ISO standards
Chapter 3

أ.م.د.عباس عبد العزيز عبد الحميد

كليـة العلـوم / قسم الحاسـوب

abbasabdulazeez@uomustansiriyah.edu.iq

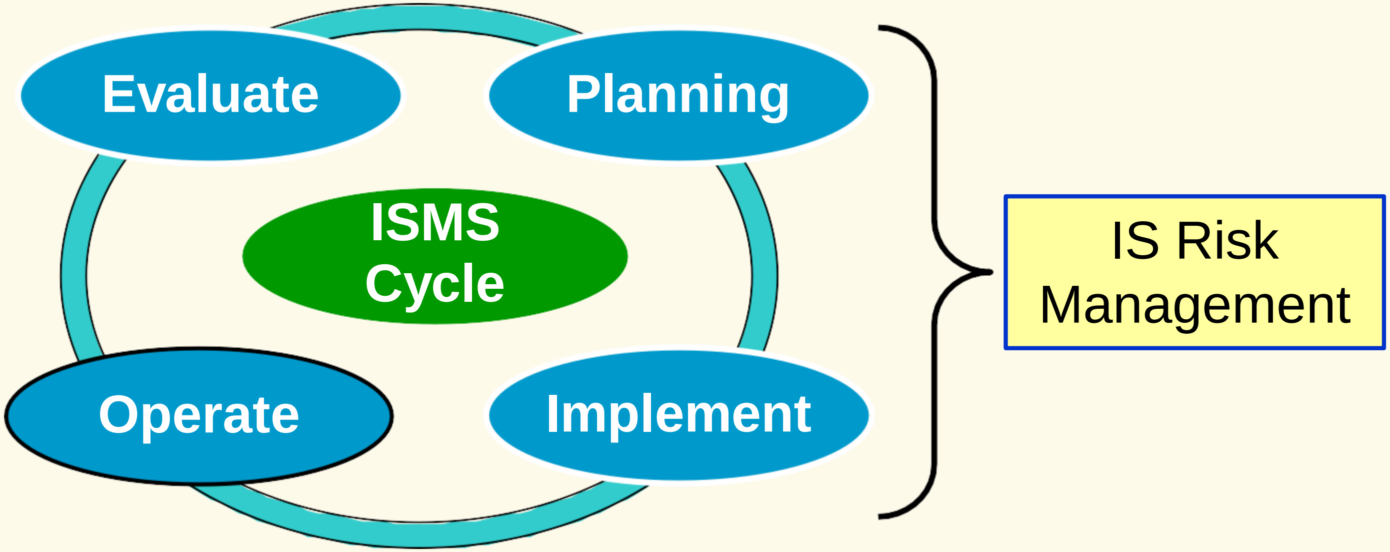
ISMS

- An Information Security Management System (ISMS) is a set of policies and procedures to systematically manage an organization's sensitive data. The goal of ISMS is to reduce risk and ensure business continuity by proactively reducing the impact of a security breach.

- An ISMS provides a systematic approach for managing the information security of an organization. Information security encompasses certain broad policies that control and manage security risk levels across an organization.

Risk Management – ISMS integration

- Risk management is an essential element of ISMS
  - Used to identify risks and their magnitude
  - Basis for selecting security controls
  - Tool for top management to understand organization's risk exposure



ISO/IEC 27000 Series = ISMS Blueprints

27000 – Glossary of terms

27001:2005 - Attainment certification

27002:2005/Cor1:2007 – Code of practice

27003 – ISMS Implementation guidance under development as of Sept 08

27004 – Information security measurement

27005-2008 – Information security – Risk management

27006:2007 – Certification vendor process

27799:2008 – Information Security for Health Care Organizations

Risk Management standards

- ISO 31000 Risk Management
- ISO 27005 Information Security Risk Management
- NIST SP800-39 Managing Information Security Risk
- NIST SP800-30 Guide for Conducting Risk Assessment
  - formerly called “Risk Management Guide for Information Technology Systems”
- NS 5831 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger –Risikohåndtering
- NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Risikoanalyse

What is risk management?

