Fundamental Concepts of Security Models

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Outline common security model types that can be leveraged, as well as examples of these security models

Outline common Security Architecture frameworks that can be employed in your organization

This is the 2nd objective of the Security Engineering domain of the CISSP® Exam

Security models provide rules for interactions between subjects and objects

Type of Security Models

Information Flow

Matrix-Based

Multilevel Lattice

Noninterference

State Machine

Information Flow Security Model

Focused on how information is allowed or not allowed between objects

Helps identify inadvertent exposure of information between objects

Example: A restricted object inadvertently is configured to write debug log data to a network share location that is accessible by other objects, exposing sensitive information about the restricted object

Matrix-Based Security Model

Granular model that individually maps the relationship between subjects and objects

Example: User A has access to folders A and C, but not B and D; while, user B has access to folders A, C, and D, but not B

Multilevel Lattice Security Model

Leverages multiple levels for subjects and objects to provide applicable access

Security labeling is provided for the multiple levels to determine whether a subject should have access to an object

Example: A subject with Secret clearance can access Secret objects, but not Top Secret objects

Noninterference Security Model

Type of Multilevel Lattice Security Model that is highly restrictive on object access across security levels

Provides more assurances that data transfer is not occurring across covert channels that bypass security controls on comingled systems

Example: Separate systems and networks for Secret objects and subjects from Top Secret objects and subjects

State Machine Security Model

Focuses on what is allowed vs. not, based on the state of the system

State is determined by system parameters during runtime or time-based

What is allowed vs. not is processed through the state of the system

Example: A firewall allows traffic to come from the Internet to an internal network, if the traffic originally initiated internally (i.e. responding to internal traffic), but not if it originated from the Internet

Common Security Model Examples

Bell-LaPadula Confidentiality

Biba Integrity

Brewer-Nash (The Chinese Wall)

