Important **CISSP** Lists & Processes

1

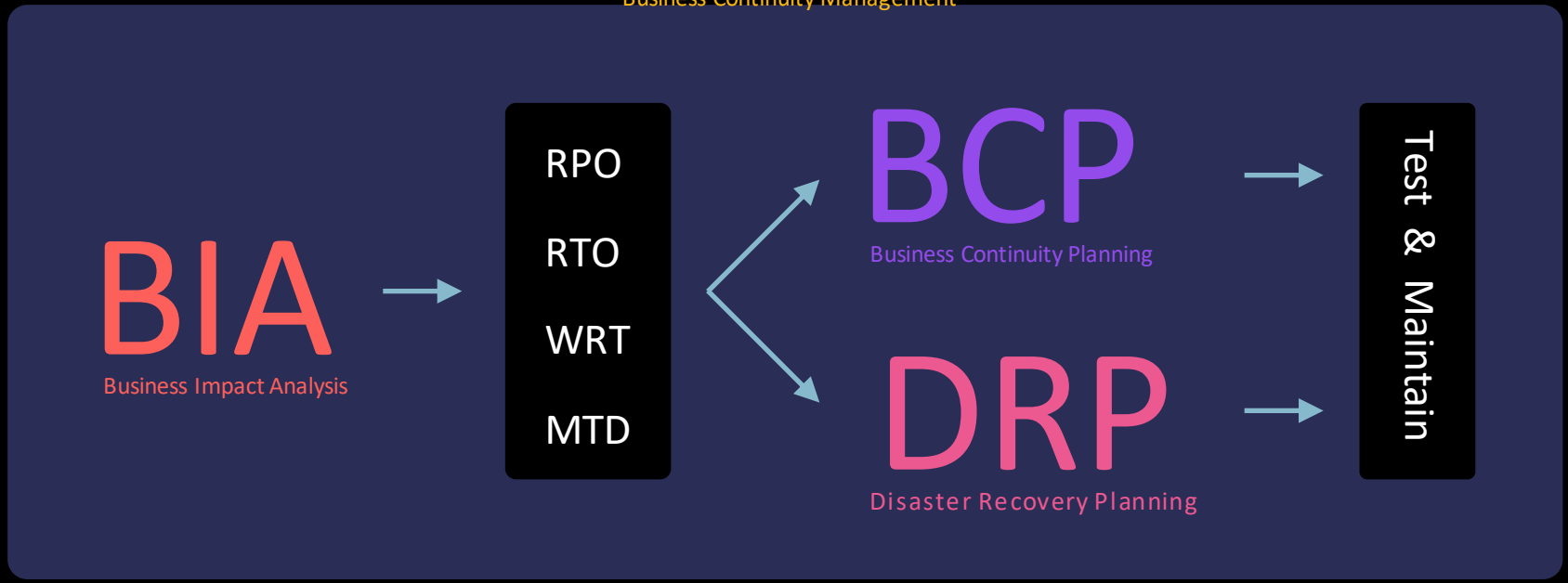
Security and Risk Management

Intellectual property

	Protects	Disclosure required	Term of protection	Prohibited by protection
 **Trade Secret**	Business information	No	Potentially infinite	Misappropriation
 **Patent**	Functional innovations Novel idea / inventions	Yes	Set period of time	Making, using or selling invention
© **Copyright**	Creative expression of an idea (books, movies, songs, etc.)	Yes	Set period of time	Copying or substantially similar work
TM / ® **Trademark**	Color, sound, symbol, etc. used to distinguish one product / company from another	Yes	Potentially infinite	Creating confusion

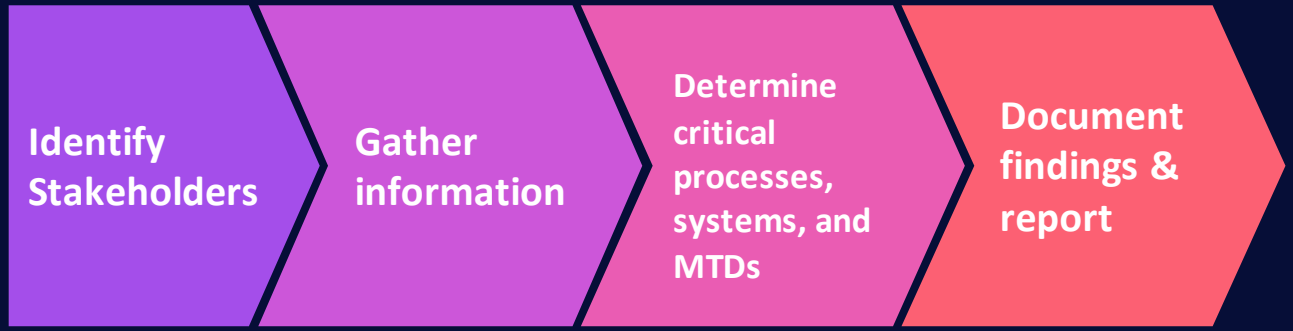
BCM

Business Continuity Management



BCP / DRP Steps

1. Develop Contingency Planning Policy	A formal policy provides the authority and guidance necessary to develop an effective contingency plan
2. Conduct BIA	BIA helps identify and prioritize information systems and components critical to supporting the organization's mission/business processes
3. Identify preventive controls	Measures taken to reduce the effects of system disruptions can increase system availability and reduce contingency life cycle costs
4. Create contingency strategies	Thorough recovery strategies ensure that the system may be recovered quickly and effectively following a disruption
5. Develop contingency plan	Develop contingency plan(s)
6. Ensure Testing, training, and exercises	Testing validates recovery capabilities Training prepares recovery personnel for plan activation Exercising the plan identifies planning gaps
7. Maintenance	Plan should be a living document that is updated regularly



