FRISC Winter School 2012
Information Security

Security Governance

Prof. Audun Jøsang

– University of Oslo

– QUT, Australia

Norwegian terms

English		Norwegian	
Security	→	Sikkerhet	✓ GOOD
Safety	→	Trygghet	
Certainty	→	Visshet	

- Security
- Safety
- Certainty

} → Sikkerhet ⊘ BAD

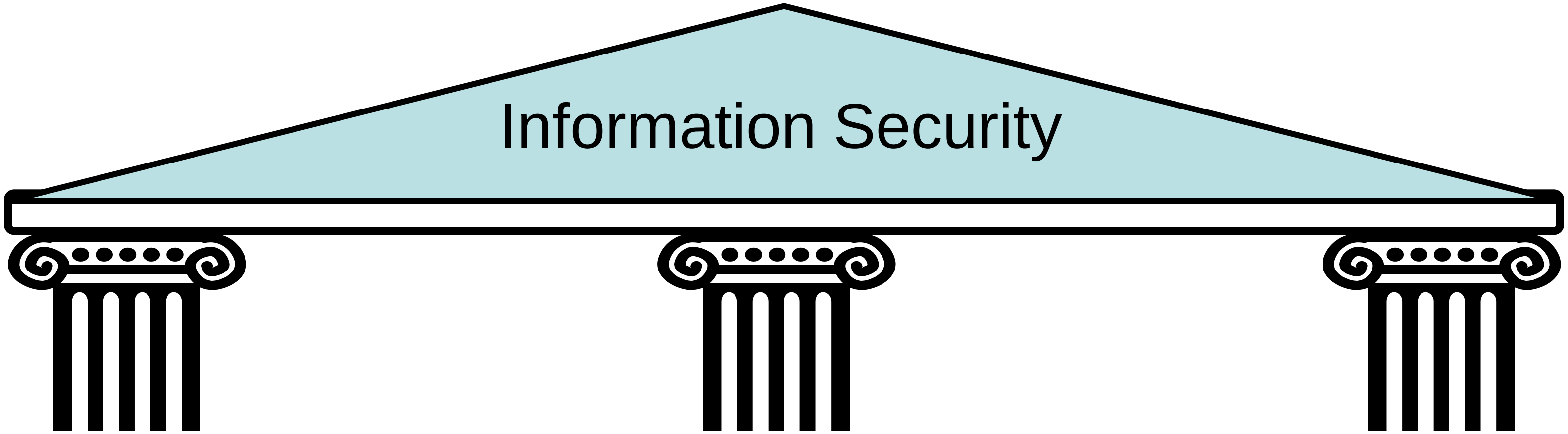
What is security in general ?

- Security is the protection of assets from damage
- Focuses on all types of assets, e.g.
  - Private and public possessions, environment, processes, social order, political stability, culture,
- Common types of security, e.g.
  - Physical security
  - National and global security
  - Information security
  - Environmental security
- Security of human health and welfare
  - Normally called safety

What is *information* security ?

- *Information* security is the protection of *information* assets from damage
- Assets to be protected are e.g.:
  - Data in storage, processing or transmission, hardware, software, IT infrastructure and IT business processes
- Threats can be intentional and accidental
  - Threat agents can be people or natural (e.g. by system failure)
  - People can cause harm by accident or by intent
- Protection aims at reducing risk to information assets
  - Reduce vulnerabilities
  - Weaken threat agents
  - Mitigate consequences of threat occurrences

Information security control categories



Physical controls

- Environmental security
- Facility security
- Physical access control and intrusion detection
- Surveillance and Monitoring

Technical controls

- Infrastructure security
- Applications security

Administrative controls (GRC)

- Information Security **G**overnance
- Information **R**isk Management
- Information Security **C**ompliance

IT Security Governance fundamentals

Information security governance is the practice of directing and controlling an organization to establish and sustain a culture of security in the organization's conduct. This culture is anchored in beliefs, behaviors, capabilities, and actions.

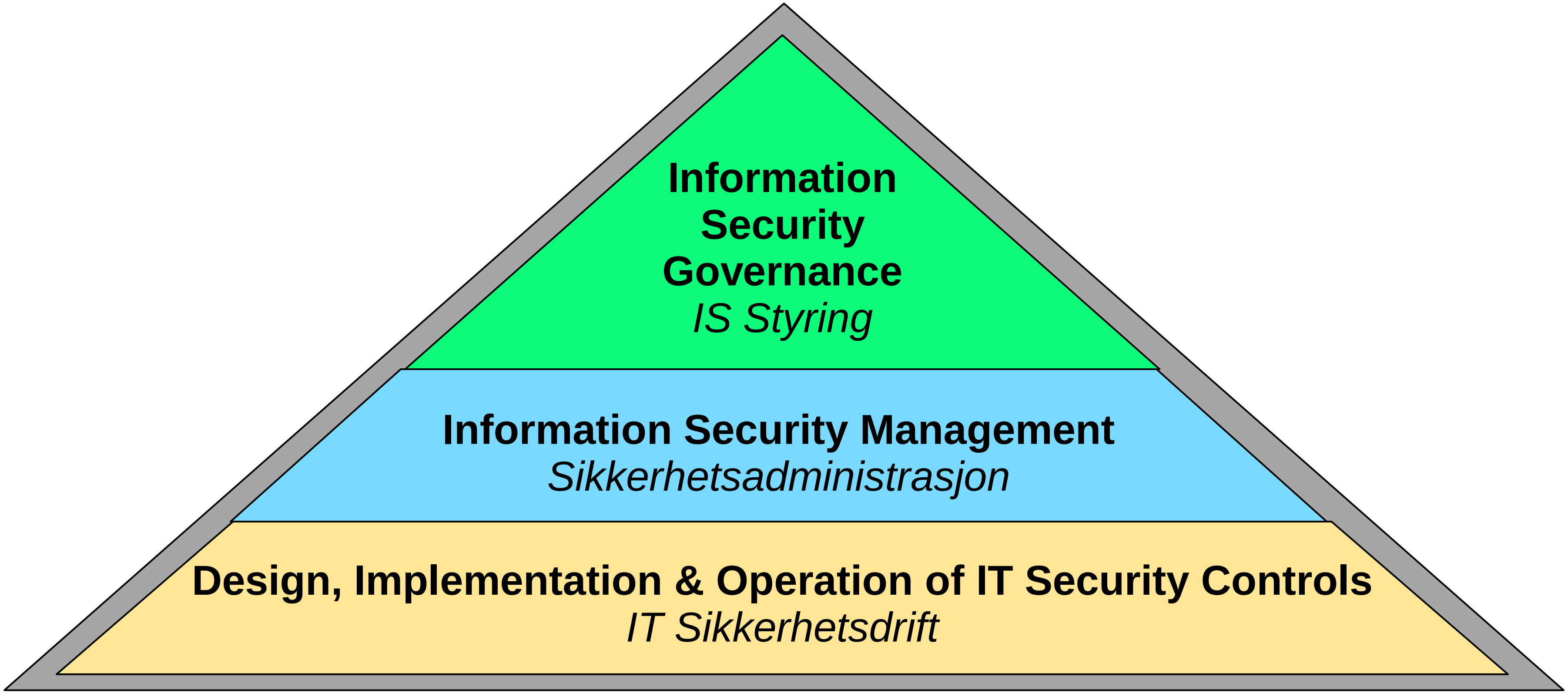
To practice information security governance implies that adequate security is a non-negotiable requirement of being in business.

Julia Allen. *Governing for Enterprise Security.* (CMU/SEI-TN-023), *June 2005.* *www.cert.org/archive/pdf/05tn023.pdf*

Goals of information security governance

1. Strategic alignment of security program
2. Risk management
3. Value delivery
4. Resource management
5. Assurance process integration
6. Performance measurement

IT security activities in the organisation



Information Security Governance
IS Styring

Information Security Management
Sikkerhetsadministrasjon

Design, Implementation & Operation of IT Security Controls
IT Sikkerhetsdrift

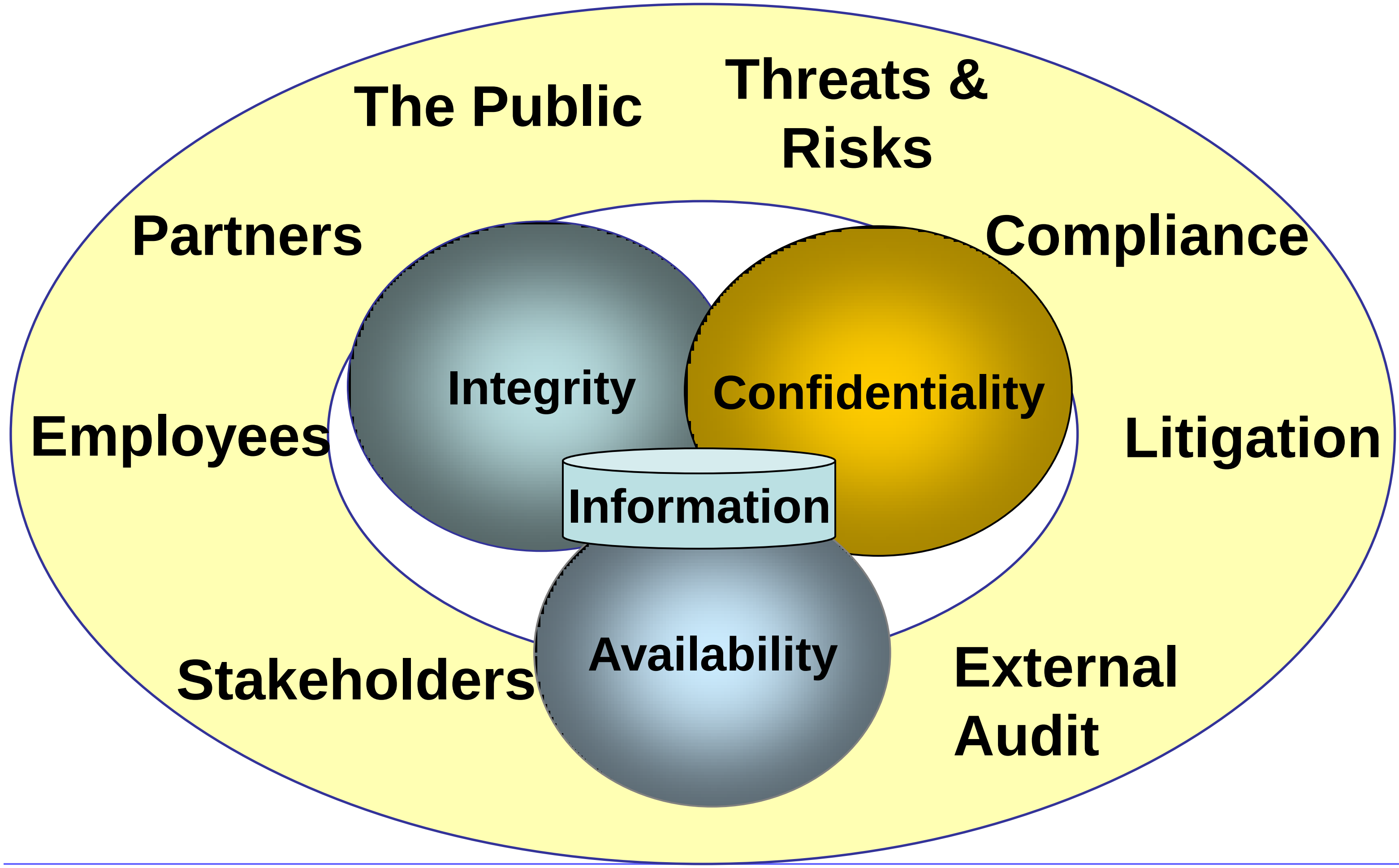
What is information security management?

IS management has as goal to reduce damage and to control risk of damage to information assets

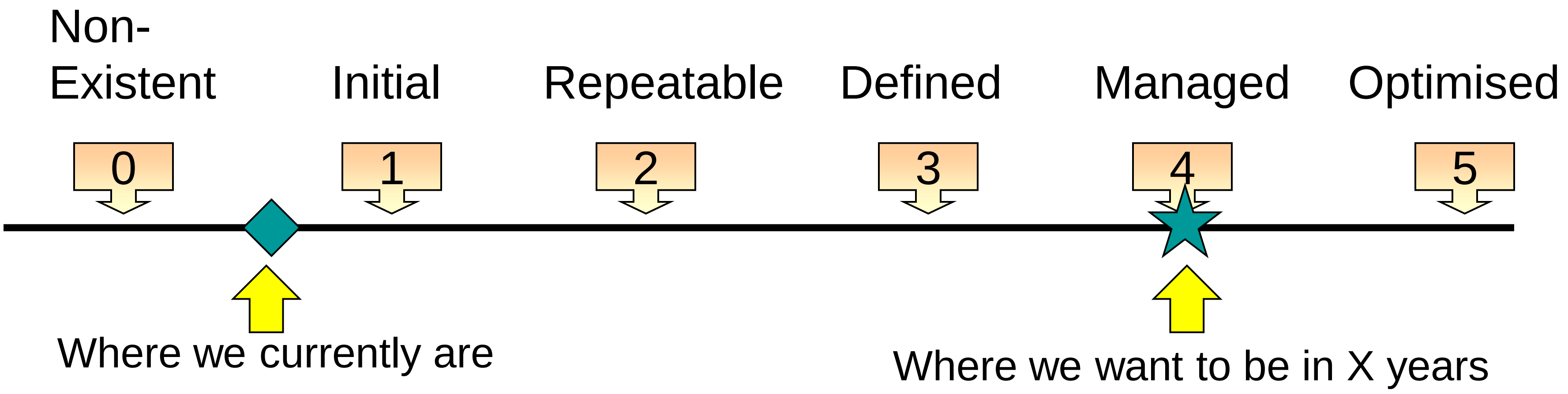
IS Management Includes:

- Definition and maintenance of security policies
- Establishing and running a security organisation (ISMS)
- Information classification
- Risk management,
- Definition of security procedures, standards & guidelines
- Deployment and maintenance of security controls
- Security education and training
- Disaster recovery and business continuity planning

Context for IS Management



COBIT Maturity Model for IS Management



Explanation for rankings:

0 - Security controls are not applied at all
1 - Security is ad hoc and disorganised
2 - Security processes follow a regular pattern
3 - Processes are documented and communicated
4 - Processes are monitored and measured
5 - Best practices are followed and automated

Who is responsible for ISM?

- Management
  - CEO, CSO, CIO
  - Allocate resources, endorse and abide security policies
- IT Security staff
- General security staff, i.e. guards, janitors etc.
  - Important for physical security
- IT staff
- Users
- Third parties
  - Outsourced information security management
  - Customers, suppliers, business partners

Terminology

- Standards: Guidelines on best practice or widely accepted methods for controlling information security and can be used as checklists for a security program.
- Best practice: Implementation of widely accepted security methods that provide the best level of assurance
- Baseline: The minimum level of security necessary to support and enforce the security policy
- Due diligence: Investigating and understanding risk
- Due care: Having security policies and implementing a reasonable security program that balances the identified risks.

