Secure Software Design and Engineering
(CY-321)

Risk Management for Software

Dr. Zubair Ahmad

- **Attendance?**

  - Active Attendance
  - **Dead Bodies.**
  - **Active Minds**
  - Mobiles in hands -> Mark as absent
  - 80% mandatory

Few Important Announcements at the end of Class

Handling Risk

Owners value assets **(software)** and wish to minimize risk to assets

All software has risks

Without risk management, small issues become disasters

Software risk management is not just about **security**—its about **reliability, trust, and business success**

Handling Risk

Scenario!!!

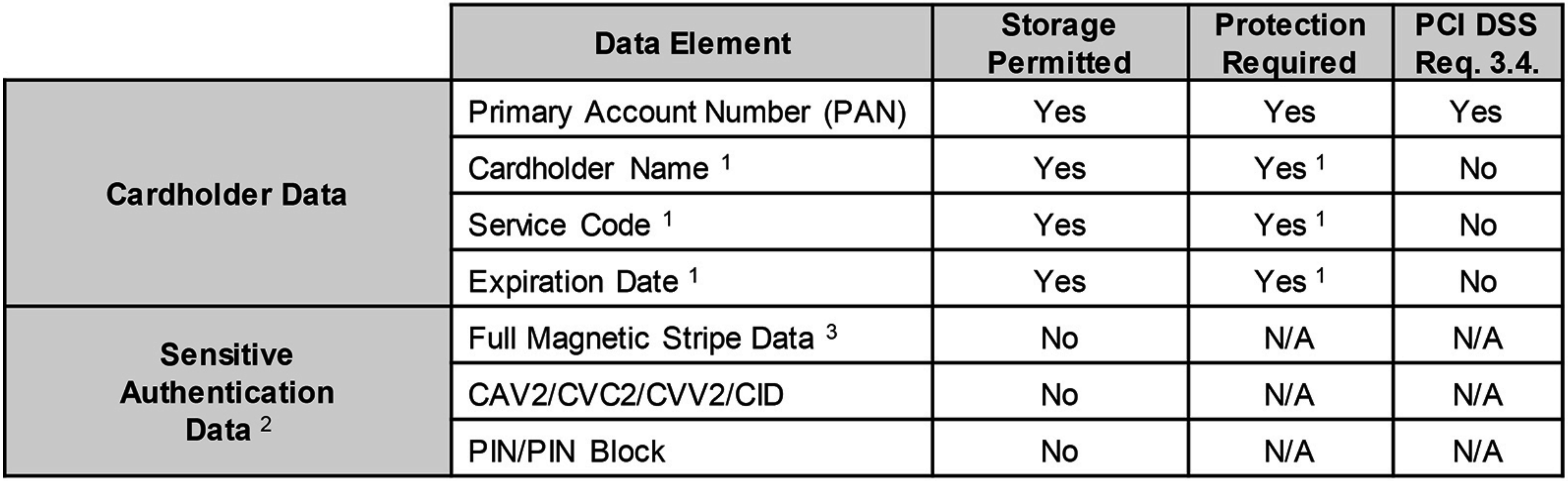
Suppose your organization operates an ecommerce store selling products on the Internet

Payment Card Industry Data Security Standard (PCI DSS) to protect card holder data

Before the PCI DSS regulatory requirement was in effect, your organization has been transmitting and storing the credit card primary account number (PAN), card holder name, **all in clear text**

PCI DSS disallows the storage of any sensitive authentication information even if it is encrypted or the storage of the PAN along with card holder name, service code and expiration data in clear text

Handling Risk



	Data Element	Storage Permitted	Protection Required	PCI DSS Req. 3.4.
Cardholder Data	Primary Account Number (PAN)	Yes	Yes	Yes
	Cardholder Name [1]	Yes	Yes [1]	No
	Service Code [1]	Yes	Yes [1]	No
	Expiration Date [1]	Yes	Yes [1]	No
Sensitive Authentication Data [2]	Full Magnetic Stripe Data [3]	No	N/A	N/A
	CAV2/CVC2/CVV2/CID	No	N/A	N/A
	PIN/PIN Block	No	N/A	N/A

Handling Risk

Mitigate the risk

Accept the risk

Ignore the risk

What If?

Transfer the risk

Avoid the risk

Risk Management – Terminologies

Asset

Items that are valuable to the organization, the loss of which can potentially cause disruptions in the organization’s ability to accomplish its missions

Assets may be tangible or intangible in nature

Vulnerability

A weakness or flaw that could be accidently triggered or intentionally exploited by an attacker

The protection of IT assets and the cost of implementing software security controls, so that the risk is handled appropriately

Risk Management – Terminologies

Probability

the chance that a particular threat can happen

Controls

Mechanisms by which threats to software and systems can be mitigated. These mechanisms may be technical, administrative or physical in nature

Security controls can be broadly categorized into **countermeasures** and **safeguards**.

The protection of IT assets and the cost of implementing software security controls, so that the risk is handled appropriately

Risk Management – Terminologies

Threat

A threat is merely the possibility of an unwanted, unintended or harmful event occurring

Anyone or anything that has the potential to make a threat materialize is known as the threat-source or threat-agent

Exposure Factor

the opportunity for a threat to cause loss

Although the probability of an attack may be high, and the corresponding impact severe, if the software is designed, developed and deployed with security in mind, the Exposure Factor for attack may be low, thereby reducing the overall risk of exploitation.

