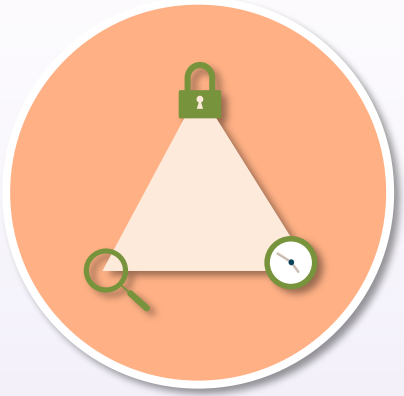
Welcome Back to the SSCP Bootcamp

Your instructor:

Michael J Shannon

- **Class will begin at 10:00 A.M. Central Standard Time (CST)**

Systems Security Certified Practitioner (SSCP) Bootcamp



Session 2

Systems Security Certified Practitioner (SSCP)

Authentication and Trust Architectures

Single-factor Authentication

- The subject must only present one form of credential to be authenticated to access a system or application
  - Open authentication and authorization
  - Anonymous authentication
  - Username and password
  - Email address and password
  - Personal identification number (PIN)
  - Username/email and passphrase
  - Single sign-on credentials
- Identity is a higher level of authentication and is a set of physical and/or behavioral characteristics by which an individual is uniquely recognizable

Dual-factor Authentication (2FA)

- 2FA adds an additional set of credentials to the original authentication factor
- If the password or PIN code is "something you know," then the additional factor would be
  - something ELSE you know (code sent through text or email)
  - something you have (token, card, smartphone, etc.)
  - something you are (biometric)
- Dual or two-factor authentication is a subset of multi-factor authentication (MFA)

