Secure Design Principles and Processes

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Show how to increase security and reduce risk for your organization through proper timing in the SDLC process

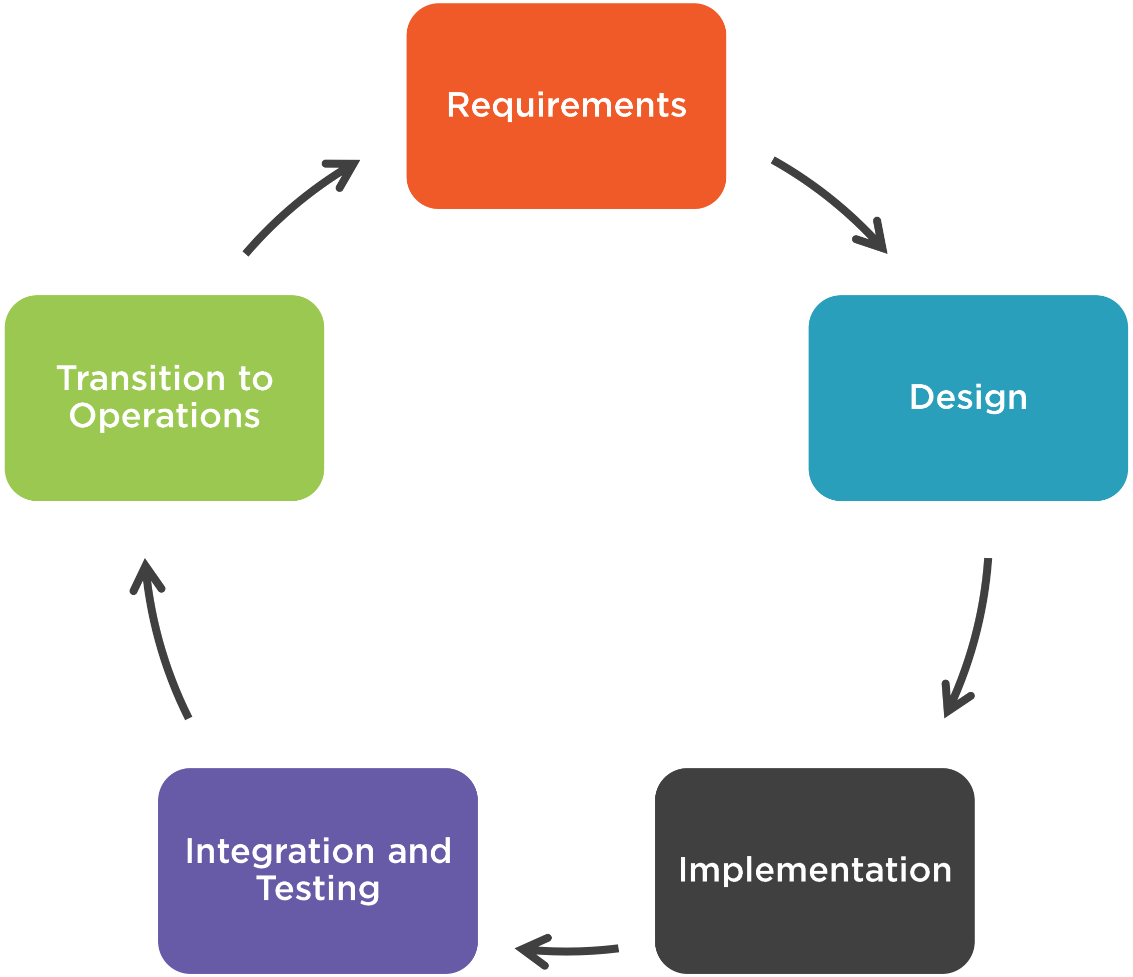
Outline and discuss the 33 Security Engineering Principles that can be applied in your organization

This is the 1st objective of the Security Engineering domain of the CISSP® Exam

Embed security into solution as early as possible,

not “bolted on” after the design / implementation.