The BIA plan needs to include:

- Confidentiality
- Integrity
- Availability

The BIA Process

NIST 800-37 Risk Management Framework

1	**Prepare** to execute the RMF (prepare the organization to manage its security and privacy risks using the RMF)
2	**Categorize** Information Systems (Determine the adverse impact to operations, assets, individuals, etc. with respect to the loss of CIA of organizational systems)
3	**Select** Security Controls (select, tailor, and document the controls necessary to protect the information system and organization commensurate with the risk)
4	**Implement** Security Controls (implement controls and to document in a baseline configuration, the specific details of the control implementation)
5	**Assess** Security Controls (determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome)
6	**Authorize** Information System (provide accountability by requiring a senior management official to determine if the security and privacy risk based on the controls, is acceptable)
7	**Monitor** Security Controls (maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions)

STRIDE

Threat	Violation	Definition
Spoofing	Authentication	An attacker pretends to be something or someone to gain unauthorized access
Tampering	Integrity	An attacker modifies data at rest (e.g. in a database) or in transit (e.g. over the internet)
Repudiation	Non-repudiation	An attacker performs an action on a system that is not attributable to them
Information Disclosure	Confidentiality	An attacker can read sensitive/private information
Denial of Service	Availability	An attacker prevents legitimate users from accessing and application / service
Elevation of Privilege	Authorization	An attacker gains elevated access rights (e.g. Administrative / root access)

2

Asset Security

Data Roles

Role	Description
Data Owner / Controller	**Accountable** for protection of data, holds legal rights and defines policies
Data Processor	**Responsible for processing** data on behalf of the owner / controller (Processor is typically the Cloud Provider)
Data Custodian	**Technical responsibility** for data (e.g. data security, availability, capacity, continuity, backup and restore, etc.)
Data Steward	**Business responsibility** for data (e.g. metadata definition, data quality, governance, compliance, etc.)
Data Subject	Individual to whom personal data relates

Categories of sanitization

Method	Description
1. **Destroy**	**Physical destruction of the media** that the data is stored on
2. **Purge**	Logical or Physical techniques to sanitize data Data **cannot** be reconstructed
3. **Clear**	Logical techniques to sanitize data Data **may not** be reconstructed

3

Security Architecture & Engineering

Functional levels

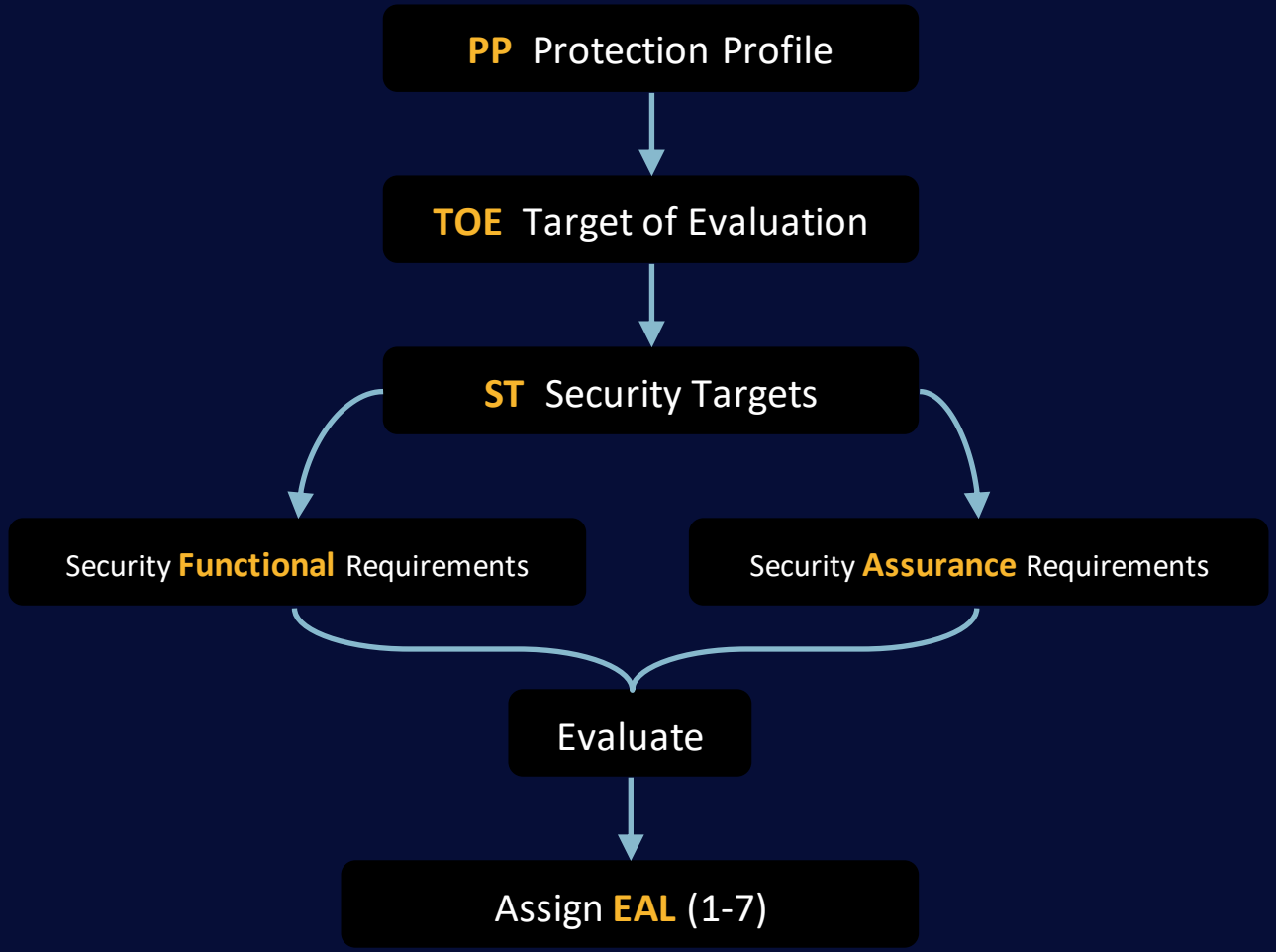
A1	Verified design
B3	Security labels, verification of no covert channels, and must stay secure during start-up
B2	Security labels and verification of no covert channels
B1	Security labels
C2	Strict login procedures
C1	Weak protection mechanisms
D1	Failed or was not tested

