

Exam Details



Exam Details

Exam Code	SY0-601
Launch Date	November 12, 2020
Exam Description	The CompTIA Security+ certification exam will verify the successful candidate has the knowledge and skills required to assess the security posture of an enterprise environment and recommend and implement appropriate security solutions; monitor and secure hybrid environments, including cloud, mobile, and IoT; operate with an awareness of applicable laws and policies, including principles of governance, risk, and compliance; identify, analyze, and respond to security events and incidents
Number of Questions	Maximum of 90 questions
Type of Questions	Multiple choice and performance-based
Length of Test	90 minutes
Passing Score	750 (on a scale of 100-900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented:

DOMAIN	PERCENTAGE OF EXAMINATION
1.0 Attacks, Threats, and Vulnerabilities	24%
2.0 Architecture and Design	21%
3.0 Implementation	25%
4.0 Operations and Incident Response	16%
5.0 Governance, Risk, and Compliance	14%
Total	100%

Cert Prep: 1 Threats, Attacks, and Vulnerabilities

Type of Malwares

1. Virus - spread by human action
2. Worms - spread by themselves
3. Trojan Horse - hide themselves
 - a. RAT (Remote Access Trojan) - provide backdoor

Malware Payload

(Potentially Unwanted Program) UNWANTED SOFTWARE

1. Adware - advertisement
2. Spyware - gather information
3. Ransomware - block access ENCRYPTED.
4. Cryptomalware - mines cryptocurrency.

Prevent Malware

Anti malware	User education	Security Patches
--------------	----------------	------------------

BACKDOOR - provide workaround access.

LOGICBOMB - deliver triggered payload.

ROOT ACCOUNTS - super user

Rookits - escalate user privilege access - **MALWARE**

- User Mode Rootkits
 - o Easy write, difficult to detect
- o Run with normal user privilege
- Kernel Mode Rootkits
 - o Run with system priv

FILELESS - remain in memory

Examples:

- Macros
- Javascripts
- Windows Registry

BOTNET (ZOMBIES) - infected machines. Need a COMMAND and CONTROL.

SCRIPT - sequence of instructions

- Threat actor = someone who wants to punch you in the face
- Threat = the punch being thrown
- Vulnerability = your inability to defend against the punch
- Risk = the likelihood of getting punched in the face
- Acceptable risk = your willingness to be punched in the face

Type of ATTACKERS

1. Script Kiddie - unskilled who use tools of other without knowing it
 2. Hacktivists - political or social agenda
 3. Criminal - financial gain
 4. Competitors - corporate war
 5. Nation State - skilled attacker and ADVANCED PERSISTENT THREAT
-

WHITE HATS - legal

BLACK HATS - no permission

GRAY HATS - middle

INSIDER THREAT - inside employee

SHADOW IT - not approved application or unapproved technology

ATTACK VECTORS - path how to hack

Examples:

- Email
- Social Media
- Wireless network
- Flash drive
- Cloud Services
- Tampering devices

ZERO DAY - vulnerability of one product that has no available patch

THREAT INTELLIGENCE - allow teams to stay up to date on current risks

OSINT (OPEN SOURCE INTELLIGENCE) - public information

THREAT INDICATORS - properties that describe a threat

FACILITATE INFORMATION SHARING

- TAXII
- STIX
- CybOX

SOCIAL ENGINEERING - manipulating people

HASH FUNCTION - mathematical function that converts a variable-length into fixed-length output

SYSTEM SPRAWL - new devices are connected but old devices are not promptly disconnected

Type of Password Attacks

1. Bruteforce - try all possibilities
2. Dictionary - list of words

3. Hybrid - add variations, example: adding Zero instead O
4. Rainbow Table - precompute hashes
5. Password Spraying - exploits common password
6. Credential Stuffing - exploits reused password

Cert Prep: 2 Secure Code Design and Implementation

ENDPOINT APPLICATION - self-contained on a device.