Software / System Development Lifecycle (SDLC)



Requirements

Idea is just becoming a project

Scope is not typically hard technology items at this point, but more abstract items

Ability to securely shape the outcome is greatest at this point

Design

Requirements have been finalized

Focus is on building a solution that meets the requirements

Technology components are being introduced to the solution

Great capability to drive a secure solution still exist at this stage

Best chance to win over the business is to avoid “No” and use “Not that way, this way”

Implementation

Technology components are being deployed

High-level items are not easily changed

Low-level items are worked through and adjusted as security concerns arise

Integration and Testing

Technology components that were previously deployed are connected

“Dry runs” or “smoke tests” are executed to ensure reality meets original design

Security testing and validation occurs in parallel with operational testing

Remediation / acceptance of security issues occurs before moving forward

Transition to Operations

Design has been fully implemented and tested previously, now it will deployed into the Production environment

Operational and security monitoring capabilities are enabled

NIST = National Institute of Standards and Technology

NIST Special Publication 800-27 Rev A = Engineering Principles for Information Technology Security (A Baseline for Achieving Security)

Outlines 33 security principles in 6 categories

Categories of Security Engineering Principles

Security Foundation

Risk Based

Ease of Use

Increase Resilience

Reduce Vulnerabilities

Design with Network in Mind

Security Foundation

Principle 1: Establish a sound security policy as the "foundation" for design

Security Foundation

Principle 2: Treat security as an integral part of the overall system design

Security Foundation

Principle 3: Clearly delineate the physical and logical security boundaries governed by the associated security policies

Security Foundation

Principle 4: Ensure that developers are trained in how to develop secure software

Risk Based

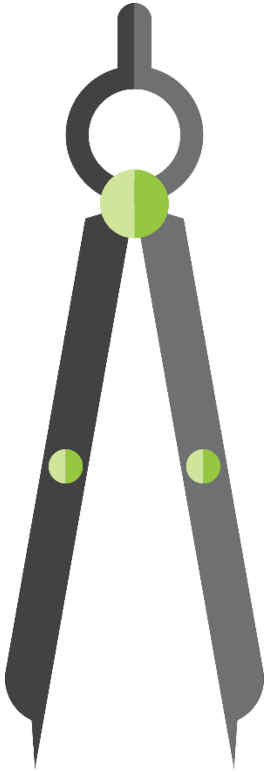
Principle 5: Reduce risk to an acceptable level

Risk Based

Principle 6: Assume that external systems are insecure

Risk Based

Principle 7: Identify potential trade-offs between reducing risk and increased costs and decrease in other aspects of operational effectiveness



Risk Based

Principle 8: Implement tailored system security measures to meet organizational security goals

Risk Based

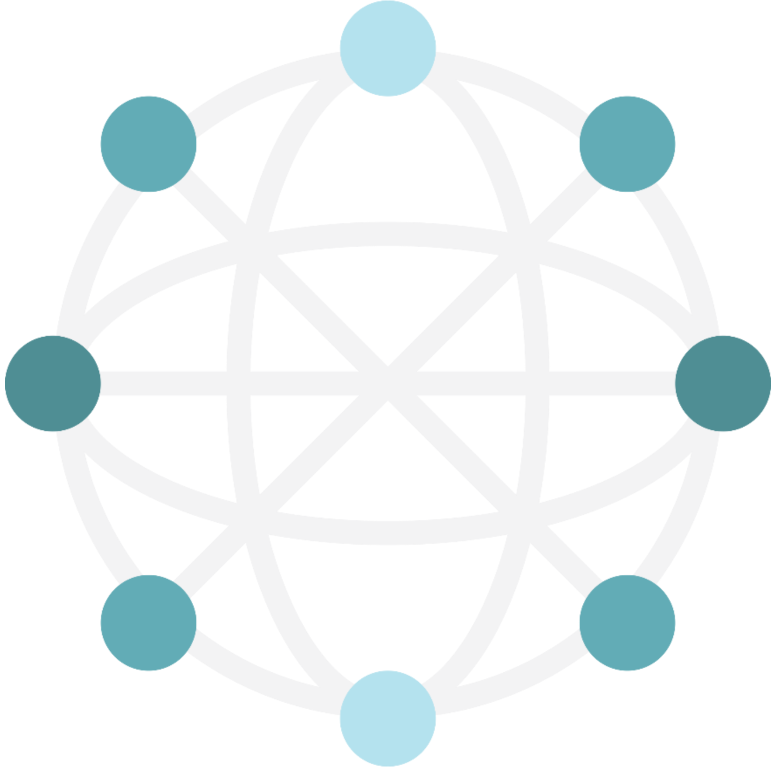
Principle 9: Protect information while being processed, in transit, and in storage

