Security Evaluation Models

Evan Morgan, CISSP, CISM

@1evanski www.evanski.com

Overview

Define what certification and accreditation are, as well as how they could be used by your organization

Outline and discuss three common product evaluation models that can be leveraged in your organization

Outline and discuss three common security implementation guidelines that can be leveraged in your organization

This is the 3rd objective of the Security Engineering domain of the CISSP® Exam

Security Evaluation Models improve the consistency at which security principles are applied to an application, system, organization, etc.

Certification and Accreditation

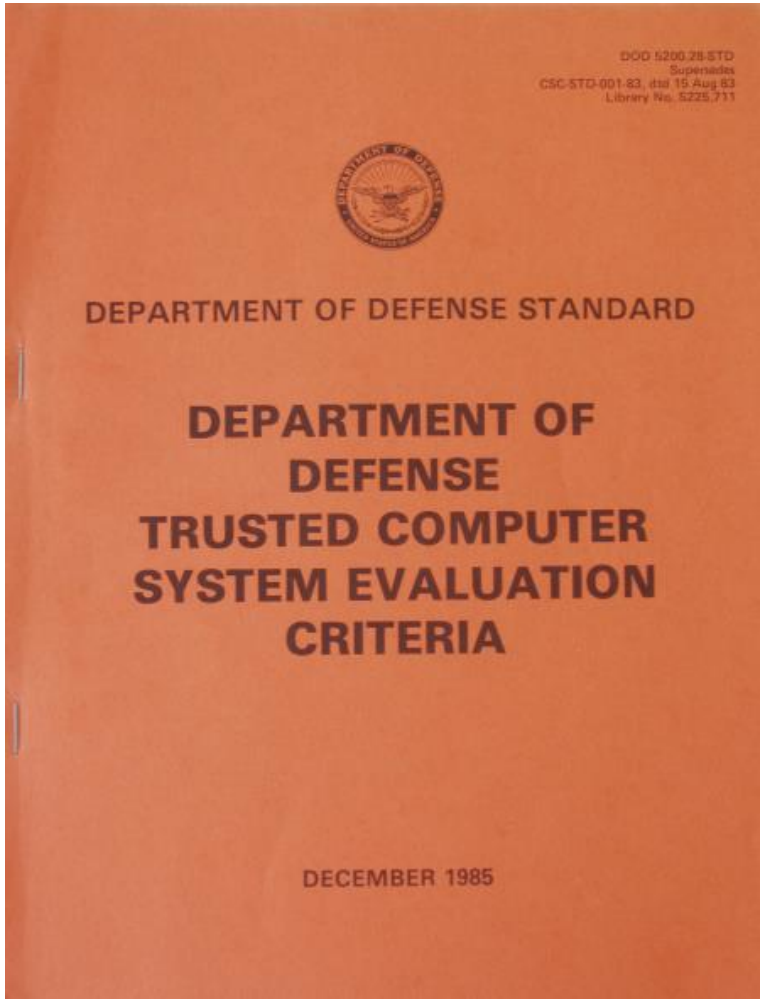
Certification	Accreditation
Assesses technology against requirements	Assesses technology against the needs of the organization
Is contextual to real world deployment (e.g., network connections, usage)	Formal acceptance of the system into the environment for a period of time
Baseline is created out of the evaluation's result	Configuration changes invalidate certification
If successful in certification, it moves on to accreditation	Expiration of accreditation also causes the need for recertification
Example: Proof of concept of a new firewall platform that is piloted with a few different IT and business teams	Example: Firewall is accredited for a year with a certain certified configuration

Product Evaluation Models

Trusted Computer System Evaluation Criteria (TCSEC)

Information Technology Security Evaluation Criteria (ITSEC)

The Common Criteria



Trusted Computer System Evaluation Criteria (TCSEC)

Also known as the “Orange Book”

First published in 1983

Considered Department of Defense standard for product evaluation to ensure security requirements are met

Confidentiality is the core focus

Introduced Trusted Computing Base (TCB) idea into product evaluation

Has been superseded by the Common Criteria

TCSEC Evaluation Criteria Divisions

Four core divisions

Some divisions have subdivisions (classes)

Evaluation Division	Evaluation Class	Degree of Trust
D – Minimal Protection	D1 – Minimal Protection	Least
C – Discretionary Protection	C1 – Discretionary Security Protection	
	C2 – Controlled Access Protection	
B – Mandatory Protection	B1 – Labeled Security	
	B2 – Structured Protection	
	B3 – Security Domains	
A – Verified Protection	A1 – Verified Design	Most

TCSEC High-Level TCB Requirements

Evaluation Division	Evaluation Class	Description
D – Minimal Protection	D1 – Minimal Protection	• Evaluated but does not meet security requirements
C – Discretionary Protection	C1 – Discretionary Security Protection	• Basic Discretionary Access Control (DAC)
	C2 – Controlled Access Protection	• Improved DAC • Individual login accountability and audit trail • Resource isolation • Essential system and user documentation
B – Mandatory Protection	B1 – Labeled Security	• Mandatory Access Control (MAC) over some subjects and objects • All discovered flaws must be mitigated

TCSEC High-Level TCB Requirements (cont.)

