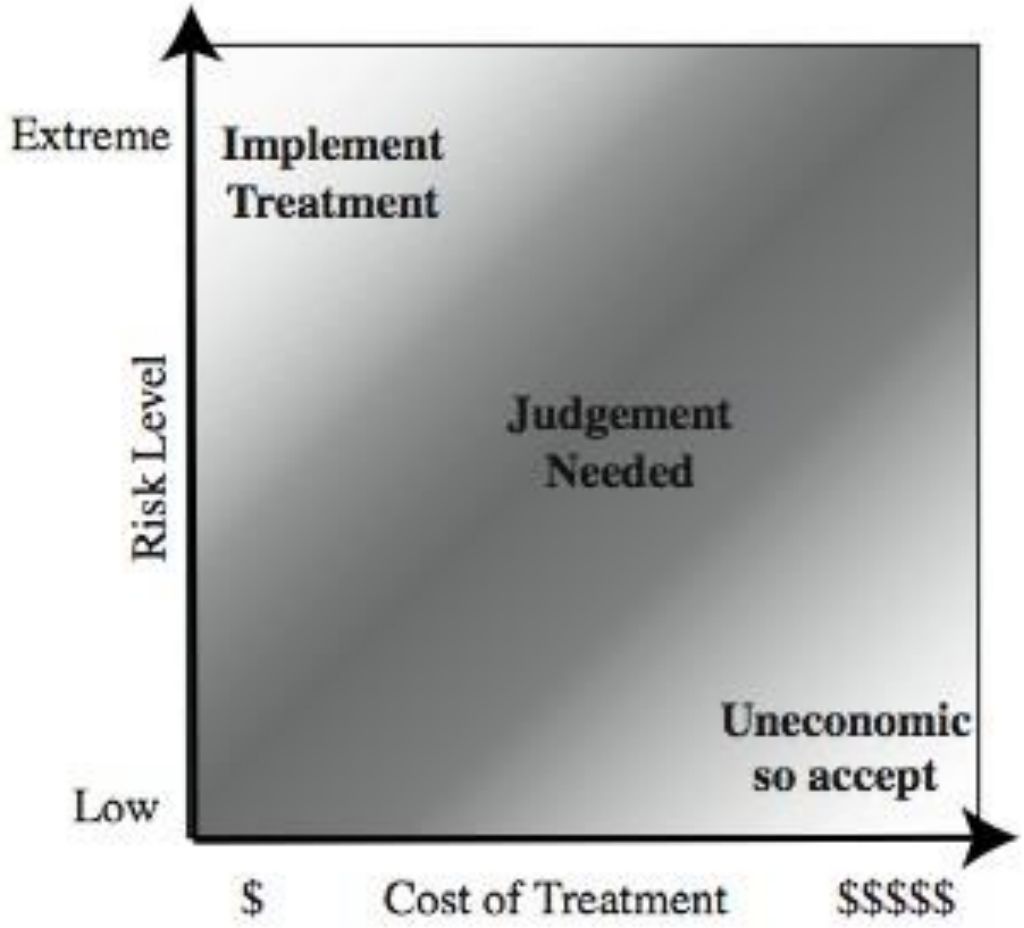
Example #2: Virus Attack

- **Situation:** Virus Attack on same system
  - You frequently swap files with other people, but have no anti-virus software running.
  - Assume an attack every 6 months (Probability = 2 per year)
  - No need to buy a new disk
  - Rebuild effort (10 + 4) hours
  - Total loss = $10 x (10 + 4) = $140
  - ALE = ($140 x 2) $pa = $280 pa

Quantitative/Qualitative approaches

Approach	Benefits	Drawbacks
Quantitative	• Risks prioritized by financial impact; assets prioritized by their financial values • Results facilitate management of risk by return on security investment • Results can be expressed in management-specific terminology	• Impact values assigned to risks are based upon subjective opinions of the participants • Very time-consuming Can be extremely costly
Qualitative	• Enables visibility and understanding of risk ranking • Easier to reach consensus • Not necessary to quantify threat frequency • Not necessary to determine financial values of assets	• Insufficient granularity between important risks • Difficult to justify investing in control as there is no basis for a cost-benefit analysis • Results dependent upon the quality of the risk management team that is created