Labelling

Most Products

Orange Book Evaluation Criteria

Common Criteria process



Common Criteria EAL levels

EAL7	Formally verified designed & tested
EAL6	Semi formally verified designed & tested
EAL5	Semi formally designed & tested
EAL4	Methodically designed, tested & reviewed
EAL3	Methodically tested & checked
EAL2	Structurally tested
EAL1	Functionally tested

Cyber Kill/Attack Chain

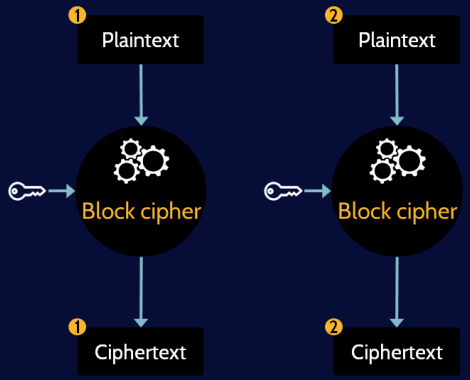
1	**Reconnaissance**	Intruder selects target, **researches** it, and attempts to **identify vulnerabilities** in the target network.
2	**Weaponization**	Intruder **creates remote access malware** weapon, such as a virus or worm, tailored to one or more vulnerabilities.
3	**Delivery**	Intruder **transmits weapon** to target (e.g., via e-mail attachments, websites or USB drives)
4	**Exploit**	Malware weapon's program **code triggers**, which takes action on target network to **exploit vulnerability**.
5	**Installation**	Malware weapon **installs access point (e.g., "backdoor")** usable by intruder.
6	**Command & Control (C&C)**	Malware enables intruder to have "hands on the keyboard" **persistent access to target network**.
7	**Actions**	Intruder takes **action to achieve their goals**, such as data exfiltration, data destruction, or encryption for ransom.

5 characteristics of cloud computing

On-demand self-service	Users can request services and sophisticated software at cloud provider automatically provisions
Broad network access	Access to cloud resources are available from multiple device types from multiple locations
Resource pooling	Easily provisionable and scalable resources which can appear infinite (compute, storage, network)
Rapid elasticity and scalability	Ability to quickly provision and de-provision resources
Measured service	Usage of resources is monitored and reported to the consumer, providing visibility and transparency of rates and costs
Multi-tenancy	Resources are allocated such that multiple consumer's (Tenant's) computations and data are isolated from and inaccessible to one another

Symmetric Block Modes

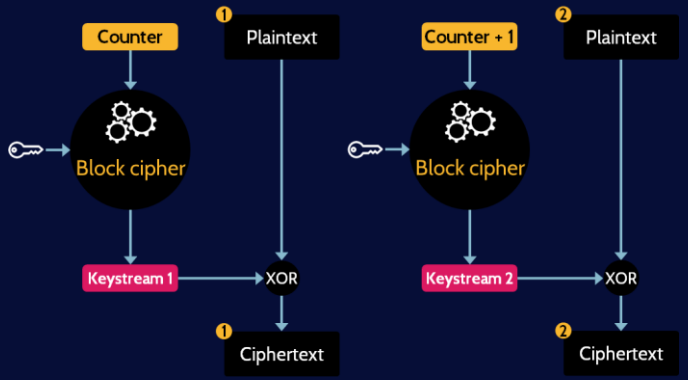
Electronic Codebook (ECB)



Least secure mode (no IV) but fastest

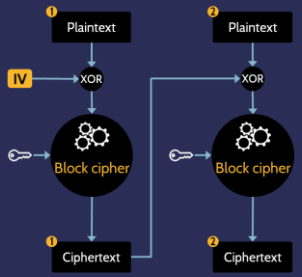
Should only be used for short bits of random text that does not repeat

Counter (CTR)

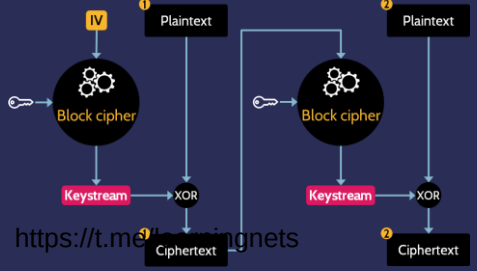


Almost most secure, and the **fastest**

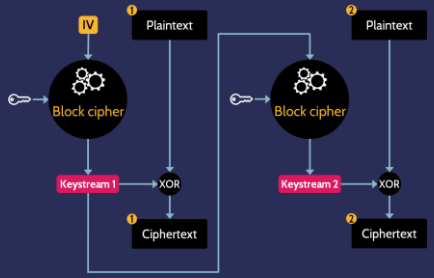
Cipher Block Chaining (CBC)



Cipher Feed Back (CFB)



Output Feed Back (OFB)



Symmetric algorithms

Strength	Name	Key Length	Block Size
 Weak	RC2-40	40	
	DES	**56**	**64**
	RC5-64/16/7	56	
 Medium	RC5-64/16/10	80	
	Skipjack	80	
 Strong	RC2-128	128	
	RC5-64/12/16	128	
	IDEA	**128**	**64**
	Blowfish	128	
	3DES	168 = **112**	**64**
 Very Strong	RC5-64/12/32	256	
	Twofish	256	
	RC6	256	
	Rijndael (AES)	**128, 192, or 256**	**128**