The protection of IT assets and the cost of implementing software security controls, so that the risk is handled appropriately

Risk Management - Terminologies

Total Risk

the likelihood of the occurrence of an unwanted, unintended or harmful event

computed using factors such as the asset value, threat, and vulnerability

This is the overall risk of the system, before any security controls are applied

This may be expressed **qualitatively** (e.g., High, Medium or Low) or **quantitatively** (using numbers or percentiles)

Residual Risk

Risk that remains after the implementation of mitigating security controls (countermeasures or safeguards)

Risk Management - Terminologies

Calculation of Risk

Risk is conventionally expressed as the product of the probability of a threat- source/agent taking advantage of a vulnerability and the corresponding impact

Calculation of risk is not a **black** or white exercise, especially in the context of software security

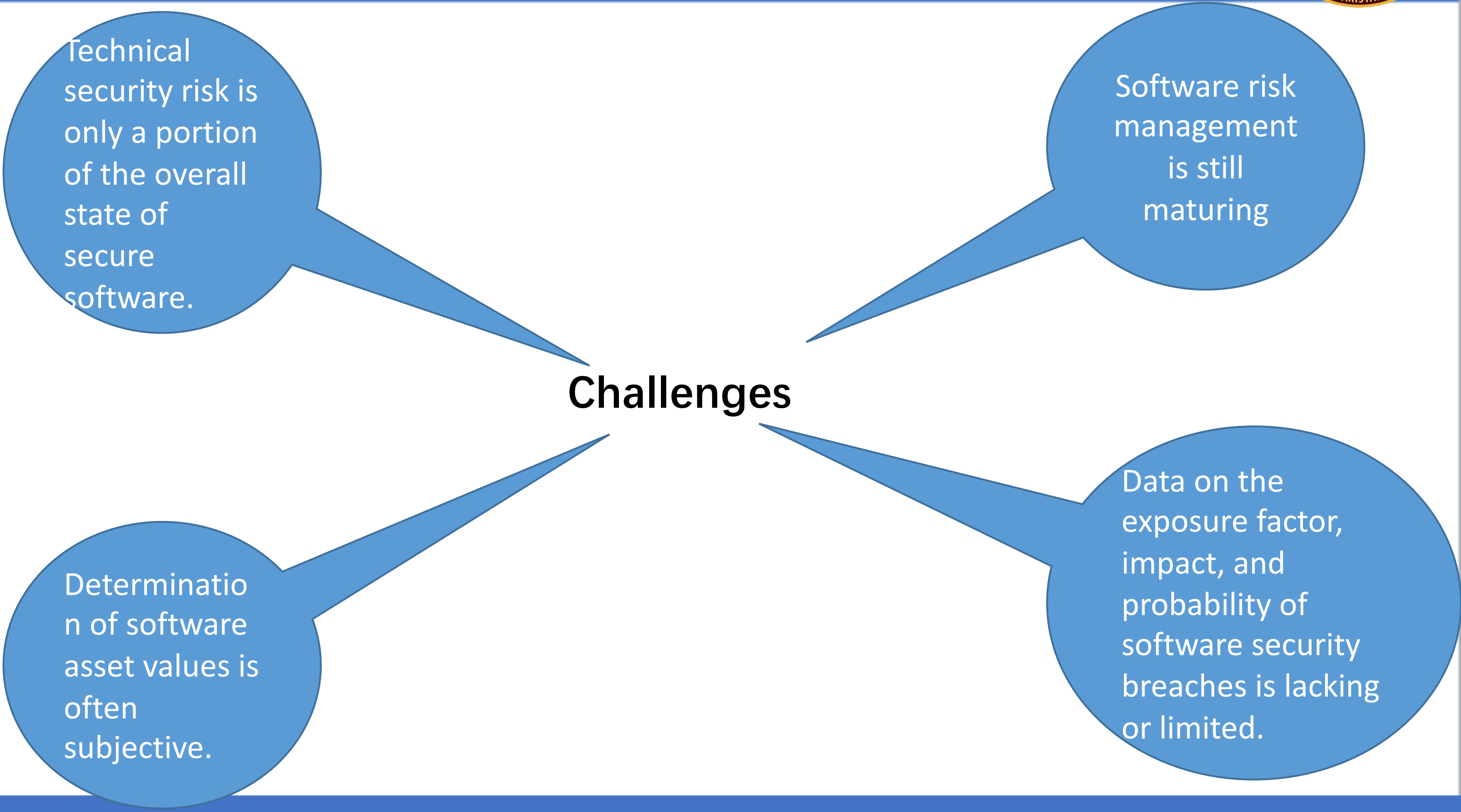
Estimation of both probability and impact are usually subjective and so quantitative measurement of risk is not always accurate.