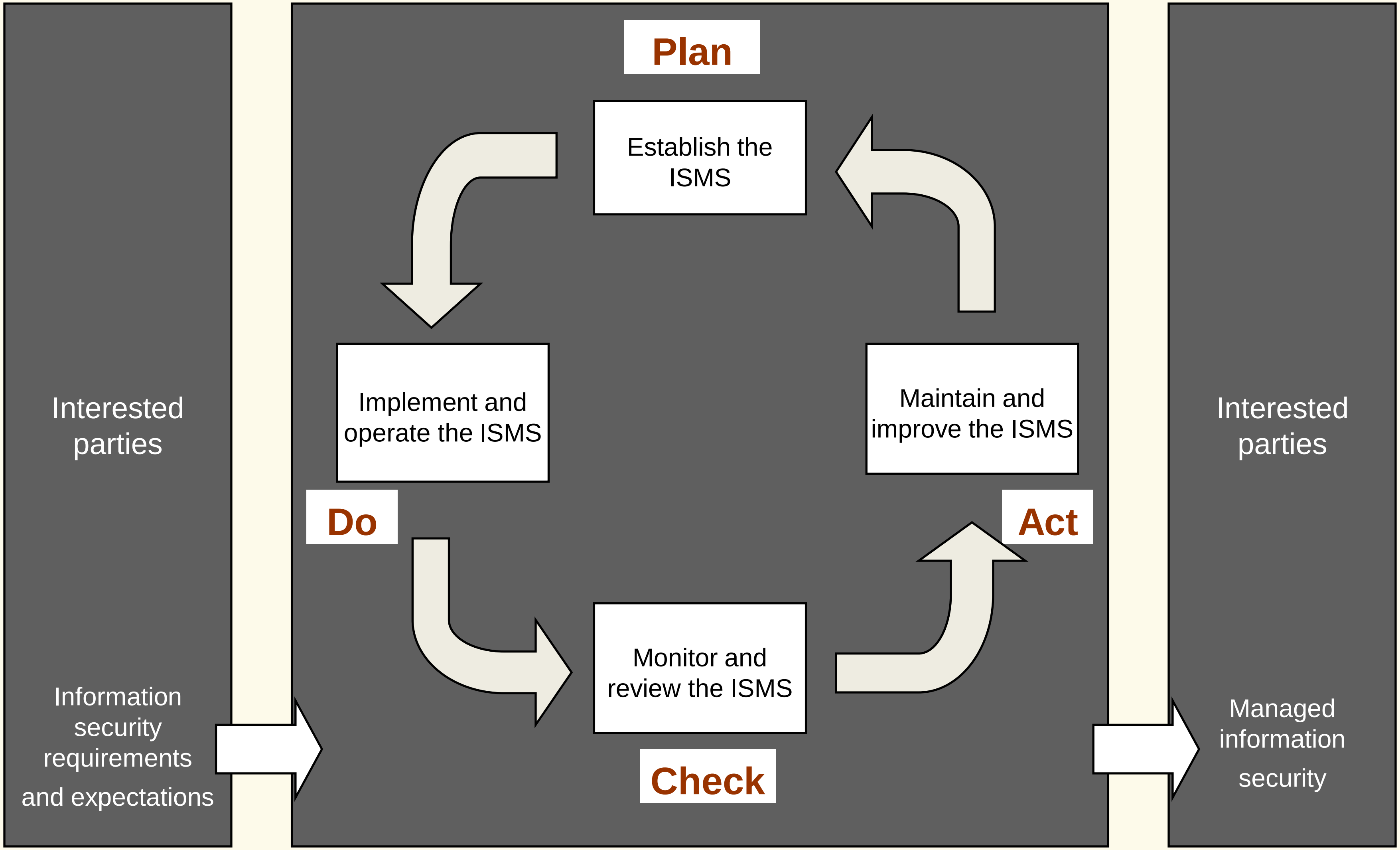
- “Risk management consists of coordinated activities to direct and control an organization with regard to risk.”
  - ISO 31000

- “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

What is ISO 27001?

- It’s a International Standard for Information Security Management
- It consists of various Specification for information Security Management
- Code of Practice for Information Security Management
- Basis for contractual relationship
- Basis for third party certification
- Can be Certified by Certification Bodies
- Applicable to all industry Sectors
- Emphasis on prevention

Plan Do Check Act Cycle (PDCA)