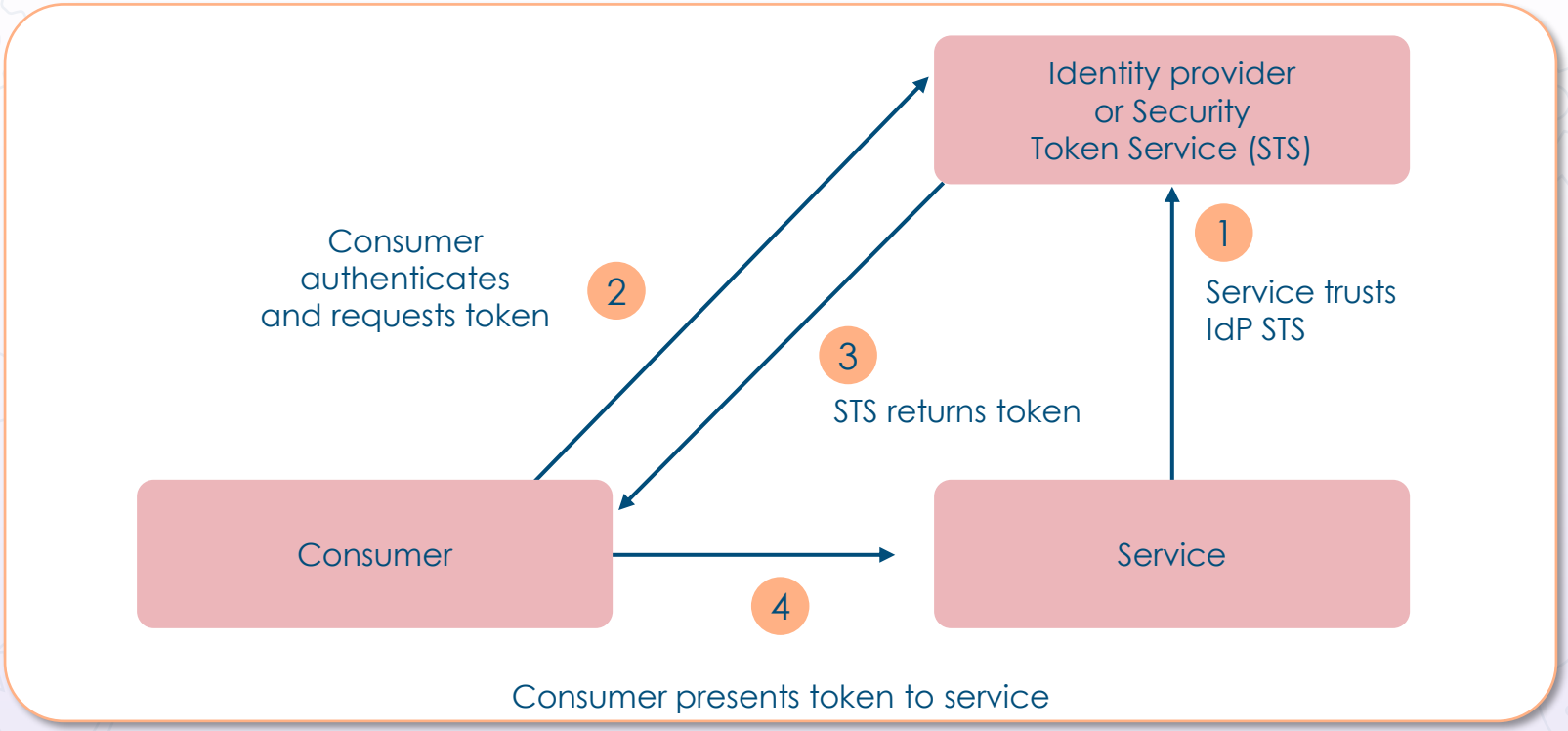
Multi-factor Authentication

- Involves using two or more authentication mechanisms
- Example: enter a username or email address, followed by a sent code or card/token, followed by a biometric, such as a fingerprint, ocular, or voice recognition
- Knowledge-based step-up authentication is an emerging form of MFA for identity management

Single Sign-on and Federated Access

- Single sign-on (SSO) is an authentication technique that allows users to securely authenticate with multiple applications and service providers by using only one set of credentials from an identity provider
- Federation involves identity providers, trusted service providers, and attestation of consumers using assertions or tokens
- When federation standards using the WWW as a transport mechanism started to mature in the early 2000s, specifically using SAML 1.1, organizations rapidly adopted trusted federation networks where identity information could easily flow between entities