Single Loss Expectancy (SLE)

Annual Rate of Occurrence (ARO)

Annual Loss Expectancy (ALE)

Risk Management for Software



Challenges

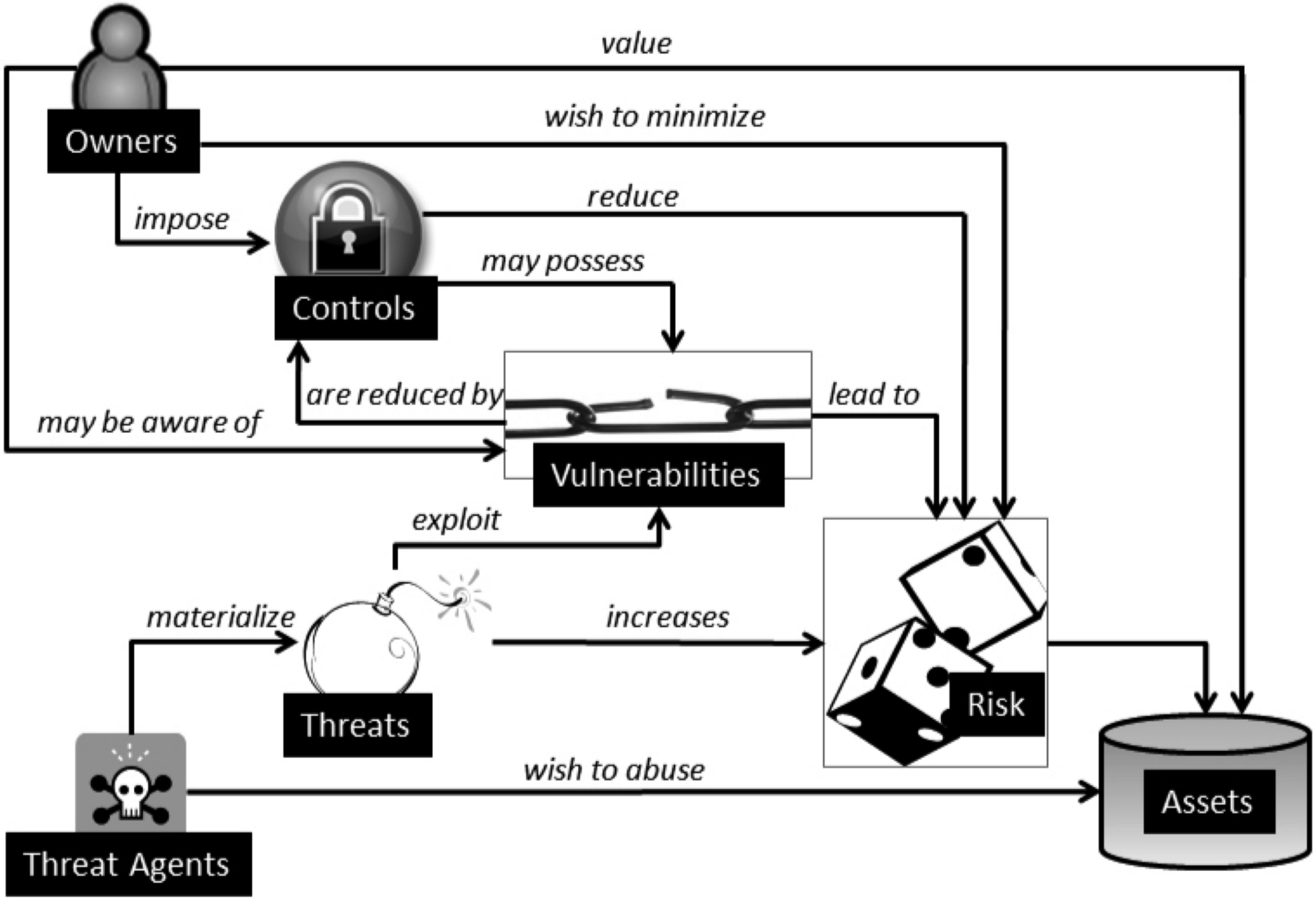
Technical security risk is only a portion of the overall state of secure software.

Software risk management is still maturing

Determination of software asset values is often subjective.

Data on the exposure factor, impact, and probability of software security breaches is lacking or limited.

Risk Management – A View



Risk Management - Five Stages

Understand the Business Context

The purpose of this stage is to gather data to answer the all-important "Who cares?" question.

Extract and describe usiness goals, priorities, and circumstances in order to understand what kinds of software risks to care about and which business goals are paramount

Risk Management - Five Stages

Identify the Business and Technical Risks

The ability to discover and describe technical risks and map them (through business risks) to business goals

The key to making risk management work for any business lies in tying technical risks to the business context in a meaningful way

Risk Management - Five Stages

Synthesize and Rank the Risks

"What shall we do first given the current risk situation?"

"What is the best allocation of resources, especially in terms of risk mitigation activities?"