Interested parties

Information security requirements and expectations

Plan

Establish the ISMS

Do

Implement and operate the ISMS

Check

Monitor and review the ISMS

Act

Maintain and improve the ISMS

Interested parties

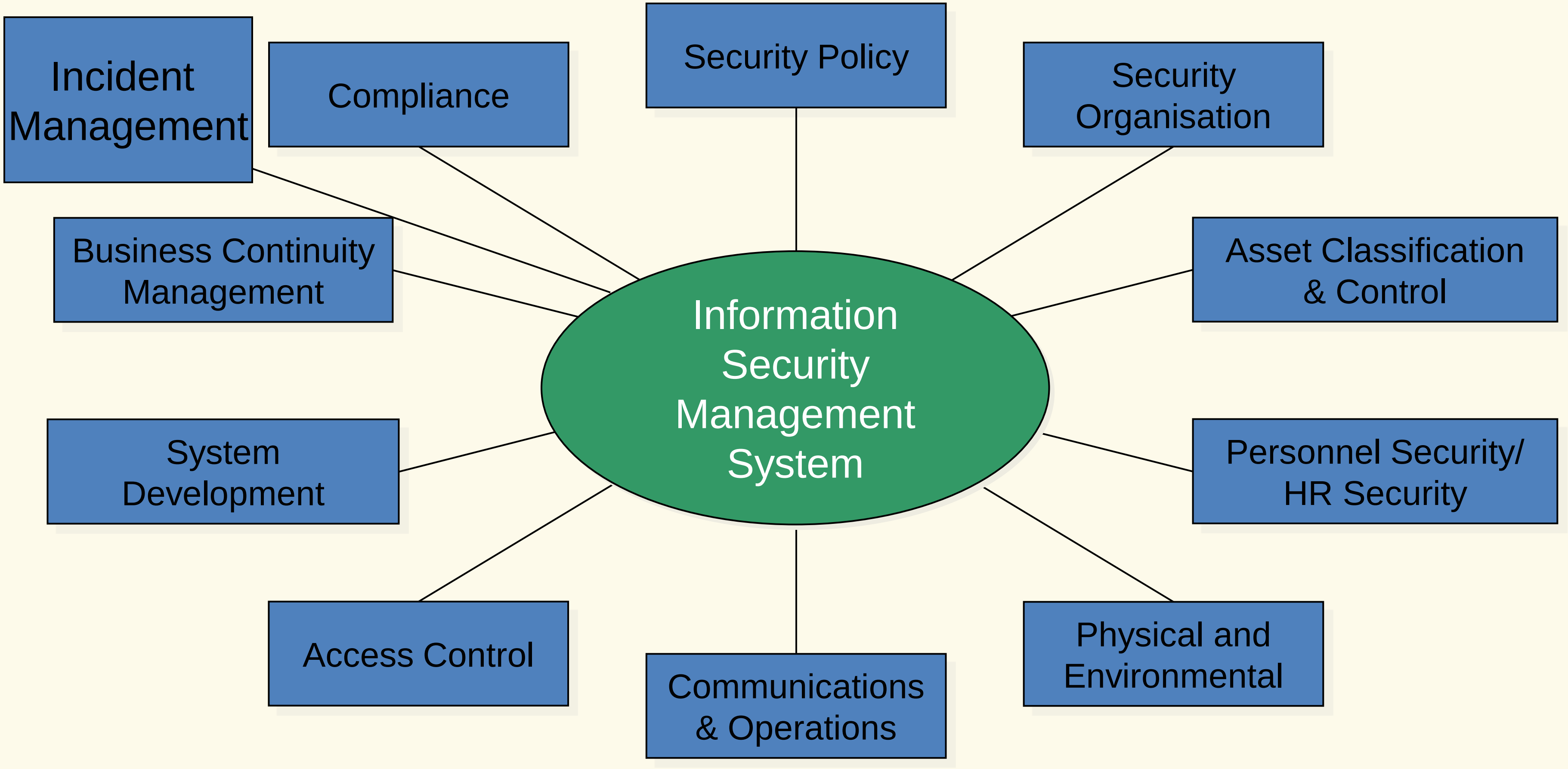
Managed information security

Important Areas of Concern

ISO27001

1. Security policy
2. Organization of information security
3. Asset management
4. Human resources security
5. Physical and environmental security
6. Communications and operations management
7. Access control
8. Information systems acquisition, development and maintenance
9. Information security incident management
10. Business continuity management
11. Compliance

ISO27001 Framework: Components


Incident Management
Compliance
Security Policy
Security Organisation
Business Continuity Management
Asset Classification & Control
Information Security Management System
System Development
Personnel Security/ HR Security
Access Control
Communications & Operations
Physical and Environmental

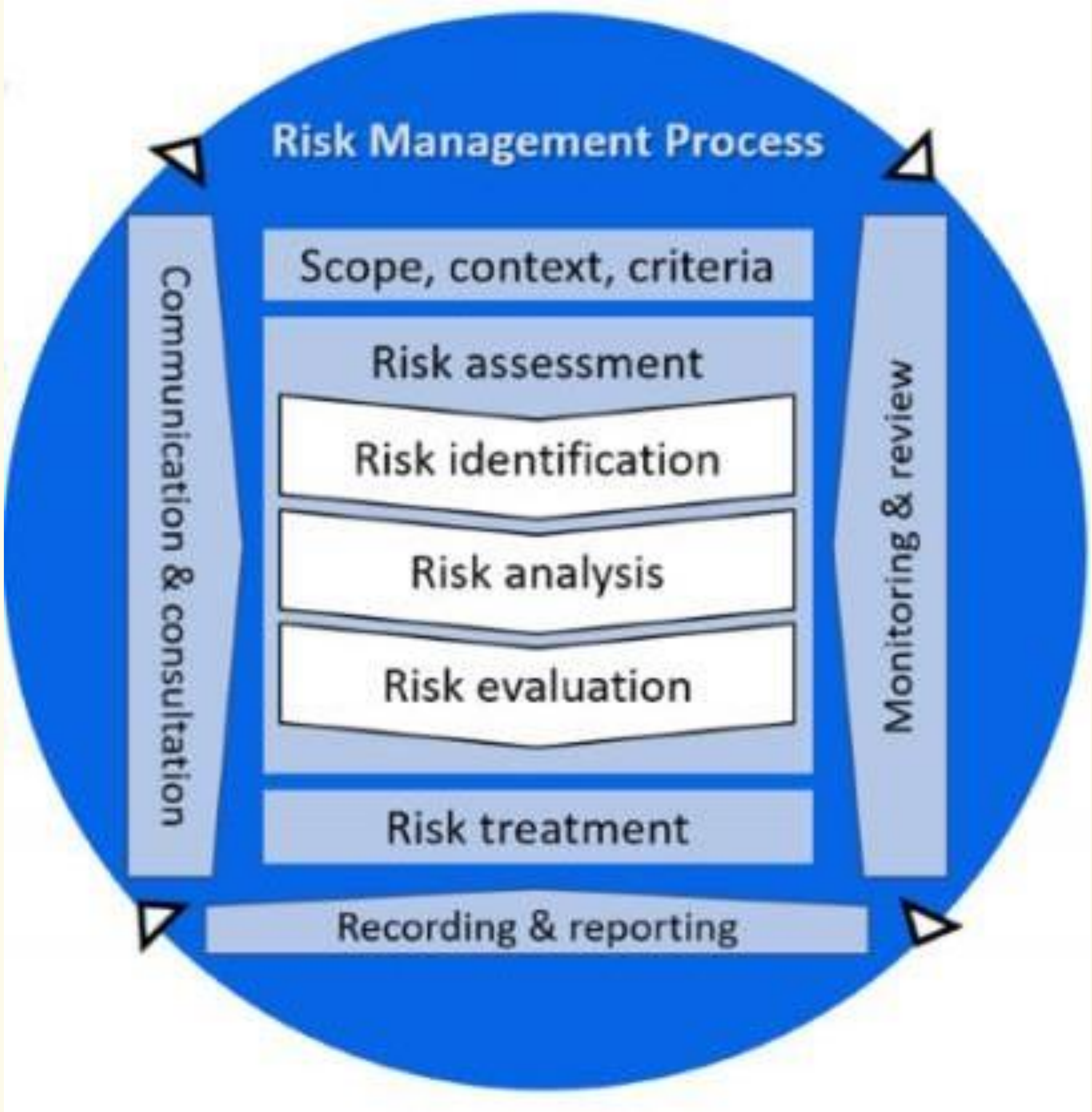
(ISMS ISO)

ISMS security controls span multiple domains of information security as specified in the ISO 27001 standard. The catalog contains practical guidelines with the following objectives:-