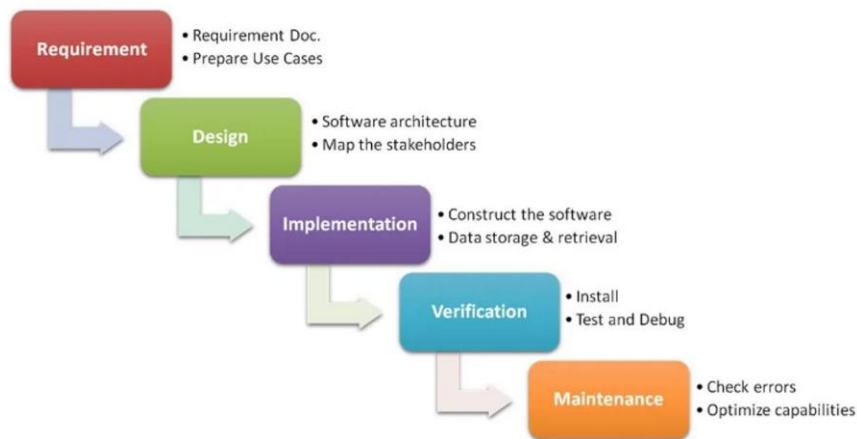
CLIENT/SERVER - interact with a server. Example database-driven application