Risk Management - Five Stages

Define the Risk Mitigation Strategy

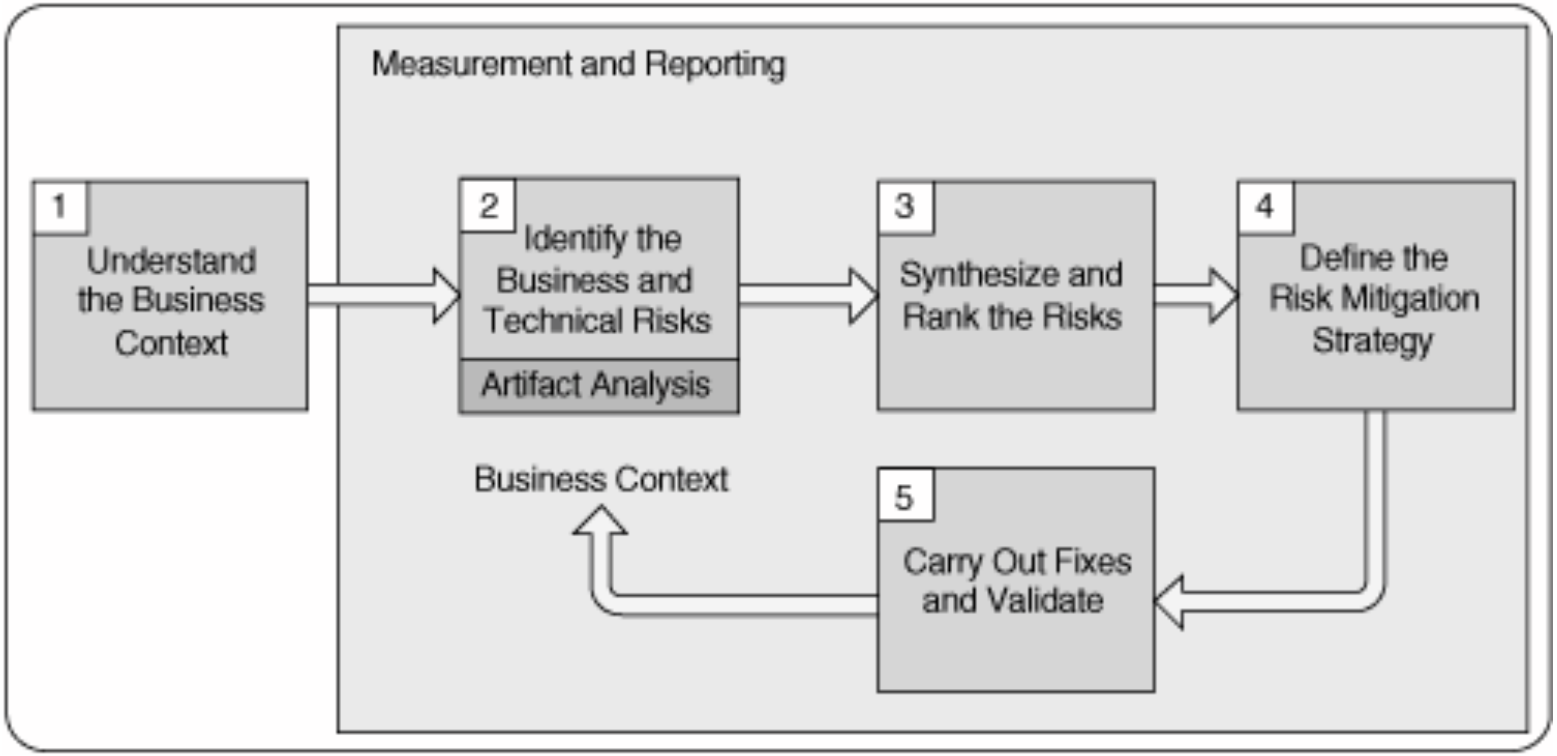
Nobody wants to hear about their problems without hearing some suggested fixes. A risk analysis is only as good as the mitigation strategy it contains

Risk Management - Five Stages

Carry Out Fixes and Validate

Risk mitigation is carried out according to the strategy defined in stage 4

Risk Management - Five Stages

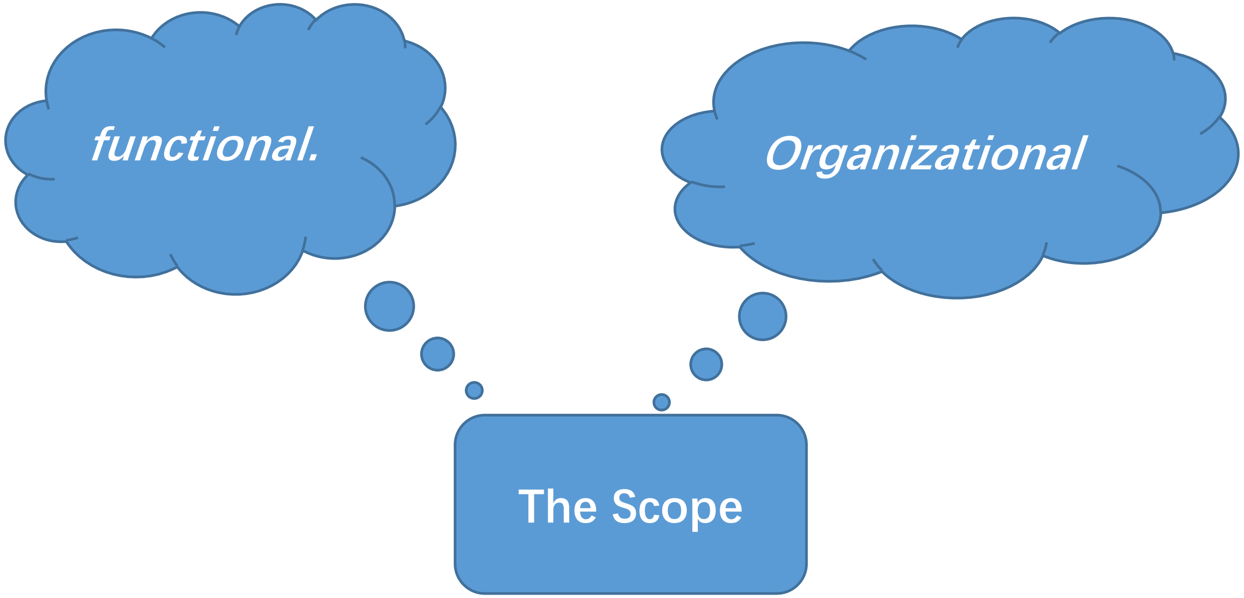

Measurement and Reporting
1
Understand the Business Context
2
Identify the Business and Technical Risks
Artifact Analysis
3
Synthesize and Rank the Risks
4
Define the Risk Mitigation Strategy
Business Context
5
Carry Out Fixes and Validate