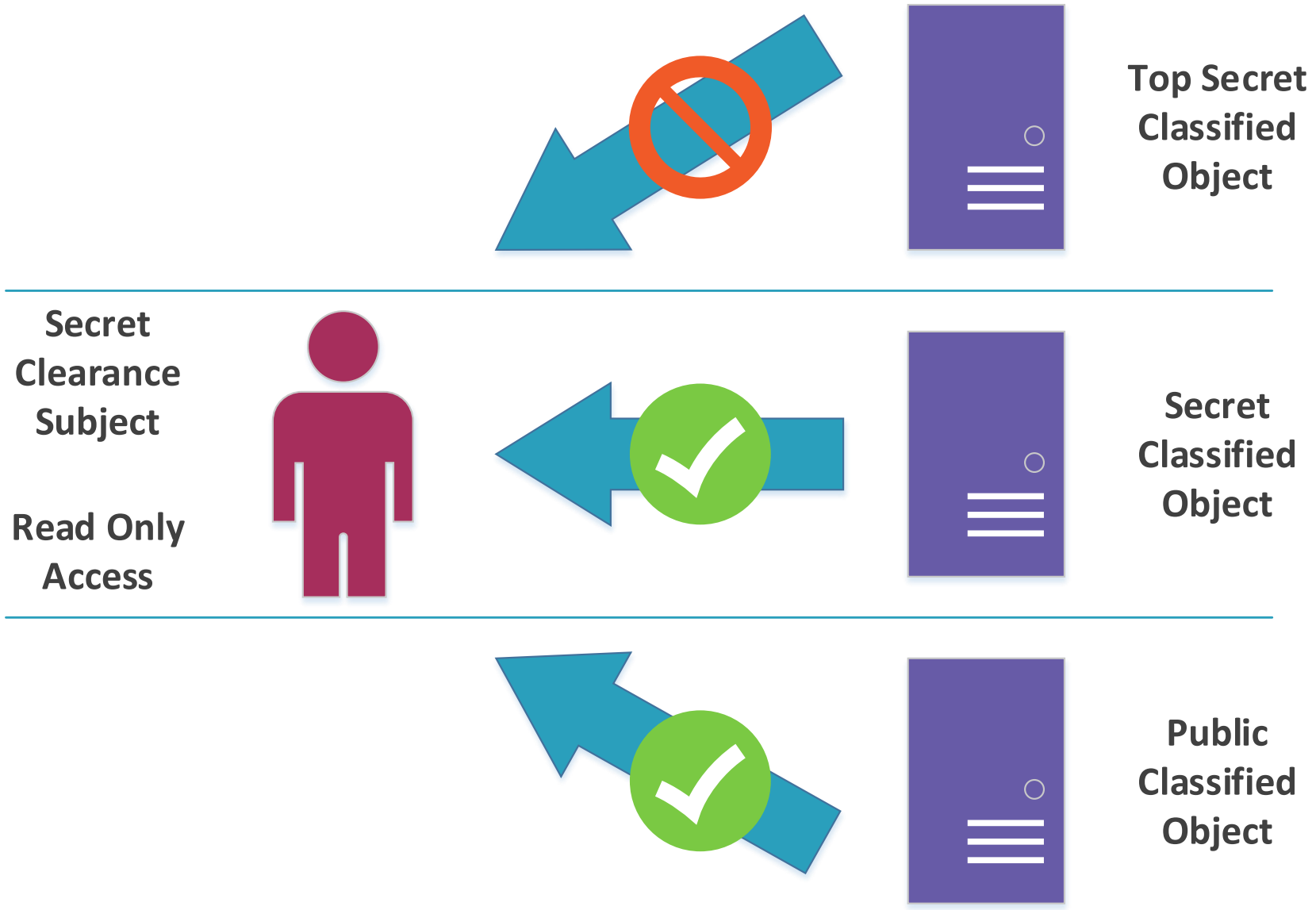
Clark Wilson Integrity

Graham-Denning

Bell-LaPadula Confidentiality Model

- Well-known and one of the oldest security models
- Widely used in government organizations (e.g., military, etc.)
- Focuses on maintaining the confidentiality of data
- Subjects are assigned a clearance level and what mode of access that can be performed on objects (e.g., write, read, etc.)
- Objects are assigned a classification level
- Depending on the read vs. write vs. read/write access of a subject and their clearance level will determine what classification level they can access