Certificate lifecycle

Enrollment	Entity submits **request for certificate** to CA
Issuance	**Identity proofing** of the entity, and issuance of certificate
Validation	Checking with CA to confirm **certificate is still valid** (not revoked or expired)
Revocation	Replacement of certificate when **private key has been compromised**
Renewal	**Renew certificate** upon expiration date

Components of PKI

Certificate Authority (CA)	**Root of trust.**
Registration Authority (RA)	**Identity proofs** on behalf of CA
Intermediate / Issuing CA	**Issues certificates** on behalf of CA
Certificate DB	List of **certificates issued** by CA and **revocation list**
Certificate Store	Repository of certificates and user's private key on **user's computer**

Fire Extinguishers

Class		Type of fire	Suppression agents
A	Ash	Common combustibles	Water, foam, dry chemicals
B	Boil	Liquid	Gas, CO_2, foam, dry chemicals
C	Current	Electrical	Gas, CO_2, dry chemicals
D	Dense	Combustible metals	Dry powders
K	Kitchen	Commercial kitchens	Wet chemicals

4

Communication and Network Security

OSI	Description	Devices & Protocols	TCP/IP
7 Application	Network capabilities of applications	Application Firewall HTTP/S, DNS, SSH, SNMP, & FTP	4 Application
6 Presentation	Formatting of data	XML, JPEG, ANSI	
5 Session	Interhost communication	Circuit Proxy Firewall	
4 Transport	End-to-end connection with error correction & detection	TCP/UDP, SRTP, iSCSI (SAN)	3 Transport
3 Network	Logical addressing, routing and delivery of datagrams	Routers & Packet Filtering Firewall IP addresses, ICMP, & NAT	2 Network
2 Data Link	Physical addressing, and reliable point-to-point connection	Switches MAC addresses, L2TP, PPTP	1 Link
1 Physical	Binary transmission of data across physical media (wire, fiber, etc.)	Hubs & NICs Network media	

Authentication protocols

Protocol	Client Authentication
PAP Password Authentication Protocol	Re-usable, static, **clear text password** NOT secure
CHAP Challenge Handshake Authentication Protocol	More secure & provides replay protection
EAP Extensible Authentication Protocol	Way more complicated and secure – support MANY different types of authentication
PEAP **Protected** Extensible Authentication Protocol	Encapsulates the EAP within an encrypted and authenticated TLS tunnel

Common types of EAP

Type	Client Authentication	Server Authentication	Security	Industry Support	Proprietary
EAP-TLS	**Certificate**	**Certificate**	**High**	**High**	**No**
EAP-TTLS	ID & Password	**Certificate**	Medium	Medium	Yes Certicom
EAP-PEAP	ID & Password	**Certificate**	Medium	**High**	Kinda Cisco, RSA & Microsoft
LEAP	ID & Password	ID & Password	Low	**High**	Yes Cisco
EAP-MD5	ID & Password	**NO!**	Low	Low	No

Private IPv4 addresses

10.0.0.0	→	10.255.255.255
172.16.0.0	→	**172.31.255.255**
192.168.0.0	→	192.168.255.255

Network Classes (subnetting)

	# of addresses
Class A	16,777,216 (2^{24}) (16,777,214)
Class B	65,536 (2^{16}) (65,534)
Class C	256 (2^{8}) (254)
Class D	Multicast address
Class E	Reserved

Common ports

21	File Transfer Protocol (FTP)
22	Secure Shell (SSH) (remote login protocol)
23	Telnet (remote command line protocol)
53	Domain Name System (DNS)
80	HyperText Transfer Protocol (HTTP)
443	Hypertext Transfer Protocol Secure (HTTPS)

	True	False
Positive	True-Positive Alarm generated & attack present	**False-Positive** Alarm generated & no attack
Negative	True-Negative No alarm generated & no attack	**False-Negative** No alarm & attack present

False Positive
False Negative

IPSec Modes

AH

Authentication Header

Provides integrity, data-origin authentication and replay protection

OR

ESP

Encapsulating Security Payload

Provides integrity, data-origin authentication, replay protection, and **confidentiality through encryption** of payload

+

Transport mode

Use header of original packet, followed by the AH or ESP header, then the payload