Security Policies

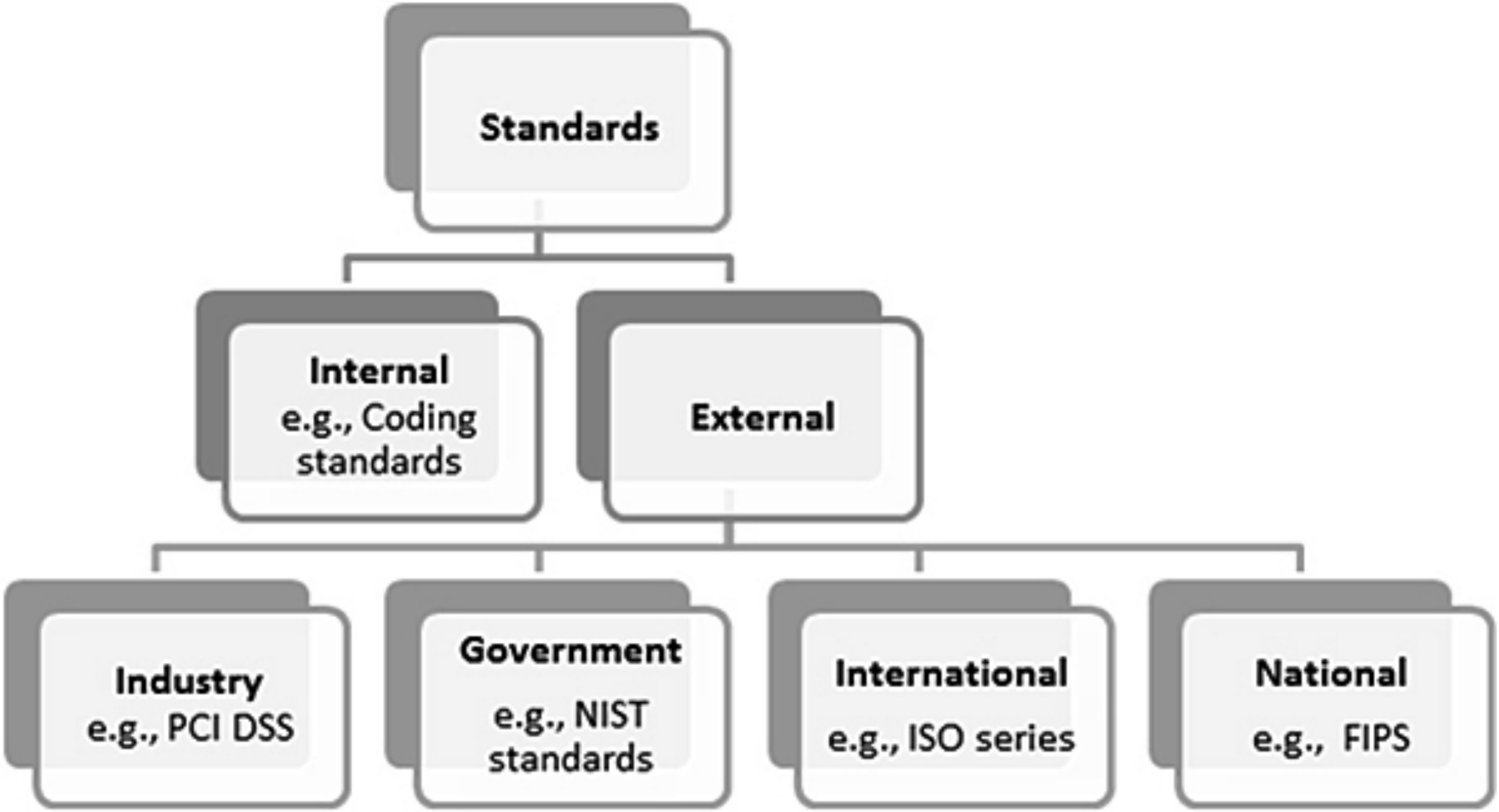
The ‘What’ and ‘Why’ for Security?

Legal and regulatory compliance has been evident as an important driver of information security spending and initiatives