Rules for Right or Wrong

- Security assumes that there is a difference between doing right or wrong, defined by rules such as:
- Law and regulation, e.g.
  - EU Data Protection Directive 1995, mandates privacy regulation
  - Norwegian “Sikkerhetsinstruksen” 1953, mandates protection of information that is considered important for national security
- Explicit company policy
  - Defines who is authorized to do what
  - Defines appropriate use
- Implicit policy
  - e.g. your own rules for using your laptop
- Ethics and social norms
  - e.g. truthful representation of goods for sale online

IS management frameworks

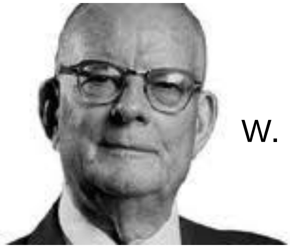
- ISO Security Management standards: 27000 Series
  - ISO/IEC 27001 Information Security Management Systems
    - NS 27001 Ledelsessystem for informasjonssikkerhet
  - ISO/IEC 27002 Code of practice for information security management
    - NS 27002 Administrasjon av informasjonssikkerhet
- USA
  - NIST (National Institute for Standards and Technology) Special Publications SP800-X series,
- Availability
  - Buy ISO standards
  - Free NIST standards

ISO/IEC 27001- Information Security Management Systen (ISMS)

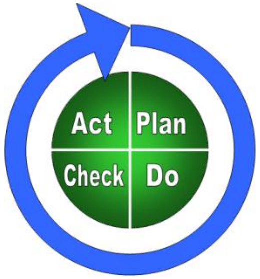
- The need to establish a certification scheme for information security management emerged late 1990s
- A general approach to security management was needed for certification purposes, not just a code of practice (check list of controls)
- BS 7799-2:1999 was created to define a comprehensive ISMS (Information Security Management System) against which certification was possible.
- Led to the dramatic conclusion that **the concept of an ISMS is perhaps of far greater and fundamental importance than the original Code of Practice**.

ISO/IEC 27001- What is it?

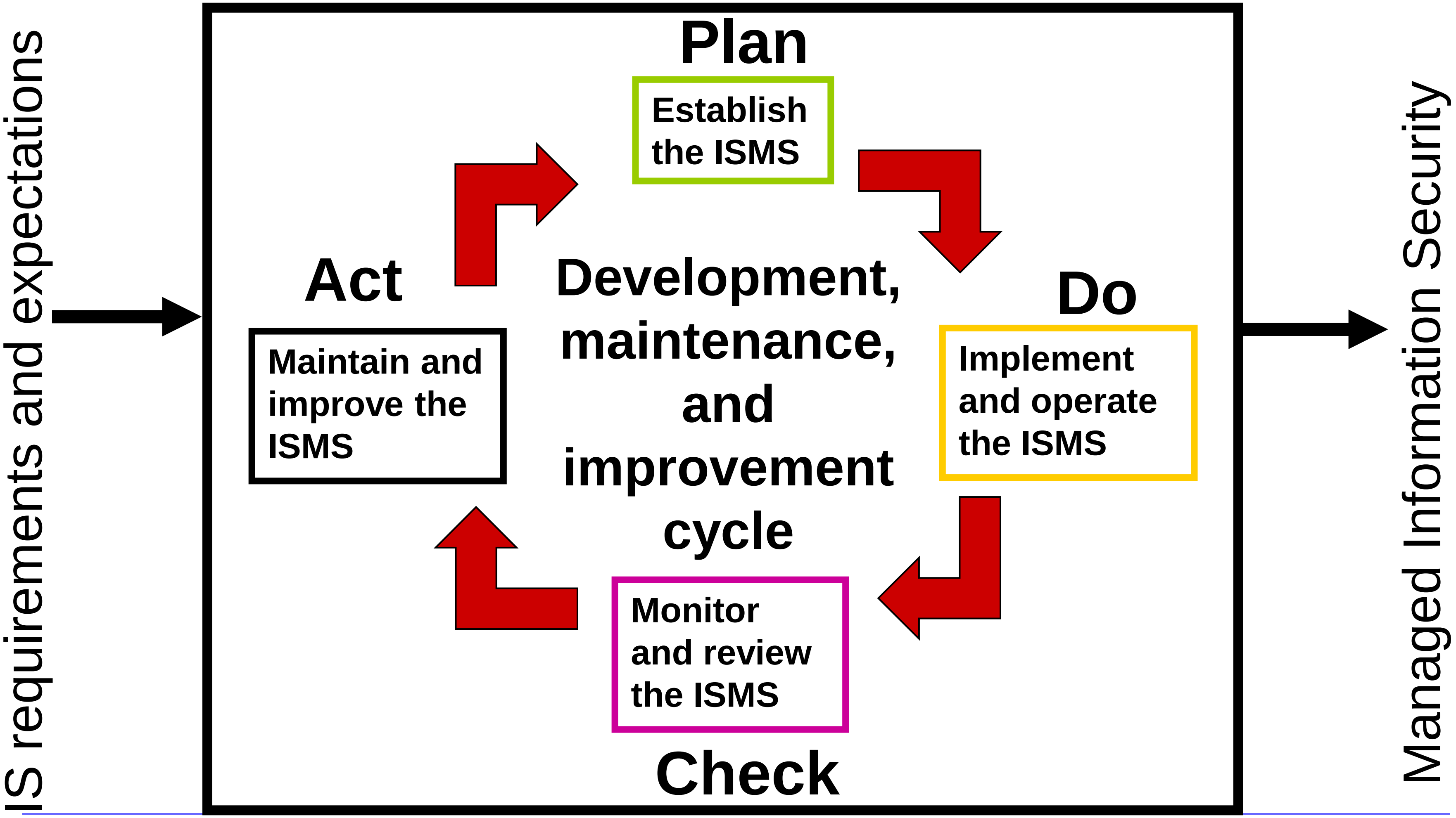
- Specifies requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS (Information Security Management System)
- A comprehensive approach to information security management
- Not just a set of goals and controls as in the code of practice ISO/IEC 27002
- Organisations can be certified against ISO/IEC 27001
- To be used in conjunction with ISO/IEC 27002
- Based on Plan-Do-Check-Act (PDCA) quality control model of Deming.



W. Edwards Deming
(1900-1993)



ISO/IEC 27001- The PDCA Model


IS requirements and expectations
Plan
Establish the ISMS
Act
Development, maintenance, and improvement cycle
Do
Maintain and improve the ISMS
Implement and operate the ISMS
Monitor and review the ISMS
Check
Managed Information Security

ISO/IEC 27001- Plan Phase

- Establish the ISMS
- Purpose: Establish policy, objectives, processes and procedures
- Steps:
  - Define scope and boundaries
  - Define policy for the security program (ISMS)
  - Analyse and identify the greatest risks
  - Identify and evaluate options for the treatment of risks
  - Select control objectives and controls for the treatment of risks
  - Obtain management approval and authorization
  - Prepare a statement of applicability

ISO/IEC 27001- Do phase

- Implement and operate the ISMS
- Purpose: Implement selected controls, and promote actions to manage identified risks
- Steps:
  - Develop blueprints for controls selected in Plan phase
  - Implement the controls selected in the Plan phase
  - Define how to measure the effectiveness of the selected controls
  - Implement training and awareness programs
  - Manage operations and resources

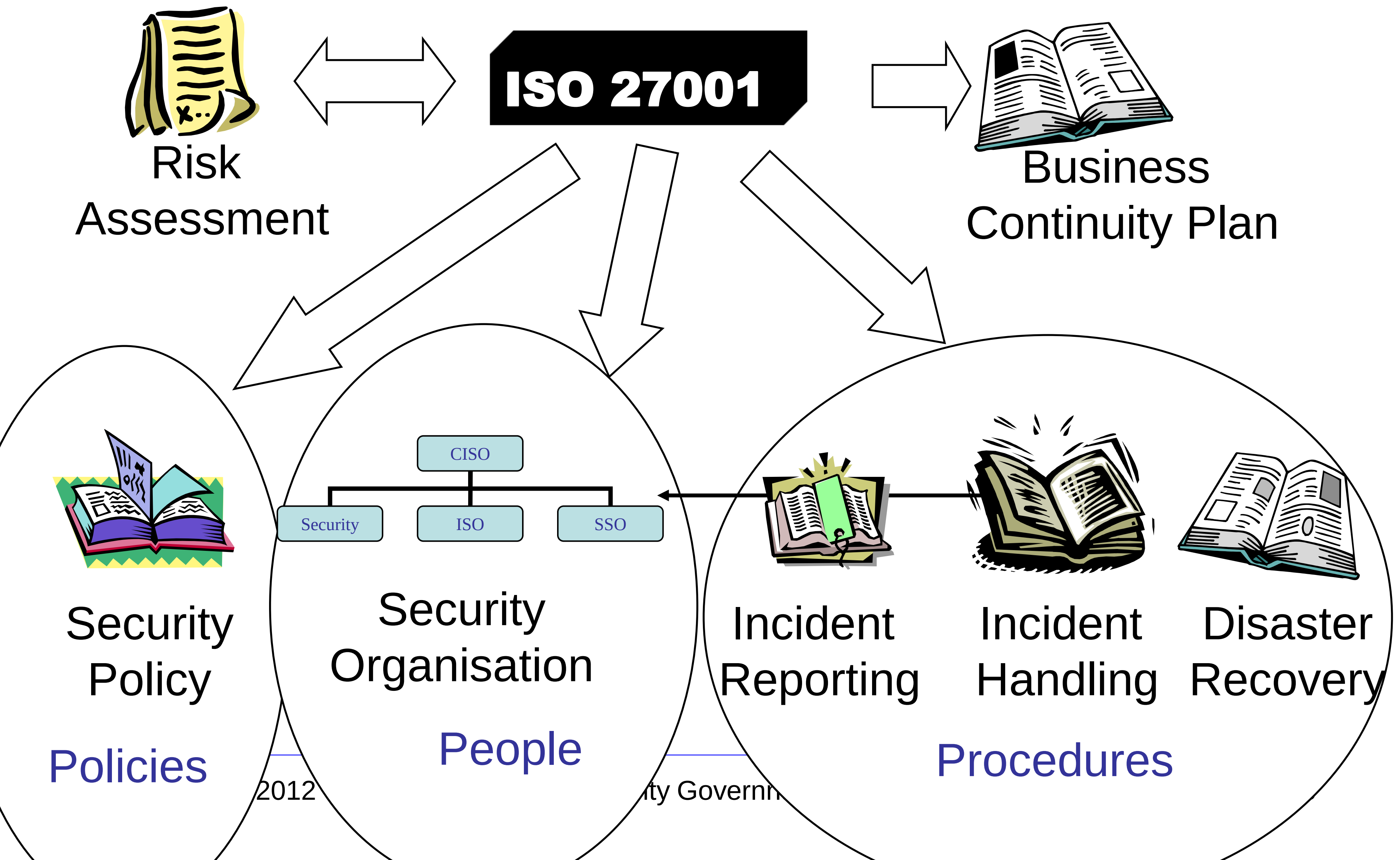
ISO/IEC 27001- Check phase

- Monitor and review the ISMS
- Purpose: to ensure that controls are working effectively
- Steps:
  - Execute monitoring procedures and other controls
  - Measure the effectiveness of controls
  - Review the level of residual risk and acceptable risk
  - Conduct internal ISMS audits at planned intervals
  - Undertake a management review of the ISMS on a regular basis (at least once per year)
  - Record actions and events that could have an impact on the effectiveness or performance of the ISMS.

ISO/IEC 27001- Act phase

- Maintain and improve the ISMS
- Purpose: Take action as a result of the Check phase
- Steps:
  - Implement identified improvements in the ISMS
  - Take appropriate corrective and preventive actions
  - Communicate the results and actions and agree with all interested parties
  - Ensure that the improvements achieve their intended objective