OR

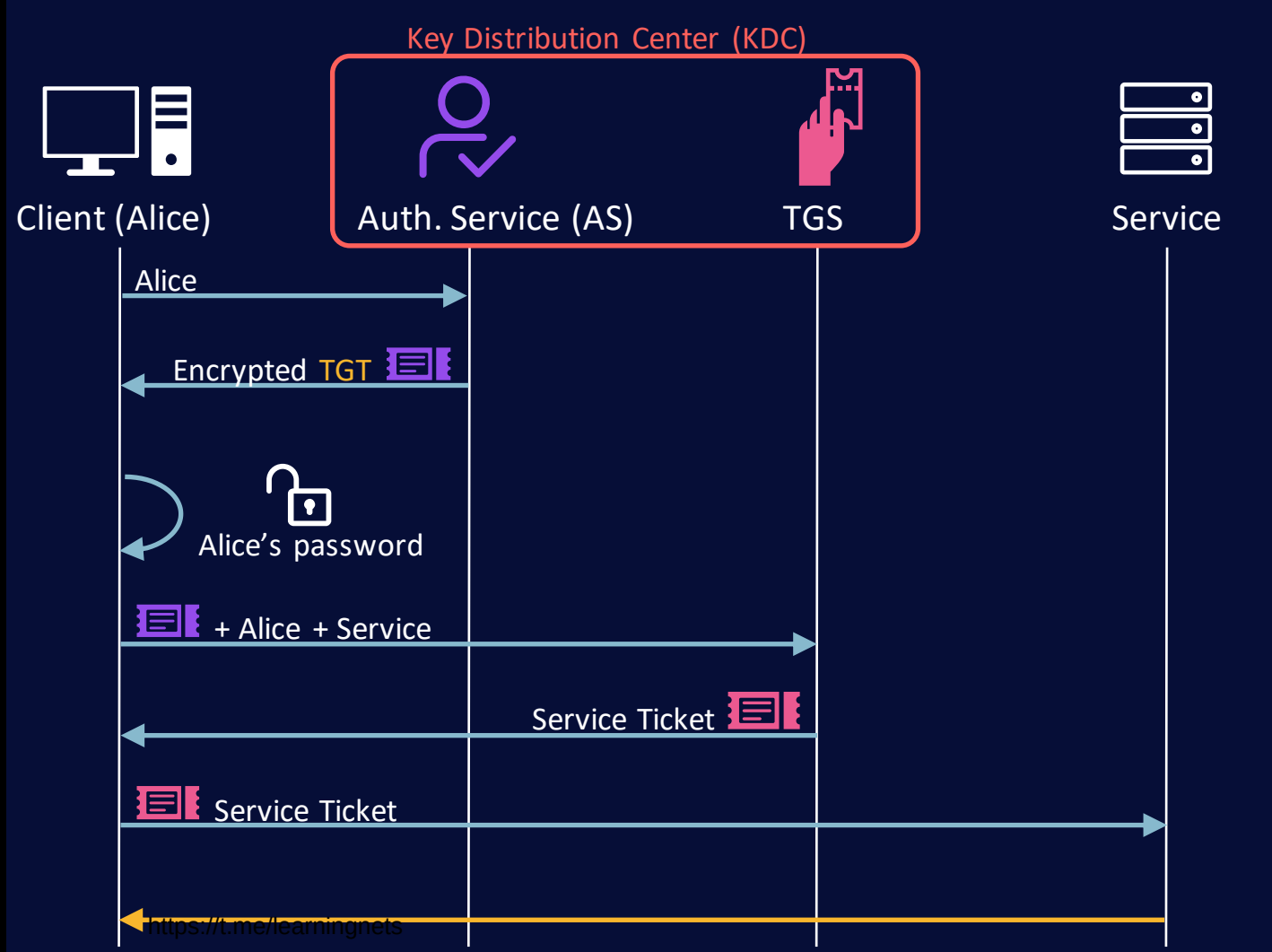
Tunnel mode

New header encapsulates the AH or ESP header and the original IP header and payload

5

Identity and Access Management

Kerberos process



Access control summary

Discretionary Access Control (DAC)	Owner determines access rules
Role-based Access Control (RBAC)	Access to resources is based on **user roles** (e.g. firewall administrator, or accounts payable clerk)
Rule-based Access Control	Access to resources is based on a **set of rules** (e.g. an Access Control List (ACL))
Attribute Based Access Controls (ABAC)	Access to resources is based on user **attributes** (e.g. OS, browser version, IP address, etc.)
Mandatory Access Control (MAC)	System determines access rules based on **labels**

Provisioning lifecycle

6

Security Assessment and Testing

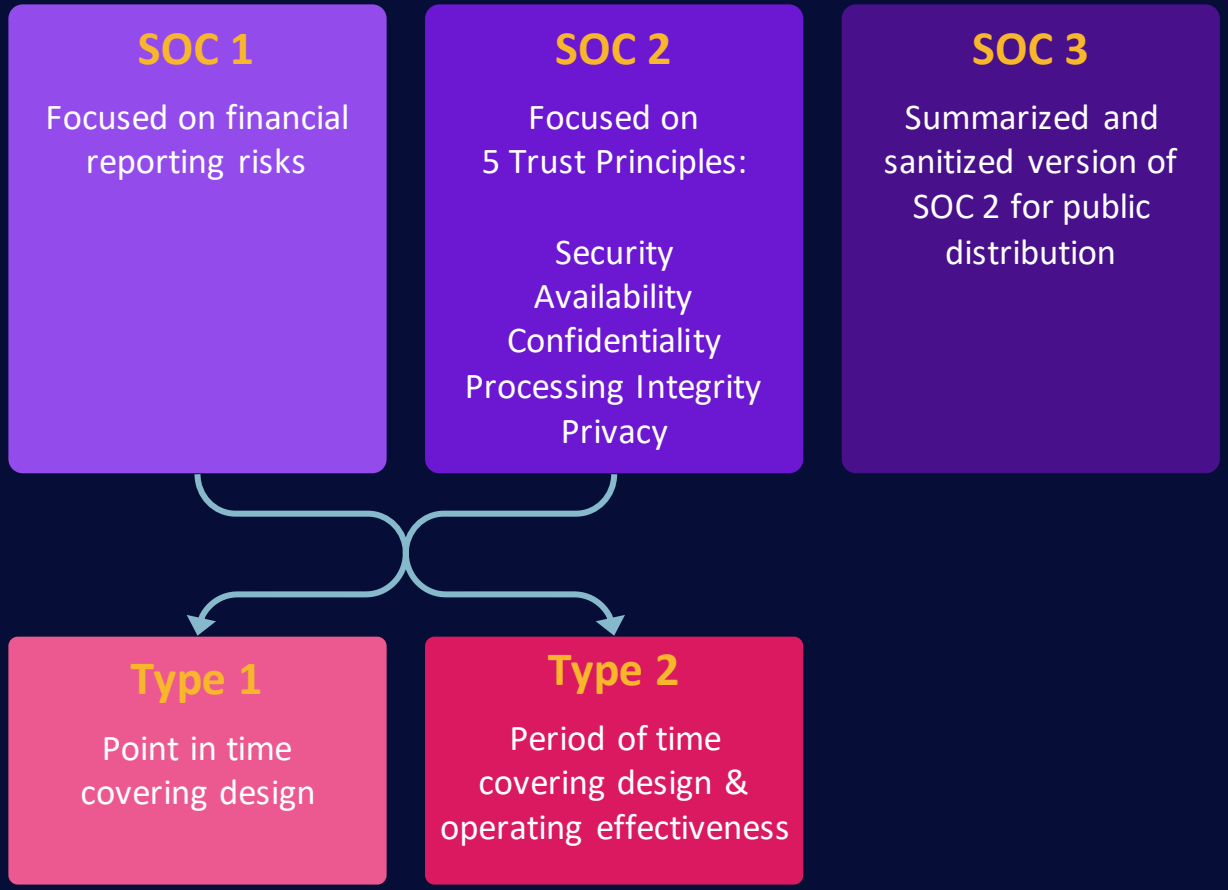
Passively gather publicly available information