Risk Based

Principle 10: Consider custom products to achieve adequate security

Risk Based

Principle 11: Protect against all likely classes of “attacks”



Ease of Use

Principle 12: Where possible, base security on open standards for portability and interoperability

Ease of Use

Principle 13: Use common language in developing security requirements

Ease of Use

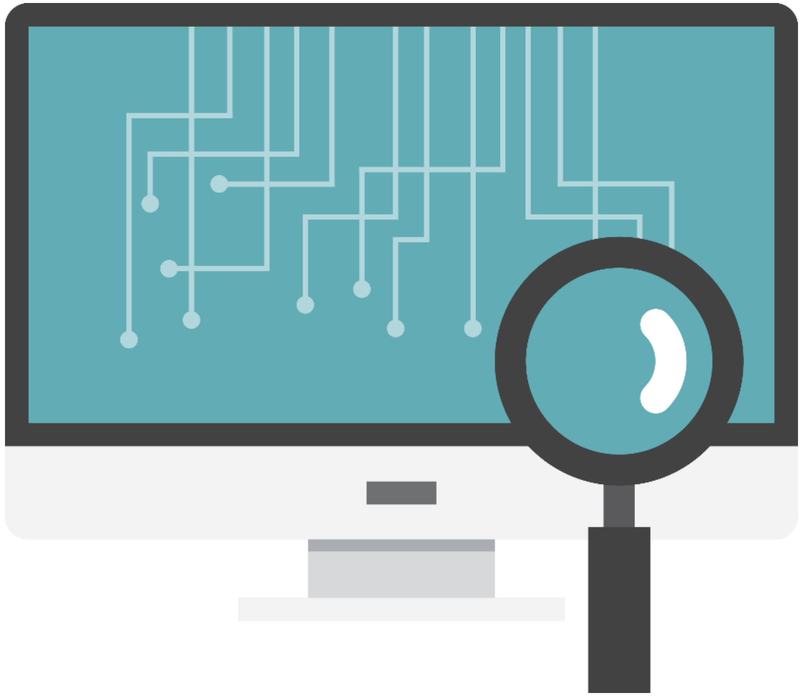
Principle 14: Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process

Ease of Use

Principle 15: Strive for operational ease of use

Increase Resilience

Principle 16: Implement layered security (ensure no single point of vulnerability)



Increase Resilience

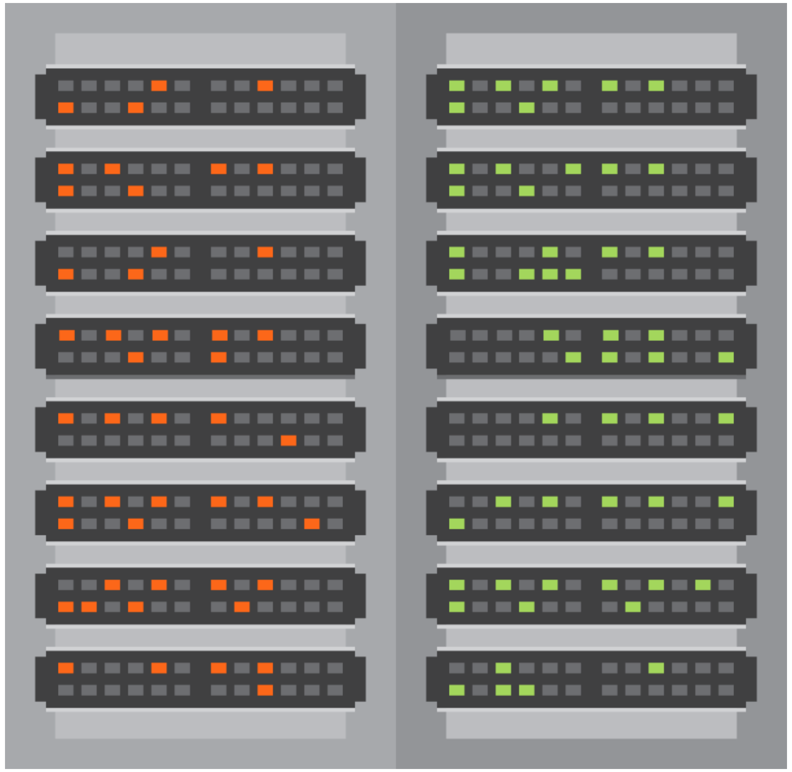
Principle 17: Design and operate an IT system to limit damage and to be resilient in response