1.Information security policies
2.Organization of information security
3.Asset Management
4.Human Resource Security
5.Physical and environmental security
6.Communications and operations management
7.Access control
8.Information system acquisition, development, and maintenance
9.Information security and incident management
10.Business continuity management.
11.Compliance
12.Cryptography
13.Supplier relationships

Risk Management Process: ISO 31000

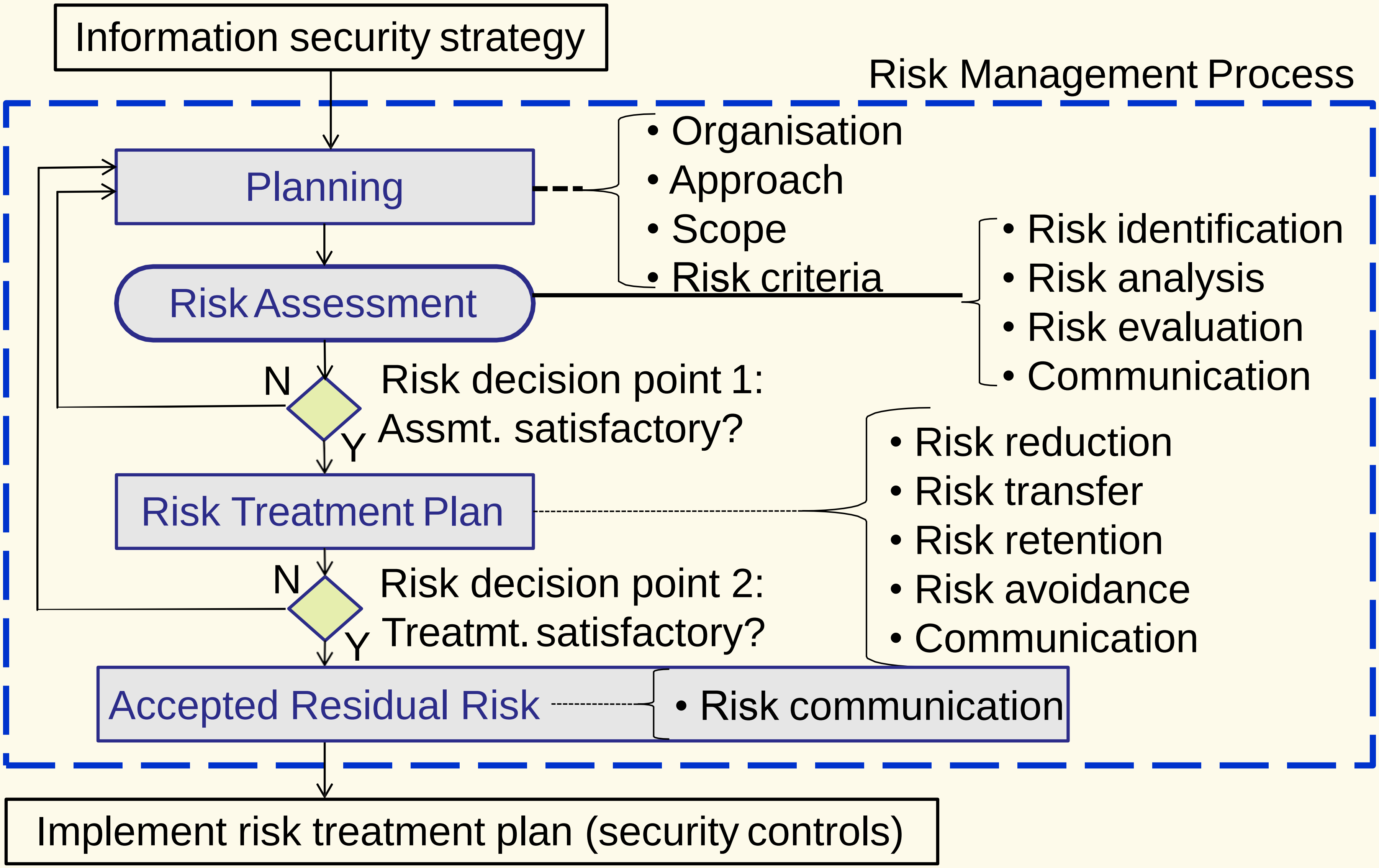
- ISO 31000 is a general standard for risk management applicable to different sectors
- The same approach is applicable to IS risk management