Evaluation Division	Evaluation Class	Description
B – Mandatory Protection	B2 – Structured Protection	• DAC and MAC enforcement for all subjects and objects • Security policy model clearly defined and formally documented • Covert storage channels are identified and analyzed • Objects are protected according to criticality • Design and implementation support thorough testing and review • Authentication mechanisms are hardened from compromise • Trusted management segregates administrator and operator privileges • Strict configuration management

TCSEC High-Level TCB Requirements (cont.)

Evaluation Division	Evaluation Class	Description
B – Mandatory Protection	B3 – Security Domains	• Can satisfy reference monitor requirements • Structured to exclude code not essential to security policy enforcement • Significant system engineering directed toward minimizing complexity • Trusted management provides security administrator function • Audits all security-relevant events • Automated imminent intrusion detection, notification, and response • Covert timing channels are identified and analyzed
A – Verified Protection	A1 – Verified Design	• Functionally identical to B3 but more formal design and verification

Information Technology Security Evaluation Criteria (ITSEC)

Like TCSEC

- Uses divisions (called levels)
- Focuses on confidentiality

Unlike TCSEC

- Requirements are defined by the consumer or vendor, not the model itself
- Two levels are provided (functional level and assurance level)
- Also focuses on integrity and availability

Requirements are the Security Target (ST)

Vendors develop Target of Evaluation (ToE) (i.e. products) to have assessed against ST

ITSEC Assurance Levels

Level	Description	Degree of Assurance
E1	• Security target and information architecture design produced • User/Admin documentation gives guidance on Target of Evaluation (ToE) security • Security enforcing functions are tested by evaluator or developer • ToE to be uniquely identified and to have delivery, configuration, startup, and operational documentation • Secure distribution methods to be utilized	Least
E2	• Information detailed design and test documentation produced • Architecture shows the separation of the ToE into security enforcing and other components • Penetration testing searches for errors • Configuration control and developers security is assessed • Audit trail output is required during startup and operation	
E3	• Source code or hardware drawings produced • Correspondence must be shown between source code and detailed design • Acceptance procedures must be used • Implementation languages should be recognized standards • Retesting must occur after the correction of errors	

ITSEC Assurance Levels (cont.)

Level	Description	Degree of Assurance
E4	• Formal model of security and semi-formal specification of security enforcing functions • Architecture and detailed design to be produced • Testing must be shown to be sufficient • ToE and tools are under configuration control with changes audited, compiler options documented • ToE to retain security on restart after failure	
E5	• Architectural design explains the inter-relationship between security enforcing components • Information on integration process and run time libraries to be produced • Configuration control independent of developer • Identification of configured items as security enforcing or security relevant, with support for variable relationships between them	
E6	• Formal description of architecture and security enforcing functions produced • Correspondence shown from formal specification of security enforcing function through to source code and tests • Different ToE configurations defined in terms of the formal architectural design • All tools subject to configuration control	Most

The Common Criteria

Like ITSEC and TCSEC

- Uses divisions/levels

Like ITSEC

- Flexible in requirements
- Functional and assurance requirements are provided
- Vendors products are still the ToE

Created category-based requirements called “Protection Profiles”

Functional and assurance requirements are grouped together in categories

Common Criteria Evaluation Assurance Levels

Short Name	Long Name	Description of When to Best Use	Level of Confidence
EAL1	Functionally tested	Accurate operation necessary, but security is not a priority	Least
EAL2	Structurally tested	Low to moderate level of independently guaranteed security	
EAL3	Methodically tested and checked	Moderate level of independently guaranteed security	
EAL4	Methodically designed, tested, and reviewed	Moderate to high level of independently guaranteed security	
EAL5	Semi-formally designed and tested	High level of independently guaranteed security	
EAL6	Semi-formally verified, designed, and tested	High risk situations requiring specialized ToEs	
EAL7	Formally verified, designed, and tested	Extremely high risk situations requiring specialized ToEs	Most

Security Implementation Guidelines

ISO/IEC 27001 and 27002 Security Standards

Control Objects for Information and Related Technology (COBIT)

Payment Card Industry Data Security Standard (PCI-DSS)

ISO/IEC 27001 vs. 27002

27001

Internationally recognized for strong security practices

Focused on higher level standardization and certification of an organization's information security management system (ISMS) (i.e. governance structure of Information Security program)

Provides guidance on how to apply ISMS concepts to an organization (e.g., who, what, how, why, etc.)