Actively enumerate through target IP addresses & ports (network discovery)

Identify potential vulnerabilities to be exploited

Attempt to exploit vulnerabilities

Identify severity of findings and report in format appropriate to audience



ISAE 3402 / SSAE18

Audit Roles & Responsibilities

Role	Responsibilities
Executive (Senior) Management	Tone from the top, promote the audit process, and provide support where needed
Audit Committee	Composed of members of the board / senior stakeholders to provide oversight of the audit program
Security Officer	Advise on security related risks to be evaluated in the audit program.
Compliance Manager	Ensure corporate compliance with applicable laws and regulations, professional standards, and company policy.
Internal Auditors	Company employees who provide assurance that corporate internal controls are operating effectively
External Auditors	Provide an unbiased and independent audit report as they are independent of the entity being audited

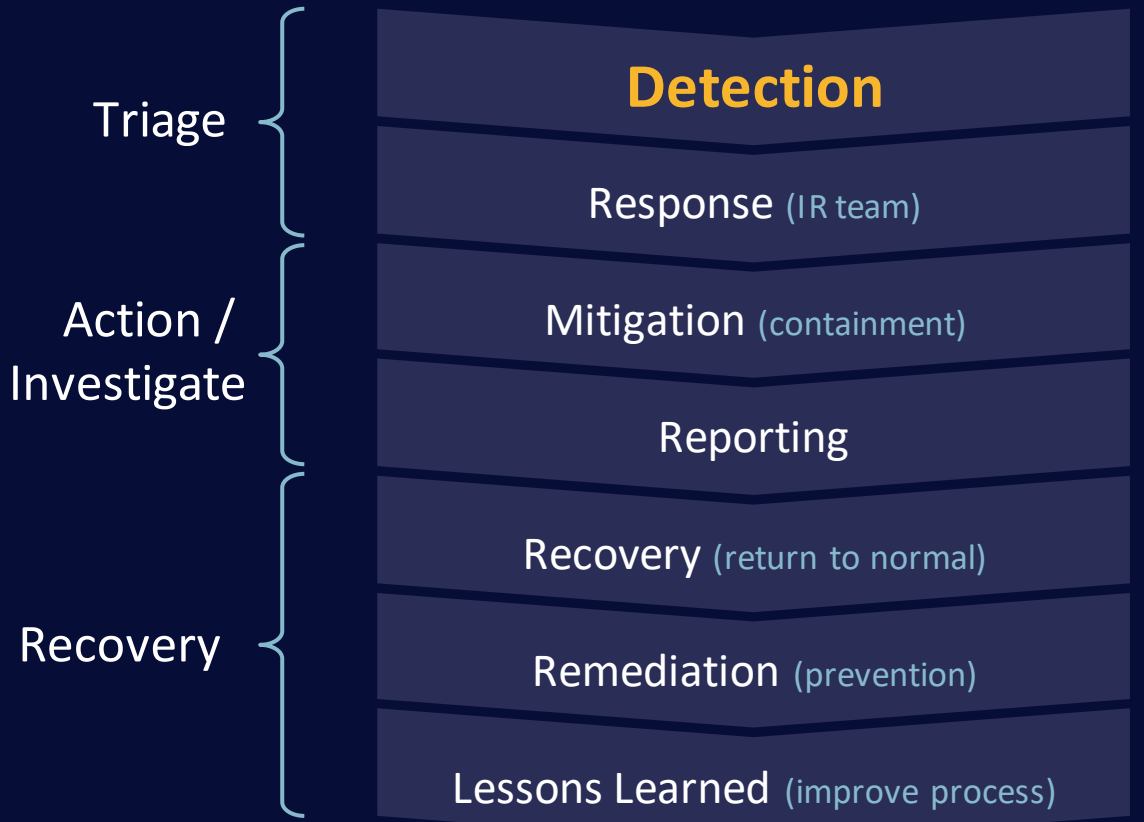
7

Security Operations

Types of evidence

Real Evidence	Tangible **physical objects** – NOT the data on them (Hard drives, SSDs, USB drives)
Direct Evidence	Speaks for itself and **requires no inference** (eyewitness accounts, confessions, smoking gun)
Circumstantial Evidence	Suggests a fact by implication or inference Can prove an intermediate fact
Collaborative Evidence	Supports facts or elements of the case, not a fact on its own, but supports other facts
Hearsay Evidence	Statements made by witnesses who were not present. No firsthand proof of accuracy or reliability.
Best Evidence Rule	**Original evidence** rather than a copy or duplicate of the evidence.
Secondary Evidence	A **reproduction** of, or **substitute** for, an original document or item of proof (e.g. print out of log files)