WEB APPLICATION - client/server over the web

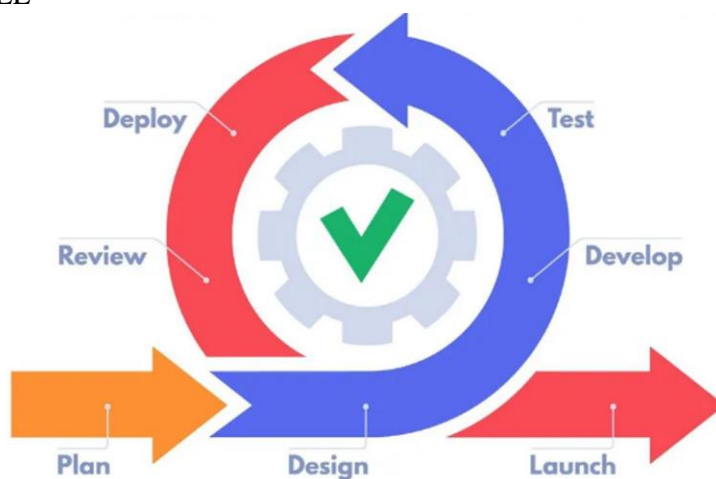
IOT - Internet of things

DEVELOPMENT METHODOLOGIES

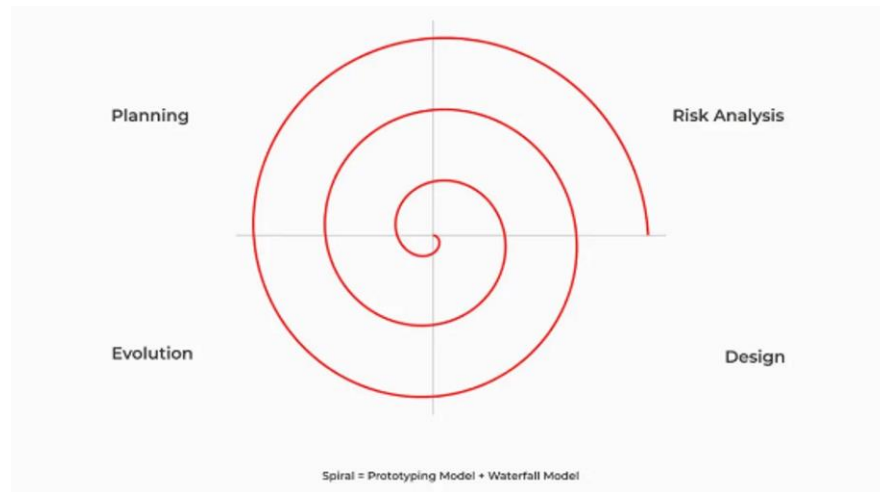
WATERFALL



AGILE



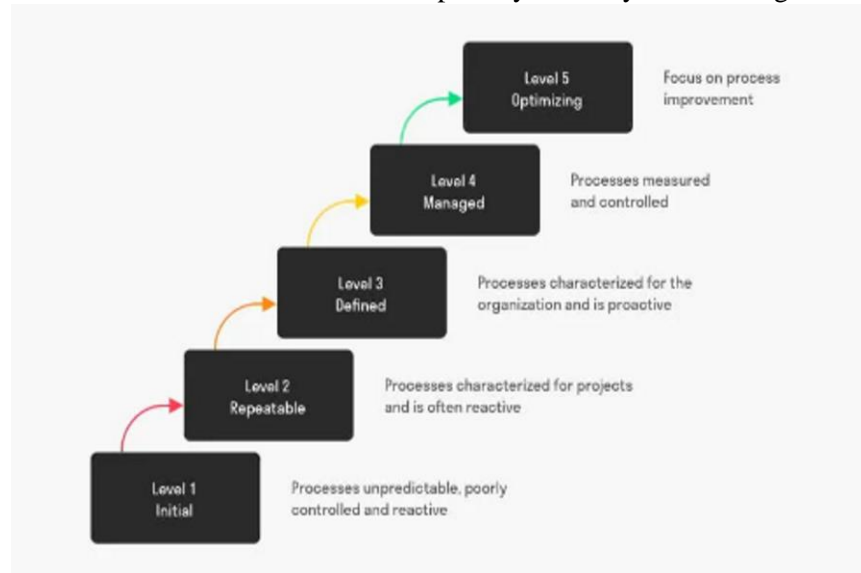
SPIRAL MODEL



MATURITY MODEL - provide standard benchmarks

Example:

CMMI - Capability Maturity Model Integration



CHANGE MANAGEMENT - standardizes code release processes

3 Elements

- Request Control
- Change Control
- Release Control

CODE ENVIRONMENT



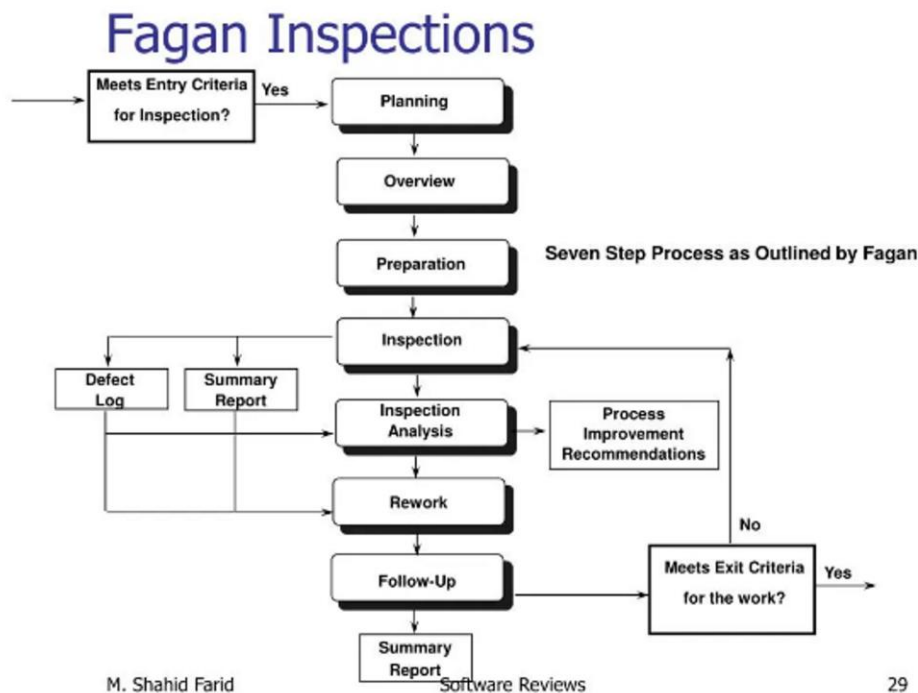
INFRASTRUCTURE AS CODE - scripts the creation of resources

DEVOPS GOALS - build collaborative relationship and embrace automation

STRESS TESTING - real world load testing or maximum capacity testing.

CODE REVIEW - use peer analysis to assess code

Example: FAGAN INSPECTION



USER ACCEPTANCE TESTING (BETA TESTING) - ensures software will work for users.

REGRESSION TESTING - checks for unexpected side effects.

CODE SECURITY - use technology to inspect software.

- STATIC TEST

- Automated techniques to analyze code for errors and security flaws without actually executing it.

- DYNAMIC TEST

- Execute code to verify that it is functioning correctly

FUZZING - is a software testing technique that feeds software many different input values in an attempt to cause an unpredictable state or unauthorized access.

CODE REPOSITORIES - store software source code files

INTEGRITY MEASUREMENT - used to verify release code is unchanged.

APPLICATION CONTROL - restrict to run software

- Whitelisting
- Blacklisting

LIBRARIES - contains shared folder

OWASP (Open Web Application Security) - maintains a list of common web security issues.