27002

Internationally recognized for strong security practices

Focused on lower level control objectives

Includes 14 areas of focus (e.g., policies, access control, cryptography, etc.)

ISO/IEC 27002 Focus Areas

Number	Area
1	Information Security Policies
2	Organization of Information Security
3	Human Resource Security
4	Asset Management
5	Access Control
6	Cryptography
7	Physical and Environmental Security
8	Operations Security
9	Communications Security
10	Information Systems Acquisitions, Development, and Maintenance
11	Supplier Relationships
12	Information Security Incident Management
13	Information Security Aspects of Business Continuity Management
14	Compliance

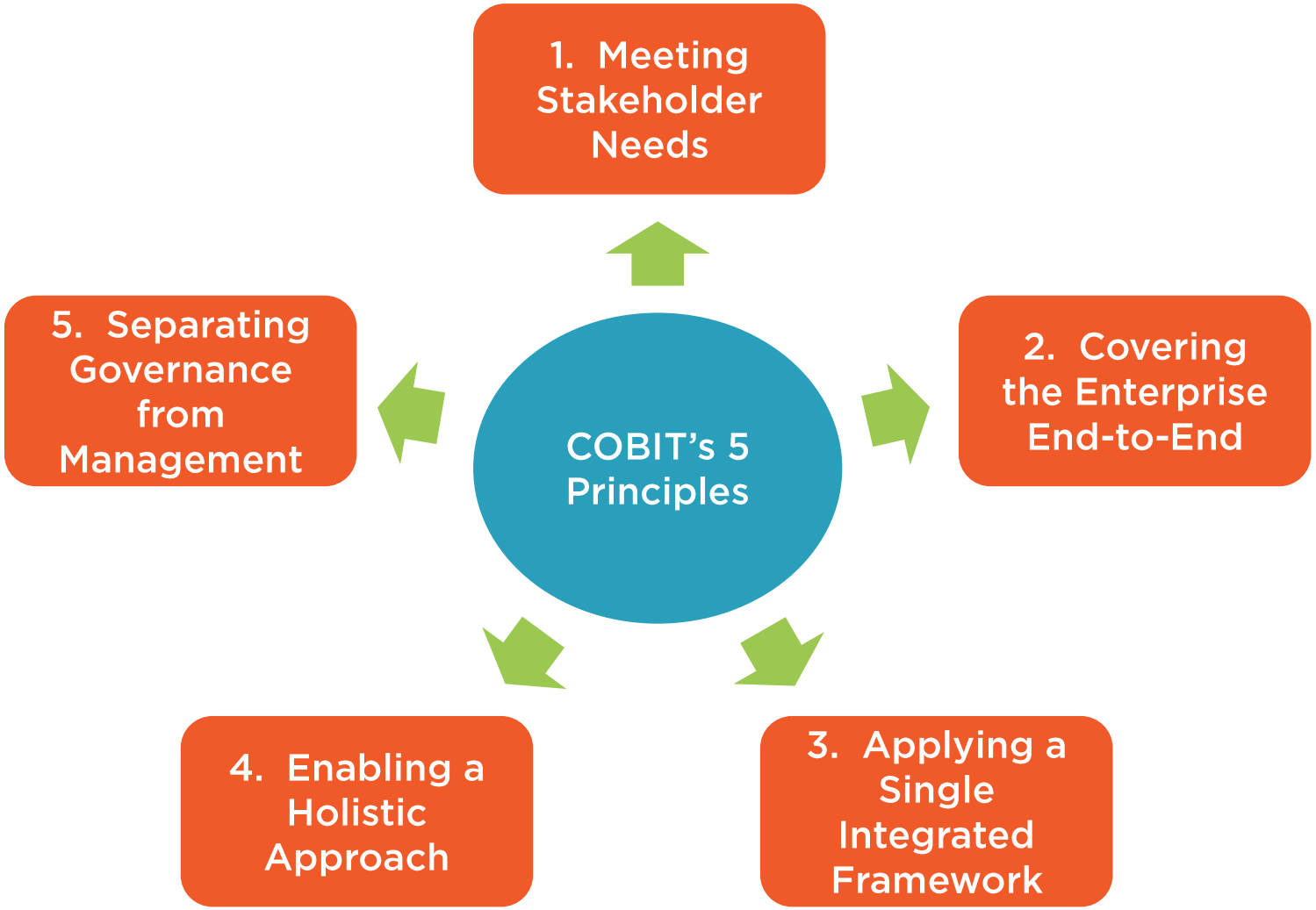
Control Objects for Information and Related Technology (COBIT)