Basis for assessing risk

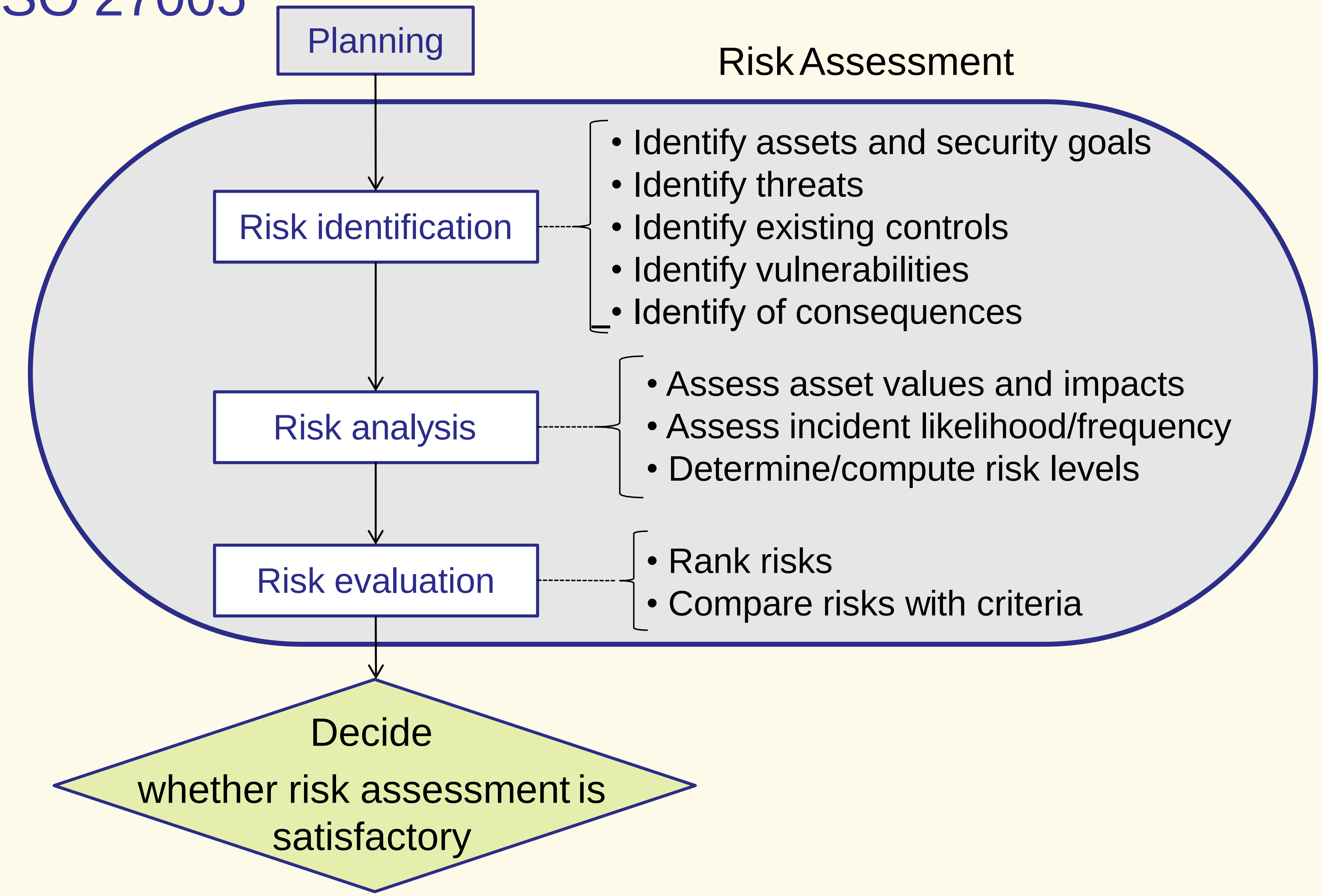
- Know the assets: identify and understand the value of information assets and systems.
- Know the threats: identify and understand relevant threat scenarios which can harm information assets and systems.
- Know the vulnerabilities which can be exploited by threats.
- Know the potential impacts of incidents.
- Know which stakeholders in the organisation are responsible for managing the identified risks.

Risk management process ISO 27005



Risk assessment process

ISO 27005



Planning

Risk Assessment

Risk identification

- Identify assets and security goals
- Identify threats
- Identify existing controls
- Identify vulnerabilities
- Identify of consequences

Risk analysis

- Assess asset values and impacts
- Assess incident likelihood/frequency
- Determine/compute risk levels

Risk evaluation

- Rank risks
- Compare risks with criteria

Decide

whether risk assessment is satisfactory

Roles involved in risk management

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

Asset and Impact Valuation

- Identify assets and relevant security CIA goals
- Estimate impact of breach of specific security goal for an asset
- For example, the impact with regard to the following aspects:
  - damages revenue/profitability or paralyses important services
  - breach of legal compliance (e.g. with regard to GDPR)
  - damages public image
- Valuation
  - Direct estimation of impact of breach of security goal for an asset
  - Alternatively, co-product (“OR” rule) of impact for different aspects, e.g.
    - Let p_1 denote relative impact on asset aspect 1, with value in [0,1]
    - The relative impact levels can be mapped to qualitative levels

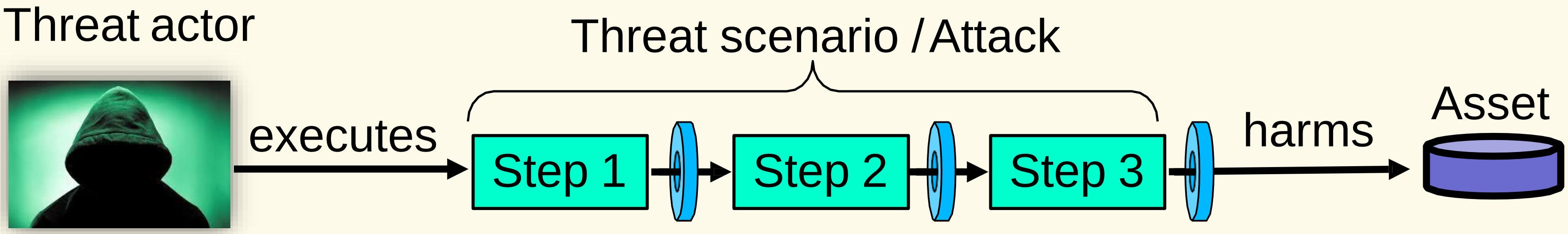
Example Asset and Impact Valuation

Asset and security goal (corresponding incident)	**Aspect 1** Impact on revenue / profit	**Aspect 2** Impact on legal compliance	**Aspect 3** Impact on public image	**Total impact of incidents** (coproduct)
Documents and data (loss of) confidentiality	0.0	0.8	0.5	0.90
Documents & data (loss of) integrity	0.4	0.0	0.0	0.40
Customer profiles (loss of) integrity	0.5	0.0	0.0	0.50
Network (un) availability	0.9	0.0	0.2	0.92
Applications (un) availability	0.9	0.0	0.1	0.91
Authentication credentials (loss of) availability (users can’t log in)	0.9	0.0	0.4	0.94
Web page integrity (defacement)	0.1	0.0	0.1	0.19
User support (un) availability	0.2	0.0	0.1	0.28

- All values are relative in the interval [0, 1]

Threat Modelling

- Threat modelling is the process of identifying, analysing and describing how assets can be harmed.