Incident Response Process



RAID summary

RAID	Data Redundancy	Read / Write Performance	Min. # **of Drives**
0 Striping	✗	Highest	2
1 Mirroring	✓	Moderate	2
1+0 Striping + Mirroring	✓	Highest	4
5 Parity	✓	High	3
6 Double Parity	✓✓	Moderate	4

Recovery Site Strategies

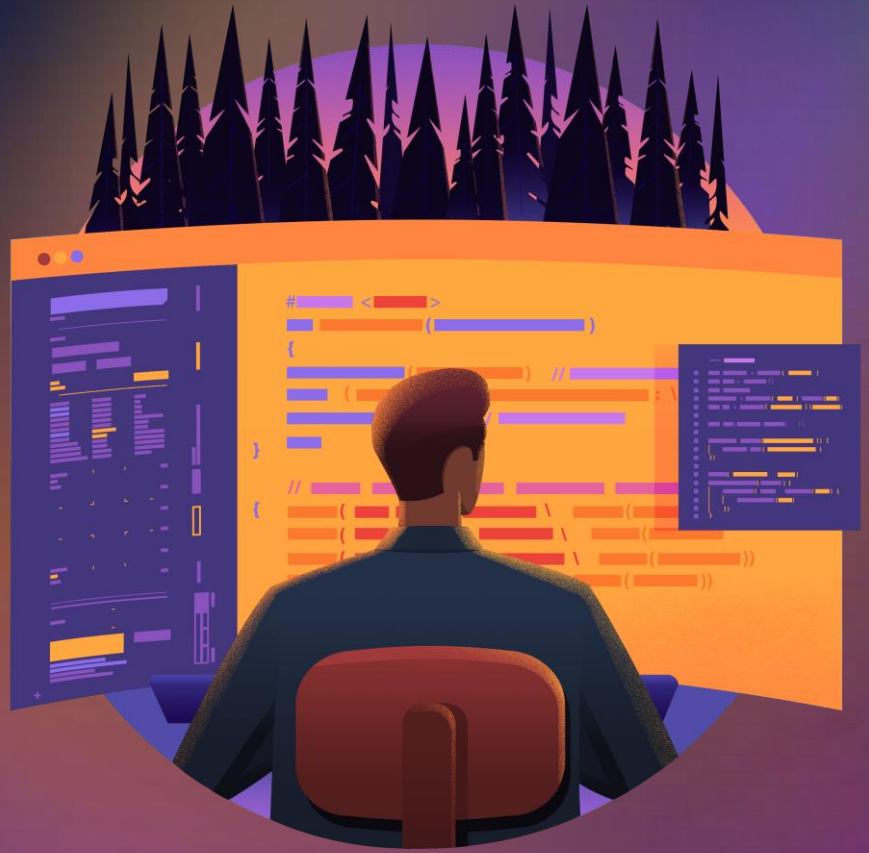
	Cold	Warm	Hot	Mobile	Mirror (Redundant)
People			*		✓
Data			*		✓
Computer Hardware			✓	✓	✓
Basic Equipment		✓	✓	✓	✓
Infrastructure / HVAC	✓	✓	✓	✓	✓
Cost	$	$$	$$$	$$$	$$$$
Recovery time	Weeks	Days	Seconds / Hours	Days / Hours	Instant / Seconds

DR Plan testing approaches

Type	Description	Affects backup / parallel systems	Affects production systems
Read-through / Checklist	Author reviews DR plan against standard checklist for missing components / completeness		
Walkthrough	Relevant stakeholders walk-through plan and provide their input based on their expertise		
Simulation	Follow plan based on simulated disaster scenario. Stop short of affecting systems or data		
Parallel	Test DR plan at recovery site / on parallel systems	✓	
Full-interruption / Full-scale	Cause an actual disaster and follow DR plan to restore systems & data	✓	✓

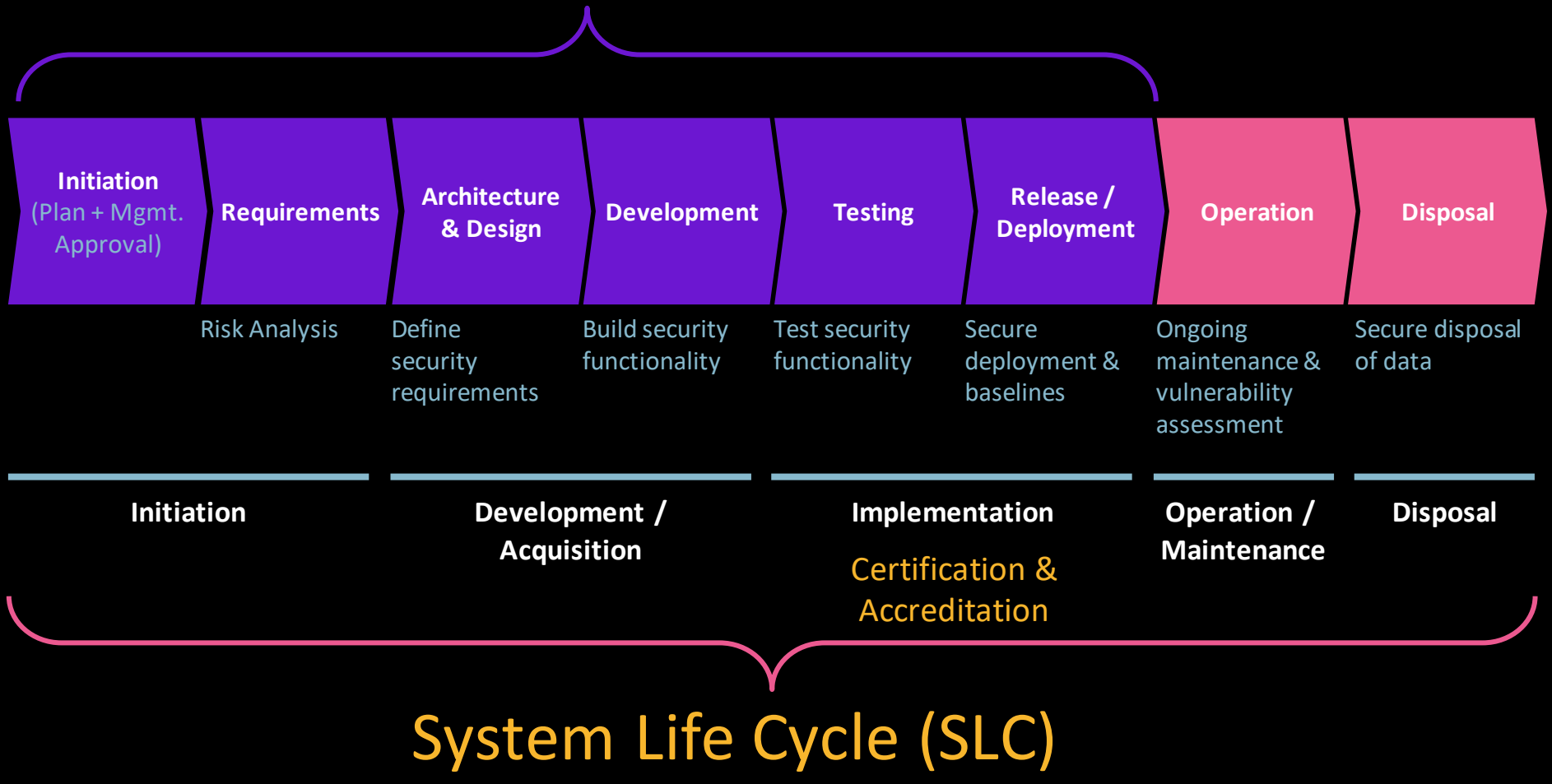
1. Safety of people
2. Minimize damage
3. Survival of business