ISO/IEC 27001Output



ISO 27001

Risk Assessment

Business Continuity Plan

CISO

Security

ISO

SSO

Security Policy

Security Organisation

Incident Reporting

Incident Handling

Disaster Recovery

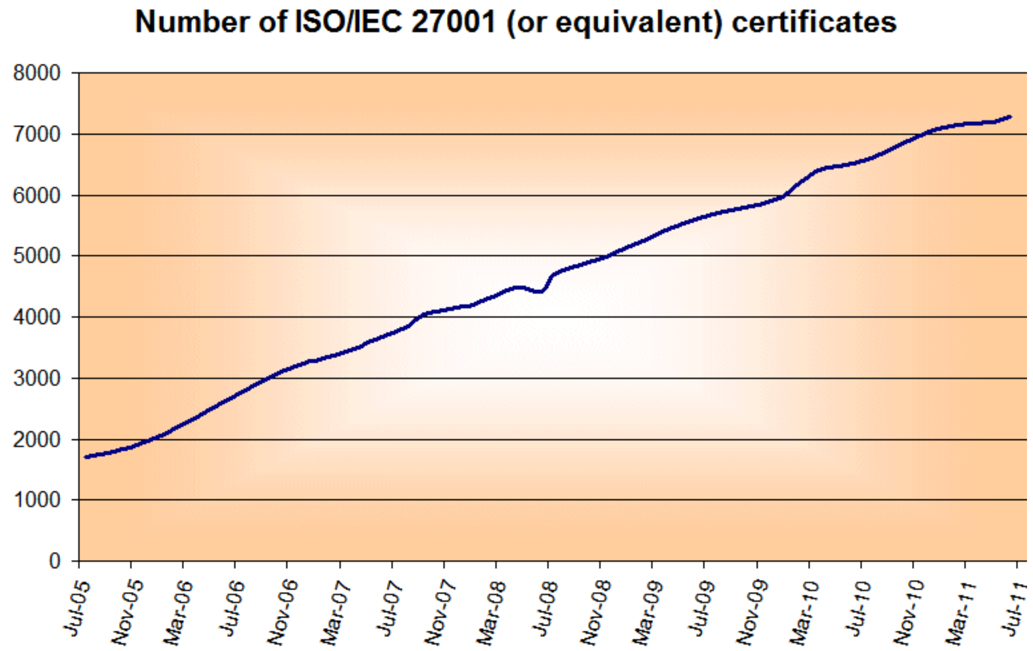
Policies

People

Procedures

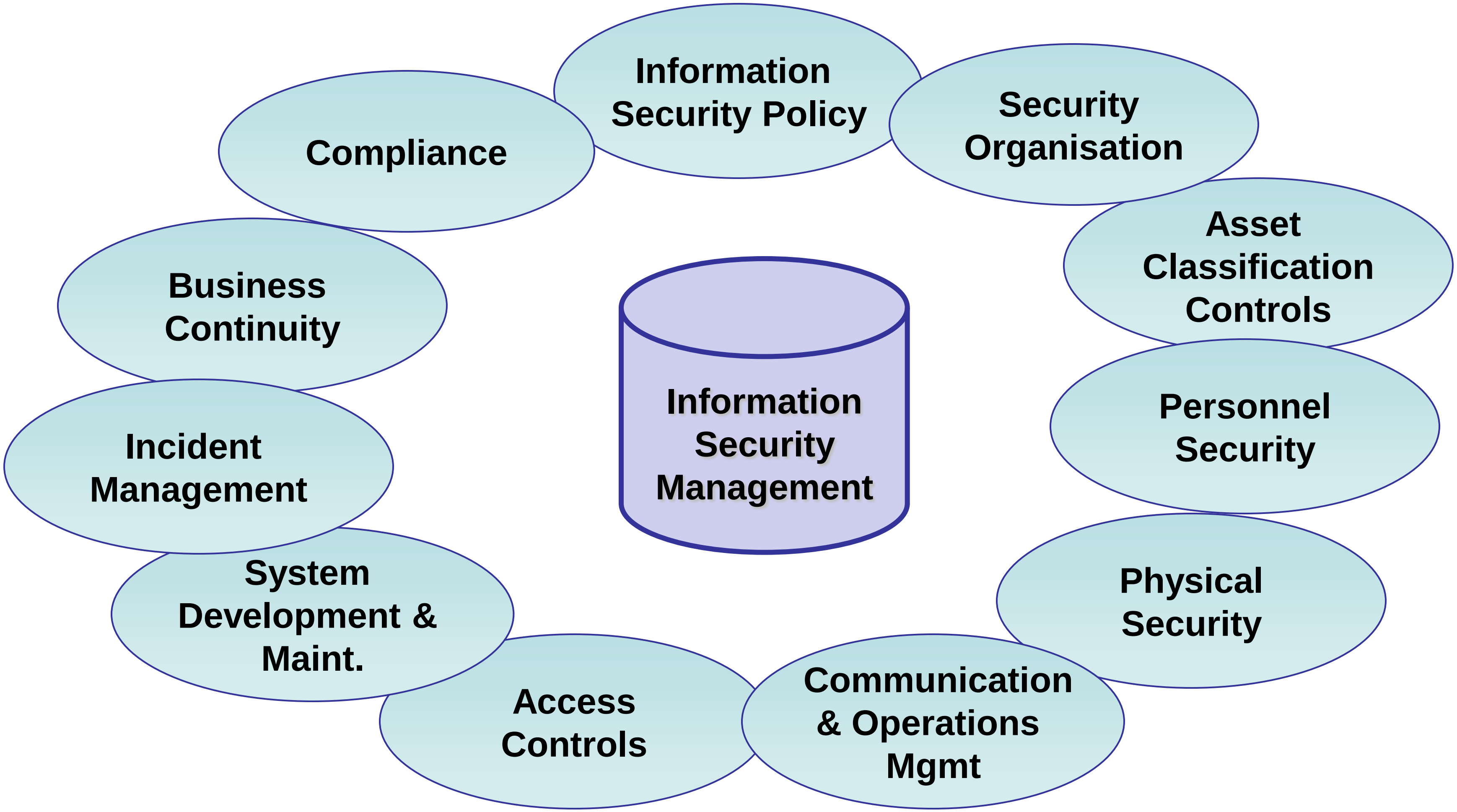
ISO/IEC 27001Certification

- Most countries have one or several organisations qualified to do ISMS certification



Source: Ted Humphrey

The 11 Objectives of ISO/IEC 27002


Information Security Policy
Security Organisation
Asset Classification Controls
Personnel Security
Physical Security
Communication & Operations Mgmt
Access Controls
System Development & Maint.
Incident Management
Business Continuity
Compliance
Information Security Management

Published ISO 27000 standards

- 27003 Information security management system implementation guidance
- 27004 Information security management: Measurement
- 27005 Information security risk management
- 27006 Requirements for bodies providing audit and certification of ISMS
- 27011 Information security management guidelines for telecommunications organizations based on ISO 27002
- 27031 Guidelines for information and communications technology readiness for business continuity
- 27033-1 Network security overview and concepts
- 27035 Security incident management
- 27799 Information security management in health

ISO 27000 Standards in preparation

- 27007 Guidelines for ISMS auditing
- 27008 Guidance for auditors on ISMS controls
- 27013 Guideline on the integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001
- 27014 Information security governance framework
- 27015 Information security management guidelines for the finance and insurance sectors
- 27032 Guideline for cybersecurity (essentially, 'being a good neighbor' on the Internet)
- 27033 IT network security, a multi-part standard based on ISO/IEC 18028:2006 (part 1 is published already)
- 27034 Guideline for application security
- 27036 Guidelines for security of outsourcing
- 27037 Guidelines for identification, collection and/or acquisition and preservation of digital evidence

NIST Special Publications 800 Series

Library of freely available resources

SP800-100: Information Security Handbook: A Guide for Managers
SP800-53: Recommended Security Controls for Federal Info Systems
SP800-35: Guide to Information Technology Security Services
SP800-39: Managing Information Security Risk
SP800-30: Guide for Conducting Risk Assessment
SP800-27: Engineering Principles for Information Technology Security
SP800-18: Guide for Developing Security Plans for Federal Info Systems
SP800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems
SP800-12: An Introduction to Computer Security: The NIST Handbook
SP800-26: Security Self-Assessment Guide for Information Technology Systems
SP800-34. Contingency Planning Guide for Information Technology Systems

More IS frameworks

- CobiT
  - Control Objectives for Information and Related Technology (CobiT) is an IT governance control framework aimed at regulatory compliance, risk management and aligning IT strategy with organisational goals

- Information Security Forum (ISF)
  - Standard of Good Practice for Information Security

- ITIL
  - Information Technology Infrastructure Library
  - Management guidelines for IT, including IT security

More IS frameworks

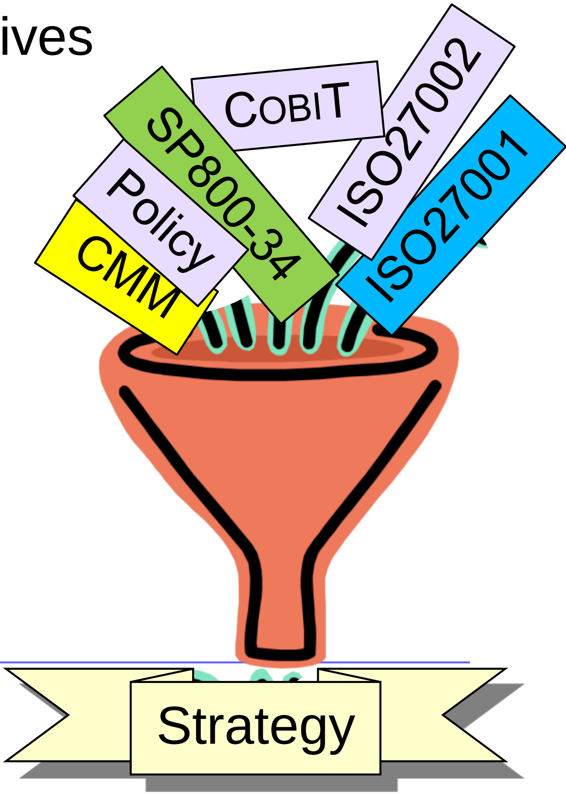
- SSE-CMM
  - The Systems Security Engineering Capability Maturity Model (SSE-CMM) is aimed at security systems development. Adapted from the SE-CMM (Systems Engineering CMM)
- COBIT CMM
  - The COBIT Capability Maturity Model is a framework for measuring and improving security management in organisations. Adapted from SE-CMM.
- Common Criteria (ISO 15408)
  - Common Criteria for Information Technology Security Evaluation
  - In practice also a framework for specification of security systems
  - Protection Profiles (PP) and Evaluation Assurance Levels (EAL1-7)

Additional IT security frameworks

- Other places to find relebant IS information
  - CERT/CC - Computer Emergency Response Team Coordination Center
    - http://www.cert.org/nav/
  - NSM – Nasjonal Sikkerhetsmyndighet
    - https://www.nsm.stat.no/Publikasjoner/
  - SCORE – Security Consensus Operational Readiness Evaluation
    - http://www.sans.org/score/

From IS frameworks to IS strategy

- No IS framework best for all
  - no one-size-fits-all in security
  - no framework should be sole source for any enterprise
  - multiple frameworks provide multiple perspectives
- IS Strategy
  - Select the best from multiple frameworks
  - Add IS policy
  - Synthesize the IS framework

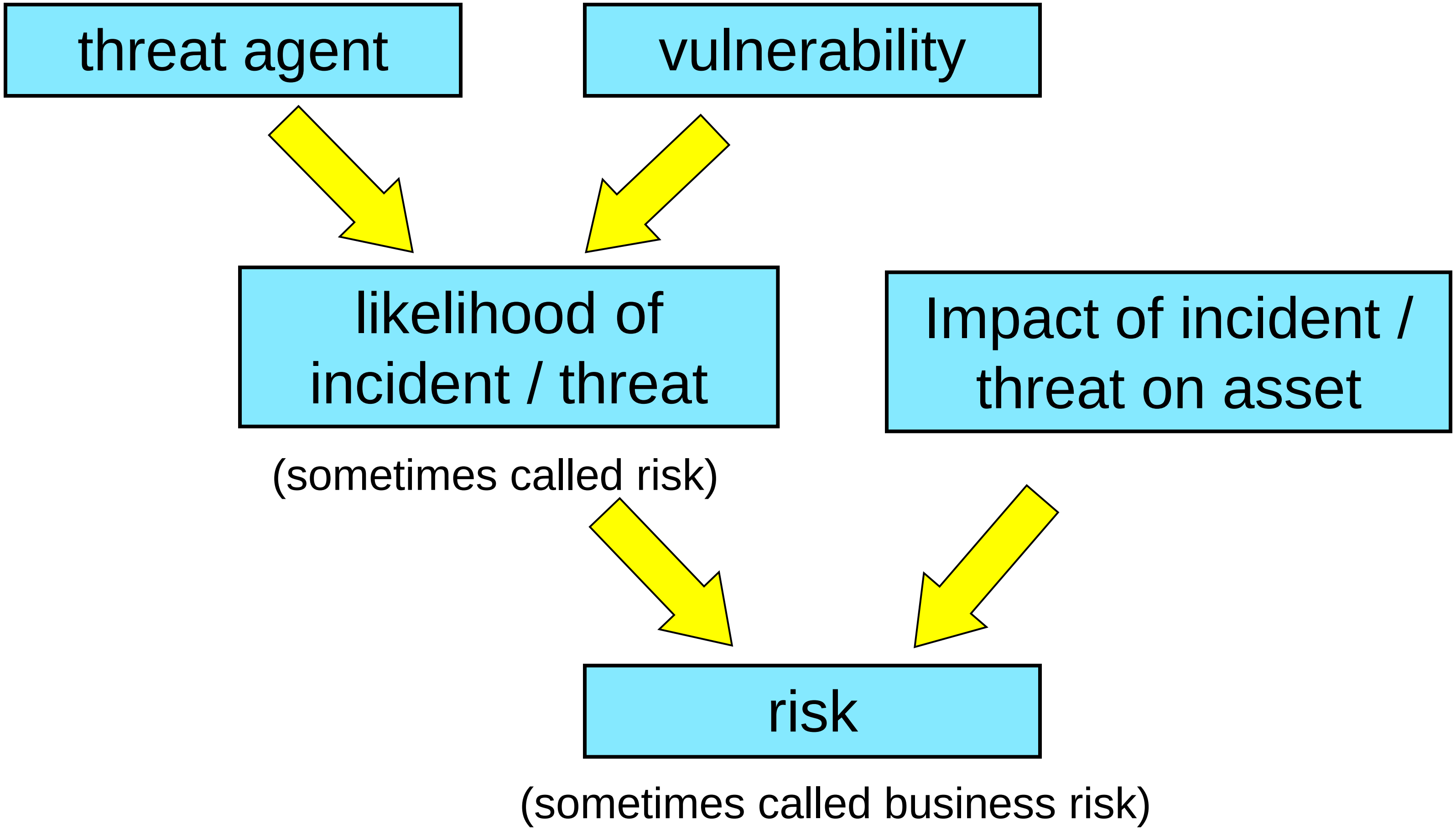


Risk Management

What is risk?

- Risk is assessed as a function of three variables:
  1. Strength of threat agent (e.g. incentive to launch an attack)
  2. Presence (severity) of vulnerabilities
  3. Potential impact of threat occurrence to the business.
  – Elements 1) and 2) are typically combined in the form of likelihood of threat occurrence. If any of these variables approaches zero, the overall risk also approaches zero.

What is risk?



threat agent

vulnerability

likelihood of incident / threat

(sometimes called risk)

Impact of incident / threat on asset

risk

(sometimes called business risk)

What is risk management?

- “IS risk management analyses what can happen and what the possible consequences can be, before deciding what should be done and when, to reduce risk to an acceptable level.”
  - ISO 27005

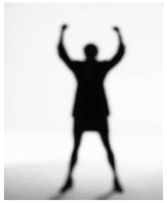
- “Risk management consists of coordinated activities to direct and control an organization with regard to risk.”
  - ISO31000 , ISO/IEC 27002

Risk Management

How much should I spend on securing ?

? Why ?

How much should I spend on securing my reputation ?



- The Proportionality Principle:
  - Identify and apply a set of controls (physical, technical and administrative controls) that match the perceived risk to, and value of, an organisation’s information assets

Basis for assessing risk

- Know yourself: identify, examine, and understand the information and systems with their vulnerabilities
- Know the enemy: identify, examine, and understand relevant threats and the motivation of attackers
- Know responsibility of each stakeholders within an organization to manage risks that are encountered

Problems of measuring risk

Businesses normally wish to risk measure in money, but many of the elements do not allow this

- Uncertain input arguments to risk assessment process
- Valuation of assets
  - Value of data and in-house software - no market value
  - Value of goodwill and customer confidence
- Likelihood of threats
  - How relevant is past data for calculating future probabilities?
    - The nature of future attacks is unpredictable
    - The actions of future attackers are unpredictable
- Measurement of benefit from security measures
  - Problems with the difference of two approximate quantities
    - How does a security control affect a ~10^{-5} probability of attack?