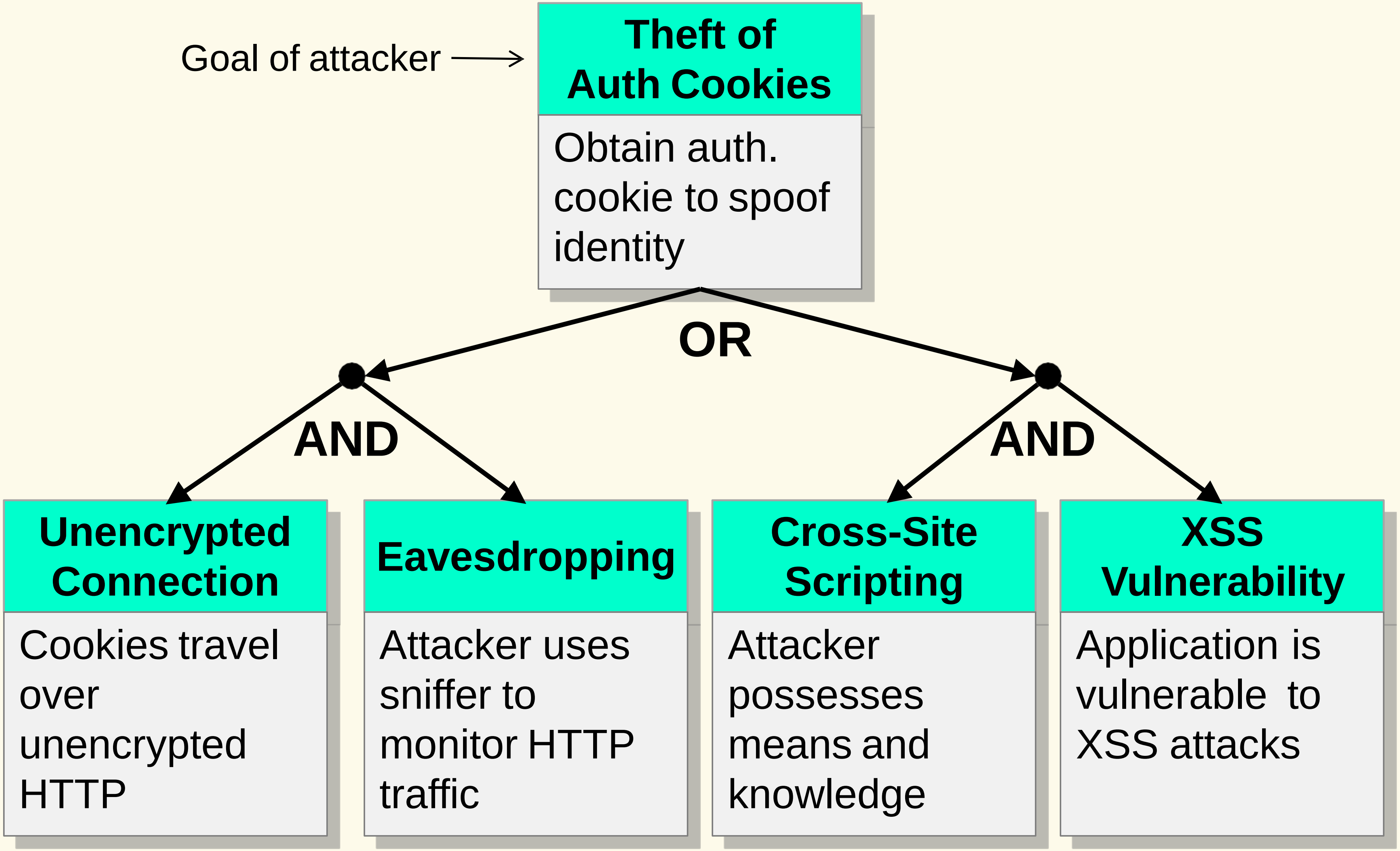


- The threat modelling process works best when people with diverse backgrounds within the organization work together in a series of brainstorming sessions.
- Threat modelling is important during system development
  - Used to identify, remove and avoid vulnerabilities when developing software and systems.
- Multiple approaches/methods for threat modelling