APPLICATION ATTACKS

- Broken Access Control - allows unauthorized access
- Cryptographic Failure - allows access to sensitive data
- Injection Flaw - inject unwanted code
- Insecure Design - fails to meet security requirements
- Request Forgery - tricks server into requesting URL

APPLICATION HARDENING - core concept of application security

- Use proper authentication
- Encrypt sensitive data
- Validate input user
- Obfuscation and camouflage

Developer set aside areas of memory called BUFFERS to store user-supplied content

BUFFER OVERFLOW ATTACKS - use input larger than the buffer

COOKIES - track user activity on the web/provide an authentication.

CODE EXECUTION ATTACKS - occur when an attacker exploits a vulnerability in a system that allows the attacker to run commands on that system

- Arbitrary Code Execution - runs command of attacker
- Remote Code Execution - attacks that take place over a network connection

PRIVILEGE ESCALATION ATTACKS - gains administrative access

RACE CONDITION - when code runs together or dependent on the sequence timing

INPUT VALIDATION - sanitize user input

STORED PROCEDURES - use parameterized queries

& - HTML Encoding

% - URL Encoding

ERROR HANDLING - avoids unpredictable states

CODE SIGNING - applies digital signatures to software

DEIDENTIFICATION - remove obvious identifiers

Type of Data Obfuscation

Hashing - replace sensitive fields with hash values

Salting - uses random values to defeat rainbow tables

Tokenization - replace sensitive fields with a random ID

Masking - redacts information

Cert Prep 3: Cryptography Design and Implementation

ENCRYPTION - protects sensitive information from unauthorized disclosure

CRYPTOGRAPHY - use mathematical algorithm to transform information into an encrypted form
CIPHERTEXT

ALGORITHMS - mathematical recipes

SYMMETRIC - same key





ASYMMETRIC - two key / key-pair

5 Goals of Cryptography

- Confidentiality - no unauthorized access
- Integrity - no unauthorized changes
- Authentication - prior of identity claims
- Obfuscation - hiding sensitive data
- Non-Repudiation - verification of origin

Boolean Operators

NOT		AND			OR			XOR		
x	F	x	y	F	x	y	F	x	y	F
0	1	0	0	0	0	0	0	0	0	0
1	0	0	1	0	0	1	1	0	1	1
		1	0	0	1	0	1	1	0	1
		1	1	1	1	1	1	1	1	0



Symmetric Cryptography

- Data Encryption Standard
- 3 DES
- BLOWFISH
- TWOFISH
- AES - Advanced Encryption Standard

Asymmetric Cryptography

- RSA
- PGP
- Elliptic-curve
- Quantum

KEY EXCHANGE

Diffie-hellman - provides symmetric key exchange capability
Elliptic-Curve Diffie-Hellman

STEGANOGRAPHY - hides data in other file

KEY ESCROW - bond/law

KEY STRETCHING - add salt to harden the key

HARDWARE SECURITY MODULES - manage encryption keys and perform cryptographic operations

WEB OF TRUST - relies on indirect relationship

HASH FUNCTION - one way function/message digest

DIGITAL SIGNATURE - certificate signed

CERTIFICATE REVOCATION LIST - includes serial numbers of revoked certificates

ONLINE CERTIFICATE STATUS PROTOCOL - provides real time certificate status verification

CERTIFICATE SUBJECT - owner of public key

Certificate Types

- Root cert - protects CA private key
- Wild card cert - cover an entire domain *

Certificate Formats

BINARY	Binary Extension	Text	Text Extention
DER	.der .crt .cer	PEM	.pem .crt
PFX	.pfx .p12	P7b	P7b

Transport Layer Security - encrypts network communication

Cert Prep 4: Identity and Access Management Design

Identification - username

Authentication - password / prove identity

Authorization - access

Accounting logs

Authentication Factors

- Something you know - password/passphrase
- Something you are - biometrics
- Something you have - phone/physical

FALSE ACCEPTANCE - system misidentifies an individual as an authorized user

FALSE REJECTION - system fails to recognize an authorized user

MULTIFACTOR AUTHENTICATION - combines authentication techniques from two or more

SINGLE SIGN ON (SSO) - authentication system that shares a single authentication session across multiple systems

RADIUS - remote access dial-in user service

TACACS - terminal access controller access control system

KERBEROS - ticket-based authentication system / port 88

LDAP - lightweight directory access protocol / port 389 LDAPS 636

SAML - security assertion markup language allow single sign-on

OAuth - authorization protocol

OpenID - authentication protocol

Least Privilege - limit the access

Separation of Duties - any critical function must require two or more individuals

Mandatory Access Control - fixed rules based

Discretionary - access control can set by owner

Cert Prep 5: Physical Security Design and Implementation

Fire Extinguisher

Class A - common combustibles (wood, chain)