Roles involved in risk management

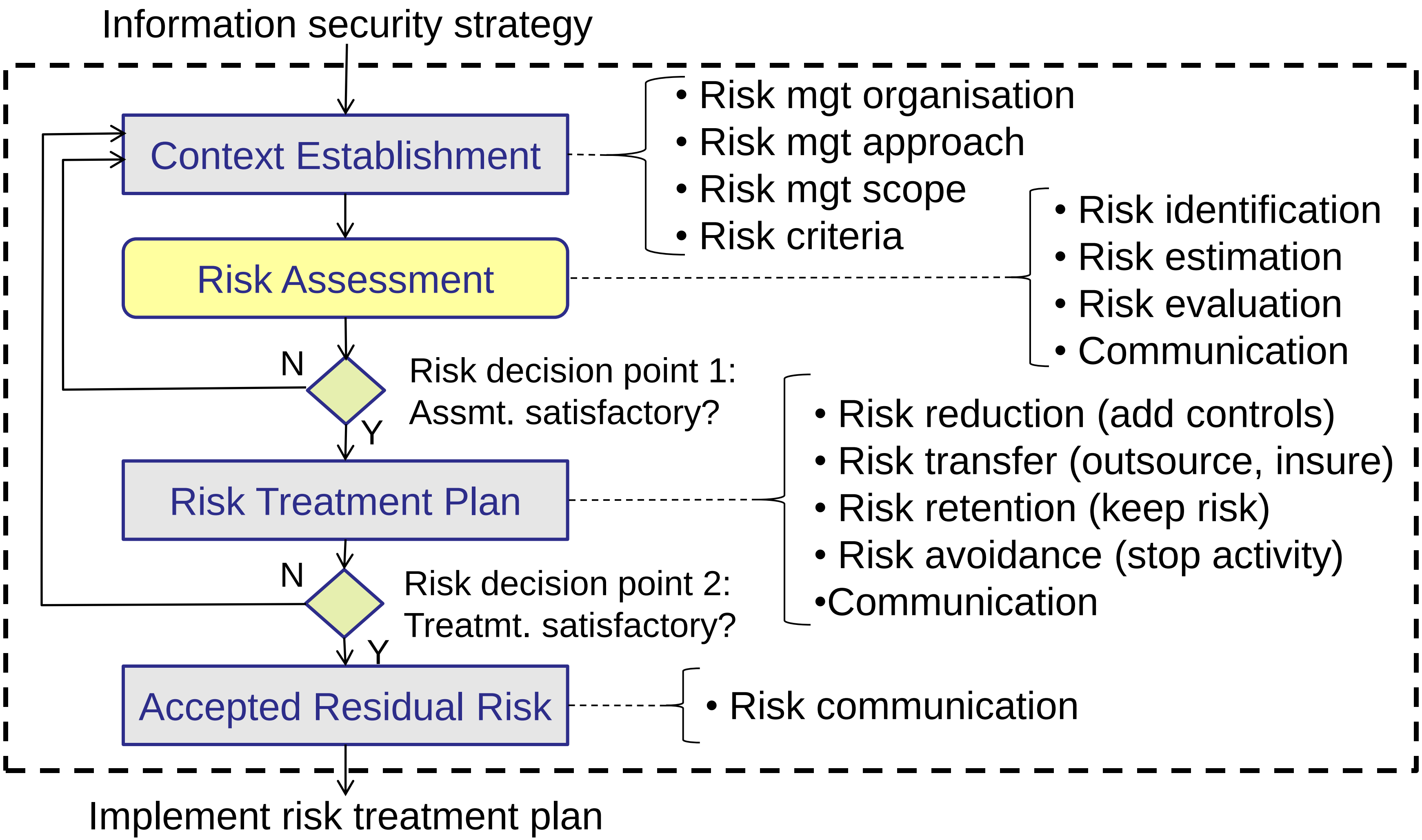
- Management, users, and information technology must all work together
  - Asset owners must participate in developing inventory lists
  - Users and experts must assist in identifying threats and vulnerabilities, and in determining likelihoods
  - Risk management experts must guide stakeholders through the risk assessment process
  - Security experts must assist in selecting controls
  - Management must review risk management process and approve controls

ISMS and Risk management

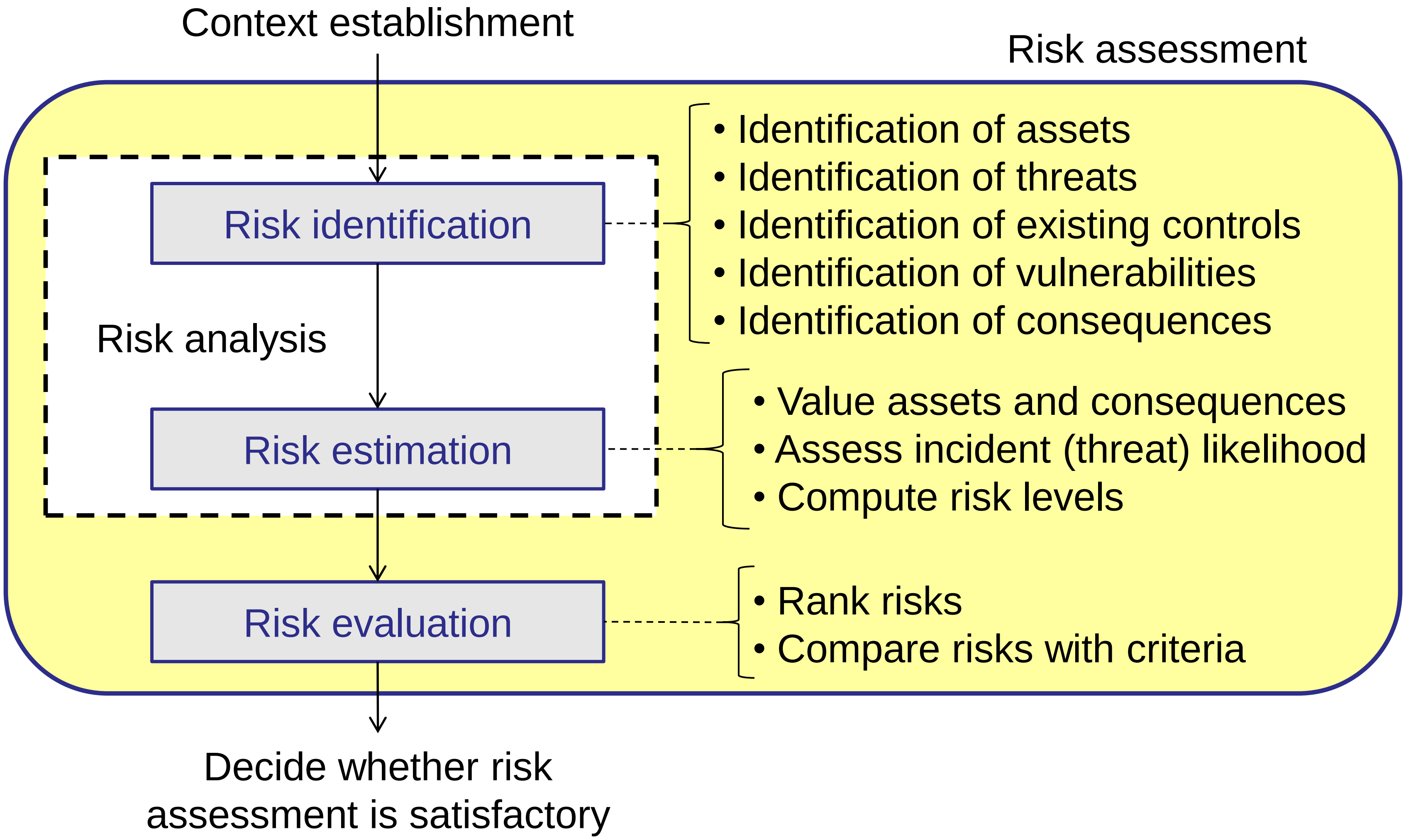
ISMS Phase	Risk management elements
Plan	Risk management process
Do	Implement risk treatment plan
Check	Monitor and review risk environment
Act	Maintain and improve risk management process

Risk management process

ISO 27005



Risk assessment process
ISO 27005



- Identification of assets
- Identification of threats
- Identification of existing controls
- Identification of vulnerabilities
- Identification of consequences

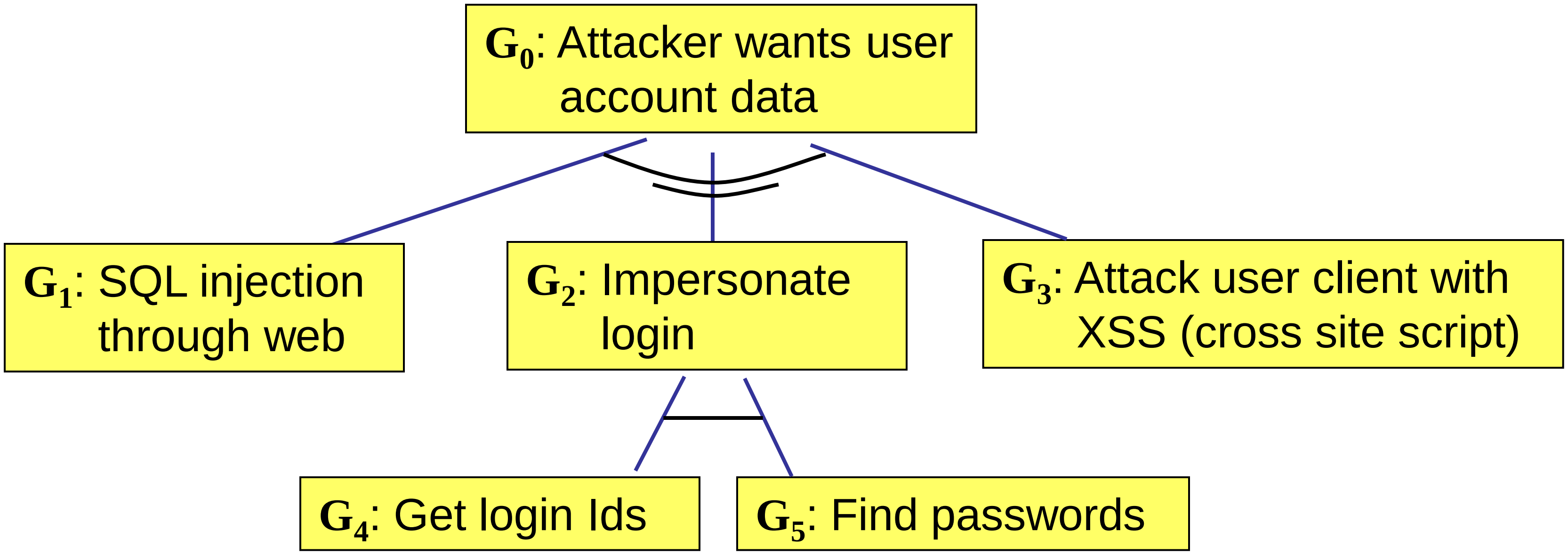
- Value assets and consequences
- Assess incident (threat) likelihood
- Compute risk levels

- Rank risks
- Compare risks with criteria

Threat Modelling and Identification

- Attacker-centric
  - Starts from attackers, evaluates their goals, and how they might achieve them through attack tree. Usually starts from entry points or attacker action.
- System-centric (aka. SW-, design-, architecture-centric)
  - Starts from model of system, and attempts to follow model dynamics and logic, looking for types of attacks against each element of the model. This approach is e.g. used for threat modeling in Microsoft's Security Development Lifecycle.
- Asset-centric
  - Starts from assets entrusted to a system, such as a collection of sensitive personal information, and attempts to identify how security breaches of CIA properties can happen.

Attacker-centric attack tree example



G_0: Attacker wants user account data

G_1: SQL injection through web

G_2: Impersonate login

G_3: Attack user client with XSS (cross site script)

G_4: Get login Ids

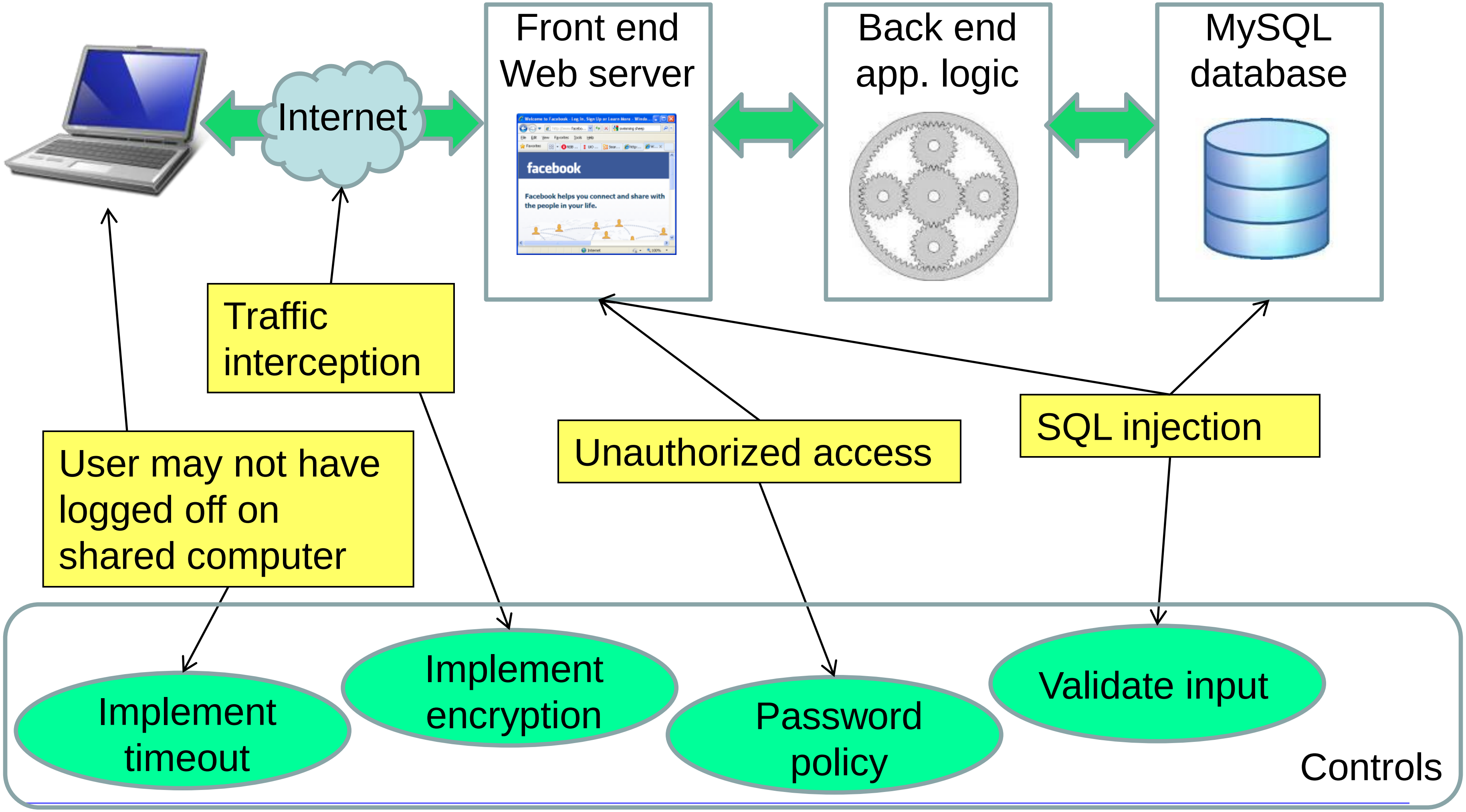
G_5: Find passwords

Legend:

G_0: Main goal	— AND (conjunctive) all subgoals needed	︾ OR (disjunctive) any subgoal needed

Probability of attack success: $p(G_0) = 1-\big(1-p(G_1)\big)\cdot\big(1-\big(p(G_4)p(G_5)\big)\big)\cdot\big(1-p(G_3)\big)$

System-centric threat modelling example



Internet

Front end Web server

Back end app. logic

MySQL database

Traffic interception

User may not have logged off on shared computer

Unauthorized access

SQL injection

Implement timeout

Implement encryption

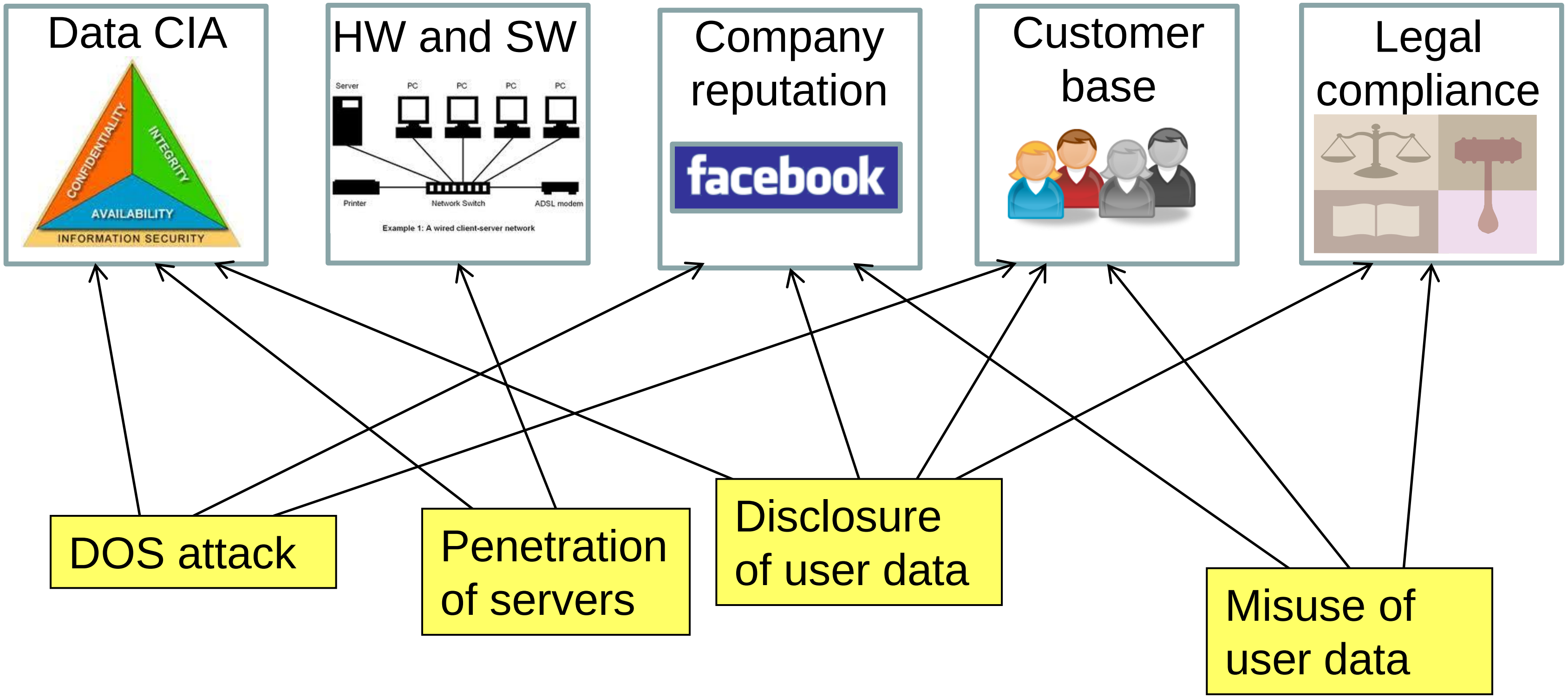
Password policy

Validate input

Controls

facebook
Facebook helps you connect and share with the people in your life.

Asset-centric threat modelling example



Data CIA

HW and SW

Company reputation

Customer base

Legal compliance

DOS attack

Penetration of servers

Disclosure of user data

Misuse of user data

Example threats

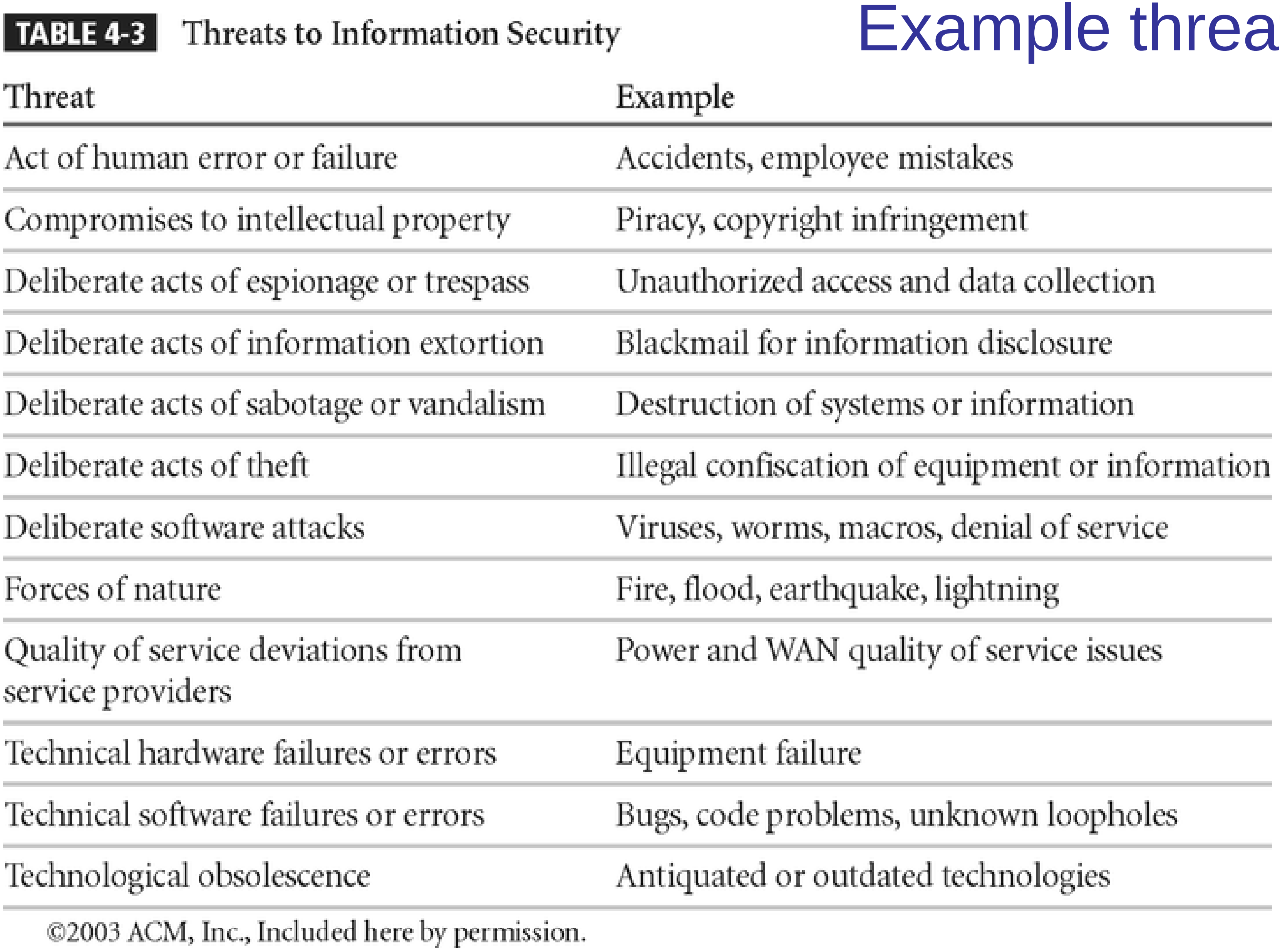


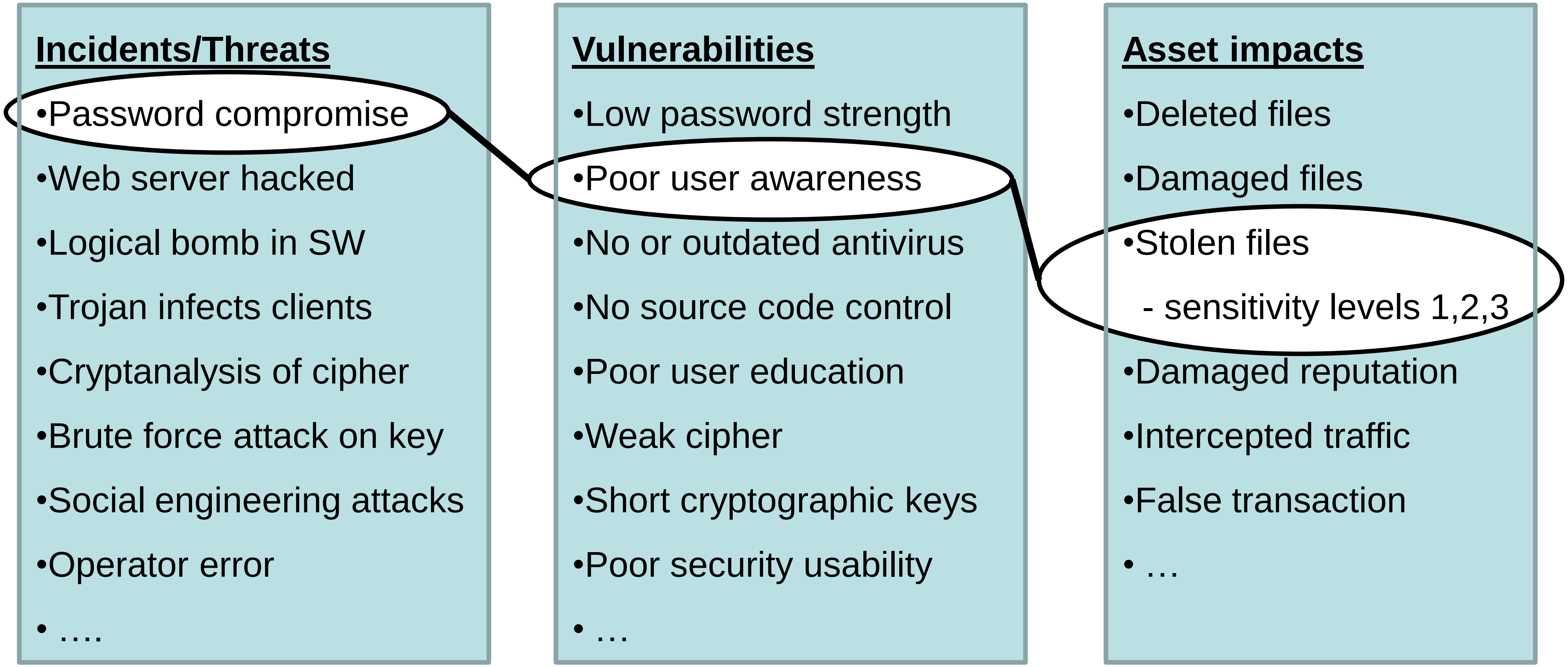
TABLE 4-3 Threats to Information Security

Threat	Example
Act of human error or failure	Accidents, employee mistakes
Compromises to intellectual property	Piracy, copyright infringement
Deliberate acts of espionage or trespass	Unauthorized access and data collection
Deliberate acts of information extortion	Blackmail for information disclosure
Deliberate acts of sabotage or vandalism	Destruction of systems or information
Deliberate acts of theft	Illegal confiscation of equipment or information
Deliberate software attacks	Viruses, worms, macros, denial of service
Forces of nature	Fire, flood, earthquake, lightning
Quality of service deviations from service providers	Power and WAN quality of service issues
Technical hardware failures or errors	Equipment failure
Technical software failures or errors	Bugs, code problems, unknown loopholes
Technological obsolescence	Antiquated or outdated technologies

Vulnerability Identification

- Vulnerabilities are weaknesses that threat agents can exploit to attack an information asset
- Examine how each incident/threat could be perpetrated and list organization’s assets and vulnerabilities
- Process works best when people with diverse backgrounds within organization work iteratively in a series of brainstorming sessions
- At end of risk identification process, list of assets and their vulnerabilities is achieved

Identifying risks



Incidents/Threats

•Password compromise

•Web server hacked

•Logical bomb in SW

•Trojan infects clients

•Cryptanalysis of cipher

•Brute force attack on key

•Social engineering attacks

•Operator error

• ….

Vulnerabilities

•Low password strength

•Poor user awareness

•No or outdated antivirus

•No source code control

•Poor user education

•Weak cipher

•Short cryptographic keys

•Poor security usability

• …

Asset impacts

•Deleted files

•Damaged files

•Stolen files

- sensitivity levels 1,2,3

•Damaged reputation

•Intercepted traffic

•False transaction

• …

- Identify valid combinations of incident, vulnerability and asset impact

Information Asset Valuation

- Questions that help in valuation of assets

- Which information asset:

– is most critical to organization’s success?

– generates the most revenue/profitability?

– would be most expensive to replace or protect?

– would be the most embarrassing or cause greatest liability if revealed?