Bell-LaPadula – Read Only Access

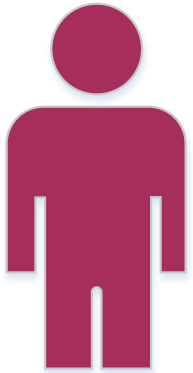


Bell-LaPadula – Write Only Access

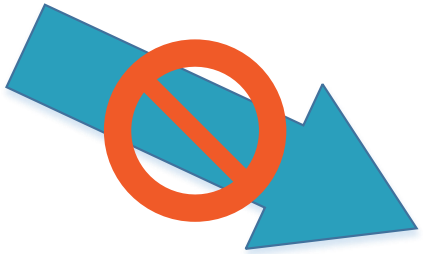
Top Secret Classified Object

Secret Clearance Subject

Write Only Access

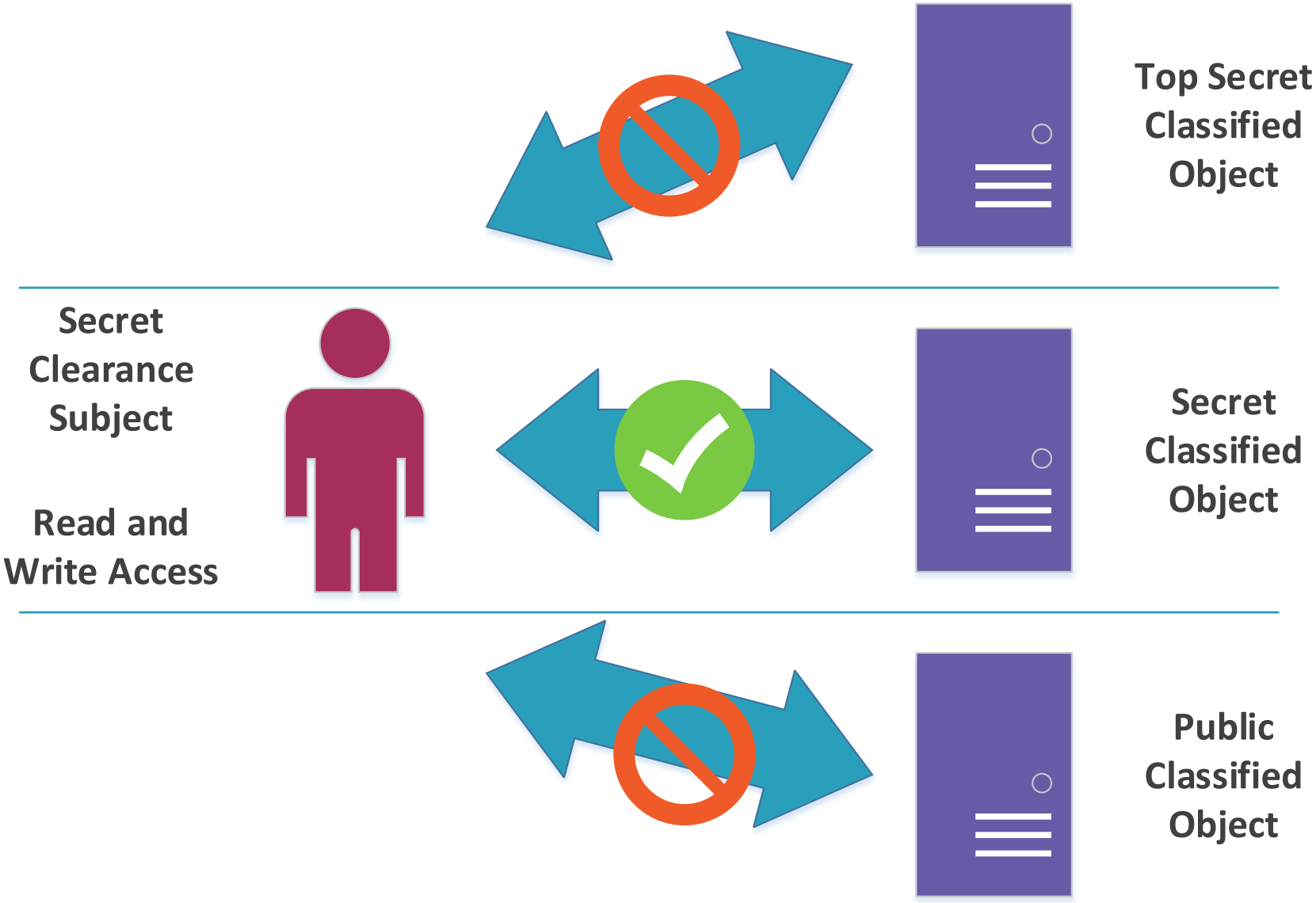


Secret Classified Object



Public Classified Object