Class B - flammable liquids (gasoline, oil)

Class C - electrical fires (data centers)

Class D - heavy metal fire (industrial app)

Class K - kitchen (fat, oil)

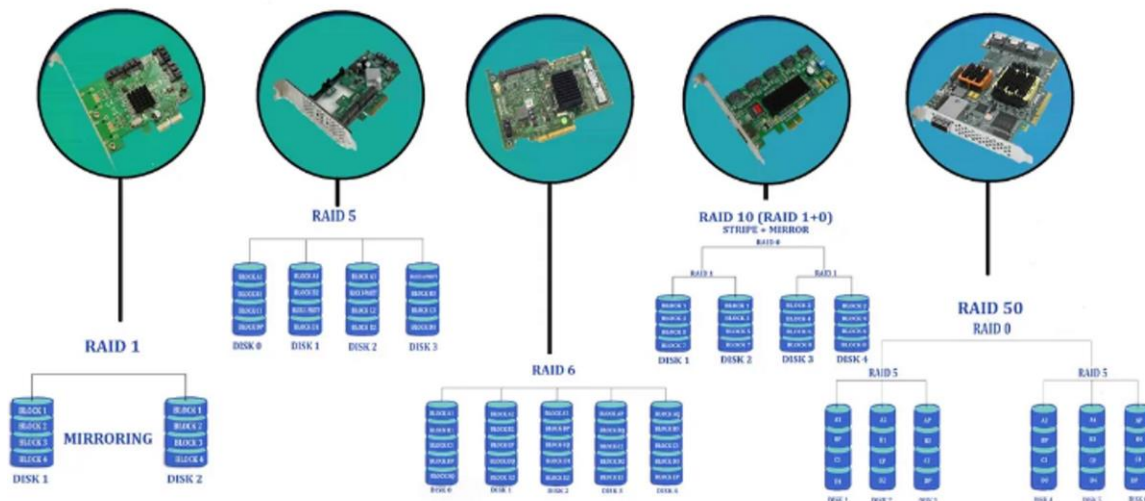
64.4 F - minimum temperature data center

BUSINESS CONTINUITY PLANNING - continuity of operations planning (coop)

HIGH AVAILABILITY - uses multiple systems to protect against service failure

FAULT TOLERANCE - makes a single system resilient against technical failures

RAID - fault tolerance not a backup strategy



DISASTER RECOVERY - ability to restore business operation immediately

RTO (RECOVERY TIME OBJECTIVE) - maximum time take to recover

RPO (RECOVERY POINT OBJECTIVE) - maximum time period of from which data may be lost

Cert Prep 6: Cloud Security Design and Implementation

CLOUD COMPUTING - delivering computing resources to a remote customer over a network

Cloud Computing Roles

Cloud Service Provider

Partner

Customer

MANAGED SERVICE PROVIDER - provide technology / 3rd party

Type of Hypervisor

TYPE 1 - Bare Metal

Type 2 - OS level

VDI (Virtual Desktop Infrastructure) - cloud desktop

Cert Prep: 7 Endpoint Security Design and Implementation

HOST SECURITY

Operating system security

- Least privilege
- Patch Management
- Remove unnecessary application (System Hardening)

Malware Prevention

Antimalware

Signature Detection - watches for known patterns of malware activity.

Behavior Detection - watches for abnormal patterns of activity.

Example: EDR (Endpoint Detection and Response) - offers real-time, advanced protection and sandboxing

Spam Filtering - prevent unwanted emails.

Application Management

Application Control - restricts software that may run

- Whitelisting - list of allow application
- Blacklisting - list of prohibited application

Host-based network security controls

Firewalls - by default, block any network connection attempts that are not explicitly allowed by a firewall rule

Network Firewalls - hardware devices that regulate connections between two networks

Host Firewalls - software components of an operating system that limit connection to server

Next-Generation Firewall - advanced security features, such as contextual information about the user and application

IDS (Intrusion Detection System) - monitor network traffic for suspicious activity and notify

IPS (Intrusion Prevention System) - block suspicious activity

File Integrity Monitoring - watches for unexpected file modification via hash value

Data Loss Prevention (DLP) - technology solutions that search systems and monitor networks for sensitive information that is unsecured and provide the ability to remove the information, block the transmission, or encrypt the data

Pattern Matching - recognizes known patterns of sensitive information

Watermarking - identifies sensitive information using electronic tags

HARDWARE SECURITY

Data Encryption - protects sensitive data by transforming it so that it may not be read by anyone without the appropriate decryption key.