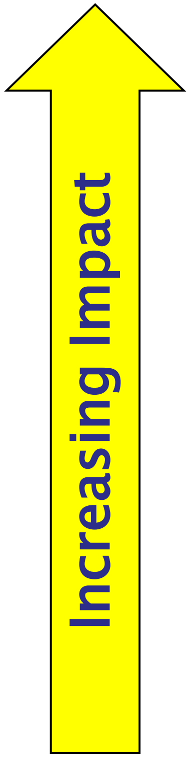
Estimate risks

Types of analysis

- **Qualitative**
  - Uses descriptive scales. Example:
    - Impact level: Minor, moderate, major, catastrophic
    - Likelihood: Rare, unlikely, possible, likely, almost certain
- **Semi-quantitative**
  - Qualitative scales assigned numerical values
  - Can be used in formulae for prioritization (with caution)
- **Quantitative**
  - Use numerical values for both consequence (e.g. $$$) and likelihood (e.g. probability value)

Qualitative risk estimation example

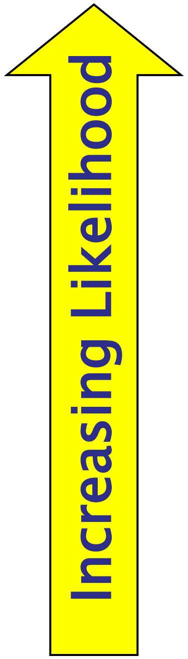
Qualitative Impact level scale



Impact Level	Description
Major	**Major problems** would occur and threaten the provision of important processes **resulting in significant financial loss**.
Moderate	**Services would continue**, but would **need to be reviewed or changed.**
Minor	Effectiveness of services would be **threatened but dealt with**.
Insignificant	Dealt with as a part of **routine operations**.

Qualitative risk estimation example

Qualitative likelihood scale



Likelihood	Description
High	Is expected to occur in most conditions (1 or more times per year).
Medium	The event will probably happen in most conditions (2 years).
Low	The event should happen at some time (5 years).
Unlikely	The event could happen at some time (10 years).

Qualitative risk estimation example

Additive risk derivation: Add likelihood & impact level

Impact level

Likelihood

	(0) Insignificant	(1) Minor	(2) Moderate	(3) Major
(3) High	(3) M	(4) H	(5) VH	(6) E
(2) Medium	(2) L	(3) M	(4) H	(5) VH
(1) Low	(1) VL	(2) L	(3) M	(4) H
(0) Unlikely	(0) N	(1) VL	(2) L	(3) M

Legend
E: extreme risk; immediate action required
(V)H: (very) high risk; senior management attention needed
M: moderate risk; management responsibility must be specified
(V)L: (very) low risk; manage by routine procedures
N: Negligible risk; To be ignored

Semi-quantitative risk estimation example

Multiplicative risk derivation: : Multiply likelihood & impact

Impact level

Likelihood

	(0) Nil	(1) Insignificant	(2) Minor	(3) Moderate	(4) Major
(4) High	(0) Nil	(4) M	(8) H	(12) VH	(16) E
(3) Medium	(0) Nil	(3) L	(6) M+	(9) H+	(12) VH
(2) Low	(0) Nil	(2) VL	(4) M	(6) M+	(8) H
(1) Unlikely	(0) Nil	(1) Neg	(2) VL	(3) L	(4) M
(0) Never	(0) Nil	(0) Nil	(0) Nil	(0) Nil	(0) Nil

Legend **M: moderate risk**; Responsibility must be specified **E: extreme risk**; Immediate action required
L: low risk; Manage by routine procedures **VH: very high risk**; Priority
action action
VL: very low risk; Manage by routine procedures **H+: high risk +**; Management attention
Neg: Negligible risk; Can be ignored **H: high risk**; Management
attention
Nil: Nil risk; No risk exists, ignore **M+: moderate risk +**;
Responsibility must be specified

Quantitative risk estimation example

Example quantitative risk analysis method

- Quantitative parameters
  - Asset Value (AV)
    - Estimated total value of asset
  - Exposure Factor (EF)
    - Percentage of asset loss caused by threat occurrence
  - Single Loss Expectancy (SLE)
    - SLE = AV × EF
  - Annualized Rate of Occurrence (ARO)
    - Estimated frequency a threat will occur within a year
  - Annualised Loss Expectancy (ALE)
    - ALE = SLE × ARO

Quantitative risk estimation example

Example quantitative risk analysis

- Risk description
  - Asset: Public image (and trust)
  - Threat: Defacing web site through intrusion
  - Impact: Loss of image
- Parameter estimates
  - AV(public image) = $1,000,000
  - EF(public image affected by defacing) = 0.05
  - SLE = AV × EF = $50,000
  - ARO(defacing) = 2
  - ALE = SLE × ARO = $100,000
- Justifies spending up to $100,000 p.a. on controls

Evaluate risks

- Compare
  - the level of risk found during risk analysis with
  - the established risk criteria
  - NOTE: Consider analysis and criteria on same basis - qualitative or quantitative
- Output: prioritized list of risks for further action
  - Risks in low or acceptable risk categories, may be accepted without further treatment

Risk listing and ranking

Incident / Threat	Existing controls & vulnerabilities	Asset impact	Impact level	Likelihood description	Likelihood	Risk level
Compromise of user password	No control or enforcement of password strength	Deleted files, breach of confidentiality and integrity	MODE RATE	Will happen to 1 of 50 users every year	MEDIUM	HIGH
Virus infection on clients	Virus filter disabled on many clients	Compromise of clients	MODE RATE	Will happen to 1 in 100 clients every year	HIGH	EXTREME
Web server hacking and defacing	IDS, firewall, daily patching, but zero day exploits exist	Reputation	MINOR	Could happen once every year	LOW	LOW
Logical bomb planted by insider	No review of source code that goes into production.	Breach of integrity or loss of data	MAJOR	Could happen once every 10 years	UNLIKELY	MODE RATE

Risk ranking complexity

Incident / Threat	Existing controls & vulnerabilities	Asset impact	Impact level	Likelihood description	Likelihood	Risk level
Router Compromise	Password only	Intrusion and disruption	MODE RATE	Many times per year	HIGH	HIGH
Physical Destruction of Data Centre	None (not addressed in BCP)	Operations Disrupted for one month	MAJOR	Could happen once in 25 years	LOW	HIGH

- Not easy to prioritize risks of same level but with different impact levels and likelihood

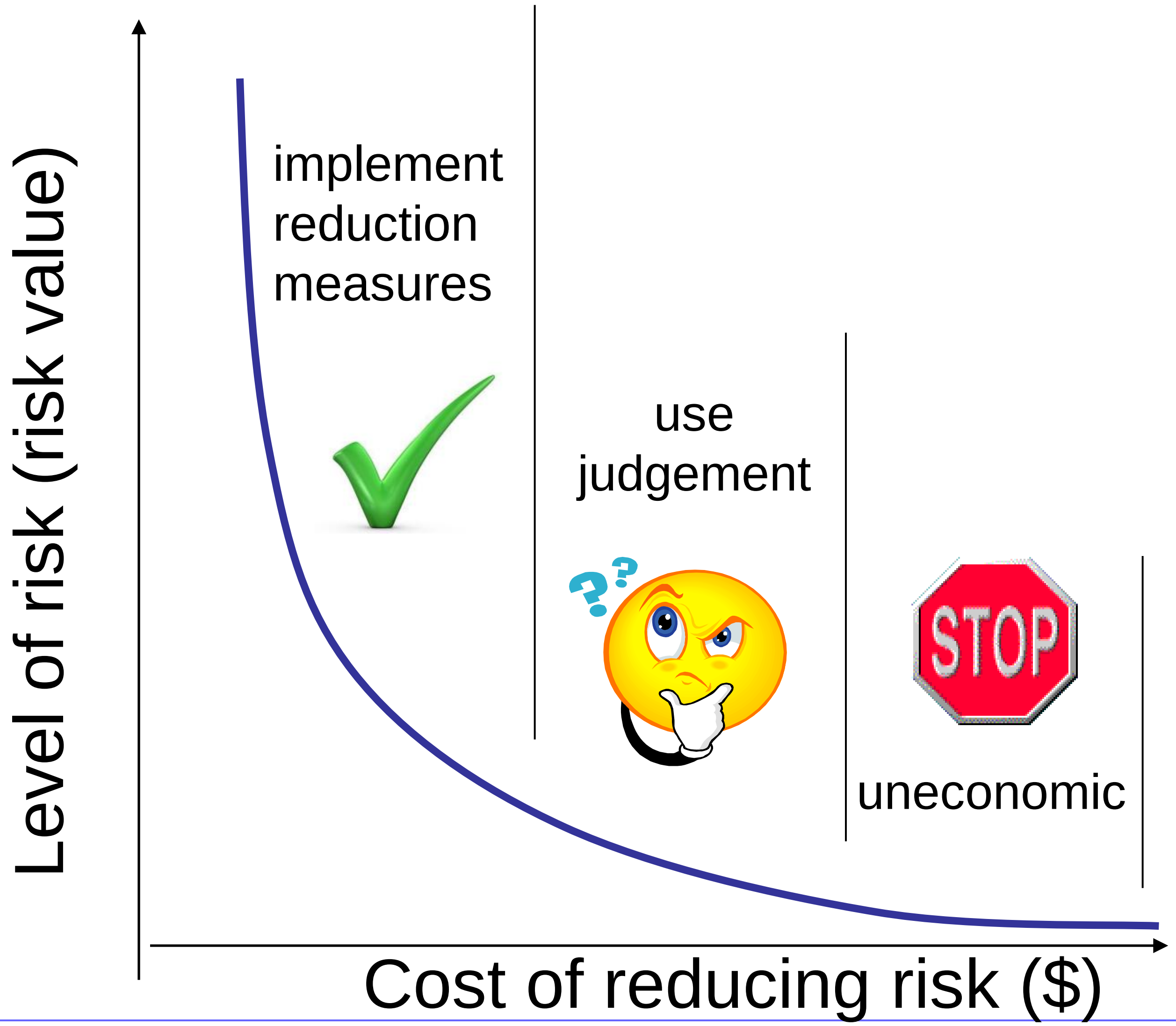
Documenting the results of risk assessment

- Final summary comprised in ranked vulnerability risk worksheet
- Worksheet details asset, asset impact, vulnerability, vulnerability likelihood, and risk-rating factor
- Ranked vulnerability risk worksheet is initial working document for next step in risk management process: assessing and controlling risk

Treat risks economically

- Assess risk treatment based on the extent of risk reduction, and any additional benefits obtained
  - High risk levels may be acceptable if beneficial opportunities arise as a result of taking the risk
- Balance cost of implementing treatment option and benefits derived (proportionality principle)
  - Large risk reductions for low expenditure should be implemented

Risk treatment economy



Risk Control Strategies

- Once ranked vulnerability risk worksheet complete, must choose one of four strategies to control each risk:
  - Reduce risk (security controls, reduce vulnerabilities)
  - Mitigate risk (incident response, business continuity)
  - Transfer risk (outsource activity that causes risk, or insure)
  - Retain risk (understand tolerate potential consequences)
  - Avoid risk (stop activity that causes risk)

Treating risk from the positive perspective

- Identify options for risk treatment by seeking opportunities that might increase positive outcomes without increasing the risk.
- Options include:
  - **Actively seek** an opportunity
  - **Change the likelihood of opportunity** to enhance the likelihood of beneficial outcome
  - **Change the consequences** to increase the extent of the gains
  - **Sharing** the opportunity
  - **Retain** the residual opportunity

Feasibility and evaluation

- To determine the most optimal security solution, explore and analyse information about economic/noneconomic consequences of vulnerability of information asset
  - e.g. CBA (Cost Benefit Analysis)

- To assess whether security solution had the desired effect, security measurements must be implemented and analysed

Cost Benefit Analysis (CBA)

- Most common approach for deciding on information security controls is economic feasibility of implementation
- CBA is begun by evaluating worth of assets to be protected and the loss in value if those assets are compromised
- The formal process to document this is called cost benefit analysis or “economic feasibility study”

Cost Benefit Analysis (CBA) Formula

- CBA determines if alternative being evaluated is worth cost incurred to control vulnerability
- Calculated using ALE assessed before and after implementation of proposed control.
- ALE(prior) is annualized loss expectancy of risk before implementation of control
- ALE(post) is estimated ALE based on control being in place for a period of time
- ACS is the annualized cost of the safeguard (control)

$$\text{CBA} = \text{ALE(prior)} – \text{ALE(post)} – \text{ACS}$$

Evaluation, Assessment, and Maintenance of Risk Controls

- Selection and implementation of control strategy is not end of process
- Strategy and accompanying controls must be monitored/reevaluated on ongoing basis to determine effectiveness and to calculate more accurately the estimated residual risk
- Implement metrics for measuring effectiveness of controls
- Process continues as long as organization continues to function

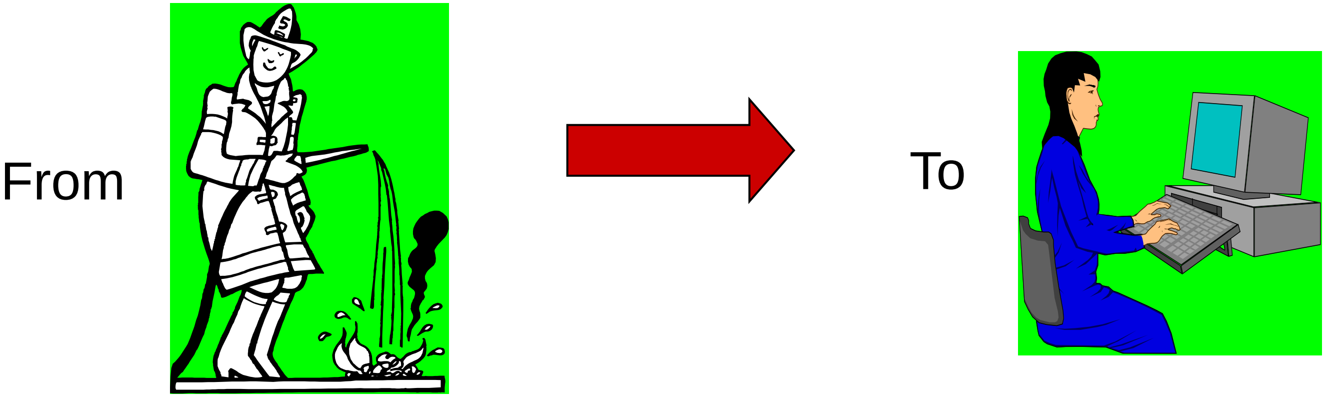
Business Continuity Planning

Business continuity management

- Establishes a strategic and operational framework to implement, proactively, an organization’s resilience to disruption, interruption or loss in conducting its business.
- Defines procedures for the recovery of an organization's facilities in case of major incidents and disasters, so that the organization will be able to either maintain or quickly resume mission-critical functions
- Typically, BC management involves an analysis of critical business processes and continuity needs
- May also include a significant focus on disaster prevention

BCP Terminology

- Business Continuity Plan
  - Plan for restoring normal business functions after disruption
- Business Contingency Plan
  - Same as Business Continuity Plan
  - Contingency means ”something unpredictable that can happen”
- Disaster Recovery
  - Restablishment of business functions after a desaster, possibly in temporary facilities