Bell-LaPadula – Read and Write Access



Biba Integrity Model

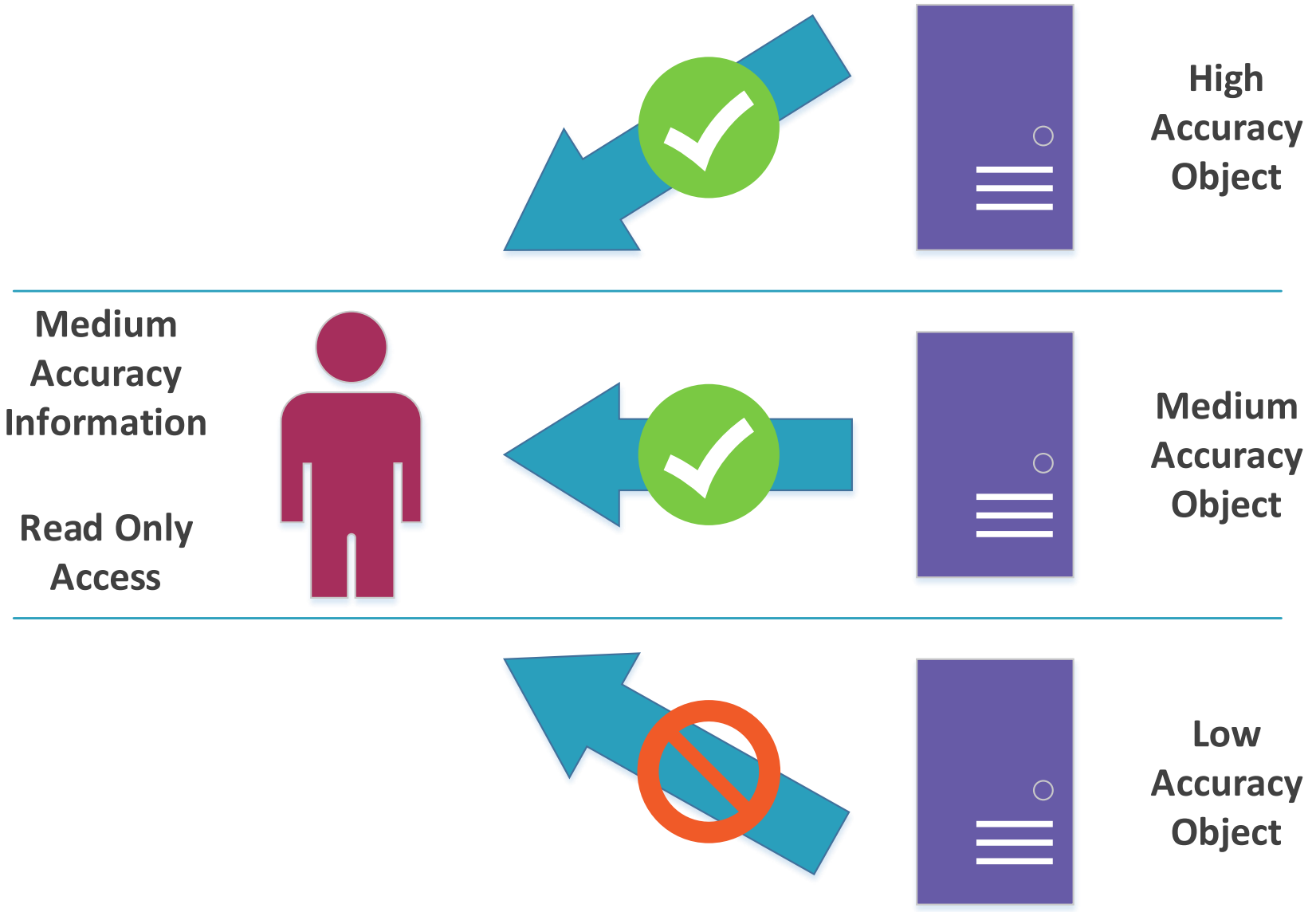
Similar to Bell-LaPadula model, but focuses on integrity instead of confidentiality

Approach is flipped in application compared to Bell-LaPadula (e.g., no read up in Bell-LaPadula = no read down in Biba)