‘What’ needs to be protected and the possible repercussions of non-compliance



Security Standards



Standards

Internal
e.g., Coding standards

External

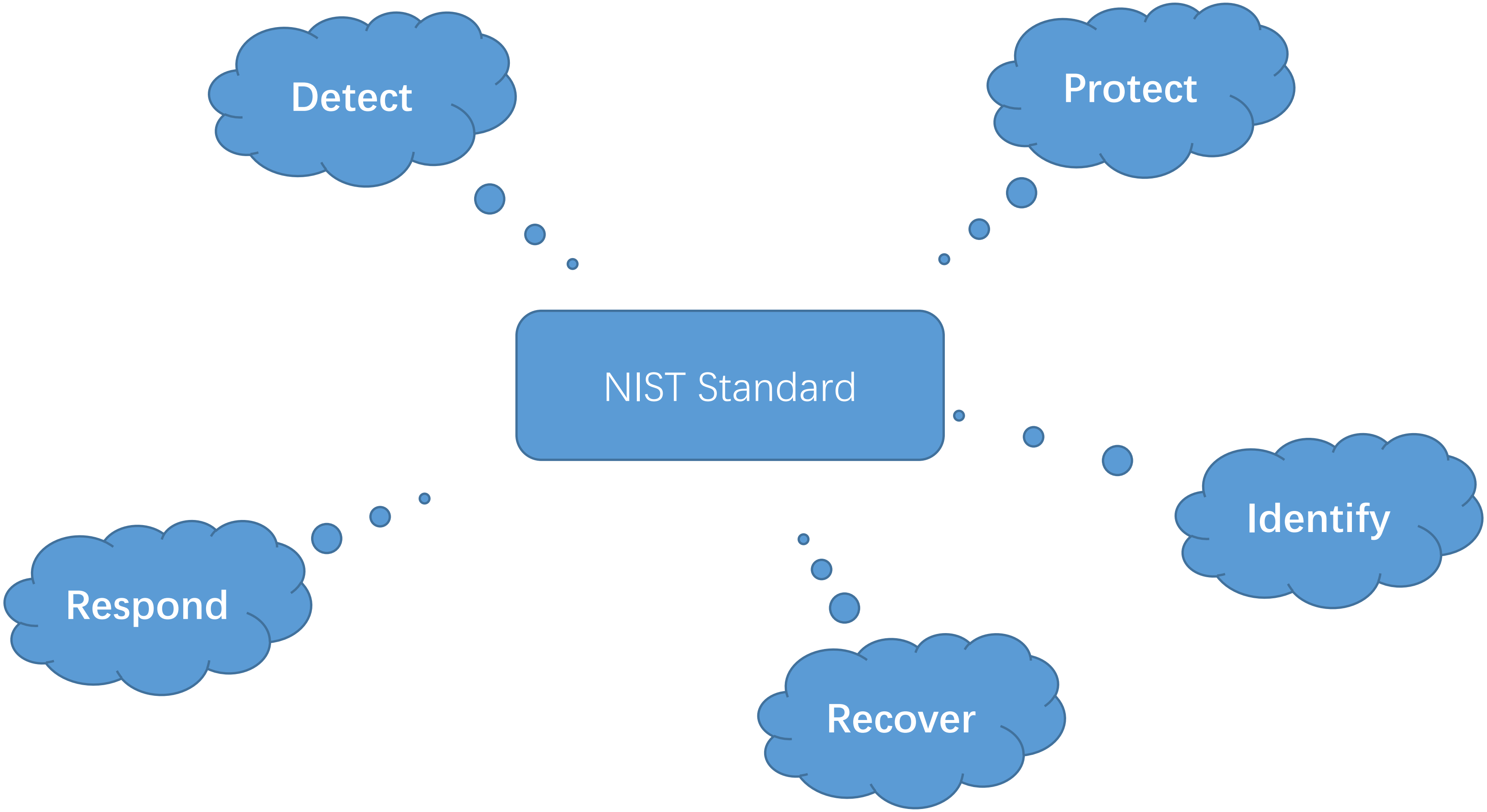
Industry
e.g., PCI DSS

Government
e.g., NIST standards

International
e.g., ISO series

National
e.g., FIPS

Security Standards



Security Standards

Federal Information Processing (FIPS) standards

Developed by **NIST** for U.S. government agencies and contractors to ensure strong security and interoperability in information system

Level 1

Basic security, software-only encryption allowed

Level 2

Includes role-based authentication and tamper-evidence

Level 3

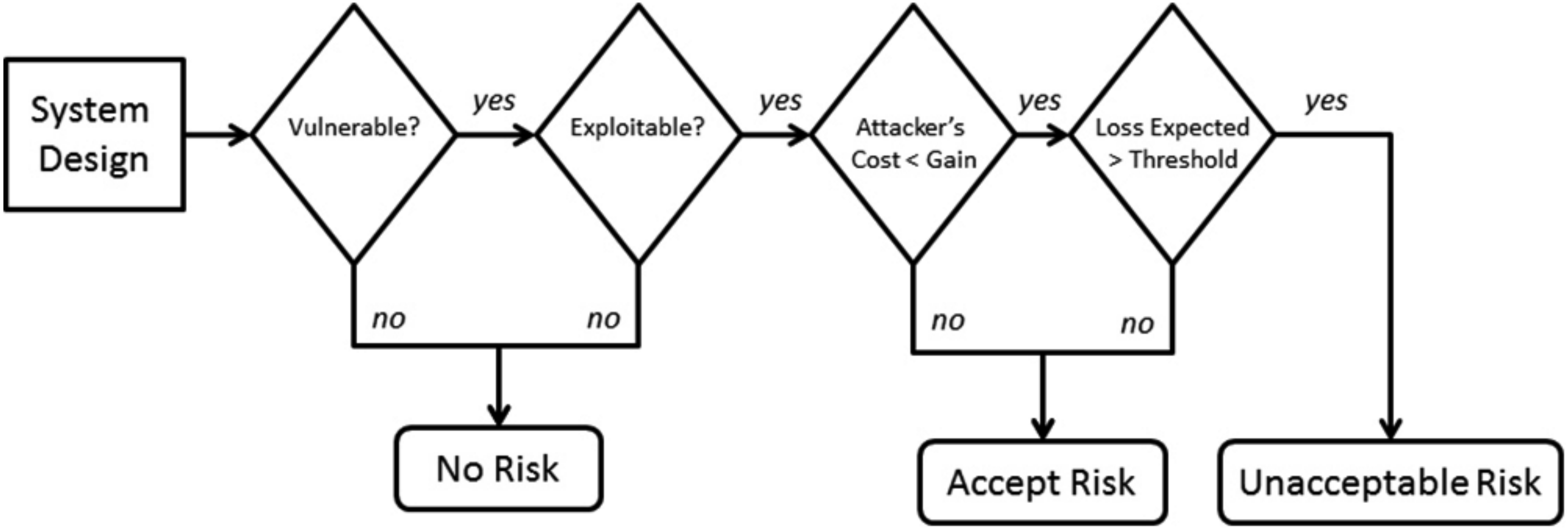
Requires physical tamper-resistance and identity-based authentication

Level 4

Offers highest security with environmental attack resistance.