From

To

Business continuity management

- How common is BCM in 'the real world'?
- 2006 CCSS extract: Most commonly reported categories of computer security policies and procedures 2006 (2005, 2004):
  - Media backup procedures - 95% (96%, 95%)
  - User access management - 93% (97%, 94%)
  - External network access control procedures - 78% (83%, 79%)
  - Documented operating procedures - 76% (80%, 83%)
  - User responsibilities policies - 72% (82%, 78%)
  - Controls against malicious software - 66% (75%, 72%)
  - Monitoring system access and use - 64% (72%, 68%)
  - Change control procedures - 60% (82%, 75%)
  - Clock synchronisation policy – 59% (59%, 43%)
  - Decommissioning equipment procedures – 59% (65%, 40%)
  - System audit policy – 58% (71%, 58%)
  - **Business continuity management – 54%** (73%, 58%)
  - Incident management procedures - 51% (67%, 64%)

Business continuity management

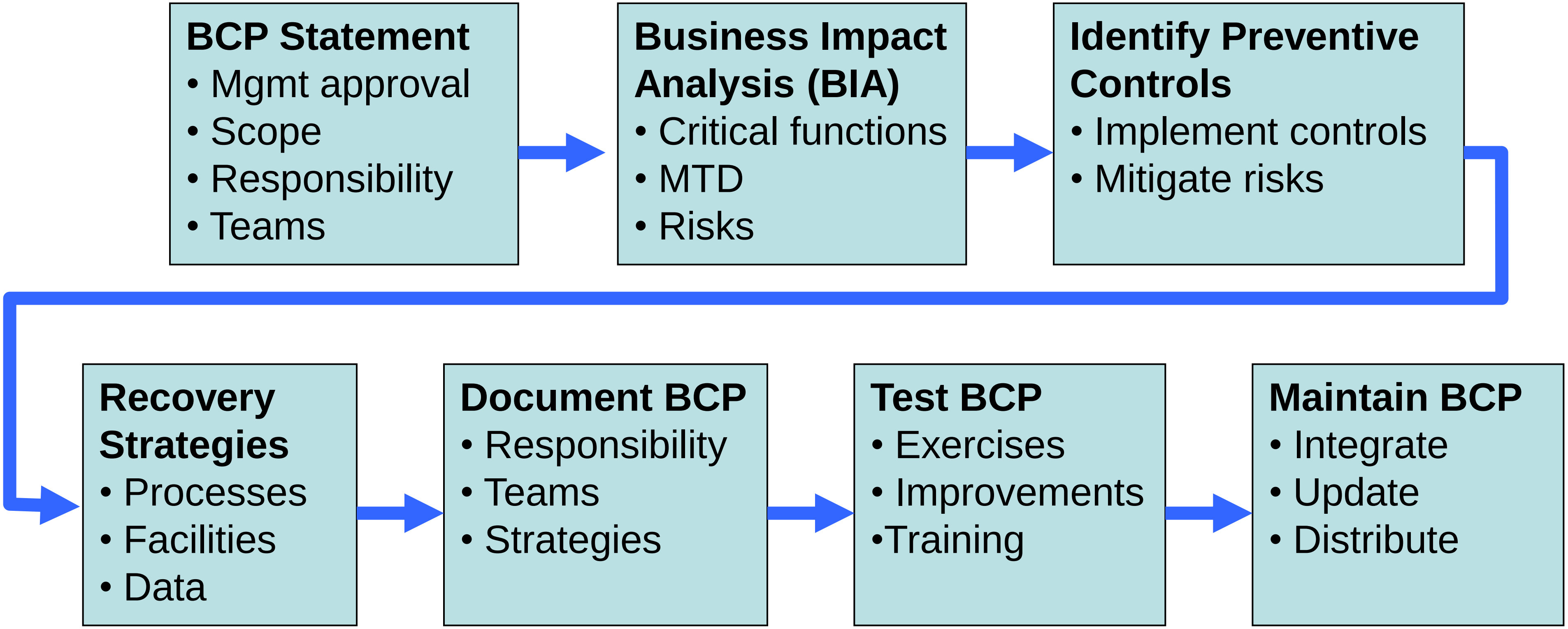
- The range of incidents and disasters to be considered include:
  - Acts of nature, for example:
    - Excessive weather conditions
    - Earthquake
    - Flood
    - Fire
  - Human acts (inadvertent or deliberate), for example:
    - Hacker activity
    - Mistakes by operating staff
    - Theft
    - Fraud
    - Vandalism
    - Terrorism

Business Continuity Plan (BCP)

The business continuity plan describes:

- a sequence of actions
- and the parties responsible for carrying them out
- in response to disasters
- in order to restore normal business operations as quickly as possible

BCP Development



BCP Statement
- Mgmt approval
- Scope
- Responsibility
- Teams

Business Impact Analysis (BIA)
- Critical functions
- MTD
- Risks

Identify Preventive Controls
- Implement controls
- Mitigate risks

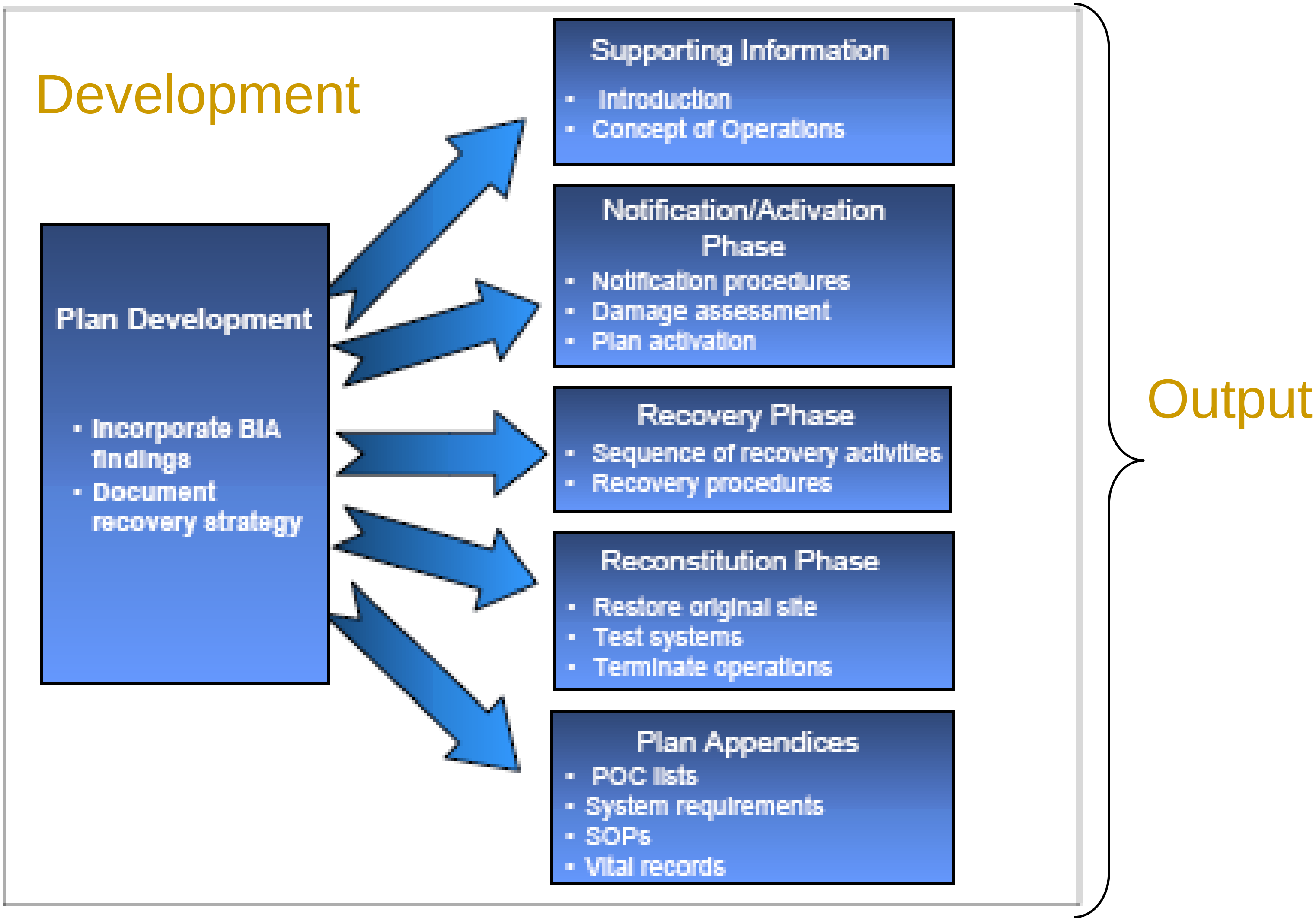
Recovery Strategies
- Processes
- Facilities
- Data

Document BCP
- Responsibility
- Teams
- Strategies

Test BCP
- Exercises
- Improvements
- Training

Maintain BCP
- Integrate
- Update
- Distribute

Source: NIST Special Publication 800-34
Contingency Planning Guide for Information Technology Systems (p.14)



Development

Plan Development

- Incorporate BIA findings
- Document recovery strategy

Supporting Information

- Introduction
- Concept of Operations

Notification/Activation Phase

- Notification procedures
- Damage assessment
- Plan activation

Recovery Phase

- Sequence of recovery activities
- Recovery procedures

Reconstitution Phase

- Restore original site
- Test systems
- Terminate operations

Plan Appendices

- POC lists
- System requirements
- SOPs
- Vital records

Output

BCP Development and Output: NIST SP800-34, p.31

BCP Development - BIA

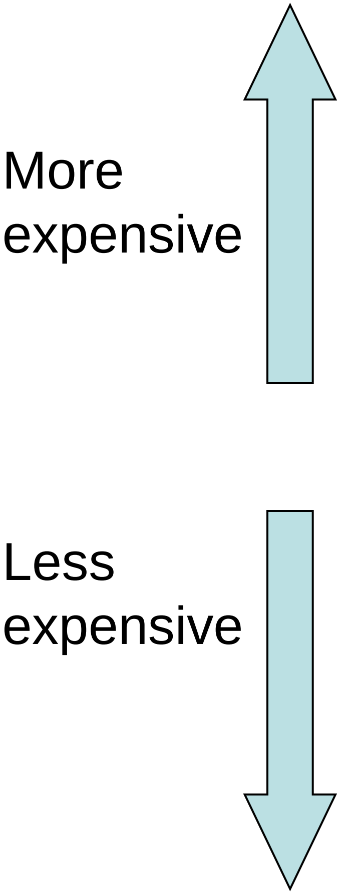
- A Business Impact Analysis (BIA) is performed as part of the BCP development to identify the functions that in the event of a disaster or disruption, would cause the greatest financial or operational loss.
- Consider e.g.:
  - IT network support
  - Data processing
  - Accounting
  - Software development
  - Payroll

Customer support
Order entry
Production scheduling
Purchasing
Communications

BCP Development - BIA

- The MTD (Maximum Tolerable Downtime) is defined for each function in the event of disaster.
- Example:
  - Non-essential = 30 days
  - Normal = 7 days
  - Important = 72 hours
  - Urgent = 24 hours
  - Critical = minutes to hours

BCP Development - Alternative Sites



More expensive

Less expensive

- Redundant site
  - Mirror of the primary processing environment
  - Operable within minutes
- Hot site
  - Fully configured hardware and software, but no data
  - Operable within hours
- Mobile site
- Warm site
  - Partially configured with some equipment, but not the actual computers
  - Operable within days
- Cold site
  - Basic electricity and plumbing
  - Operable within weeks

BCP Development – Strategy Selection

- Analyse alternative disaster recovery strategies
  - Choosing data and software backup facility
  - Choosing alternative site type and contract
  - Human resources
  - Insurance
  - Reciprocal and mutual aid agreements
  - Multiple processing centres
  - Data processing service bureaus

  with respect to BIA, cost, restoration time and practicality

BCP Components

- Supporting information
  - Establish purpose, applicability and scope
  - System description and staff responsibilities
- Notification/Activation Phase
- Recovery Phase
- Reconstruction Phase
- Appendices
  - Contact information
  - SOPs and checklists
  - Equipment and system requirements lists

BCP Phases

- A security incident can vary in magnitude from minor incident to major disaster.
- Different sub-plans needed for different phases in the business continuity process.
  - Plan for activation phase
  - Plans for recovery phase
  - Plan for reconstitution phase

BCP Activation Phase Plan

- Actions to take immediately after incident
  - Procedures for contacting recovery teams
  - Assessment of damage to primary site facilities
    - Estimated outage time at primary site
    - Compare with predefined MTD and activation criteria
  - Notify BC management
  - Management declares a disaster if criteria are met
  - Start implementing BCP
- BCP activation responsibility
  - Only one person
  - CEO or other predefined role
  - Succession of responsibility must be predefined

BCP Recovery Phase Plans

- Evacuation and safety of personnel
  - Always first priority
- Notifying alternative sites
- Securing home site
- Activation of recovery teams
- Relocation to alternative sites
- Resumption of critical business functions
- Reviewing how the organisation will interface with external parties (customers, partners) from alternative site

BCP Reconstitution Phase Plan

- Plan for returning to normal operations at primary site
  - Repairing primary site, or prepare new site
  - Installing hardware and software
  - Testing business functions
  - Migrating business functions stepwise
    - Least critical functions first
    - Most critical functions last
  - Shutting down alternative site
  - Securing and removing sensitive data from alternative site

BCP Appendices

- Include
  - Contact information for key personnel
    - Call tree data
  - Contact information for vendors and alternative site providers
    - Including SLA and reciprocal agreements
  - Checklists for recovery processes
  - Equipment and systems requirement lists
  - Description of and directions to alternative site

BCP Testing

- Checklist test
  - Copies of the BCP distributed to departments for review
- Structured walk-through test
  - Representatives from each department come together to go through the plan
- Simulation test
  - All staff in operational and support functions come together to practice executing the BCP
- Parallel test
  - Business functions tested at alternative site
- Full interruption test
  - Business functions at primary site halted, and migrated to alternative site in accordance with the BCP

ISMS Implementation

- The security organisation
- Security program challenges
- The Capability Maturity Model
- Security metrics

Essential elements of security program

1. The development of the security program must be the execution of an appropriate information security strategy, closely aligned with and supporting organisational objectives.
2. Cooperation and support from management and stakeholders is a condition for the security program.
3. Effective metrics must be designed for the program implementation phase, as well as for the subsequent ongoing security program operation, in order to assess the effectiveness of the program.

The security organisation

Board of Directors

Recognise security as a strategic priority.
Review Risk assessment & Business Impact Analysis
Define penalties for non-compliance of policies

Executive Mgmt

Define security objectives,
institute security organization,
approve security policy, risk assessment
and risk treatment plan

Senior representatives
of business functions
ensures alignment
of security program
with business
objectives

Security Steering Committee

Chief Info Security Officer (CISO)

Other positions:
Chief Risk Officer (CRO)
Chief Compliance Officer (CCO)

Security Positions

Security Architect

- Design secure network topologies, access control, security policies & standards.
- Evaluate security technologies
- Work with compliance, risk mgmt, audit

Security Administrator

- Allocate access to data under data owner
- Prepare security awareness program
- Test security architecture
- Monitor security violations and take corrective action
- Review and evaluate security policy

Setting up a IS Steering Committee

A security steering committee is crucial for effective management of security.

