Welcome Back!!

CISSP Crash Course Part 2

January 18, 2018

Day 2 Crash Course Agenda

Segment 1: Domain 4 Communications and Network Security (45 min)

Segment 2: Domain 5 Identity and Access Management (30 min)

Segment 3: Domain 6 Security Assessment and Testing (30 min)

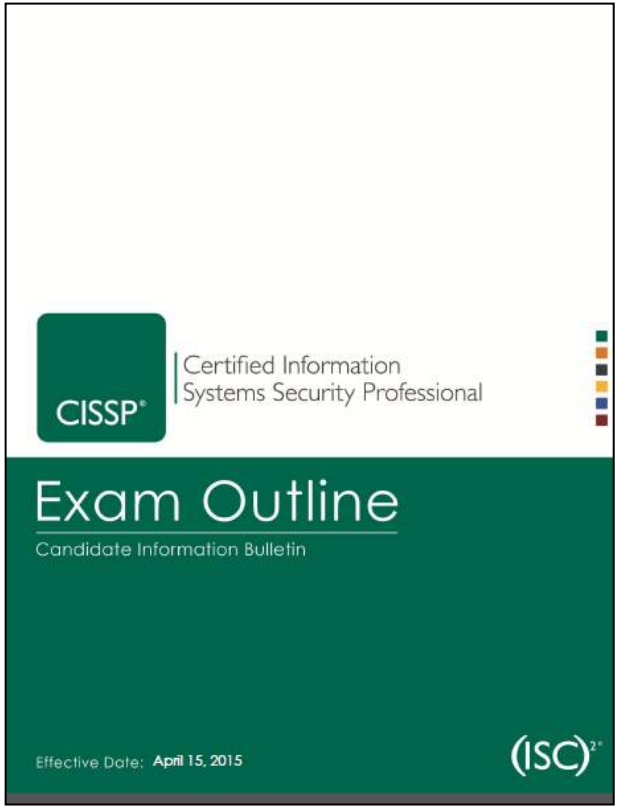
Segment 4: Domain 7 Security Operations (60 min)

Segment 5: Domain 8 Software Development Testing (45 min)

Segment 6: Preparing for Test Day! (10 min)

Definetely, ask questions and continue the group chat!

Candidate Information Bulletin



This is a crash course and not a comprehensive course. We will touch on each of the objectives.

- My Complete CISSP 24hr. Video Course
. dives deep into every topic.
- My CISSP Exam Prep 7 hr. Video Course dives extra deep into challenging and/or unfamiliar topics.

Note: Revised exam scheduled to be released in April 2018. Current content is applicable.

New Test Format

Effective Dec. 18, 2017 $(ISC)^2$ will introduce Computerized Adaptive Testing (CAT)

- This more precise evaluation reduces the maximum exam administration time from 6 hours to 3 hours, and it reduces the items necessary to accurately assess a candidate's ability from 250 items on a linear, fixed-form exam to as little as 100 items (to a maximum of 150) on the CISSP CAT exam.
- You cannot review a question.
- 25 unscored questions will be included.
- The exam content outline and passing standard for both versions of the examination are exactly the same. Each candidate will be assessed on the same content and must demonstrate the same level of competency regardless of the exam format.

https://www.isc2.org/Certifications/CISSP/CISSP-CAT

DAY 2 - Segment #1

Domain 4:

Communication and Network Security

Domain 4 Security Engineering

A. Apply secure design principles to network architecture	**D. Design and establish secure communication channels**
B. Secure network components	**D. Prevent or mitigate network attacks**

A

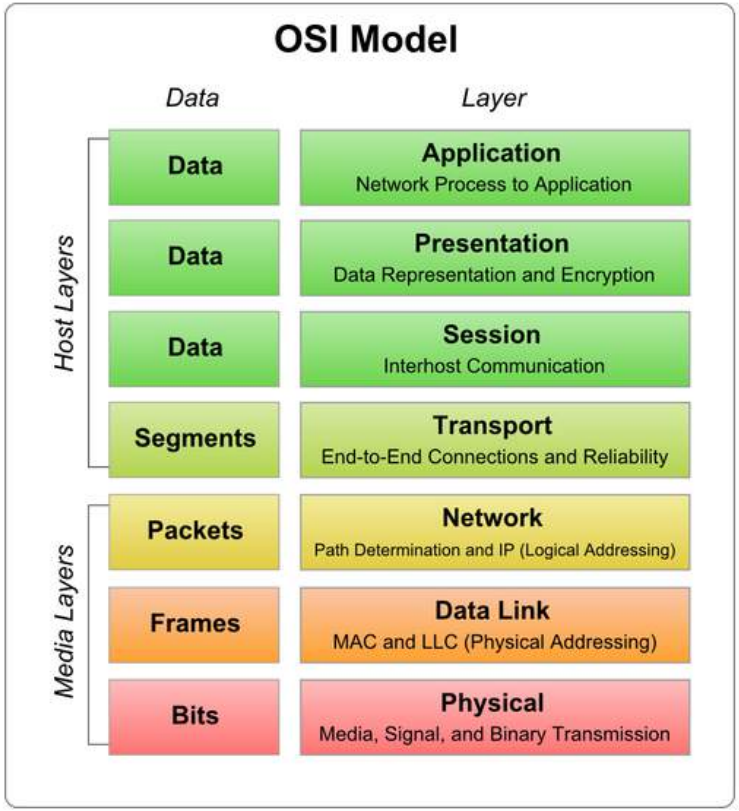
Network Models

Network models describe layers of communication. From a security perspective, it is important to understand what happens at each layer, the dependencies, and the weaknesses:

- The *Open Systems Interconnection (OSI)* reference model is structured into seven layers:
  - The OSI model was defined in 1984 and published as ISO/IEC 7498-1.
- The *TCP/IP* (also known as the Department of Defense – DoD) reference model is structured into four layers.

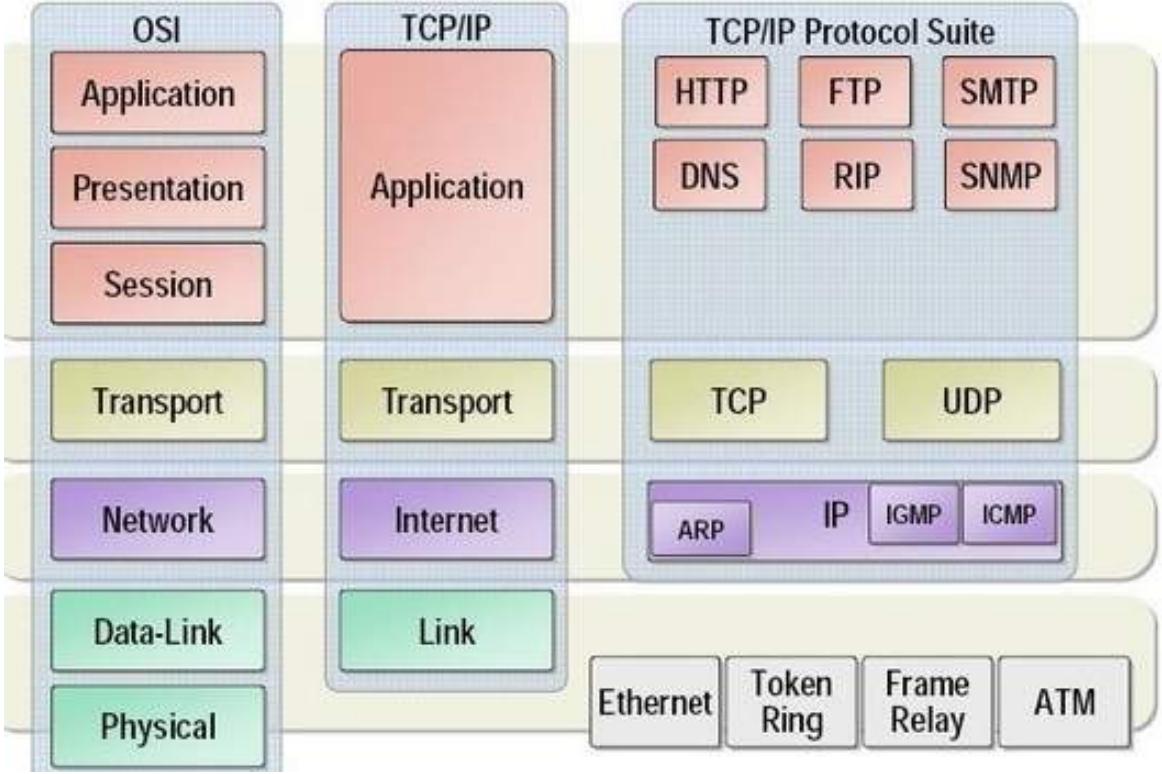
A

OSI Model



A

OSI | TCP/IP Relationship



Pearson

A

IP Convergence

IP Convergence is the use of the Internet Protocol (IP) as the standard transport for transmitting all information (voice, data, music, video, TV, teleconferencing, and so on).

- Introduces standardization
- Reduces the number of service providers
  - Introduces single point of failure (SPOF)
  - Introduces consolidated attack vectors

Extensibility is additional functionality or the modification of existing functionality without significantly altering the original structure or data flow.

Open standard is a standard that is publicly available and can be freely adopted and extended.

A

Non-IP Networking Protocols

Multiprotocol Label Switching (MPLS) is a scalable, protocol-independent network transport architecture.

- MPLS operates in-between Layers 2 and 3.

Distributed Network Protocol (DNP3) is a Layer 2 open standards-based communications protocol used between components in process automation systems (e.g. electric, water).

- DNP3 ensures the reliability of communications within the harsh environments of utilities (error checking).

Fibre Channel over Ethernet (FCoE) is a Layer 2 standards-based protocol that allows Fibre Channel frames to be carried over Ethernet links (not routable at the IP layer).

- FCoE, network (IP), and storage (iSCSI) data traffic can be consolidated using a single network.