Full-Disk Encryption - encrypts an entire disk

Hardware and Firmware Security

UEFI - replaces BIOS with a flexible alternative

Example:

- Secure boot

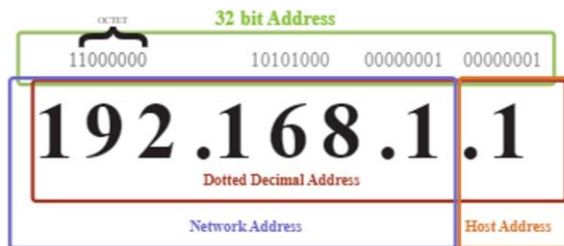
Cert Prep: 8 Network Security Design and Implementation

Internet Protocol - routes information across networks

ICMP (Internet Control Message Protocol) - housekeeping protocol of internet. (Troubleshooting)

Inet - IPv4 = 4 octet

8 bits per octet = 32 bits

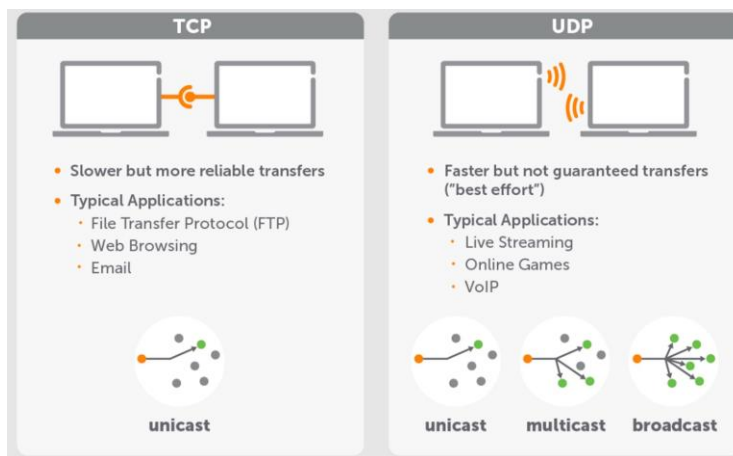


Inet6 - IPv6 = 16 octet

8 bits per octet = 128 bits

::1/128 loopback address

::FFFF:0:0/96 IPv4 mapped address



Port Ranges

0 - 1,023 - well-known ports

1,024 - 49,151 - registered ports

49,152 - 65,535 - dynamic ports

Common Ports and Protocols

- TCP

- FTP (21)
- SSH (22)
- Telnet (23)
- SMTP (25)
- DNS (53)
- HTTP (80) / HTTPS (443)
- POP3 (110)
- SMB (139 + 445)
- IMAP (143)

- UDP

- DNS (53)
- DHCP (67, 68)
- TFTP (69)
- SNMP (161)

TCP Flags

SYN - initiate / hello

ACK - hello reply / received

FIN - Done / Termination

RST - Uncorrect termination

PSH - move packet for real time push

URG - import / priority packets

Secure Network Design

DMZ (Demilitarized Zone) - accessible in internal and external

Intranet - local network only

Extranet - Intranet segments extended to business partners

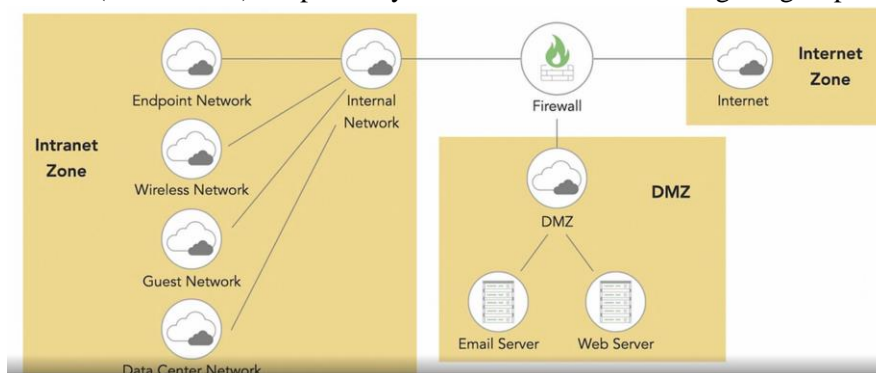
Honeynet - Decoy networks designed to attract attackers

Ad Hoc Network - Temporary networks that may bypass security controls

East-West Traffic - network traffic between systems located in the data center

North-South Traffic - network traffic between systems in the data center and systems on the internet

VLAN (Virtual Lan) - separate systems on a network into logical groups.