Risk Treatment

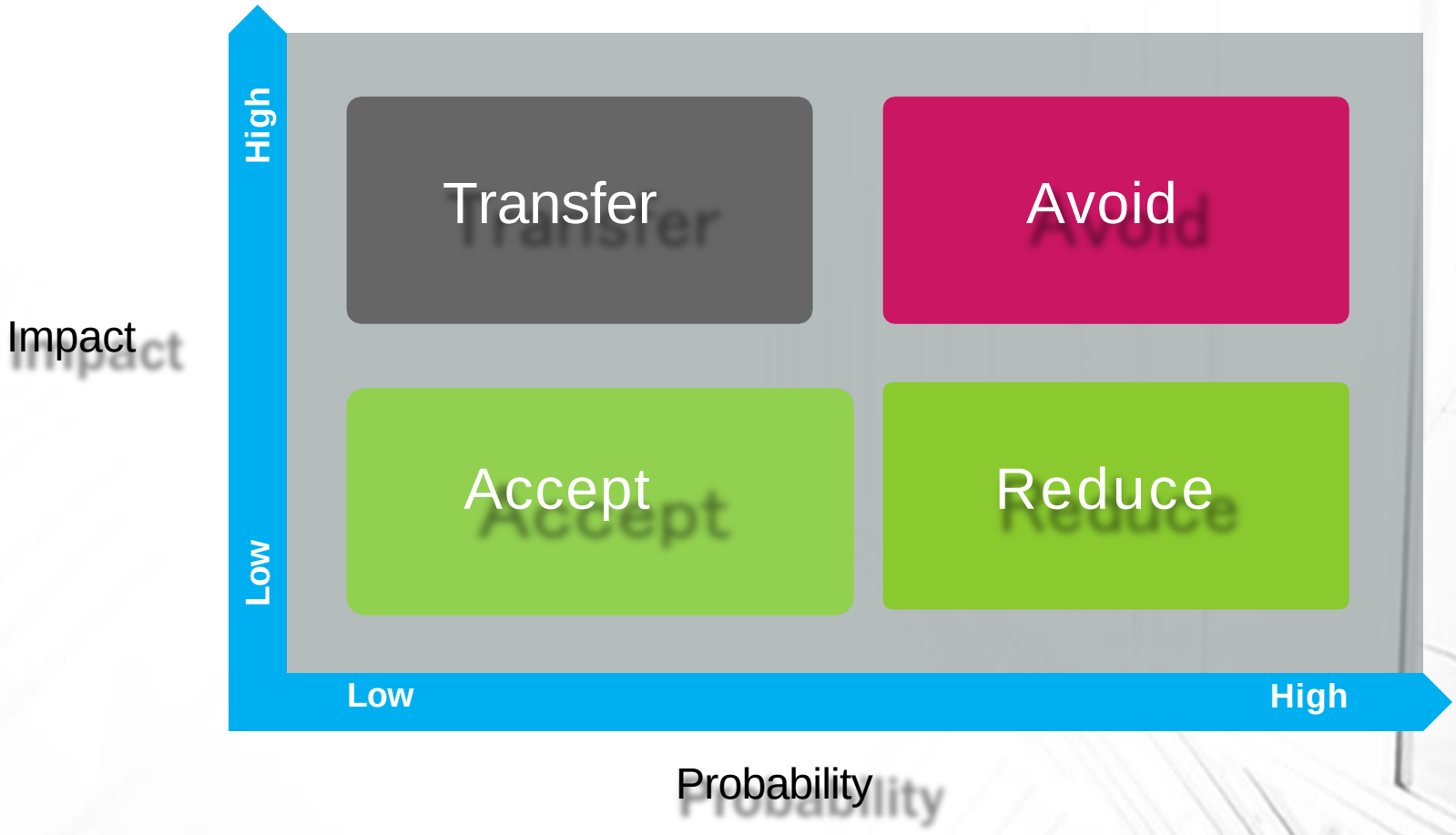


Risk mitigation

- Risk Mitigation is the process of identifying areas of risk that are unacceptable; and estimating countermeasures, costs and resources to be implemented as a measure to reduce the level of risk

- Because elimination of all risk is impossible, we must use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission

Risk quadrant



What options for mitigation?

- Accept the Risk – Continue operating while being aware of the existence of the risk
- Avoid the Risk – Stop running the vulnerable service
- Transfer the Risk – Use options to compensate for the loss, such as insurance
- Reduce the Risk – Implement controls that lessen the likelihood

Risk mitigation methodology

1. Prioritize based on risk levels presented
2. Evaluate recommended control options
3. Conduct a cost-benefit analysis
4. Select additional controls, as necessary
5. Assign responsibility
6. Develop an action plan, if necessary
7. Implement the selected controls

Cost-benefit analysis

- If control reduces risk more than needed, see if a less expensive alternative exists
- If control would cost more than the risk reduction provided, then find something else
- If control does not reduce risk sufficiently, look for more controls or a different control
- If control provides enough risk reduction and is cost-effective, then use it

Security measures

- Best practices

- Accountability
- Auditability
- Publically available,
- Simple design
- Trusted source
- Independence
- Consistently applied
- Cost-effective
- Reliable
- Distinct from other countermeasures

- Ease of use
- Minimum manual intervention
- Sustainable
- Secure
- Protects confidentiality, integrity, and availability
- Can be “backed out”
- Creates no additional issues
- Leaves not residual data behind

Residual risk

- The risk remaining after the implementation of new or enhanced controls is the residual risk
- If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level