Security Standards

SP 800-30: Risk Management Guide for IT


System Design

Vulnerable?

Exploitable?

Attacker's Cost < Gain

Loss Expected > Threshold

yes

yes

yes

yes

no

no

no

no

No Risk

Accept Risk

Unacceptable Risk

Security Standards

ISO Standards

Primary body that develops International Standards for all industry sectors

ISO/IEC 15408 – ***Evaluating Criteria for IT Security (Common Criteria)***

The ISO/IEC 15408 Standard and Software Security

ISO/IEC 21827:2008 – ***Systems Security Engineering Capability Maturity Model® (SSE-CMM®)***

ISO/IEC 25000:2005 – ***Software Engineering Product Quality***

ISO/IEC 27000:2009 – ***Information Security Management System (ISMS) Overview and Vocabulary***

Exception

- Electrotechnology
- Telecommunications

Electrotechnology standards are developed by International Electrotechnical Commission (IEC) and telecommunication standards are developed by the International Telecommunications Union (ITU)

Security Standards

Payment Card Industry Data Security Standard (PCI DSS)

Build and Maintain a Secure Network

Requirement 1 Install and maintain a firewall configuration to protect cardholder data

Requirement 2 Do not use vendor-supplied defaults for system passwords & other security parameters

Protect Cardholder Data

Requirement 3 Protect stored cardholder data

Requirement 4 Encrypt transmission of cardholder data across open, public networks

Security Standards

Payment Card Industry Data Security Standard (PCI DSS)

Maintain a Vulnerability Management Program

Requirement 5 Use and regularly update anti-virus software

Requirement 6 Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7 Restrict access to cardholder data by business need-to- know

Requirement 8 Assign a unique ID to each person with computer access

Requirement 9 Restrict physical access to cardholder data

Security Standards

Payment Card Industry Data Security Standard (PCI DSS)

Regularly Monitor and Test Networks

Requirement 10 Track and monitor all access to network resources and cardholder data

Requirement 11 Regularly test security systems and processes

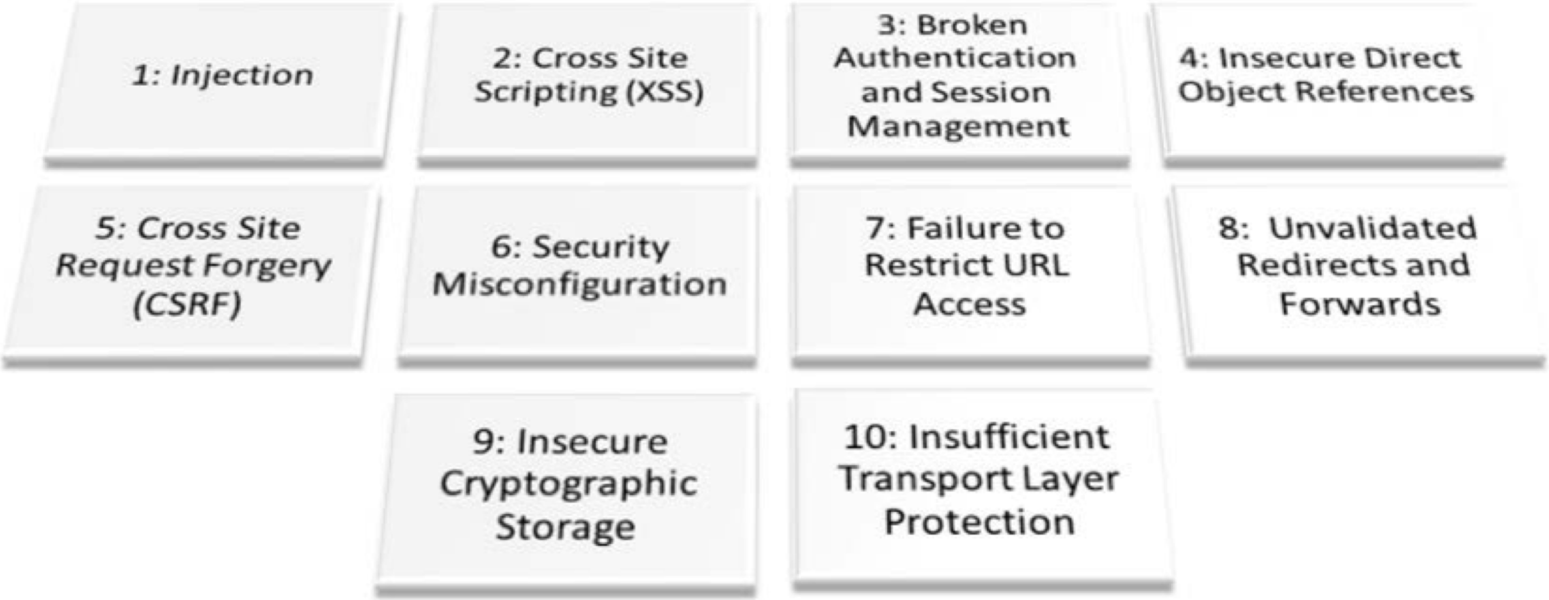
Maintain an Information Security Policy

Requirement 12 Maintain a policy that addresses information security

Security Standards

Open Web Application Security Project (OWASP)