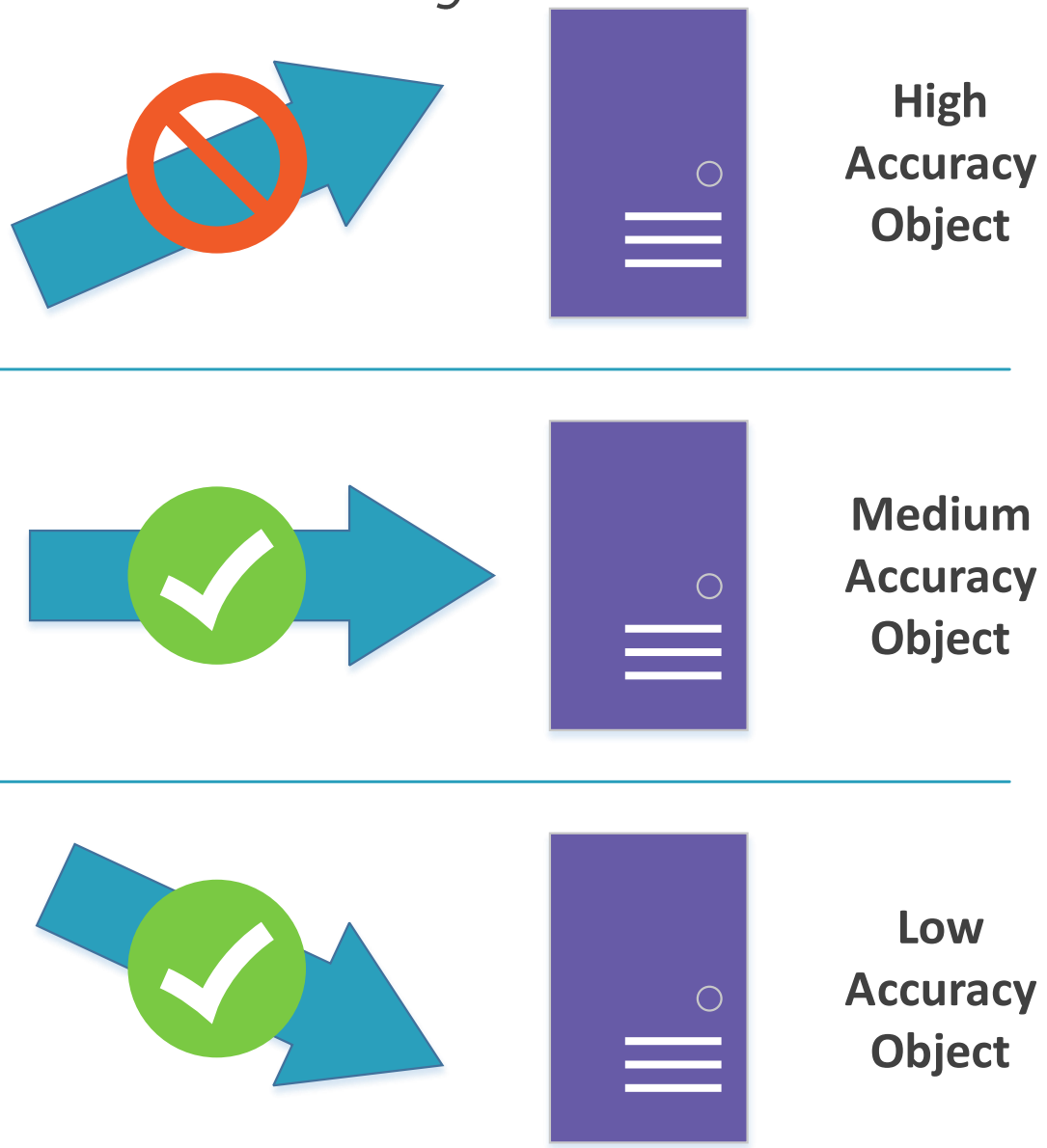
Biba assigns integrity levels to subject and objects, based on how trustworthy they are

Focuses on preventing unauthorized subjects from modifying objects

Biba – Read Only Access



Biba – Write Only Access



Brewer-Nash (The Chinese Wall) Model

Focuses on preventing subjects from sharing sensitive information between competing parties

Even if a subject has access to both parties' objects, their access decision one negates their access to the other

Overall helps prevent conflict of interest situations among subjects

Clark-Wilson Integrity Model

Improves upon the integrity capabilities of Biba Integrity Model

Changes made by authorized subjects that were undesirable and consistent system behavior are additional goals

Separation of duties where one party reviewed the changes of another party before committing the transaction reduced undesirable changes by authorized subjects

Strict definition of well-formed transactions improved system behavior consistency

Graham-Denning Model

Focused on three areas:

- How subjects and objects are created
- How subjects are assigned rights or privileges
- How ownership of objects is managed

Eight protection rights exist:

- Create and Delete Subjects
- Create and Delete Objects
- Read, Grant, Delete, and Transfer Access Rights

Security Architecture frameworks help support the goals of Security Models

Common Security Architecture Frameworks

The Open Group Architecture Framework (TOGAF)

Zachman Framework

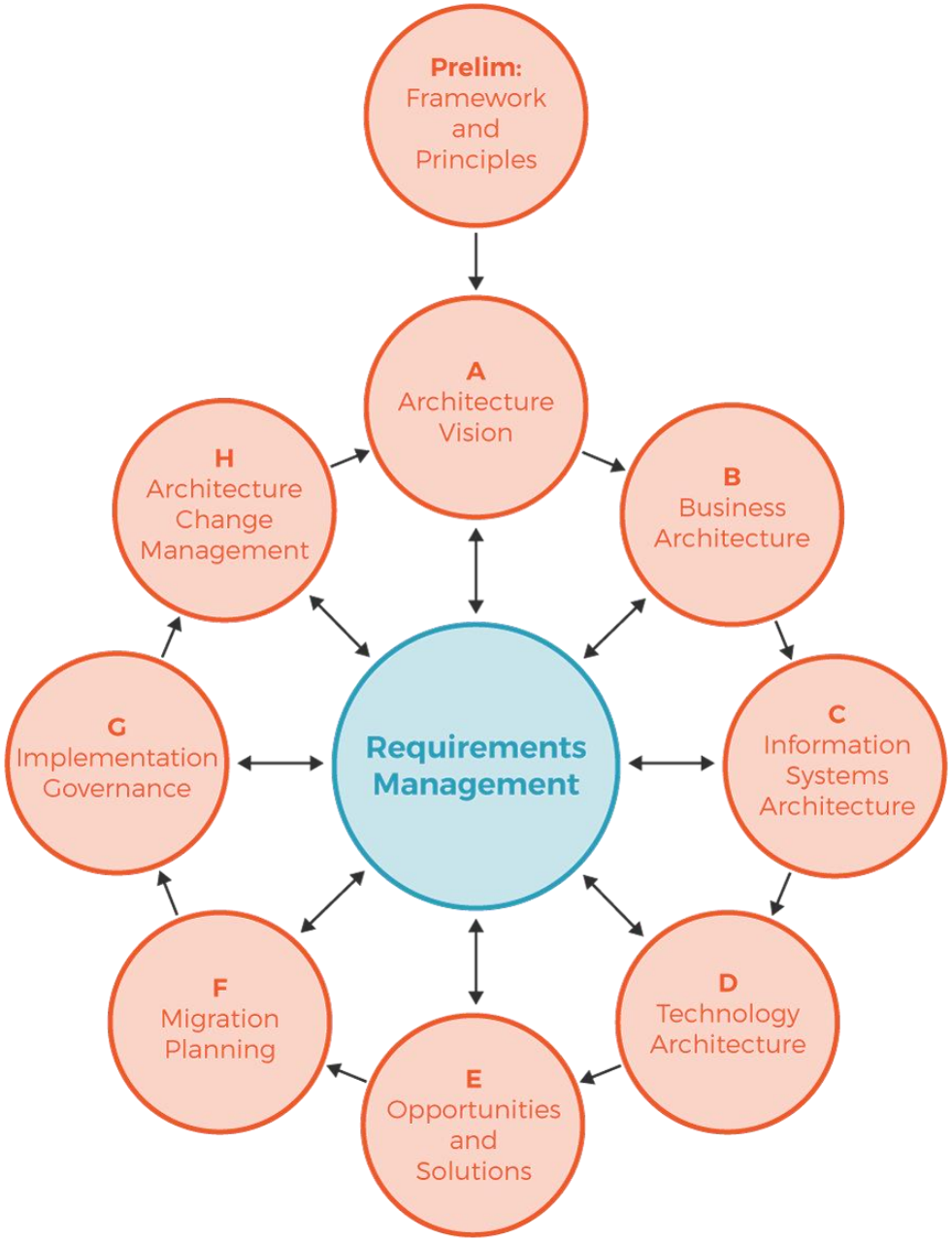
Sherwood Applied Business Security Architecture (SABSA)