Increase Resilience

Principle 18: Provide assurance that the system is, and continues to be, resilient in the face of expected threats

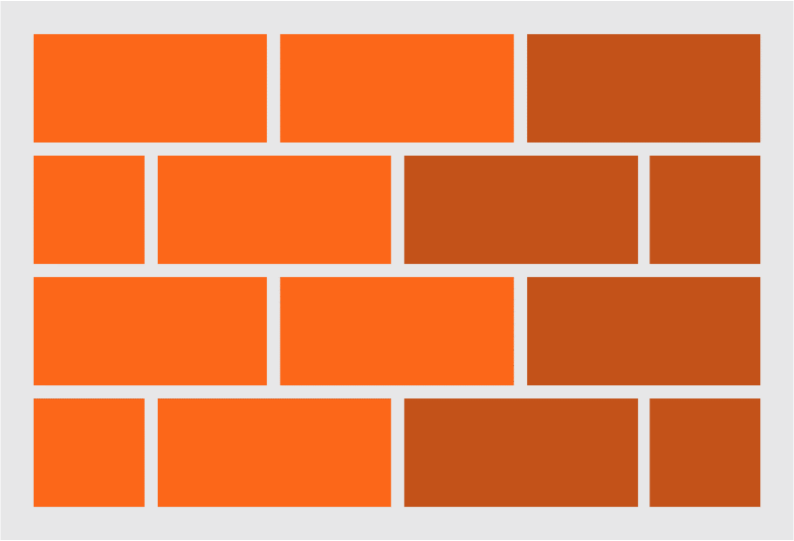
Increase Resilience

Principle 19: Limit or contain vulnerabilities



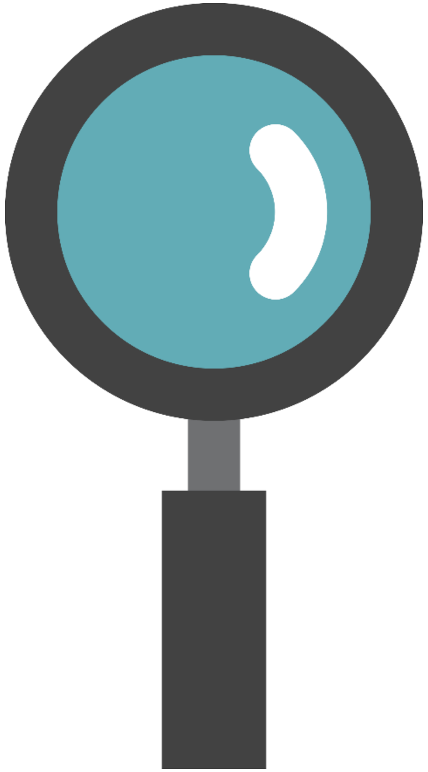
Increase Resilience

Principle 20: Isolate public access systems from mission critical resources (e.g., data, processes, etc.)