Worldwide free and open community that is focused on application security and predominantly web application security



1: Injection

2: Cross Site Scripting (XSS)

3: Broken Authentication and Session Management

4: Insecure Direct Object References

5: Cross Site Request Forgery (CSRF)

6: Security Misconfiguration

7: Failure to Restrict URL Access

8: Unvalidated Redirects and Forwards

9: Insecure Cryptographic Storage

10: Insufficient Transport Layer Protection

Security Standards

Open Web Application Security Project (OWASP)

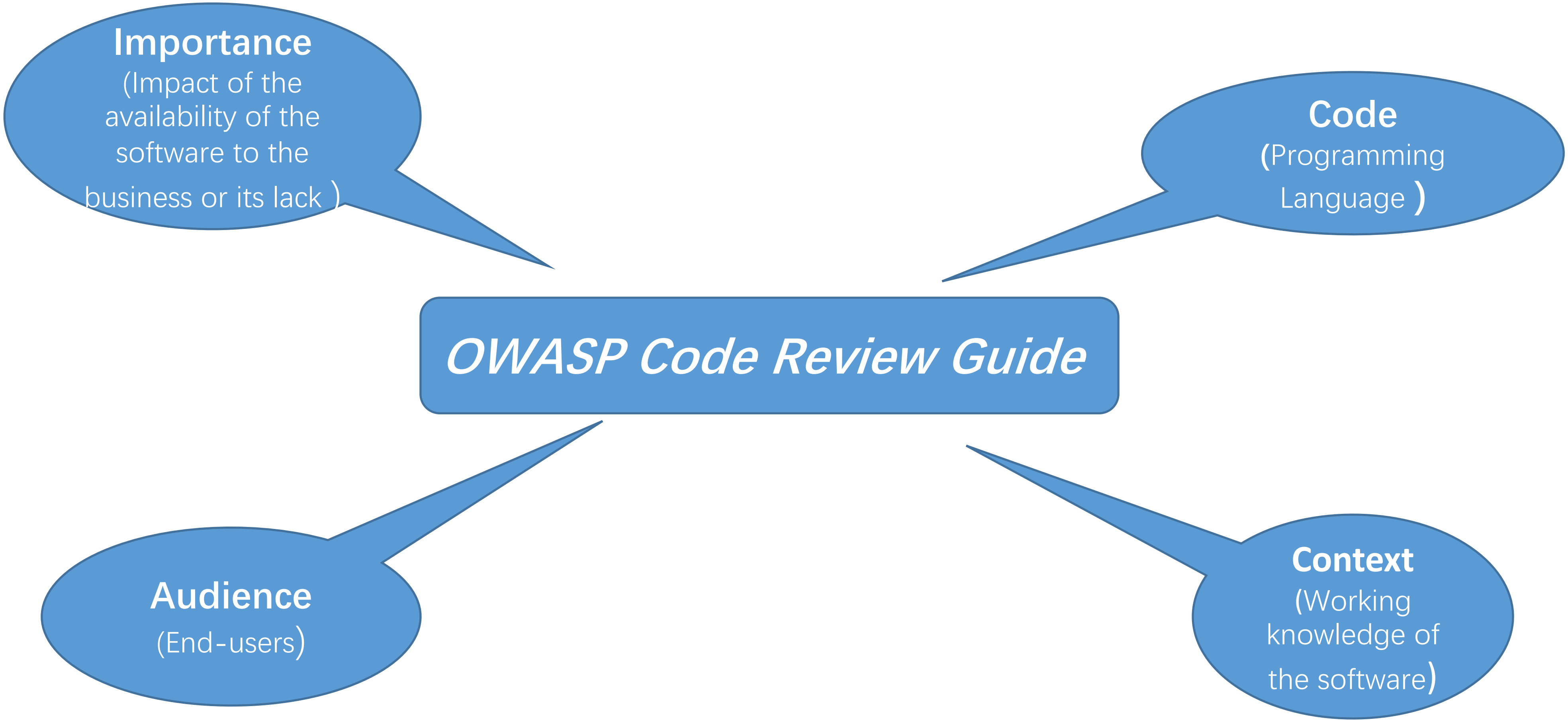
The OWASP Development Guide

Comprehensive manual for designing, developing and deploying secure web applications and web services

The **target audiences** for this guide are architects, developers, consultants and auditors

Security Standards

Open Web Application Security Project (OWASP)



Importance
(Impact of the availability of the software to the business or its lack)

Code
(Programming Language)

OWASP Code Review Guide

Audience
(End-users)

Context
(Working knowledge of the software)

Security Standards

Open Web Application Security Project (OWASP)

The OWASP Testing Guide

Covers the procedures and tools that are necessary to validate software assurance

The target audiences for this guide are software developers, software testers and security specialists.

Security Standards

Internal Coding Standards

One of the most important internal standards that has a tremendous impact on the security of software is the coding standard

The coding standard specifies the requirements that are allowed and that need to be adopted by the development organization or team while writing code (building software)

Coding standards need not be developed for each programming language or syntax but can include various languages into one

Important!!!!!

- First Quiz and Assignment – May be in this week/next week

- Course meeting – each group = 5 students – Will share the time later

Questions??

zubair.ahmad@giki.edu.pk

Office: G14 FCSE lobby