The Open Group Architecture Framework (TOGAF)

Not just Security Architecture

Designed in the 1990s

Open framework consisting of common terms, development method, building blocks, and reference models

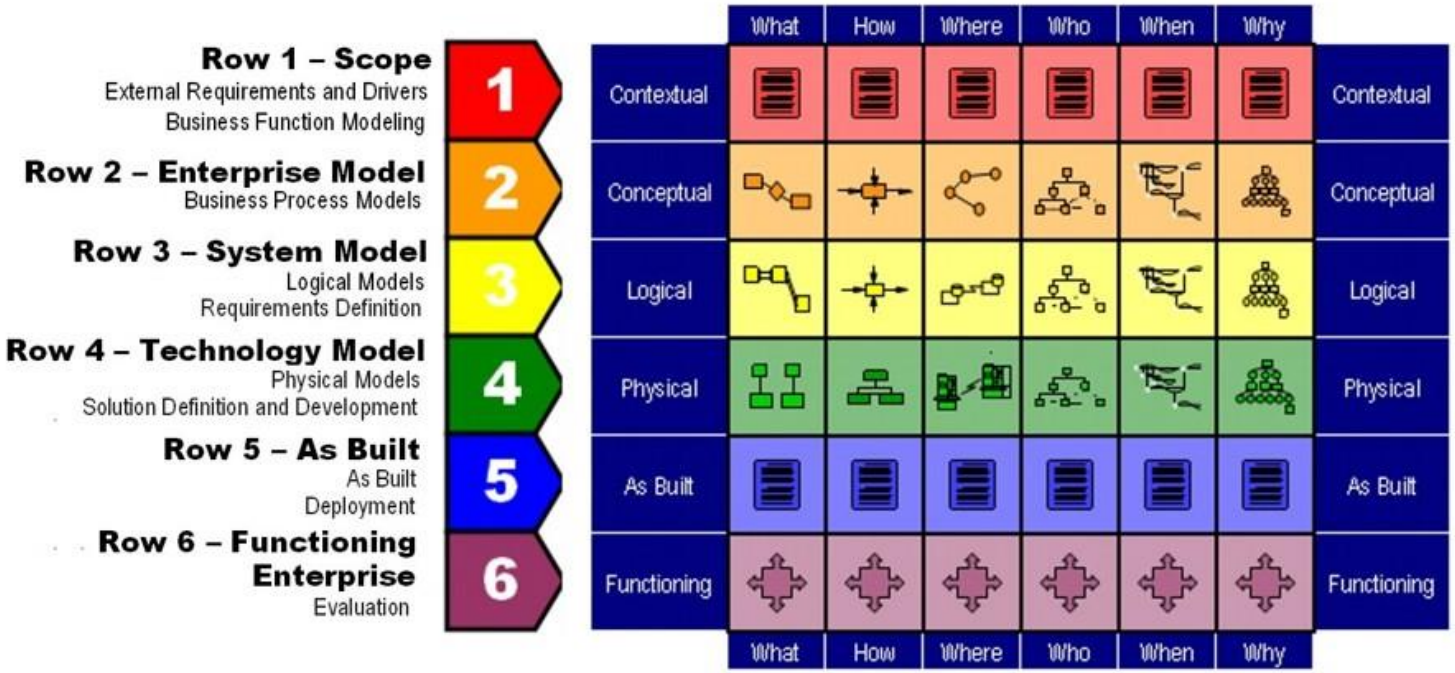


Zachman Framework

Not just Security Architecture

Designed in the 1980s

Aimed at developing a common context for understanding complex environments and architectures