A

Wireless Network Configurations

Type	Description	IEEE Standard
WPAN	Wireless Personal Area Network A.K.A. Bluetooth	802.15 standard Interconnects devices within a limited range (e.g. keyboards)
WLAN	Wireless Local Area Network	802.11 standard
WMAN	Wireless Metropolitan Area Network	802.16 standard
WWAN	Wireless Wide Area Network	Point-to-point microwave links

A

802.11 Security

Control	WEP	WPA	WPA2
Authentication	Preshared Key (PSK) or open	Enterprise RADIUS, Certificate or Personal PSK	Enterprise RADIUS, Certificate or Personal PSK
Key	64- or 128-bit key All users and services use the same key	Separate keys (TKIP) 256-bit key	Separate keys 256-bit key and block size
Encryption	RC4 Stream Cipher	RC4 Stream Cipher	AES Block Cipher
Integrity	32-bit CRC Hash	64-bit MIC	CCMP
Status	Insecure	Temporary fix. Superseded by WPA2	Current standard Vulnerable if using Wi-Fi Protected Setup (WPS)

A

Secure Communications Protocols

Acronym	Name
SSL/TLS	Secure Socket Layer/Transport Layer Security
HTTPS	Hyper Text Transfer Protocol Secure
FTPS	File Transfer Protocol Secure (FTP Secure)
SSH	Secure Shell
SRTP	Secure Real-time Transport Protocol
SNMP	Secure Network Management Protocol
S/MIME	Secure/Multipurpose Internet Mail Extensions
Secure POP3	Secure Post Office Protocol 3 (SSL-POP, POP3S)
Secure IMAP	Secure Internet Message Access Protocol (IMAP4-SSL)

B

Networking Devices

Layer #	Layer	Device
Layer 1	Physical	Hubs and Repeaters
Layer 2	Data Link	Bridges and Wireless Access Points Switches
Layer 3	Network	Multilayer Switches Router
Layer 4	Transport	Load Balancer

B

Internet Facing Devices

Device	Primary Function
IDS / IPS (Network)	Monitors and reports on intrusions (IDS) and can take action (IPS)
Firewalls	Controls ingress and egress traffic
Filters	Filters access (e.g. SPAM, Content, DLP, URL)
Proxy	Acts on behalf of a client (e.g. forward, transparent)
VPN concentrator	End point for a network/site VPN connection
SSL accelerators	Offloads processor intensive SSL/TLS encryption and decryption
Load balancers	Distribution of workload across multiple resources (server farm)

- It is critical to harden all Internet facing devices and to keep the firmware/OS/application up to date.

B

Endpoint Devices / Software

Device	Primary Function
NAC	Governs connections to the network based on configuration requirements (e.g. patch level, AV)
Firewall	Protective boundary for the local device that monitors and restricts ingress and egress access
HIDS/HIPS	Monitors and analyzes local behavior as well as network activity and can (if IPS functionality is available) be configured to take a corresponding action.
AV/Anti-Malware	Identifies, contains, and in some cases eliminate known malicious code.
Browser /Email Sandbox	A sandbox is an isolated environment running in a restricted memory/ processing area.

B

Decision States

State	Description
True Positive	Normal activity is correctly identified
False Positive	Normal activity is incorrectly identified as abnormal
True Negative	Abnormal activity is correctly identified
False Negative	Abnormal activity is incorrectly identifies as normal

- Positive state always refers to normal activity.
- Negative state always refers to abnormal activity.

C

VoIP

Voice over IP (VoIP) is the transmission of voice traffic over IP-based networks instead of using traditional analog circuits.

- VoIP is also the foundation for more advanced communications technologies such as web and video conferencing.
- IP Telephony refers to a full suite of VoIP enabled services previously provided by a PBX.
- Unified Communications is the unification all forms of communication independent of location, time or device.

C

Multimedia and Content

Multimedia collaboration has significantly impacted how we work, communicate, and entertain.

- Remote (sometimes referred to as virtual) meetings are designed to connect participants in real-time and support audio and video conferencing, file and desktop sharing, and remote control.
- Instant messaging and chat services were initially designed for real-time text communication but have expanded to include voice, video, screen sharing, file exchange, and remote control.
- A content distribution network (CDN) is a large distributed system of servers, Internet service providers, and network operations. The goal of a CDN is to serve content to end users with high availability and high performance.

C

Remote Access Applications

Application	Description
Telnet Terminal Emulation **Port 23**	Telnet facilitates the connection to a remote system and the execution of commands. • Telnet provides basic authentication (user name and password) • Telnet communication is clear text
Secure Shell (SSH) Terminal Emulation **Port 22**	SSH facilitates the connection to a remote system and the execution of commands. • SSH creates a secure encrypted tunnel to the remote system
Remote Desktop Software (RDP) **Port 3389**	Software or OS feature that allows a desktop environment to be run remotely
Virtual Private Network (VPN) **Port depends upon protocol**	VPN is a secure private connection between two end points – • Host-to-Host, Host-to-Network, or Network-to-Network

C

Virtual Private Network

A *virtual private network* (VPN) is designed to facilitate secure remote access communication over a public network.

- VPNs are a cost-effective alternative to dedicated point-to-point connections by transforming the Internet into a secure circuit.
- VPNs isolate the network frames from the surrounding networking using a process known as *encapsulation* or *tunneling.*
- *Full tunneling* requires all traffic to be routed over the VPN.
- *Split tunneling* allows the routing of some traffic over the VPN while letting other traffic directly access the Internet.

C

VPN Protocols

Protocol	Description
PPTP	Microsoft's implementation of secure communication over a VPN • Designed to secure Point-to-Point protocol (PPP) • No longer considered secure
L2TP	Cisco's implementation of secure communication over a VPN • Combines Layer 2 Forwarding and PPTP • Can be used on IP and non-IP networks
IPsec	Defacto standard for IP-based VPNs (host/host, host/network, network/network)
SSL	Uses SSL *or its successor TLS* for single or multiple connections using a browser • User connects to a SSL Gateway or endpoint • SSL VPN Portal is a single connection to multiple services

C

Virtualization

Server virtualization allocates the resources of the host to guest server (virtual) computers.

- The physical *host computer* hardware has processor, memory, storage, and networking components. Specialized software dynamically allocates resources. Guest computers (virtual machines) act exactly as though they are physical machines each with independent operating systems, applications, and network connections

Network virtualization (NSX) is the complete reproduction of a physical network in software.

- Network virtualization presents logical networking devices and services (e.g. logical ports, switches, routers, firewalls, load balancers, VPNs).

Virtual Desktop Infrastructure (VDI) is virtualization technology that hosts a desktop operating system on a centralized server in a data center.

D

Network Attack Categories

Category	Description
Spoofing	Impersonating an address, system, or person • Enables an attacker to act as the trusted source and redirect/manipulate actions (e.g. IP address, MAC, Web, Email)
Poisoning	Manipulating a trusted source of data (e.g. DNS) • Enables an attacker to act as the trusted source and redirect/manipulate actions (ARP cache, DNS cache)
Hijacking	Intercepting communication between two systems • Enables an attacker to eavesdrop, capture, manipulate, and/or reuse data packets (e.g. MiTM, MiTB, Replay, Domain, URL, Clickjacking)
Denial of Service (DoS)	Overwhelming system resources • Enables an attacker to make services unavailable for their intended use
Code	Exploiting weaknesses in server or client side code or applications • Enables an attacker to take control (XSS, CSFR, Injection, Buffer Overflow)

D

Zero-Day

A zero-day threat is the discovery of a previously unknown vulnerability for which there is no fix.

- A *zero-day attack* occurs in the time period between when a exploit is developed and when a patch has been released or a compensating control identified.

Domain 3 Security Engineering

A. Apply secure design principles to network architecture	**D. Design and establish secure communication channels**
B. Secure network components	**D. Prevent or mitigate network attacks**

Assessment Q1

SSH is can be used to provide a command shell on a remote device. SSH is a cryptographic replacement for _____.

A. HTTP
B. FTP
C. Telnet
D. LDAP

Assessment Q2

This type of VPN uses a client-side web browser and can be a gateway to multiple services.

A. PPTP VPN
B. L2PT VPN
C. IPsec VPN
D. SSL VPN

Assessment Q3

If you wanted to gain a better understanding of potential web server attacks, where would you locate a honeypot?

A. Enclave network
B. Extranet
C. Internet facing segment
D. Internal network

Assessment Q4

An attack that impersonates a MAC address, domain name or email sender is known as a _____ attack.

A. APT
B. Spoofing
C. MiTM
D. Poisoning

Assessment Q5

Which protocol does not operates at the OSI network |TCP/IP internet layer?

A. ICMP
B. ARP
C. SNMP
D. IGMP

DAY 2 Segment #2

Domain 5:

Identity and Access Management

Domain 5 Identity & Access Management

A. Control physical and logical access to assets	E. Implement and manage authorization mechanisms
B. Manage identification and authentication of people and devices	F. Prevent or mitigate access control attacks
C. Integrate identity as a service	G. Manage the identity and access provisioning lifecycle
D. Integrate third-party identity services	

A

Access Control Attributes

An identification schema, authentication method, authorization model and accounting process are common attributes of all access control systems.

- An *identification schema* is used to identify unique records in a set.
- An *authentication method* is how identification is proven to be genuine.
- An *authorization model* defines how access rights and permissions are granted.
- *Accounting processes* are used to track subject actions.

A

Access Control Concepts

Term	Definition
Rights	Ability of a subject to take an action (e.g. install software)
Permissions	Functions that a subject can perform on a object, file, or folder (e.g. read)
Privilege	Overriding capabilities; trumps rights and permissions (e.g. Root)
Need to know	Demonstrated reason for requiring access
Least privilege	Assigning the minimal rights and permissions needed to accomplish a task
Default deny	Any access or action not explicitly allowed — is forbidden
Default allow	Any access or action not explicitly denied — is allowed
Time/Location Restrictions	Restrictions that are based upon time of day or physical/logical location
Dual control	Requiring more than one subject or key to complete a task
Separation of duties	Breaking a task into segments so that no one subject is in complete control

B

Identity Management Systems

Identity management (IdM) describes the management of user identities (including authentication and authorization) within and/or across enterprise boundaries.