Threat Modelling Methods

- 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: Threat Tree Example



Goal of attacker

Theft of Auth Cookies

Obtain auth. cookie to spoof identity

OR

AND

Unencrypted Connection

Cookies travel over unencrypted HTTP

Eavesdropping

Attacker uses sniffer to monitor HTTP traffic

AND

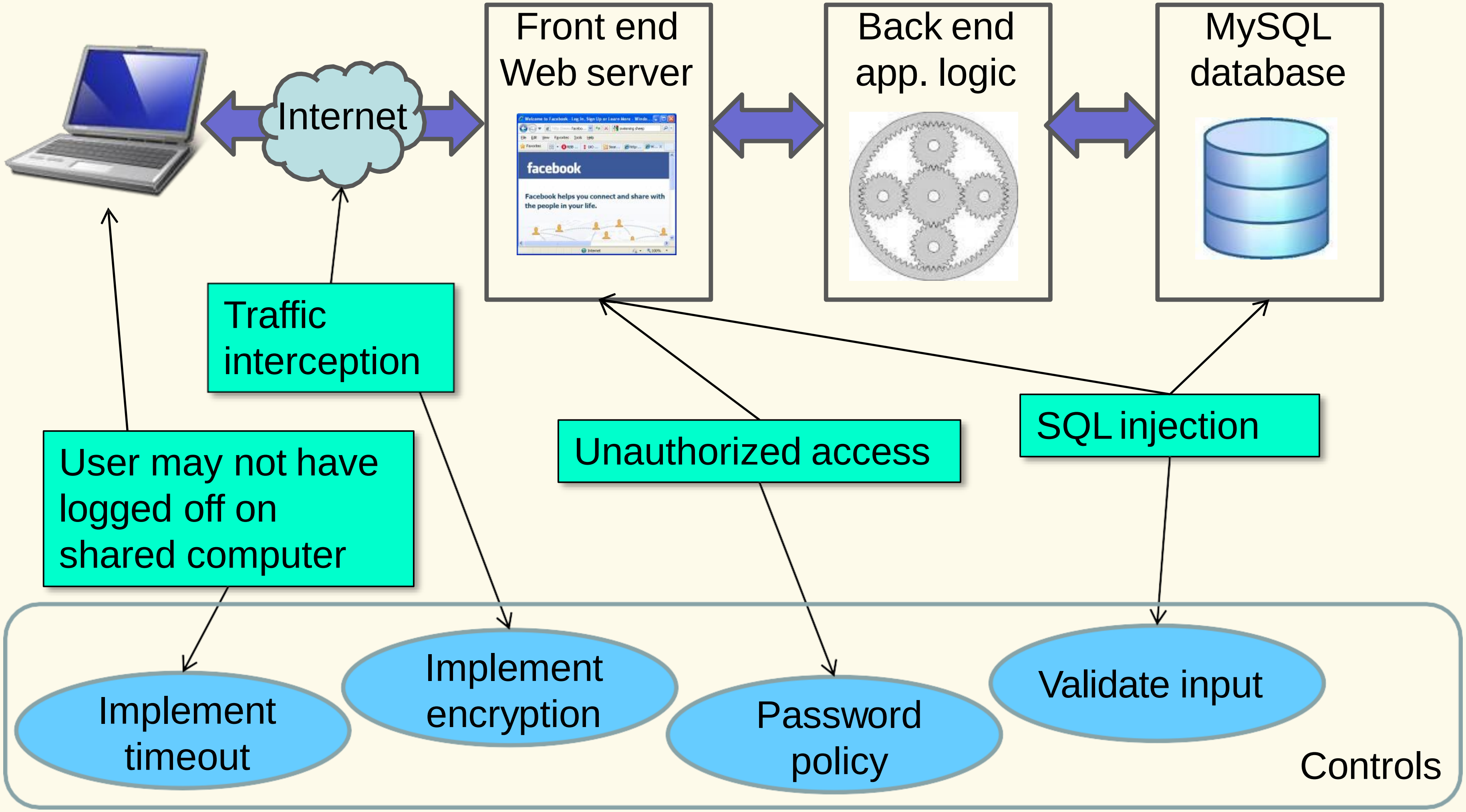
Cross-Site Scripting

Attacker possesses means and knowledge

XSS Vulnerability

Application is vulnerable to XSS attacks

System-centric threat modelling example



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

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

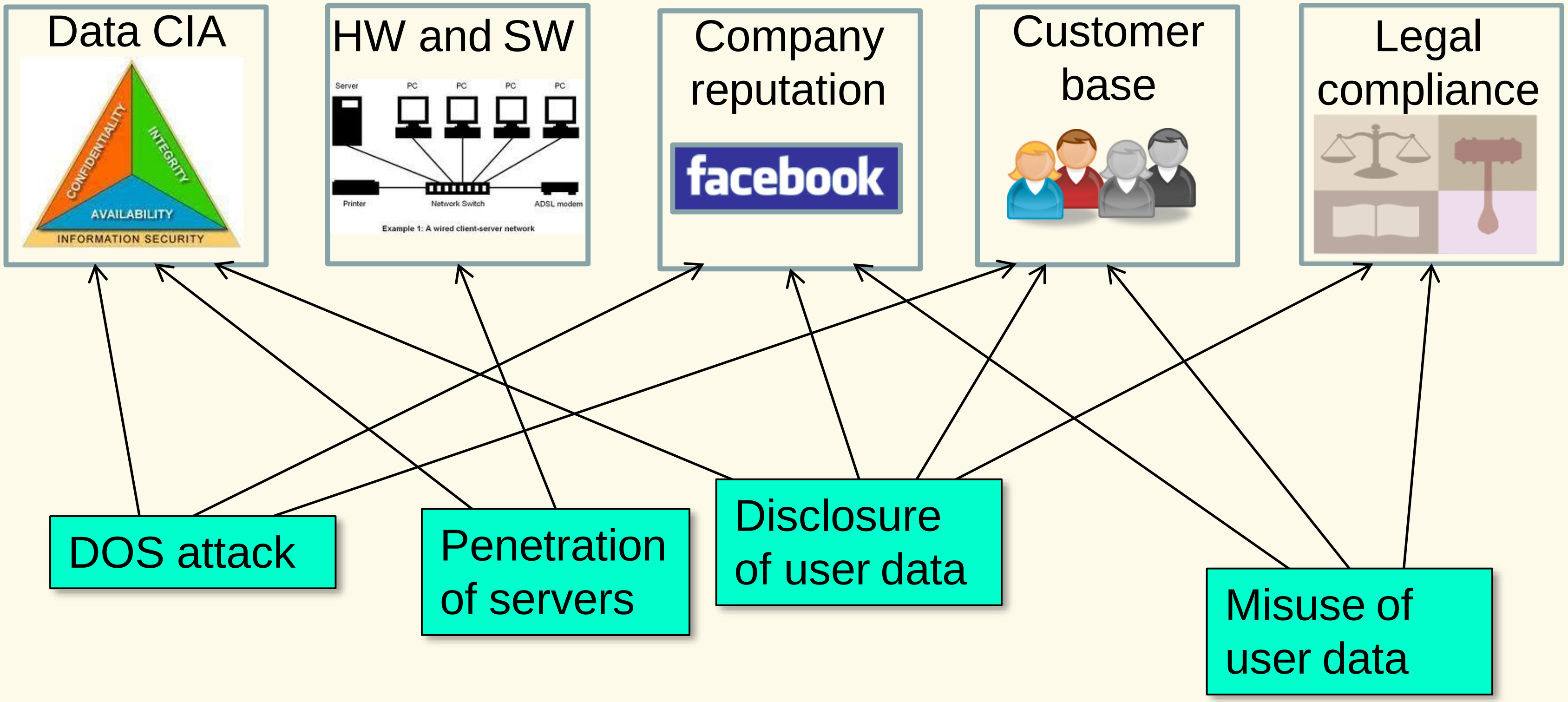
Implement encryption

Password policy

Validate input

Controls

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

Vulnerability Identification

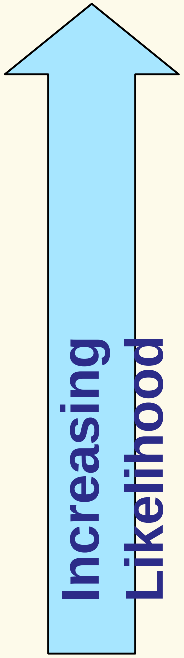
- Vulnerabilities are specific opportunities that threat actors can exploit to attack systems and information assets.
- Generic vulnerability identification
  - To identify a vulnerability is the same as to determine how to block a specific threat scenario.
  - Removing a vulnerability is the same as blocking a threat.
  - A vulnerability is **the absence of barriers** against a threat.
  - Blocking a threat (i.e. removing a vulnerability) is done with a security control.
- Tool-based and checklist-based vulnerability identification
  - **Vulnerability scanners** are automated tools to detect known vulnerabilities in networks and systems, e.g. Wireshark
  - **Check lists of vulnerabilities** are used by teams when doing risk assessment and removing vulnerabilities, e.g. OWASP Top 10.

Estimating and analysing risk levels

Types of analysis

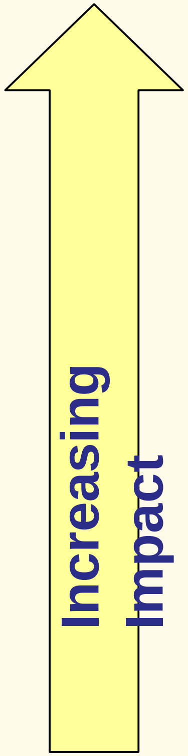
- **Qualitative**
  - Uses descriptive scales. Example:
    - Impact level: Minor, moderate, major, catastrophic
    - Likelihood: Rare, unlikely, possible, likely, almost certain
- **Relative**
  - Relative numerical values assigned to qualitative scales
  - Gives relatively good distribution of risk levels
- **Quantitative**
  - Use numerical values for both consequence (e.g. $) and likelihood (e.g. probability value)

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 (every 2 years).
Low	The event should happen at some time (every 5 years).
Unlikely	The event could happen at some time (every 10 years).

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