Increase Resilience

Principle 21: Use boundary mechanisms to separate computing systems and network infrastructure



Increase Resilience

Principle 22: Design and implement audit mechanisms to detect unauthorized use and to support incident investigations

Increase Resilience

Principle 23: Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability

Reduce Vulnerabilities

Principle 24: Strive for simplicity

Reduce Vulnerabilities

Principle 25: Minimize the system elements to be trusted

Reduce Vulnerabilities

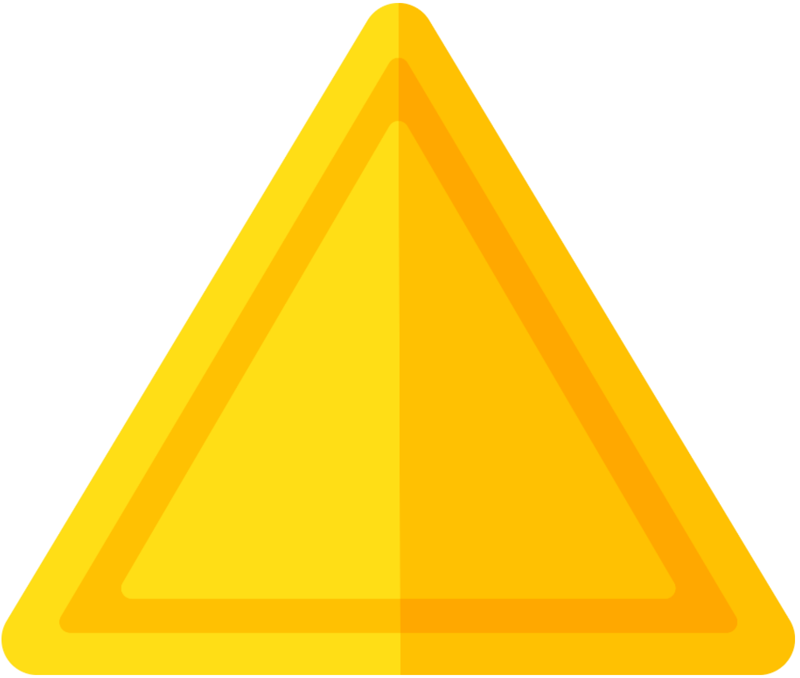
Principle 26: Implement least privilege

Reduce Vulnerabilities

Principle 27: Do not implement unnecessary security mechanisms

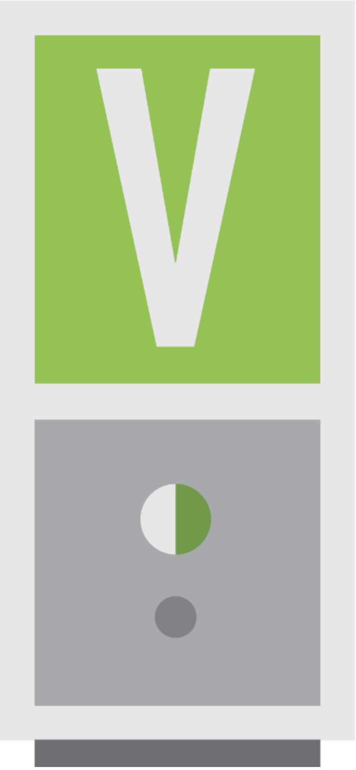
Reduce Vulnerabilities

Principle 28: Ensure proper security in the shutdown or disposal of a system



Reduce Vulnerabilities

Principle 29: Identify and prevent common errors and vulnerabilities



Design with Network in Mind

Principle 30: Implement security through a combination of measures distributed physically and logically

Design with Network in Mind

Principle 31: Formulate security measures to address multiple overlapping information domains

Design with Network in Mind

Principle 32: Authenticate users and processes to ensure appropriate access control decisions both within and across domains

Design with Network in Mind

Principle 33: Use unique identities to ensure accountability

Summary

Showed how to increase security and reduce risk for your organization through proper timing in the SDLC process

Outlined and discussed the 33 Security Engineering Principles that can be applied in your organization

This is the 1st objective of the Security Engineering domain of the CISSP® Exam

What's Next?

Fundamental Concepts of Security Models

What are they?

How do they relate to this module and the other modules?

Why are they important to this course and the CISSP® exam?