Technologies include:

- Directory services (LDAP, AD)
  - Scalable (billion + user entries), distributable and synchronizable
- Single sign-on (SSO)
  - SSO system intercepts requests for identification and authentication.
- Federated identity management (FIM)
  - Partners establish a mutual trust
  - Identity is portable

B

Federated Identity Management

Federated identity management (FIM) is an arrangement made among multiple enterprises that allows users (and sometimes objects) to use the same identification data to obtain access to disparate resources.

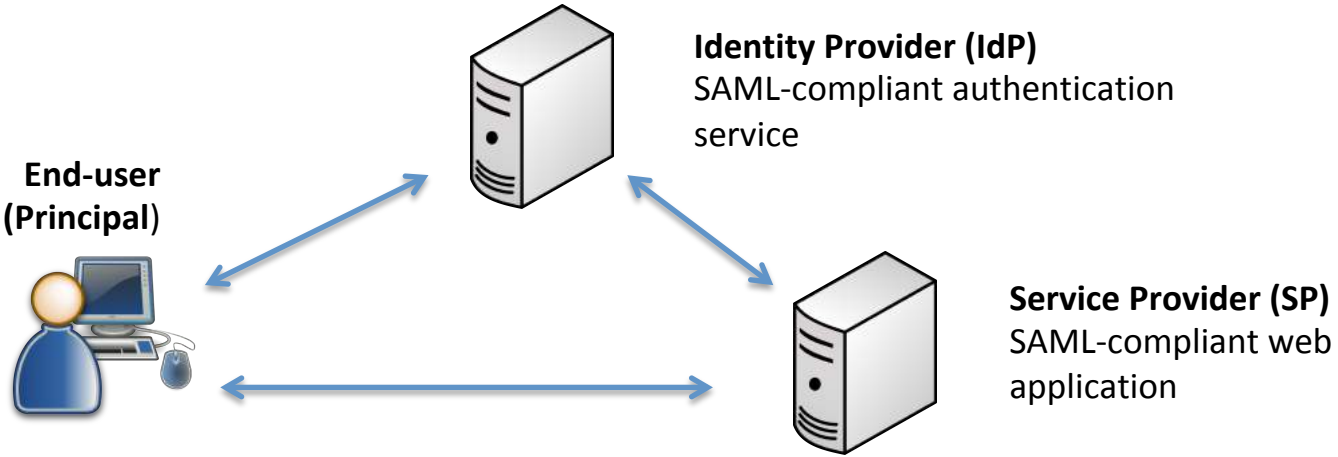
- Technologies used for federated identity include Security Assertion Markup Language (SAML), OAuth, OpenID Connect, and Shibboleth.

B

SAML

Security Assertion Markup Language (SAML) is an open standard that provides user authentication and authorization services.

- One-to-many model.



B

Authentication Controls

Factor	Description	Example
Knowledge	Something a user knows	Password/Passphrase/PIN
Possession	Something a user has	Token, Smartcard
Biometric	Something a user is Something a user does	Physiological Behavioral
Location	Somewhere a user is	GeoIP, Lat/Long

B

Authentication Factor Requirements

Factor	Description
Single-factor	Only one factor is required for authentication
Multi-layer	Two or more of the same type of factor is required for authentication
Multi-factor	Two or more different types of factors are required for authentication
Out-of-Band	Use of more than one communication channels to required for authentication

B

Authentication Decisioning

Decisions regarding the authentication control and number of factors should always be commensurate with the business value of what is being protected, regulatory requirements, and contractual obligations.

- Authentication controls should be subject to periodic risk assessments.

C

Identity as a Service

Identity as a Service (IDaaS) is an authentication infrastructure that is built, hosted and managed by a third-party service provider.

E

Authorization & Access Control

Authorization is the process of granting users and systems (subjects) access to resources (objects).

An *Access Control Model* is a framework that dictates how subjects access objects or how objects access objects.

- Access control models are built-in to operating systems and some applications.

E

Subject-based Access

Technique	Description	Enforcement
Mandatory Access Control (MAC)	Access is based on the relationship between subject clearance and need to know and the object classification level	Security Labels
Discretionary Access Control (DAC)	Data owners decide subject access	Access Control Lists Capabilities Tables
Role-Based Access Control (RBAC) **[Non-discretionary]**	Access is based on the subject's assigned roles Many-many relationships allowed	Access Control Lists Capabilities Tables Security Policy

E

Object-based Access Controls

Technique	Description	Enforcement
Rule-based	Access based on situational if-then statements	Rules
Content Dependent	Filter based on the data being acted upon	Keywords, Categories
Context Dependent	Access based on a collection or sequence of actions	Rules, Security Policy
Constrained Interface • **Menus and shells** • **Database views**	Access restricted by functionality	Design, Configuration

E

ABAC (emerging)

*Attribute-based access control (ABA**C**)* is a logical access control model that controls access to objects by evaluating rules against the attributes of entities (both subject and object), operations, and the environment relevant to a request.

- ABAC supports a complex Boolean rule set that can evaluate many different attributes.
- The policies that can be implemented in an ABAC model are limited only to the degree imposed by the computational language and the richness of the available attributes.
- An example of an access control framework that is consistent with ABAC is the Extensible Access Control Markup Language (XACML).

F

Authentication Attacks

Broken Authentication attacks use leaks or flaws in the authentication or session management functions (e.g., exposed accounts, passwords, session IDs) to impersonate users and gain system access.

Pass-the-Hash is a technique in which an attacker captures hashed account credentials on one computer and reuses the credentials to authenticate to another computer.

F

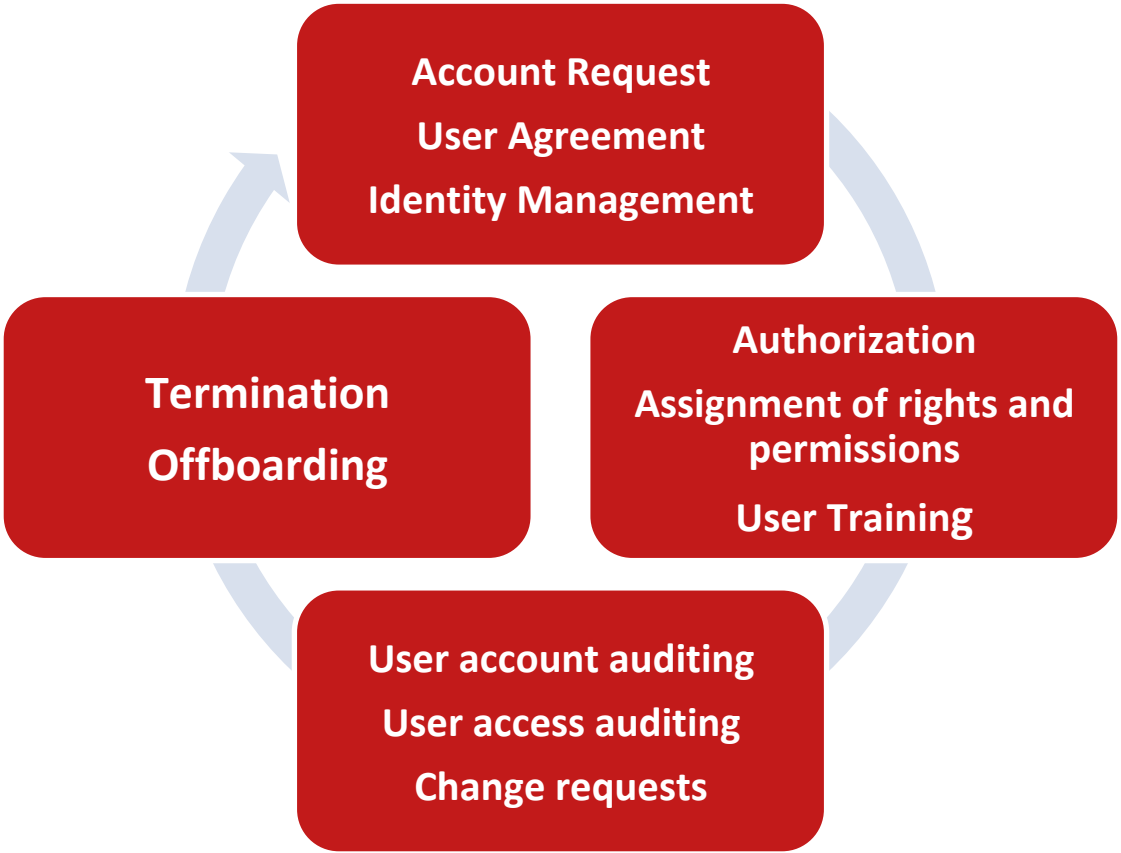
Access Control Attacks

Privileged Escalation attacks are designed to gain elevated access to resources that are normally protected from an application or user (generally by exploiting a vulnerability or weak authentication).

An *Advanced Persistent Threat (APT)* is a sophisticated attack in which intruder establishes a presence on a network to mine private data.

G

Provisioning Lifecycle



Pearson

Domain 5 Identity & Access Management

A. Control physical and logical access to assets	E. Implement and manage authorization mechanisms
B. Manage identification and authentication of people and devices	F. Prevent or mitigate access control attacks
C. Integrate identity as a service	G. Manage the identity and access provisioning lifecycle
D. Integrate third-party identity services	

Assessment Q1

Authentication factors include all but which one of the following?

A. Location
B. Possession
C. Knowledge
D. Rule

Assessment Q2

Assigning the minimal rights and permissions needed to accomplish a task is known as?