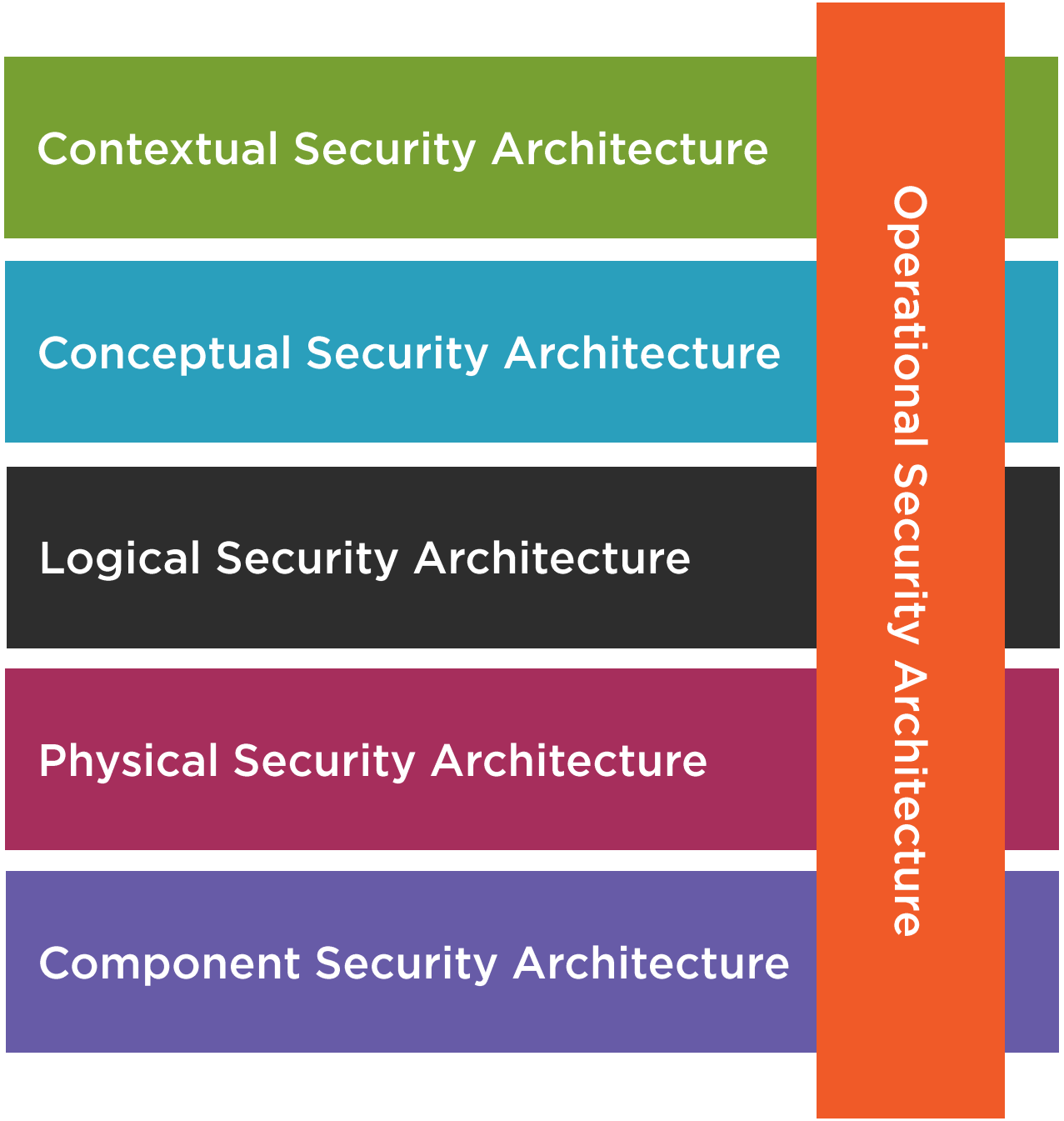


Sherwood Applied Business Security Architecture (SABSA)

Very similar to Zachman

Focuses on assessing business requirements related to security architecture

Builds upon the prior phases' perspective



Summary

Outlined common security model types that can be leveraged, as well as examples of these security models

Outlined common Security Architecture frameworks that can be employed in your organization

This is the 2nd objective of the Security Engineering domain of the CISSP® Exam

What's Next?

Security Evaluation 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?