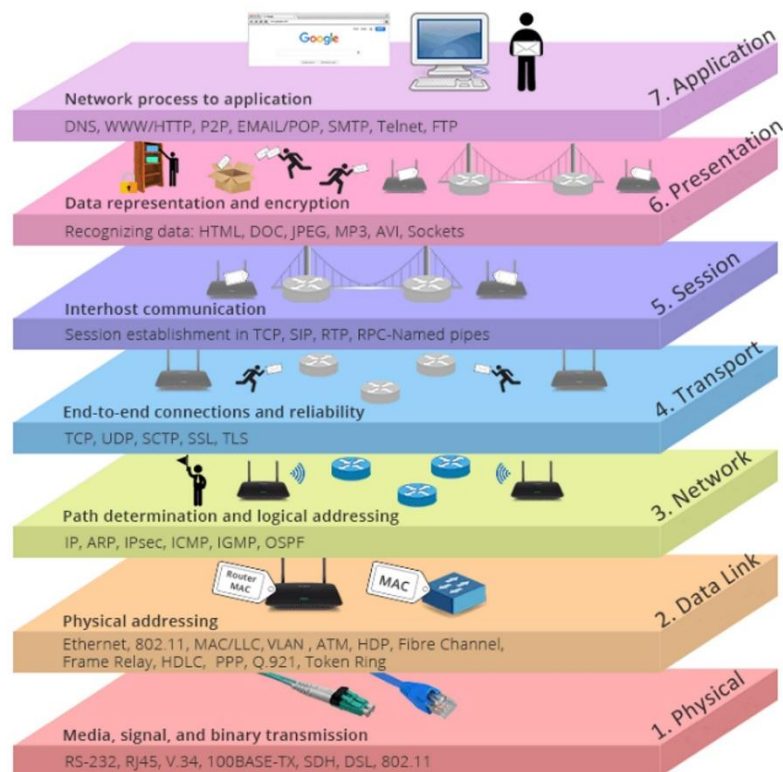
Private IP Address

Network Class	Network Numbers	Network Mask	No. of Networks	No. of Hosts per Network
CLASS A	10.0.0.0	255.0.0.0	126	16,646,144
CLASS B	172.16.0.0 to 172.31.0.0	255.255.0.0	16,383	65,024
CLASS C	192.168.0.0 to 192.168.255.255	255.255.255.0	2,097,151	254
LOOPBACK (localhost)	127.0.0.0 to 127.0.0.7	255.255.255.0	-	-

Public IP Address

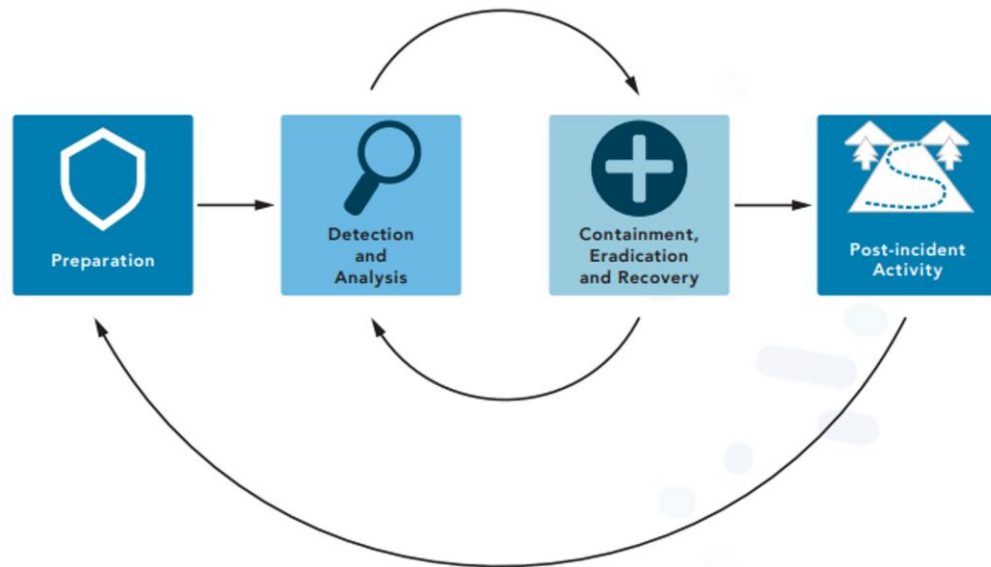
Class	Public IP Ranges
A	1.0.0.0 to 9.255.255.255 11.0.0.0 to 126.255.255.255
B	128.0.0.0 to 171.255.255.255 173.0.0.0 to 191.255.255.255
C	192.0.0.0 to 195.255.255.255 197.0.0.0 to 223.255.255.255
D	224.0.0.0 to 247.255.255.255 Multicast Addresses
E	248.0.0.0 to 255.255.255.254 Experimental Use