- Identify the right members for the committee. Apart from the CISO, consider representatives from HR, finance, internal audit, legal and admin team, major departments
- Setup a membership approval process. Any addition to the ISSC must be approved by the CEO and CIO
- Identify the committee responsibilities. This is crucial as it should not happen that the quarterly meetings end up only as review meetings with the CISO on incidents.

Security steering committee tasks

- Interviews by security manager of department leaders and business process owners should identify
  - Major organisational issues and concerns
- Steering committee drafts policies for security program
- Steering committee initiates security projects
- Members of security steering committee represent business interests, security goals will by definition be strategically aligned with business objectives

IS program = set of IS control activities

Security control activities

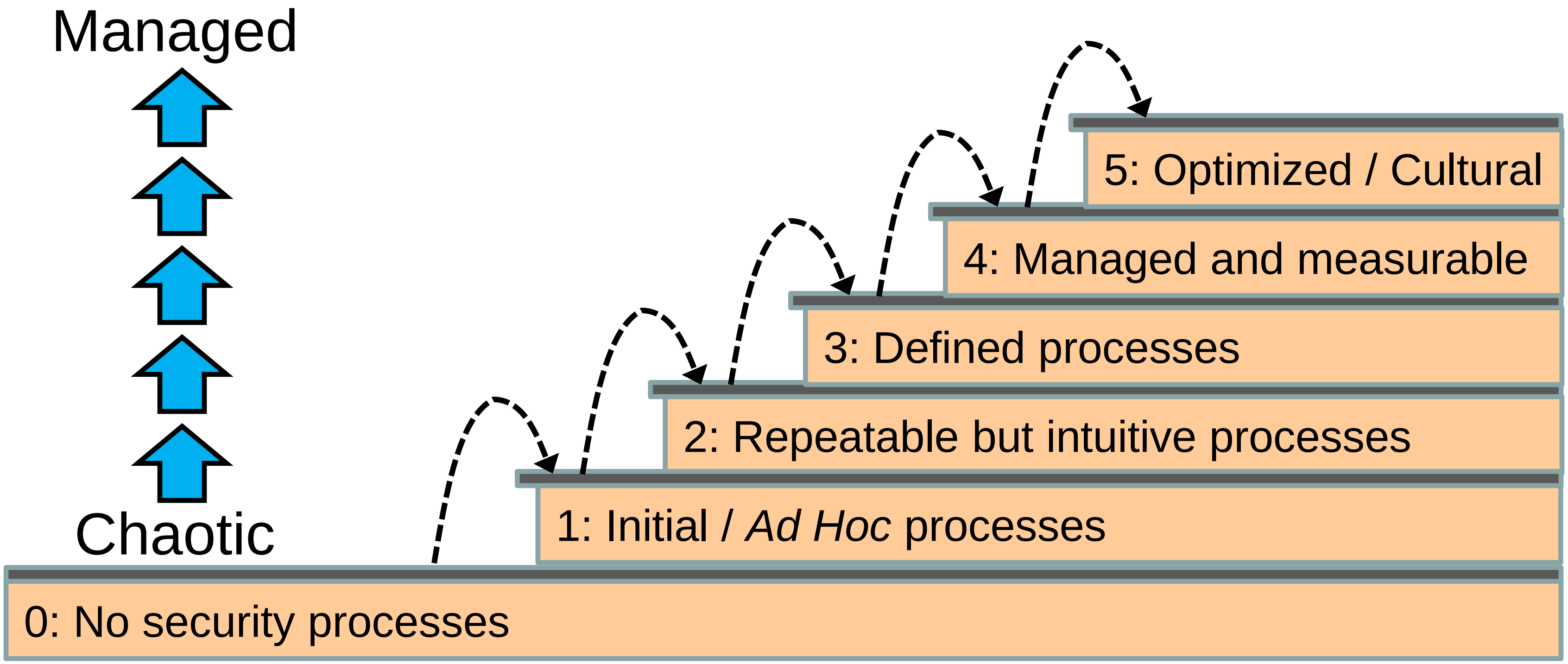
IS project

IS program

- A security project is distinct from the security control activity itself. Once the project is accomplished, then the security control is operational.

COBIT CMM (Capability Maturity Model) for IS management

Considerable effort and time is required to reach each next level in the maturity model.



Managed

Chaotic

5: Optimized / Cultural

4: Managed and measurable

3: Defined processes

2: Repeatable but intuitive processes

1: Initial / *Ad Hoc* processes

0: No security processes

CMM levels 1 - 3

1. Initial / Ad Hoc
   - Processes are ad-hoc and disorganised.
   - Risks are considered on an ad hoc basis, but no formal processes exist.
2. Repeatable but intuitive
   - Processes follow a regular pattern.
   - Emerging understanding of risk and the need for security
3. Defined process
   - Processes are documented and communicated.
   - Company-wide risk management.’
   - Awareness of security and security policy

CMM levels 4 - 5

4. Managed and measurable
   - + Processes are monitored and measured.
   - + Risks assessment standard procedures
   - + Roles and responsibilities are assigned
   - + Policies and standards are in place
5. Optimized
   - + Security culture permeates organisation
   - + Organisation-wide security processes are implemented, monitored and followed

Measuring CMM

- Measuring Capability maturity is not straight forward.
  - Adding up scores?
- **It takes “time and effort”** to complete CMM assessments.
  - ISO 27001: 133 controls consisting of 500+ CMM statements
  - CobIT: 1000+ CMM statements
- Not an exact science, difficult to use as absolute measure. Can give unreasonable results e.g. when consultants and auditors are too lenient or too strict.
- Makes most sense when audit conducted by the same person/time every year, as a measure of improvement.

Security control objectives

ISO 27002

1. Risk assessment
2. Security policy
3. IS governance
4. Asset management
5. HR security
6. Physical and envir. security
7. Comm. & networks security
8. Access control
9. Security in applications
10. IS incident management
11. Business continuity
12. Compliance

COBIT

1. Management of IT security
2. IT Security Plan
3. Identity management
4. User account management
5. Security testing, surv. & mon.
6. Security incident definition
7. Protection of security tech.
8. Crypto key management
9. Malicious SW prev, det. & corr.
10. Network security
11. Exchange of sensitive data

Security awareness training

- Back up and protection of work related information
- Passwords
- Email and web hygiene and acceptable use
- Recognising social engineers
- Recognising and reporting security incidents
- Responsibilities and duties for security
- Consequences of negligence or misbehaviour
- Security principles for system and business processes

Security metrics

- How do we know how “secure” an organization is?
  - Metrics help define “secure”
  - Metrics let us benchmark our security investments against other organizations
  - Compliance
  - The metrics “gathering” process often leads to identification of security inconsistencies or holes

Why do we care: Example

- The CEO asks, *“Are we secure?”*
- Without metrics:
  “Well, it depends on how you look at it.”
- With metrics:
  “Yes, our evidence tells us that we are. Look at our risk score before we implemented that firewall project. It’s down 10 points. We are definitely more secure today than we were before.”

Why do we care: Example

- The CEO asks: *“Have the changes that we implemented improved our security posture?”*
- Without metrics:
  “They must have, that’s why we did the changes”
- With metrics:
  “Absolutely. Look at our risk exposure before we implemented the recommended changes, it’s down by 25 points. No question, the changes reduced our security risk.”

What is a metric?

- NIST define metrics as tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.
- Security metrics are simply methods of measuring an organization’s security posture.
- Although there are some published standards for measuring security, ideally security metrics should be adjusted and tuned to fit a specific organization or situation.

Examples of metrics

- Total number of remote connections over a one month period (VPN, ISDN, dial-up, remote desktop)
- The percentage of total applications that have a contingency plan by application criticality.
- Time to analyze and recommend action on a security event
- Number of Linux servers at least 90% compliant with the Linux platform security standard

Security Metric Categories

- Platform
  - Number of Linux servers that are compliant with file encryption policy
- Network
  - DMZ port scans
- Incident
  - Number of hosts infected with worm XYZ
- People
  - Number of terminated employees with system access
- Industry
  - Number of public security incidents in sector with severity score Z
- Political
  - Hacktivism scores, amount of sites listing sector/company ABC as potential target

Security Metric Types

- Real Time
  - Number of concurrent connections to VPN
  - Usually from incident response systems
- Polled
  - Number of password reset requests (monthly),
  - Usually from SA’s or SME’s
- Incident based
  - Number of machines infected with worm XYZ
  - Number of vendors suffering from infections of worm XYZ
  - Usually from industry intelligence/incident response/SA’s and SME’s

How do we decide which one’s to collect?

- Policy Mining / Easy to Spot Anomalies
- Risk Scoring
- ROI / Vendor Evaluations
- Regulatory / Cover the industry standards
- “Tips” / Visionaries

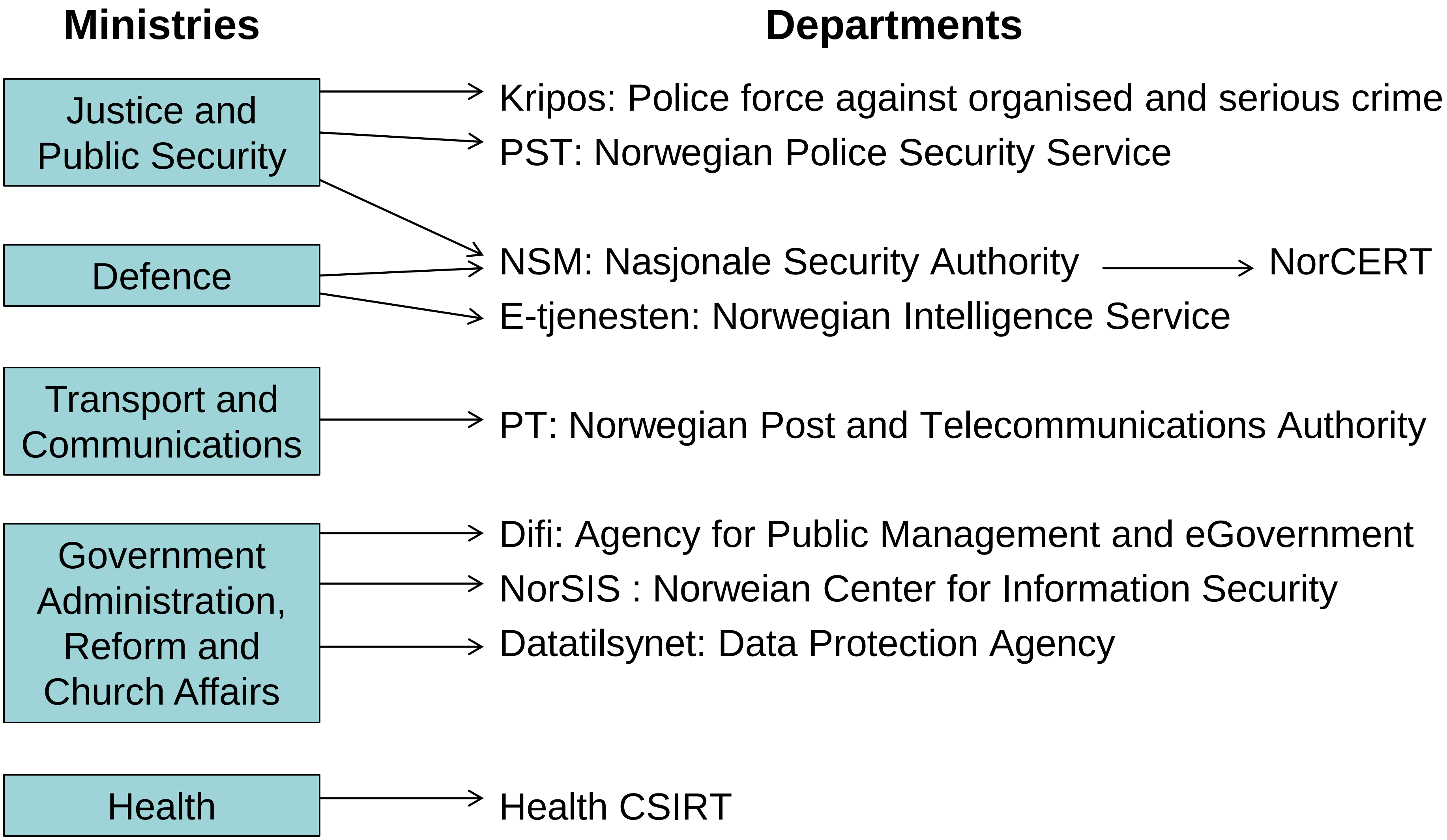
Effective risk analysis through security metrics

- How to make security management decisions based on the collected metrics?
  - Correlate metrics with high impact risks items.
  - Derive conclusion about the change in risk for those items
- It makes most sense to spend money collecting metrics that are relevant for high risk items

National Security

- CIP (Critical Infrastructure Protection)
  - Most critical components of modern society depend on IT
- CIIP (Critical Information Infrastructure Protection)
  - Specific IT systems are by themselves critical components
- The accumulated set of non-critical systems (e.g. servers and networks in SMEs) becomes critical
- IT systems are both targets and weapons of attack in industrial, political and international conflicts
- The vulnerability of the critical information infrastructure is worrisome and needs attention

National Authorities on Information Security



Ministries

Departments

Justice and Public Security

Defence

Transport and Communications

Government Administration, Reform and Church Affairs

Health

Kripos: Police force against organised and serious crime

PST: Norwegian Police Security Service

NSM: Nasjonale Security Authority → NorCERT

E-tjenesten: Norwegian Intelligence Service

PT: Norwegian Post and Telecommunications Authority

Difi: Agency for Public Management and eGovernment

NorSIS : Norweian Center for Information Security

Datatilsynet: Data Protection Agency

Health CSIRT

Private umbrella organisations focusing on Information Security in Norway

- Næringslivets Sikkerhetsråd
  - Industry Security Council
- ISF
  - IT Security Forum
- ISACA
  - Information Systems Audit and Control Association

Private umbrella organisations focusing on Information Security in Norway

- Næringslivets Sikkerhetsråd
  - Industry Security Council
- ISF
  - IT Security Forum
- ISACA
  - Information Systems Audit and Control Association

Can you know if your organisation is secure?

- You can never know for sure
  - Kant’s philosophy: Das Ding an sich und das Ding für mich
- Systems are becoming increasingly complex
  - Impossible to know all their properties
- We can only have a subjective perception of robustness
- *Information Assurance* is the concept used to reflect our insight into the security of information systems
  - “Assurance Level” is used to denote the level of perceived security of systems certified e.g. according to the Common Criteria
- ***“Information security is a well-informed assurance that information risks and controls are in balance”***