- Define risk matrix with risk levels according to requirements
  - Number of qualitative levels of likelihood, impact and risk
- Use the risk matrix as a look-up table for each identified risk

Qualitative impact levels

Qualitative likelihood

Qualitative risk levels	Insignificant	Minor	Moderate	Major
High	M	H	VH	E
Medium	L	M	H	VH
Low	VL	L	M	H
Unlikely	N	VL	L	M

Legend

E: extreme risk; Risk must be handled with priority

(V)H: (very) high risk; Risk must be handled

M: moderate risk; Risk to be handled according to budget

(V)L: (very) low risk; Risk with low priority, handle if there is opportunity

N: Negligible risk; To be ignored

Relative risk estimation

Example

Relative risk levels: Product of likelihood & impact level

Relative likelihood levels

	Relative Impact levels				
Relative risk levels	**(0.0) Nil**	**(0.1) Insign.**	**(0.2) Minor**	**(0.4) Moderate**	**(1.0) Major**
(1.0) High	**0**	**0.10**	**0.20**	**0.40**	**1.00**
(0.4) Medium	**0**	**0.04**	**0.08**	**0.16**	**0.40**
(0.2) Low	**0**	**0.02**	**0.04**	**0.08**	**0.20**
(0.1) Unlikely	**0**	**0.01**	**0.02**	**0.04**	**0.10**
(0.0) Never	**0**	**0**	**0**	**0**	**0**

Relative risk estimation can give a better distribution of risk levels than with purely qualitative models.

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

Risk listing and ranking

Threat scenario:	**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	MEDIUM	MODE RATE
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

Challenges for measuring risk

Businesses normally wish to measure risk in money, but almost impossible to do this

- Valuation of assets
  - Value of data, hard to assess
  - Value of goodwill and customer confidence, very vague
- Likelihood of incidents
  - Past events not always relevant for future probabilities
    - The nature of future attacks is unpredictable
    - The actions of future attackers are unpredictable
- Measurement of benefit from security control
  - Problems with the difference of two approximate quantities
    - Estimation of past and present risk

Risk Control Strategies

- After completing the risk assessment, the security team must choose one of four strategies to control each risk:

1. Reduce risk by implementing security controls
2. Share/transfer risk (outsource activity that causes risk, or buy insurance)
3. Retain risk (understand and tolerate potential consequences)
4. Avoid risk (stop activity that causes risk)