Federated Identity Providers

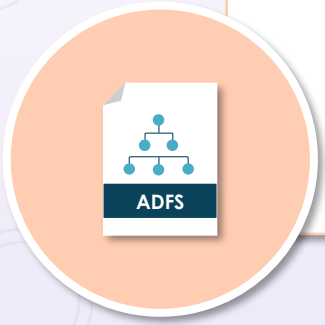


Directory Services

Active Directory is very common

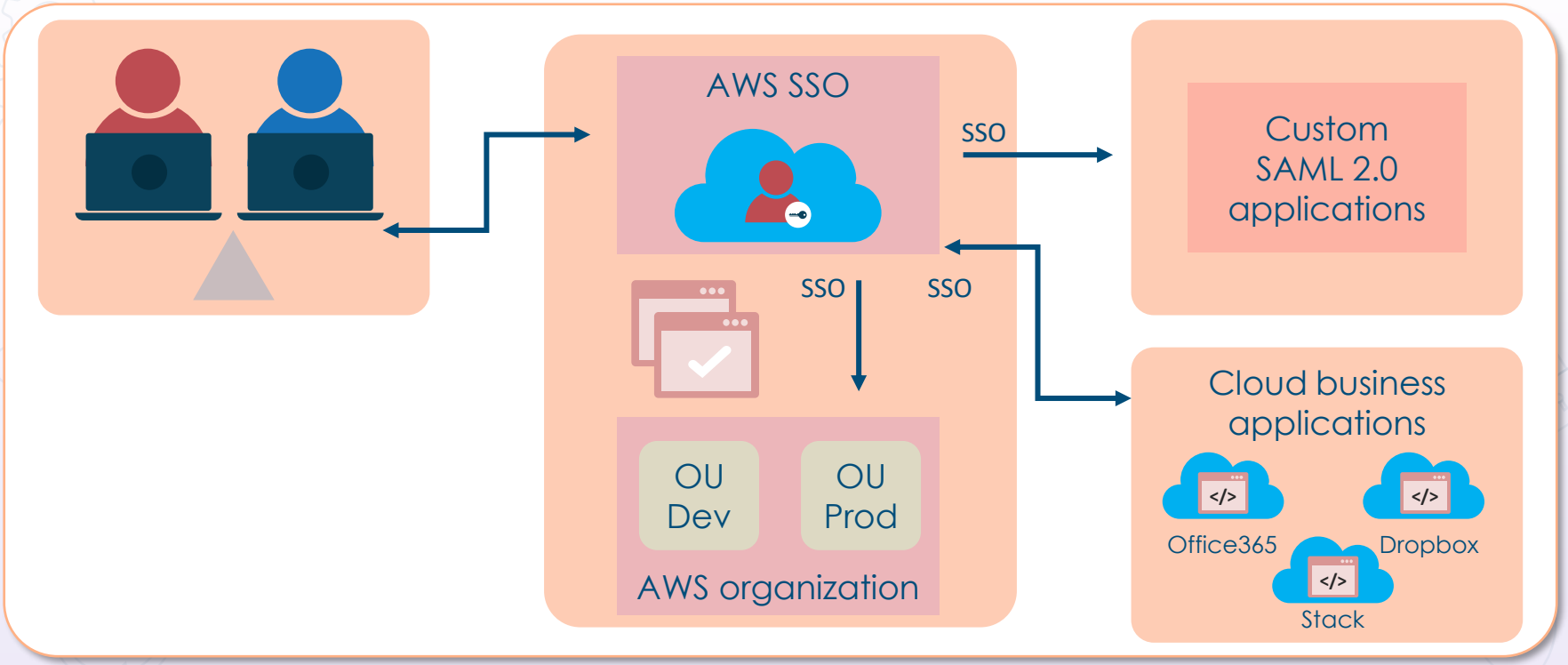
- A directory service is a vital AAA system for the SMB to large global enterprise
- It is a hierarchical structure that stores data about network objects
- Active Directory Domain Services (AD DS) is one of the world's most popular, and it stores usernames, passwords, phone numbers, departments, assigned devices, and much more
- It also allows other authorized users and systems on the same network to access this information

Active Directory Federation Services (ADFS)

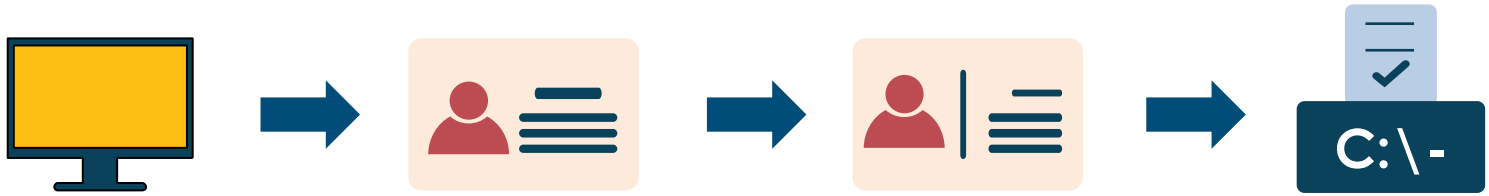


- Active Directory Federation Services (ADFS) is a Microsoft component that runs on Windows Server operating systems to provide users with single sign-on access to systems and applications that are incapable of using Integrated Windows Authentication (IWA) via Active Directory (AD)
- Identity federation is established between two organizations or forests by setting up trust between the two security domains

AWS SSO Service



AWS SSO Service



Enable AWS SSO

Connect corporate identities

Grant SSO access to your accounts and applications

Centrally manage user permissions

Security Assertion Markup Language 2.0

- SAML 2.0 is an XML-based open-source SSO standard from 2004
- It is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs
  - The SAML identity provider declares the identity of the user along with additional metadata in an assertion
  - The service provider takes the assertion and passes the identity data to an application or service
- Common service providers are cloud services and social media sites