A. Need to know
B. Least privilege
C. Default deny
D. Dual control

Assessment Q3

Technologies used for _____ include SAML, OAuth, OpenID, and Simple Security Tokens.

A. LDAP
B. Single Sign-on
C. Federated Identity Management
D. IDaaS

Assessment Q4

This access control model compares the subject's clearance and need to know with the object's security label.

A. DAC
B. MAC
C. RBAC
D. Constrained

Assessment Q5

This type of attack exploits session IDs to impersonate users.

A. Broken authentication
B. Pass-the-hash
C. Advanced persistent threat
D. Privilege escalation

Day 2 - Segment #3

Domain 6:

Security Assessment and Testing

Domain 6 Security Assessment & Testing

A. Design and validate assessment and test strategies	**D. Analyze and report test outputs**
B. Conduct security control testing	**E. Conduct or facilitate internal and third party audits**
C. Collect security process data	

A

Information Security Assessment

An *information security assessment* is the process of determining how effectively the entity being evaluated meets specific security criteria (assurance).

- The objective of an assessment is to substantiate strengths and to identify weaknesses and failures.
- The target of the assessment is known as the *assessment object.*
- The security assessment process is often referred to as *T&E* (testing and examination).

A

Assessment Methodologies

There are two assessment methodologies.

- *Examination* is the process of reviewing, inspecting, studying, and observing to facilitate understanding, comparing to standards or baselines, or to obtain evidence. Examination is a passive activity.
- *Testing* is the process of exercising objects under specified conditions to compare actual and expected behaviors. Testing is a active activity.

A

Examination & Testing Comparison

Methodology	Strengths	Weaknesses
Examination	• May gain insight not otherwise available • Broad scope of coverage with limited resources	• May not provide assurance that the security controls are working as intended
Testing	• Can provide a real-world picture of an organization's security posture • Can evolve over time and mimic current attacker techniques	• May not provide a comprehensive evaluation due to limitations of time, resources, or tester • May be intrusive

A

Rules of Engagement

A rules of engagement (ROE) document details the parameters and expected assessor conduct of the assessment (exam/test). ROE components include:

- Scope, assumptions, limitations, and risks
- Logistics such as personnel, test schedule, test site, and equipment
- Communications plan
- Target system
- Testing expectations and data handling requirements
- Reporting

A

Legal Considerations

Legal considerations include authorization, liability, indemnification, nondisclosure, and privacy.

- Authorization is often required from third parties that host assessment objects; not doing so is a violation of a contract.
- Contracts with external assessors may include SLAs, limitation of liability, and indemnification clauses that should be reviewed by legal counsel.
- Potential privacy violations should be identified.
- Nondisclosure contracts or agreements should protect disclosure of data collection and findings.

B

Security Control Assessment

Vulnerability Assessment	Identify host attributes, known CVE's, outdated software versions, missing patches, misconfigurations and security policy, or standards deviations.
System Configuration	Identify weakness in security configurations, baseline variations, and nonconformance with industry standards and recommendations.
Log Reviews	Ensure adherence to log monitoring and management policies, standards, and procedures.
Penetration Testing	Evaluate the security of a target by identifying and attempting to exploit vulnerabilities, improper configurations, and hidden points of entry.

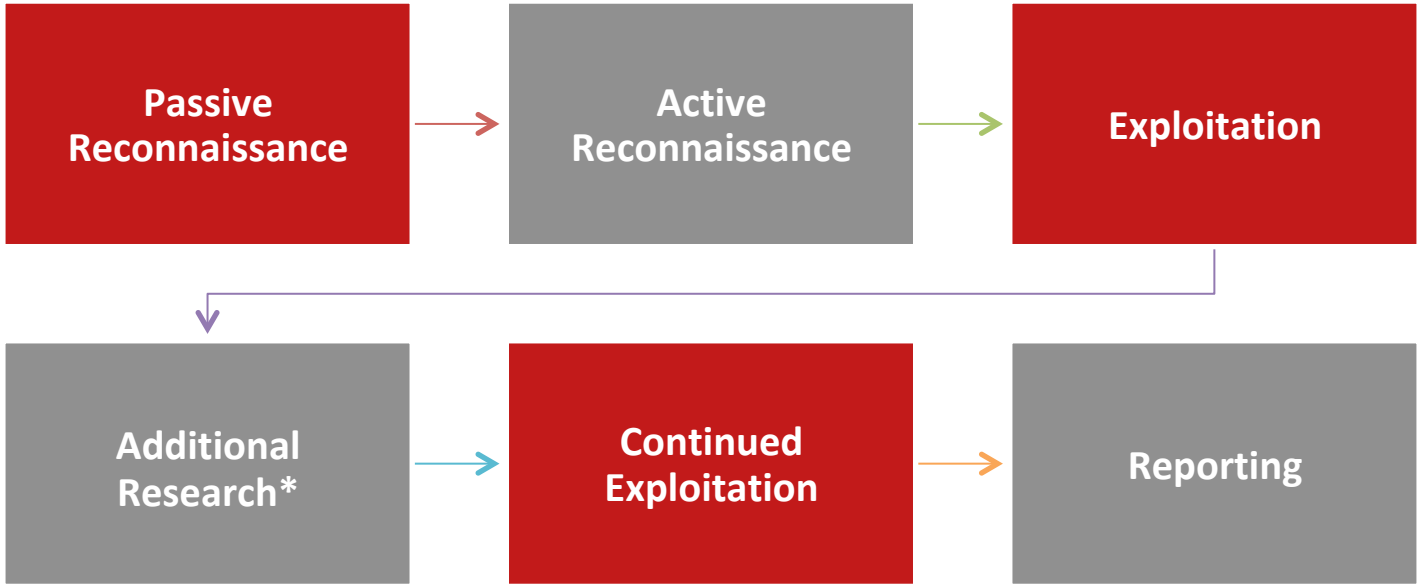
B

Penetration Testing Approach

Position	Description
Black Box (Blind)	Penetration testing team is not provided any details of the target environment .
Double Blind	Penetration testing team is not provided any details of the target environment Target personnel have no knowledge of the test.
Gray Box	Penetration testing team is provided limited information about the target environment.
White Box (Targeted)	Both the penetration testing team and internal personnel are knowledgeable and work in concert .
Red Team	External entities that emulate the behaviors and techniques of likely attackers.
Blue Team	Internal security team (defenders).

B

Penetration Test Phases



* Research and exploitation are iterative processes.

B

Code Security Assessment

Synthetic Transactions	Measurement of availability and response times using recorded actions that emulate a specific interaction.
Security Code Review	Examination of source code to verify that the proper security controls are present and work as intended.
Static Code Analysis	Examination of non-running code (static) for vulnerabilities.
Dynamic Analysis	Examination of running code for vulnerabilties (automated).
Fuzzing	Automated testing technique used to discover coding errors and security loopholes by inputting invalid, unexpected, or semi-random data, called *fuzz*, and monitoring the application response.
Use Case	Positive testing determines if the application works as expected [use case] Negative testing ensures that the application can gracefully (and securely) handle invalid input or unexpected behavior [misuse case].

C

ISCM Defined

Information security continuous monitoring (ISCM) is defined by NIST* as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

The objective of ISCM is to continually measure and report on the effectiveness of organizational security controls.

- Requires processes to collect, analyze, and report on security metrics and supporting data (e.g. account management, risk assessments, DR/BCP, training, backup and replication, host, enterprise and border security controls).
- Agreed upon Key Performance Indicators (KPI's)

*Special Publication 800-137 Information Security Continuous Monitoring for Federal Information Systems and Organizations

C

Host Security Controls

Tool	Purpose	Output
HIDS/HIPS	Host intrusion detection and prevention	Local suspicious activity Response taken (if HIPS)
Antivirus	Block malicious code Scan for signatures	Malicious files identified Blocked, quarantined, deleted files
File Integrity Monitoring	Identify changes in files or file structure by comparing a known good checksum with a current checksum	File changes including time, date and file size
Firewall	Control ingress and egress traffic	Allowed and denied traffic (including attacks)
Data Execution Prevention (DEP)	Monitors program memory use	Denied/blocked executables

C

Enterprise Security Controls

Tools	Purpose	Output
Application whitelisting	Explicitly specify allowed application	Application access (allowed and denied)
RMC Removable Media Control	Control access to and use of removable media (USB, CD/DVD)	Media access (allowed and denied)
Advanced Malware Tools	Identify malicious code that could evade or subvert anti-virus software	Suspicious or malicious files Suspicious or malicious endpoint activity Suspicious or malicious traffic
Patch Management Tools	Inventory patches Identify missing patches Manage deployment	Patch inventory Missing patches Patch deployment schedule Patching errors

C

Border Security Controls

Tools	Purpose	Output
UTM Unified Threat Management	Multiple (network firewalling, network intrusion detection/ prevention (IDS/IPS), gateway antivirus (AV), etc.)	Depends upon what the device is being used for.
DLP Data Loss Prevention	Prevent malicious and accidental date exfiltration	Allowed and denied activity Quarantined activity (queued)
WAP Web Application Firewall	Filters, monitors, inspects and blocks HTTP traffic to and from a web application	Suspicious traffic and requests including SQL injection and XSS.
Log Analysis	Generate a detailed time-stamped computer generated record of events	Report on operational and security information including predictors and indicators of compromise

E

Audit process

An audit examination provides independent assurance based on evidence (examination) and testing.

- Auditing standards require that sufficient, relevant, and reliable evidence is obtained to support audit conclusions and opinion.
- Audits should be conducted by qualified audit professionals.
- The audit plan is a high level description of audit work to be performed in a specific time frame. The plan may include objectives, scope, resource requirements, intended evidence collection techniques, target audience, and reporting expectations.

E

Audit Standards and Frameworks

Widely used information security audit control standards and frameworks for internal and operational auditing include:

- ISACA COBIT 4.1 IT Controls and Assurance Objectives
  - Deliver and Support Domain
  - DS5 Ensure Systems Security (DS5.1 –DS5.11)
- AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE18)
  - Formally known as a SSAE 16 and before that SAS 70

Assessment Q1

What is the primary difference between an examination and a test?