Framework for IT management

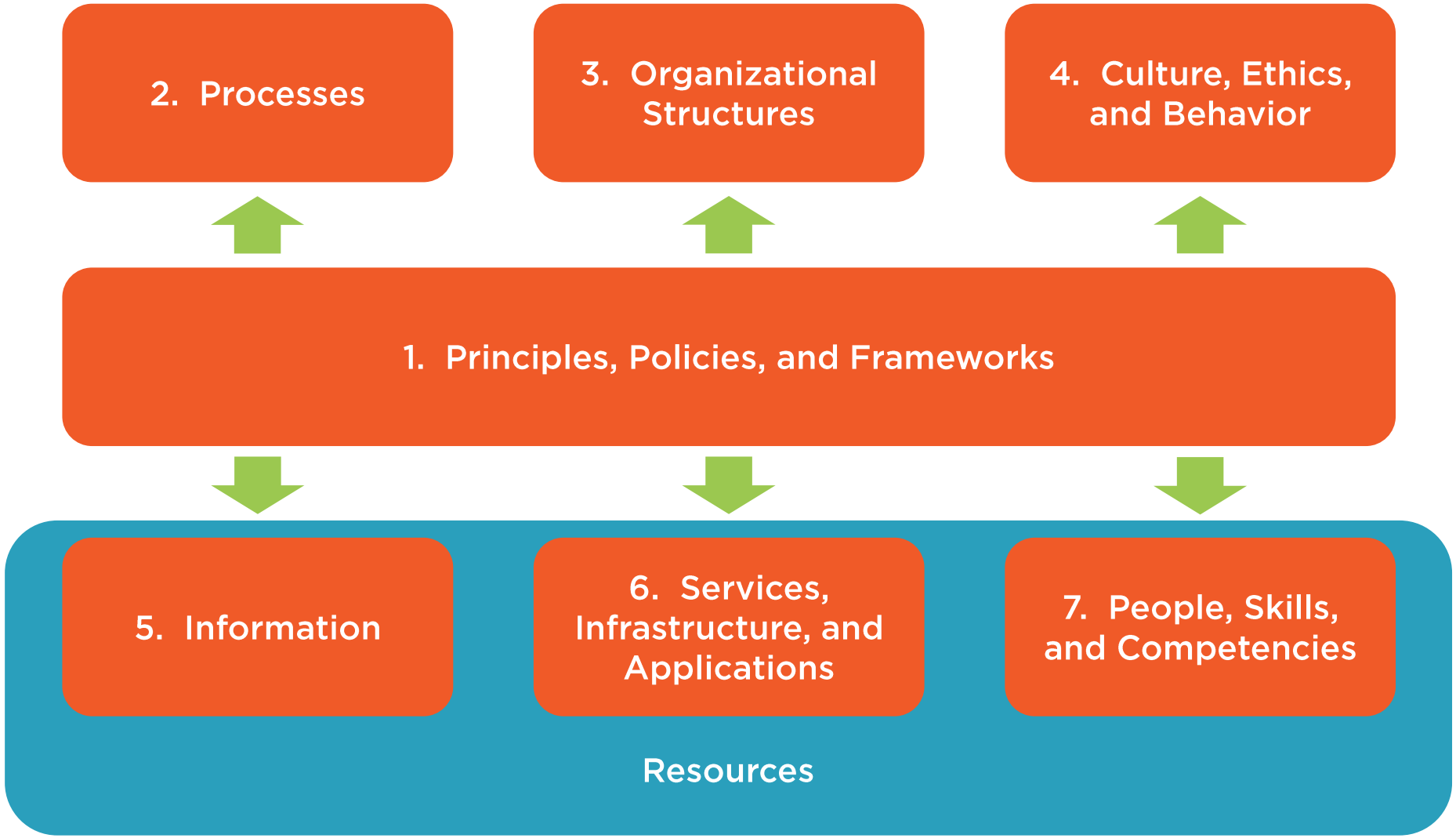
Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in the early 90s

Considered to be the bare minimum security services that an organization has

COBIT's 5 Principles



COBIT's 7 Enablers



Payment Card Industry Data Security Standard (PCI-DSS)

Framework of specifications for the safe processing, storing, and transmission of cardholder information

Focused on compliance with the standard

Created by the Payment Card Industry Security Standards Council

Targeted at merchants and service providers and any systems involved in payment card services

Leverages broad goals, each with lower level requirements, that have even lower level sub objectives

PCI-DSS Goals and Requirements

Goals	Requirements
1. Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-specific supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
3. Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs
	6. Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know
	8. Assign unique ID to each person with computer access
	9. Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
6. Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

Summary

Defined what certification and accreditation are, as well as how they could be used by your organization

Outlined and discussed three common product evaluation models that can be leveraged in your organization

Outlined and discussed three common security implementation guidelines that can be leveraged in your organization

This is the 3rd objective of the Security Engineering domain of the CISSP® Exam

What's Next?

Security Capabilities of Information Systems

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?