OSI Model



Cert Prep: 9 Operations and Incident Response

Components of the Incident Response Plan



Preparation

- Develop a policy approved by management.
- Identify critical data and systems, single points of failure.
- Train staff on incident response.
- Implement an incident response team. (covered in subsequent topic) • Practice Incident Identification. (First Response)
- Identify Roles and Responsibilities.
- Plan the coordination of communication between stakeholders.
- Consider the possibility that a primary method of communication may not be available.

Detection and Analysis

- Monitor all possible attack vectors.
- Analyze incident using known data and threat intelligence.
- Prioritize incident response.
- Standardize incident documentation.

Containment

- Gather evidence.
- Choose an appropriate containment strategy.
- Identify the attacker.
- Isolate the attack.

Post-Incident Activity

- Identify evidence that may need to be retained.
- Document lessons learned.

The response team has four primary responsibilities:

- Determine the amount and scope of damage caused by the incident.
- Determine whether any confidential information was compromised during the incident.
- Implement any necessary recovery procedures to restore security and recover from incident-related damage.
- Supervise the implementation of any additional security measures necessary to improve security and prevent recurrence of the incident.

Business continuity planning (BCP) is the proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization.

Here are some common components of a comprehensive business continuity plan:

- List of the BCP team members, including multiple contact methods and backup members
- Immediate response procedures and checklists (security and safety procedures, fire suppression procedures, notification of appropriate emergency-response agencies, etc.)
- Notification systems and call trees for alerting personnel that the BCP is being enacted
- Guidance for management, including designation of authority for specific managers
- How/when to enact the plan
- Contact numbers for critical members of the supply chain (vendors, customers, possible external emergency providers, third-party partners)

Business continuity planning is about maintaining critical business functions, disaster recovery planning is about restoring IT and communications back to full operations after a disruption.

RTO - T for TIME - how long your service can be offline.

RPO - P for POINT - how much data you can lose - till what point do you have data backed up.

Cert Prep: 10 Governance, Risk, and Compliance

Risk Assessment - identifies and prioritizes risks

$$\text{Vulnerability} + \text{Threat} = \text{RISK}$$

Key Terms

Threats - external force jeopardizing security

Threat vector - specific method that use to exploit vulnerability

Vulnerability - weaknesses in system

Likelihood - probability that a risk will occur

Impact - amount of expected damage

Type of Risk Assessment

Qualitative Risk Assessment - uses subjective ratings to evaluate risk likelihood and impact

		Probability		
		Low	Medium	High
Impact	High	Medium	High	High
	Medium	Low	Medium	High
	Low	Low	Low	Medium

Quantitative Risk Assessment - uses objective numeric ratings to evaluate risk likelihood and impact

Asset Value - cost of asset

Exposure Factor - expected percentage of damage to an asset

Single-Loss Expectancy - expected dollar loss if a risk occurs one time

$$\text{AV} * \text{EF} = \text{SLE}$$

Annualized Rate of Occurrence (ARO) - number of times a risk expected each year

Annualized Loss Expectancy (ALE) - expected dollar loss from a risk in any given year

$$\text{SLE} * \text{ARO} = \text{ALE}$$

Mean Time to Failure (MTTF) - average time a nonrepairable component will last

Mean Time Between Failures (MTBF) - average time gap between failures of a repairable component

Mean Time to Repair (MTTR) - average time required to return

RISK Types

Internal Risk - arise within organization

External Risk - arise from outside the organization

Multiparty Risk - shared across many organizations

Legacy Risk - arise from unsupportable systems

Classification Levels

Military Classification	Business Classification
Top Secret	Highly Sensitive
Secret	Sensitive
Confidential	Internal
Unclassified	Public

Risk Management Strategies

Risk Avoidance - changes the business process

Risk Transference - insurance to another organization

Risk Mitigation - reduces the likelihood or impact of risk

Risk Acceptance - accepts the risk without taking further action

Risk Management Framework