A. Examinations are passive; tests are active.
B. Examinations are annual; tests are on-going
C. Examinations are facilitated by internal personnel; tests are conducted by independent personnel.
D. Examinations are intrusive; testing has minimal operational impact.

Assessment Q2

In a planned exercise scenario, the _____ attacks and the _____ team defends.

A. outsiders, insiders
B. bad guys, good guys
C. white hats, black hats
D. red team, blue team

Assessment Q3

The ISCM process was designed to support the _____ risk management framework used by _____.

A. NIST, federal agencies
B. COBIT, the private sector
C. ISO 27005, international organizations
D. OCTAVE, small businesses

Assessment Q4

File integrity monitoring works by comparing _____.

A. a known good checksum with a current checksum
B. file properties include date of last access
C. the last two message digests
D. registry modifications

Assessment Q5

The objective of using synthetic transactions is to _____.

A. measure bandwidth utilization
B. measure number of transaction
C. measure accuracy
D. measure availability and response time

DAY 2 Segment #4

Domain 7:

Security Operations

Domain 7 Security Operations

A. Understand and support investigations	H. Operate and maintain preventative measures
B. Understand requirements for investigation types	I. Implement and support patch and vulnerability management
C. Conduct logging and monitoring activity	J. Participate in and understand change management practices
D. Secure the provisioning of resources	K. Implement recovery strategies
E. Understand and apply foundational security concepts	L. Implement disaster recovery processes M. Test disaster recovery plans N. Participate in business continuity planning and exercises
F. Employ resource protection techniques	O. Implement and manage physical security
G. Conduct incident management	P. Participate in addressing personnel safety concerns

A

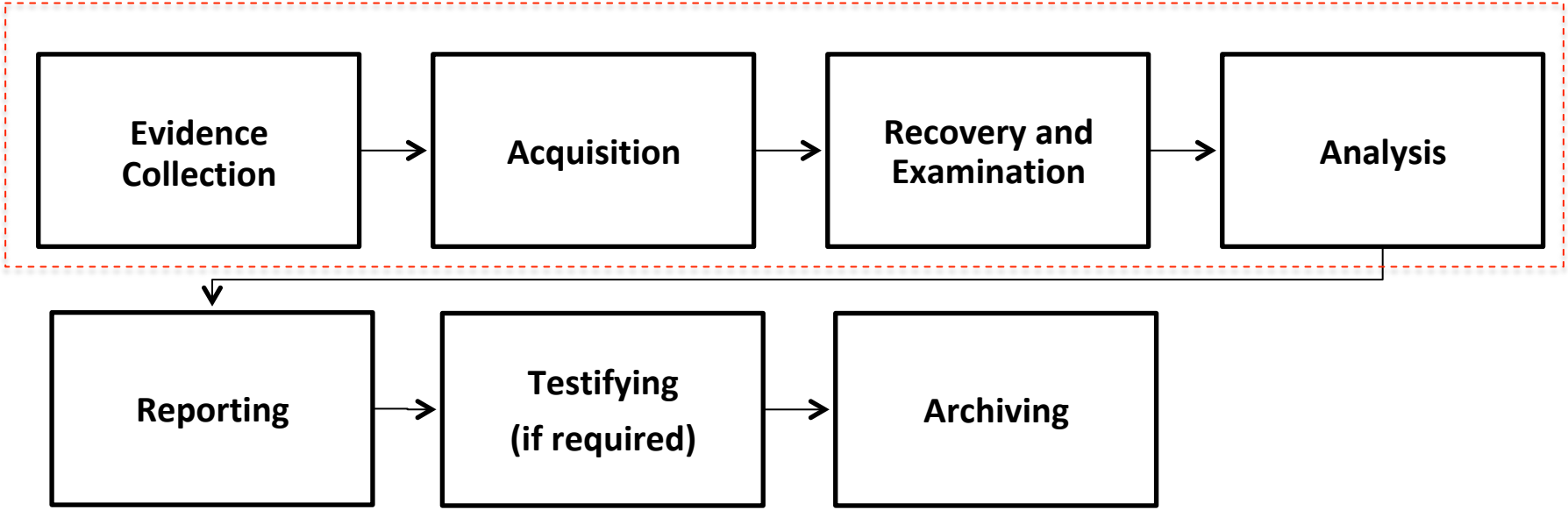
Forensics

Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence.

- *Digital forensics* is the application of science to the identification, collection, examination, and analysis of data (evidence) while preserving the integrity of the information.

A

Digital Forensics Process



A

Evidence Collection and Preservation

Collection and preservation of physical and digital evidence is a critical aspect of forensic investigations. Rule of thumb—assume evidence will be used in a court of law and act accordingly.

- Preservation is key
- Act in order of volatility
- Maintain an evidentiary chain (*chain of custody*) for all physical and electronic evidence collected during the investigation

A

Chain of Custody

A chain of custody establishes the proof that the items of evidence collected at the crime scene is the same evidence that is being presented in a court of law.

- Identifying information (e.g., the location, serial number, model number, hostname, media access control (MAC) addresses, and IP addresses of a computer).
- Name, title, and phone number of each individual who collected or handled the evidence during the investigation.
- Time and date (including time zone) of each occurrence of evidence handling.
- Locations where the evidence was stored.

B

Type of Investigations

	Criminal	Civil	Internal
Basis	Law must be broken	Contact violation or dispute	Incident
Intent	Intent required	Intentional or accidental	Intentional or accidental
Burden of Proof	Beyond a reasonable doubt	Preponderance of evidence	N/A
Litigation	Government	Individuals or companies	Administrative
Investigation	Assist law enforcement obtain evidence	Provide evidence of wrongdoing or damage	Prove/disprove event and/or impact

B

eDiscovery

eDiscovery (also called *electronic discovery*) refers to any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.

- *Federal Rules of Civil Procedure (FRCP*) and *Federal Rules of Evidence (FRE)* apply to the process of preparing and producing electronically stored information (.ESI), as well as for resolving related disputes.

C

Audit and Event Logs

Audit and event logs are a chronological record of events and actions.

- Critical log sources include firewalls, IDS/IPS devices, proxy servers, authentication servers and devices, operating systems, and key applications.
- Audit logs are both a near-time and historical detective control.
- Routine log analysis is beneficial for monitoring access, identifying security incidents, policy violations, fraudulent activity, and operational issues.
- Logs are critical components of internal investigations and forensic analysis. Logs should be stored on a WORM (write once/read many) device.

C

Log Analysis Tools

Type	Description
Trend/ Variance Detection	Identifies anomalies in system or user behavior
Attack Signature Detection	Identifies “known” event or sequence of events
Security Information and Event Management (SIEM)	Automation tool • SIEM products can analyze data from many sources, identify significant events, report outcomes, and send alerts • SIEM products may integrate with threat intelligence feeds • SIEM products may also include security knowledge bases, incident tracking, and reporting capabilities

C

DLP

Data loss prevention (DLP) tools are designed to detect and prevent data exfiltration (unauthorized release or removal of data).

- DLP technologies locate and catalogue sensitive data (based on a predetermined set of rules or criteria).
- DLP tools monitor target data while in use, in motion, and at rest.

C

DLP Location

Location	Description
Network-based (On premise)	Network-based (hardware or virtual appliance) deals with data in motion and is usually located on the network perimeter.
Storage-based	Storage-based (software) operates on long-term storage (archive)
End-point based	End-point based (software) operates on a local device and focuses on data-in-use.
Cloud-based (off premise)	Cloud-based operates in “the cloud” data in use, motion, and at rest

D

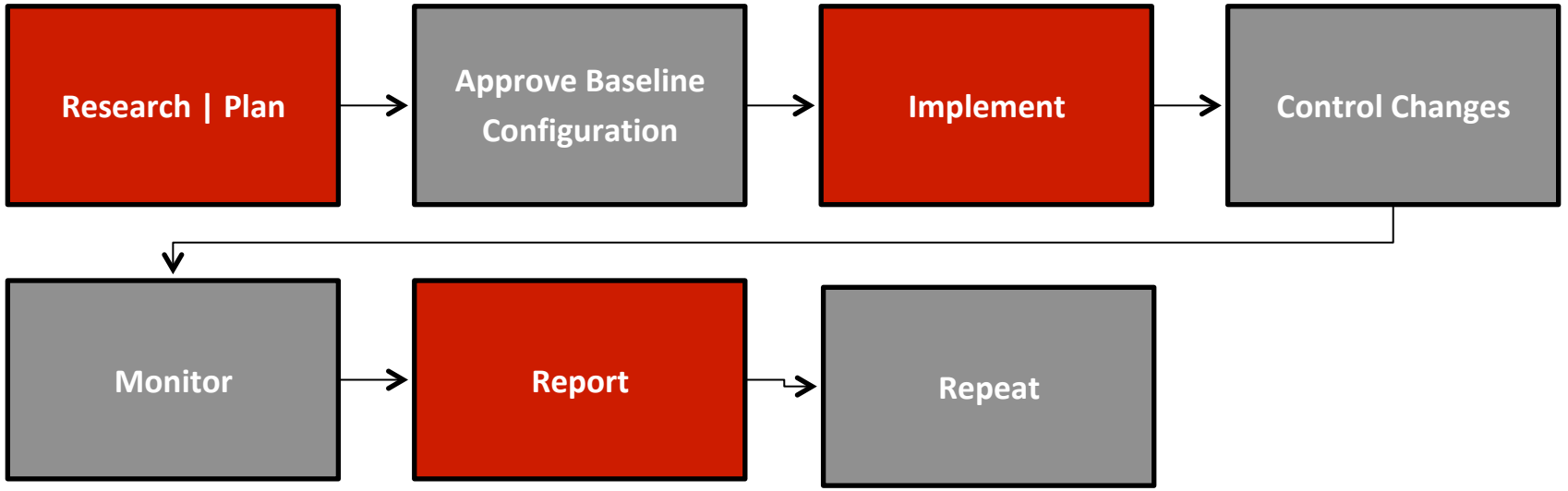
Configuration Management

Configuration Management is a set of practices designed to ensure that systems are deployed in a consistent state and stay that way through their lifetime.