Goals of BCM

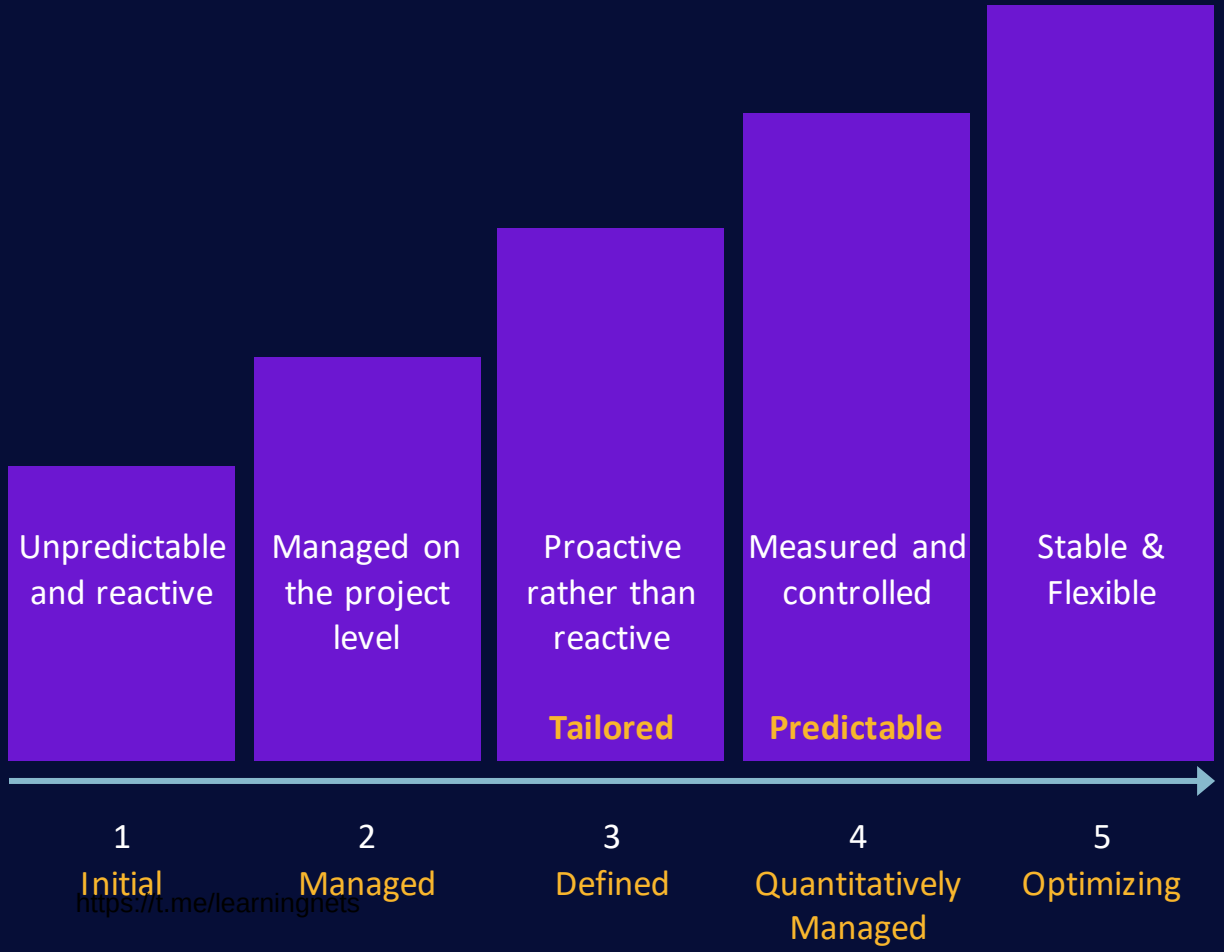


8

Software Development Security



Capability Maturity Model Integration (CMMI)



Maturity Models