- A baseline configuration (BC) is a set of specifications for a configuration item (CI), that has been reviewed and agreed on and which can be changed only through change control procedures.

D

Configuration Management Process



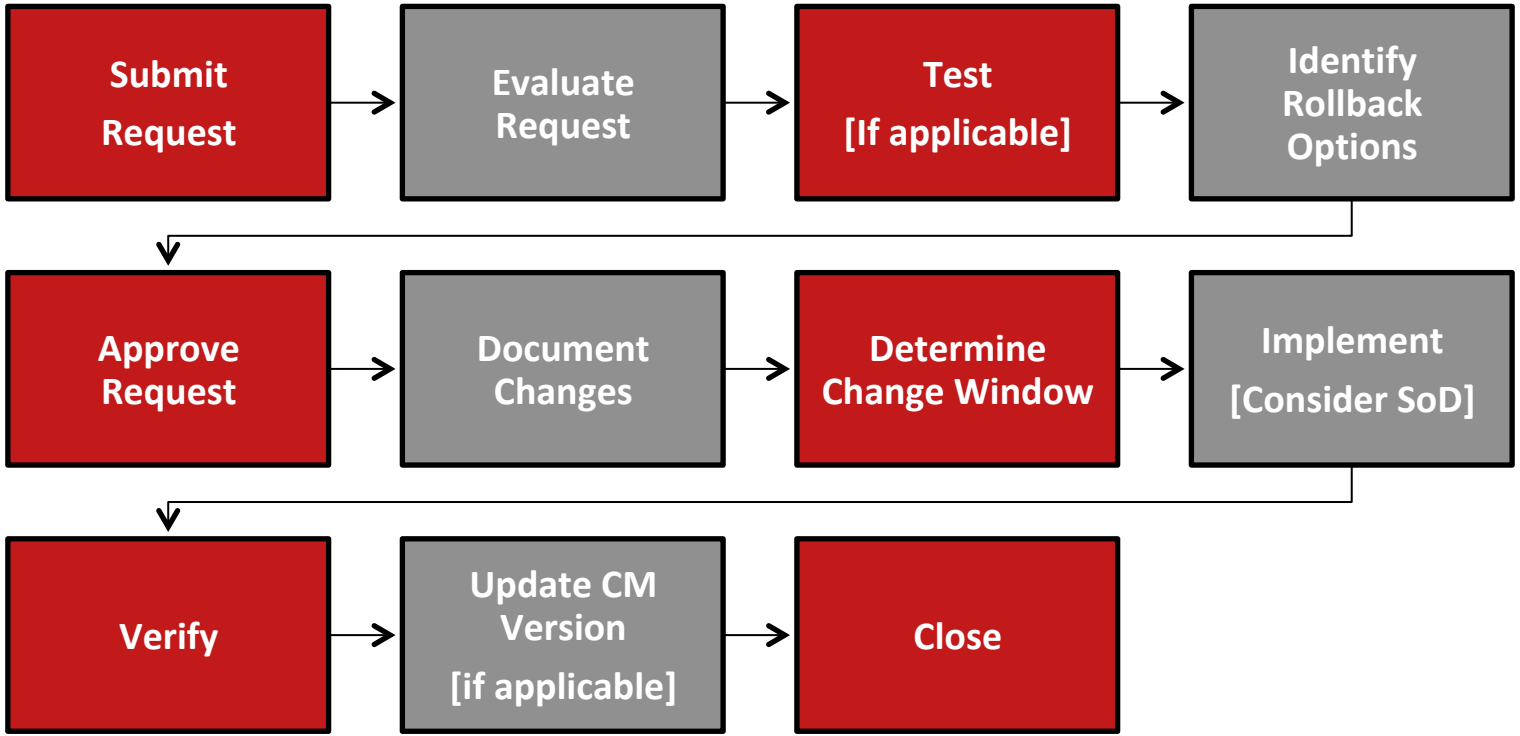
D

Change Management

Change management practices are designed to ensure that all changes are evaluated, documented, tracked, and controlled.

D

Change Management Process



G

Security Incident

An *security incident is* an event or action that endangers the confidentiality, integrity, or availability of information or information systems.

- A *data breach* is when data is exfiltrated or extracted or there is a loss of control. A data breach may trigger reporting and notification requirements.

G

Incident Response Phases

Phase	Objective(s)
Preparation	Establish response capability Prevent incidents from occurring
Detection	Identify and analyze predictors of compromise (POC) and indicators of compromise (IOC) • Examples include IDS, SEIMS, AV, File integrity checking, logs, network flows, threat intelligence, people
Containment	Minimize the damage • Examples include shutting down a system, disconnecting it from a network, disabling certain functions
Eradication	Eliminate components of the incident • Examples include deleting malware, disabling breached accounts, mitigating associated vulnerabilties
Recovery	Restore systems to normal operations

G

Disclosure

A incident that is classified as a confirmed or high-probably breach (due to absence on forensic evidence) or compromise may trigger disclosure and notification protocols and requirements.

- Legal counsel should also be consulted.
- Notification is complex, conflicting and cumbersome.
  - Sector specific federal security legislation (e.g. GLBA and HIPAA) have risk assessment and breach notification requirements.
  - Forty-eight states, the District of Columbia, Guam, Puerto Rico, and the Virgin Islands have enacted data breach notification legislation related to disclosure of personally identifiable information.
  - PCI-DSS has breach notification requirements.
  - Contractual obligations may have breach notification requirements.

H

Preventative Measures

Device	Description
Firewall	Monitors and filters ingress and egress traffic
IDS/IPS	Monitoring, reporting and responding to (IPS) intrusion attempts
Whitelisting/Blacklisting	Explicit allow or deny application, protocol or service control
Network Access Control (NAC)	Governs connections to the network based on configuration requirements (e.g. patch level, AV)
Data Loss Prevention (DLP)	Inspects content with the objective of preventing data exfiltration (inadvertent or intended)
Sandbox	Isolated environment
Honeypots/Honeynets	Decoy systems used to examine attacker activity and techniques
Anti-Malware	Software used to detect and respond to malicious code

H

Hardening

Hardening a device or system is the process of configuring security settings, rules, and policies and removing unnecessary applications and services (*least functionality*) in order to minimize vulnerabilties and exposure to threats.

Vulnerability Management

Vulnerability management is the process of identifying, mitigating, and responding to known or anticipated vulnerabilities.

Threat intelligence is evidence-based information about threats, vulnerabilities, and exploits. The value of threat intelligence is in its application.

- Changing the security model from reactive to proactive–if you understand your adversaries you can develop tactics to combat current attacks and plan better for future threats.
- Driving better, more informed responses to security incidents.

Patch Management

Security patches are designed to correct security issues and functionality problems in software and firmware.

Patch management is the process of identifying, acquiring, installing, and verifying patches.

- Timely deployment of security patches reduces the likelihood of exploitation.
- Patch management delays should be evaluated in light of organizational risk tolerance and if applicable, brought to management's attention.

K

Recovery Strategies

A key component of recovery is the ability to restore systems and data. Restoration requires that accurate and reliable copies of data and system configurations are maintained and tested.

- Traditional backup strategies (full, incremental differential) use removable media (generally tape).
- Current/emerging strategies include automation and replication (local, off-site, cloud).

Cost vs. Complexity vs. Availability

Traditional Recovery

- Tape backup
- Low complexity
- Low cost
- Recovery measured in hours to days

Enhanced Recovery

- Automated Solutions
- Medium complexity
- Low cost
- Recovery measured in hours to days
- More recoverable data

Rapid Recovery

- Asynchronous Replication
- High complexity
- Moderate cost
- Recovery measured in hours

Continuous Availability

- Synchronous Replication
- High complexity
- High cost
- Recovery measured in seconds

K

Availability and Resiliency

Availability is a measure of a system's uptime — the percentage of time that a system is actually operational and providing its intended service.

- For example, “five nines” means the device should be up 99.999% of time and experience no more than 5.26 minutes of downtime per year.

Resiliency is the capability to continue operating even when there has been a attack, disruption, or abnormal operating conditions.

- Fault tolerance is the capability of a system to continue to operate in the event of failure of one or more system components.

Fault Tolerance

State	Description
Failover	Transition to a standby device
High availability	Automatic failover
Active / Passive Pair	The passive device does not come online unless the primary device fails
Active / Active Pair	Two or more components are operational and work as a team In case of a failure, remaining components continue to operate
RAID	Disk technology that combines multiple disk drive components into a logical unit for the purposes of data redundancy or performance improvement
Fail-secure	Principal that a failure will result in a secure or trustworthy state

K

Alternate Locations & Processing Sites

Cold Site	A *cold* site has basic HVAC infrastructure; no server-related or communications equipment.
Mobile site	A *mobile* site is a transportable modular unit. The delivery site must provide access roads, water, waste disposal, power, and connectivity.
Warm Site	A *warm* site has HVAC, servers, and communications infrastructure and equipment. Systems might need to be configured. Data needs to be restored.
Hot Site	A *hot* site has HVAC, servers, and communications infrastructure and equipment. Systems are preconfigured. Data is generally near-time.
Mirrored Site	A *mirrored* site is fully redundant with real-time replication from production site. Mirrored site can assume processing with virtually no interruption
Reciprocal site	A *reciprocal* site is based on a agreement to have access to/use of another organization's facilities

Alternate Business Process Strategies

Alternate business process strategies assume that normal dependencies (technology, facilities, personnel) may not be available. Options include, but are not limited to:

- manual processes
- using cross-trained personnel
- notification of delay
- outsourcing

DR/BCP Readiness

A disaster recovery /business continuity plan (DR/BCP) should be maintained in a state of readiness, which includes

- Personnel trained to fulfill their roles and responsibilities within the plan.
- Plans and strategies exercised to validate their content (including external relationships and communications).
- Systems and system components tested on a scheduled basis to ensure their recovery and operability.
- Plan examination and auditing to ensure compliance with business objectives.

M|N

Plan Exercise and Testing

Test	Description	Objective
Read-through [Desk check]	Personnel or departments review their plans and procedures for accuracy and completeness	Accuracy Familiarity
Walk-through [Tabletop]	Scenario-based group workshop focuses on the application of plans and procedures as well as participant readiness	Coordination Communication
Preparedness [Parallel] [Functional] [Simulation]	Localized scenario that simulates an actual event and limits material and equipment to what would be possible if the situation were an actual event	Evidence of localized readiness
Interruption [full-scale]	Tests all components of the designated plan simultaneously	Evidence of enterprise readiness

Physical Security

Physical security focuses primarily on preventive, deterrent, and detective access controls and workplace safety.

Physical security is based upon a layered defense model.

- *Obstacles* to frustrate trivial attackers and delay serious ones.
- *Detective controls* make it likely that attacks will be noticed.
- *Response mechanisms* to repel, catch, or frustrate attackers.

Building Security Controls

Control	Description
Lighting	Lighting for personnel safety and intruder deterrence • Intruders are less likely to enter well-lit areas • Lighting can be continuous, motion triggered, random, timed, or standby • Lighting should be damper proof and have a backup power supply
Signs	Signs for personnel safety and intruder deterrence • Warning signs indicate surveillance (“someone is paying attention”)
Physical Barrier	Fences, walls , gates, barricades, and bollards define the perimeter • They serve to prevent, deter, or delay (increase workfactor) an attack • Turnstiles and mantraps create barriers
Surveillance	Security personnel, CCTV and cameras, and IDS/IPS
Locks	Including conventional, pick resistant, cipher, digital and biometric

Emergency Safety Plans and Drills

Safety plans including evacuation routes and “safe locations” should be posted and personnel trained.

- Meeting places should be pre-assigned.
- Evacuation, shelter-in-place, and lock-down drills practiced.
- If circumstances allow, personnel should be instructed to secure confidential material and take access control devices with them.
- **No matter what else is happening — human life and safety is always the number one priority.**

Domain 7 Security Operations

A. Understand and support investigations	H. Operate and maintain preventative measures
B. Understand requirements for investigation types	I. Implement and support patch and vulnerability management
C. Conduct logging and monitoring activity	J. Participate in and understand change management practices
D. Secure the provisioning of resources	K. Implement recovery strategies
E. Understand and apply foundational security concepts	L. Implement disaster recovery processes M. Test disaster recovery plans N. Participate in business continuity planning and exercises
F. Employ resource protection techniques	O. Implement and manage physical security
G. Conduct incident management	P. Participate in addressing personnel safety concerns

Assessment Q1

The principle of “least functionality” is best described as?

A. Having a limited number of Administrative accounts.
B. Limiting account rights and permissions based on assignments.
C. Removing unnecessary applications and services.
D. Requiring appropriate clearance.

Assessment Q2

Which statement best describes URL whitelisting?

A. Deny by default; only pre-approved sites are allowed,
B. Allow by default; only known bad sites are blocked.
C. Allow by default; unless the site has a suspicious URL.
D. Deny by default; except if the site is approved by the IDS.

Assessment Q3

Data loss prevention (DLP) tools are designed to detect and prevent _____.

A. unauthorized access
B. privacy violations
C. data exfiltration
D. data modification

Assessment Q4

Which traditional removable media backup strategy backs-up the fastest and restores the slowest.

A. Full backup
B. Differential backup
C. Incremental backup
D. Archival backup

Assessment Q5

The IT department has proposed a plan to activate and test backup systems on a rotating basis (e.g. Messaging Platform in January, Firewall in February, etc.). This methodology is known as _____.

A. Interruption testing
B. Table-top testing
C. Full-scale testing
D. Parallel (functional) testing

DAY 2 Segment #5

Domain 7:

Software Development Security

Domain 8 Software Development Security

A. Understand and apply security in the software development lifecycle	**C. Assess the effectiveness of software security**
B. Enforce security controls in development environments	**D. Assess security impact of acquired software**

A

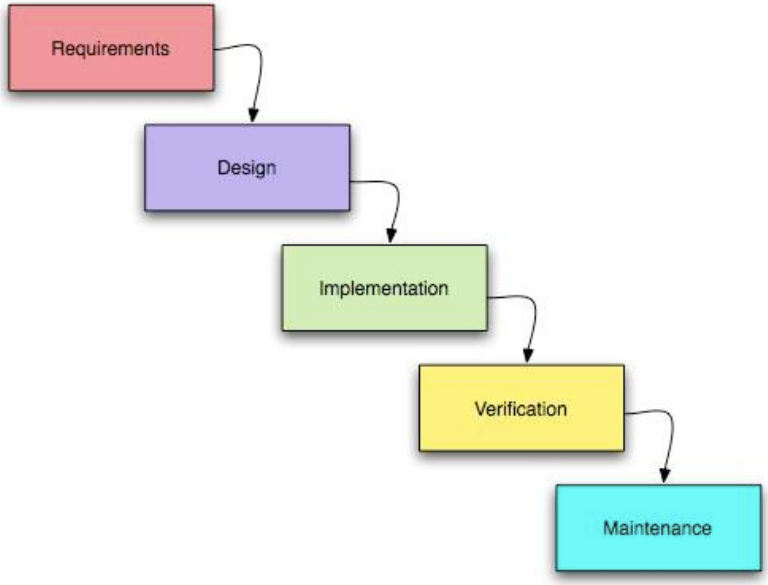
Traditional Software Development

The traditional software development model is known as SDLC (system development lifecycle). SDLC is a linear (sequential) model.

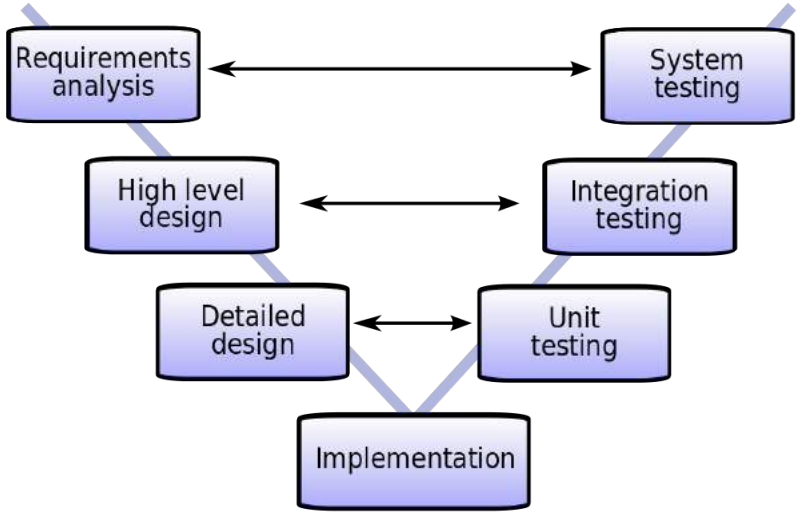
- The *Waterfall* model requires that each phase must be completed before moving on to the next phase.
- The *V-model* emphasizes verification and validation at each phase and testing to take place throughout the project.

A

Linear Models Visualization



Waterfall Model



V-Model

A

Evolutionary Models

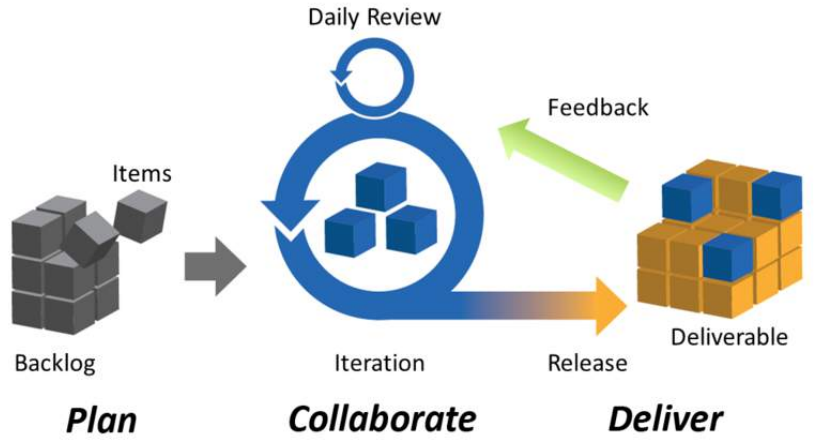
Iterative and incremental project models develop software by using repeated cycles (*iteration*) related to specific functionality (*incremental*).

- The *Agile* model uses iterative and incremental processes that emphasizes timebox team-based collaboration.
- *Rapid application development* (*RAD*) combines prototyping and iterative procedures.

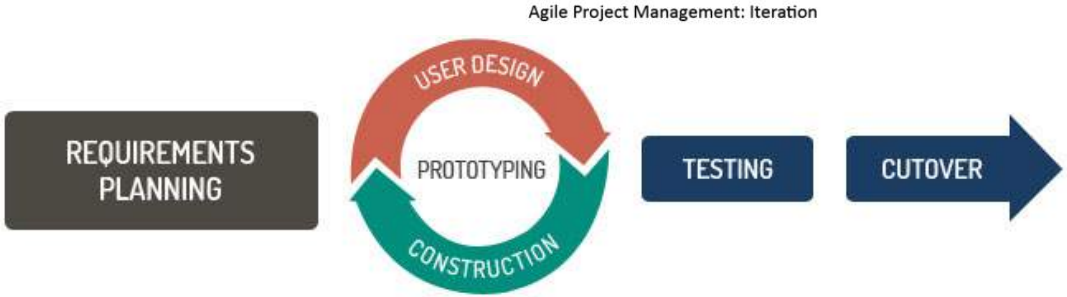
A

Agile & RAD Visualization

Agile Model



RAD Model



A

DevOps

The *DevOps* development methodology is built on the premise that collaboration between developers and the operations team is essential.

- The initial push for DevOps stemmed from the need to integrate operations to make software development more efficient and of higher quality.
- *Integrated DevOps* mandates that the operations team remains involved throughout the software development lifecycle to ensure a smooth, efficient process through transition and deployment.

A

Secure DevOps

Instead of security continuing to exist as a standalone, isolated entity, *Secure DevOps* aims to integrate security into the development processes from inception.

- The Secure DevOps approach enables developers to learn more about what they are developing and how it can be exploited.
- Secure DevOps proactively focuses on surviving by providing reliable software with a reduced attack surface.

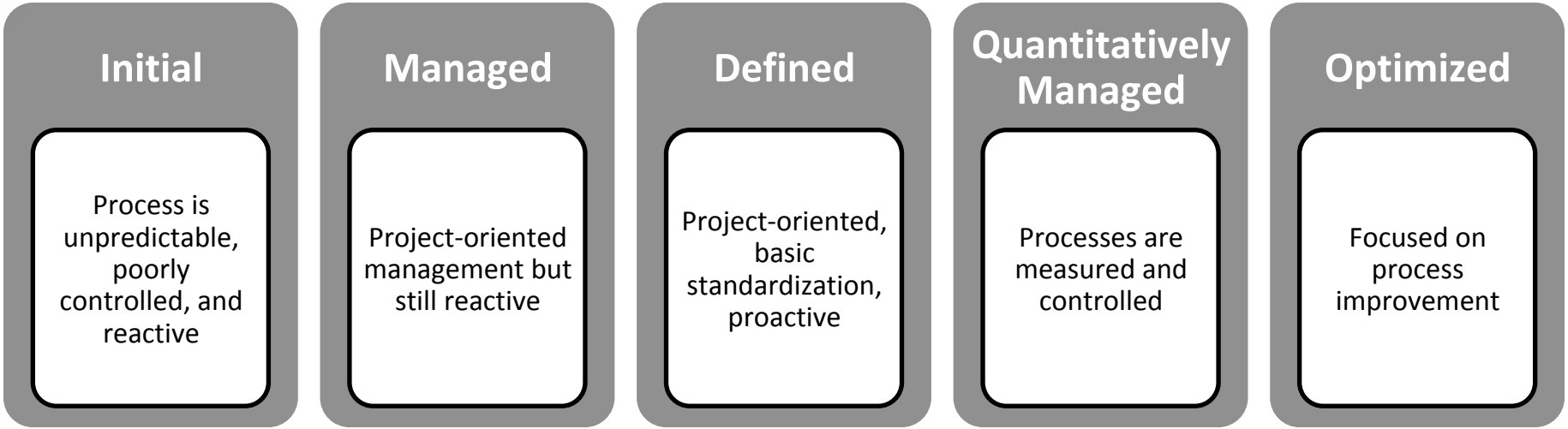
A

Capability Maturity Model

The Capability Maturity Model (CMM) is a methodology used to develop and refine an organization's software development process. The model describes a five-level evolutionary path of increasingly organized and systematically more mature processes.

A

Maturity Model Visualization



B

Source Code Vulnerability

A *source code vulnerability* is an error, failure, or fault in a computer or program that causes it to produce an incorrect or unexpected result or unintentional behavior and/or response.

- Source code flaws can affect functionality, performance, and security.

B

Common Code Security Flaws

Issue	Description	Impact
Improper Input / Output Handling	Tricking an application into including unintended commands in the data sent to an interpreter (e.g. OS, LDAP, SQL) resulting in disclosure.	Can result in database, schema, account, and/or operating system access.
Improper Error Handling	Generation of error messages that reveal implementation, debugging details and/or system information.	Disclosure Recon “clues”
Buffer Overflow	Overrunning the memory allocated (buffer) for data input and writing the excess data into non-allocated system memory.	The excess data can contain instructions that the processor will execute.
Memory Leak	Failure of a OS or program to free up dynamically requested memory	Slow response time (sluggishness) Denial of service

B

Secure Coding

Secure coding is the practice of following secure coding standards coupled with the use of testing tools to detect code vulnerabilities.

- Eliminating vulnerabilities during development can result in a two to three orders-of-magnitude reduction in the total cost of repairing the code versus making the repairs afterwards. https://www.cert.org/secure-coding/

B

Secure Coding Best Practices

Practice	Explanation
Default Deny	Deny all except what is explicitly allowed.
Input | Output Validation	Syntactic validation enforces correct syntax of structured fields (e.g. SSN, date, currency symbol). Semantic validation enforce correctness of values (e.g. start date is before end date, price is within expected range).
Stored Procedures	Restrict direct user access by requiring that all commands use stored procedures.
Memory Management	Allocate sufficient memory for an object. Free dynamically allocated memory when do longer needed.
Code Reuse **Third-party Libraries and SDKs**	Only reuse code that is known to be trusted. Only use libraries and SDKs that have been vetted and known to be trusted.

B

Software Development Testing

Test Type	Description
Unit	Testing of small discrete chunks of codes
Integration	Testing multiple units of code to ensure that the proper information flows between them
Validation	Testing to verify that the product meets the design specifications
Vulnerability	Testing for security vulnerabilities and potential exploits Testing for privacy violations and potential exposures
Acceptance	Testing the end user performs to verify the functionality of the software and acceptance of the product (including security controls – e.g. access controls, logging, reporting and auditing)
Regression	Testing of all major functions after an update or a patch is applied to verify that the changes didn't disrupt functionality

C

Supporting Processes

Three important internal processes support the software development process.

- *Version control* tracks files, source code, and configurations over time.
- *Change control* manages changes to artifacts, such as code changes or documentation changes.
- *Provisioning* deploys (makes available) versions to various resources for simultaneous development.

D

Acquisition

Acquisition is the process of getting something.

- *Procurement* is the process of finding, acquiring, buying goods, services, or works from an external source, often via a competitive bidding process.
  - *Request for Information (RFI)* is used to solicit advice in addressing and/or solving a problem.
  - *Request for Proposal (RFP)* is used to solicit bids (including approach, experience, capability, proof of concept, support) for a product or service.
  - *Invitation to Tender (ITT)* is used when a product or service is known in advance and the objective is the best price and/or service.

D

Procurement Security Evaluation*

Criteria	Description
Security Testing	Independent security testing
Security Documentation	Documentation of security controls and options
Workload	Ability to handle the anticipated volume of work
Utilization | Availability	System availability versus system downtime
Turnaround Time	Time that a vendor takes to “fix” a problem (post report)
Disclosure	Vulnerability disclosure policy
Vulnerability Management	Patch/ update development and deployment

**In addition to vendor due diligence, contractual terms, SLA and product evaluation*

D

Source Code Escrow

Source code escrow is a mechanism for access to source code in the event that the vendor goes out of business or violates contractual obligations to maintain the code.

- A neutral trusted third party holds the source code.

Benefits include

- Risk mitigation
- Business continuity
- Leverage

D

Certification and Accreditation

Certification and Accreditation (C&A) is a two-step process.

- *Certification* is the process of verifying that a system meets specified requirements
- *Accreditation* is the process of an authority (management) granting approval to operate a system for a specified period of time with the understanding of the residual risks identified during the certification process.

Assessment Q1

This software development model is sequential and emphasizes verification and validation at each phase and testing the take place throughout the project.

A. Waterfall
B. V-Model
C. RAD
D. Agile

Assessment Q2

Software regression testing should be scheduled _____.

A. during development
B. during staging
C. concurrent with product launch.
D. whenever a update or patch is applied

Assessment Q3

This automated testing technique is used to discover coding errors and security loopholes by inputting invalid, unexpected or random data.

A. Unit testing
B. Vulnerability assessment
C. Fuzzing
D. Penetration testing

Assessment Q4

What is the very first step in secure software acquisition and implementation?

A. Selection criteria.
B. Vendor due diligence.
C. Business requirements.
D. Risk assessment.

Assessment Q5

Identify the origin of this statement. “Safety of the commonwealth, duty to our principals (employers, contractors, people we work for), and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior”.

A. 2015 State of the Union Address
B. ISO 27000
C. $(ISC)^2$ Code of Ethics Preamble
D. None of the above

Day 2 Segment #6

Preparing for Test Day!

Study Plan

Create a study plan and stick to it!

- Watch my videos – The Complete CISSP & The Exam Prep Video course (bundled together as a Safari Books Online “Learning Path”)
- Study with a buddy.
- Make flash cards.
- Talk to yourself, seriously.

The Week Before

The last week should be all about review – not new material.

- Don’t crowd your week. This isn’t the week to be launching a new project at work, be facing a looming deadline, or taking a trip to your in-laws. Purposely make exam week as stress free as possible.

Test Day

What should you do on test day?

- To begin with, the night before plan to go to bed early and get a good night's sleep. Wake up refreshed and ready to go.
- Eat an energizing meal.
- Prepare light healthy snacks and drinks with you – fruits and carbohydrates.
- Wear layered clothing. The test center may be the perfect temperature. It may also be too hot or too cold for your liking. Dress for comfort.
- Give yourself plenty of time to get to the testing center. If you're late – you may not be able to take your exam. If you live far away, consider staying at a hotel close.
- Don't forget to bring proper identification.
- Lastly, maintain a positive can do attitude. Relax. Breathe deeply. Enjoy the experience. You've got this!!

Let's study together. Stay in Touch

e: Sari@sarigreene.com

t: @sari_greene

l: https://www.linkedin.com/in/sarigreene/

Next CISSP Crash Course – February 21st and 22nd