OAuth

- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access

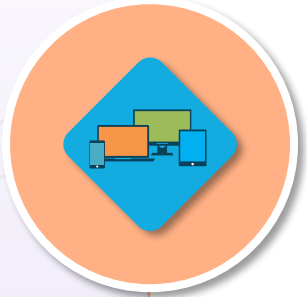
OAuth

- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OpenID Connect (OIDC)

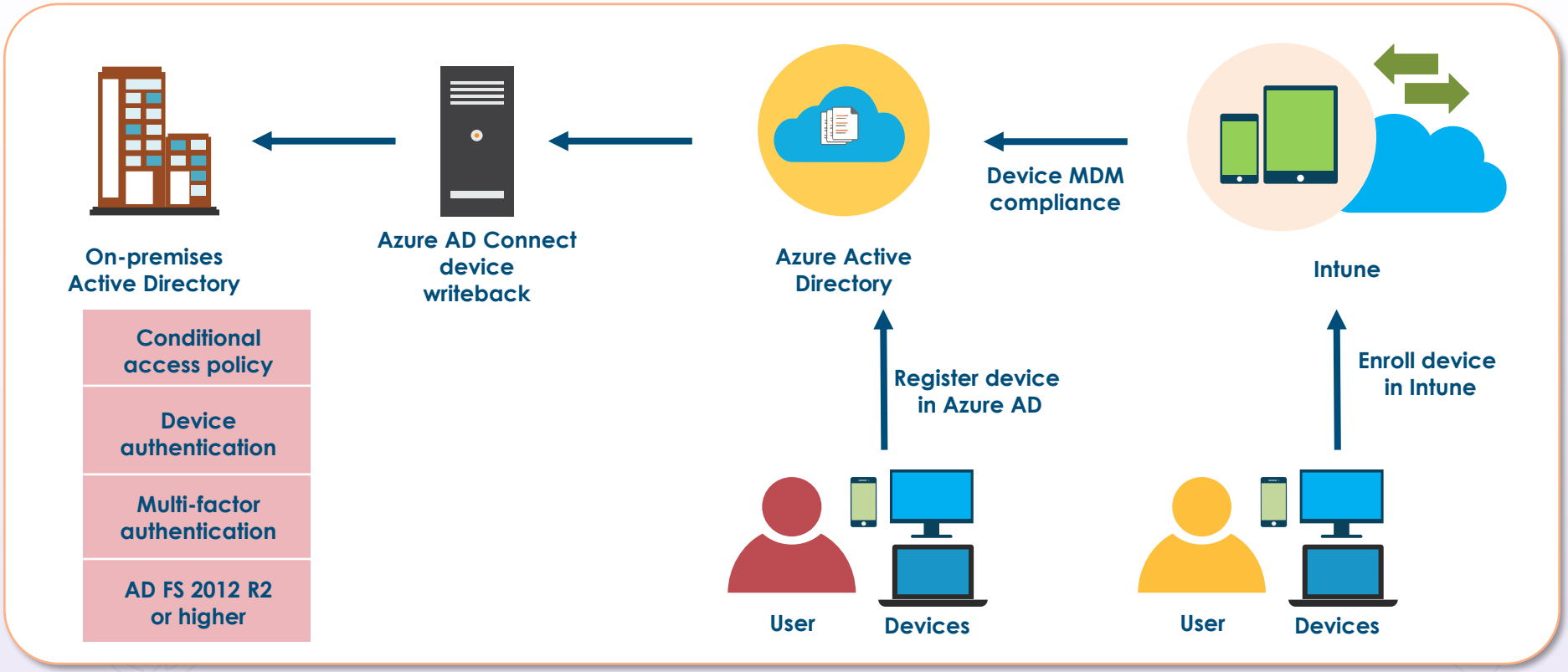
- OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible, as functionality can be added

Device Authentication

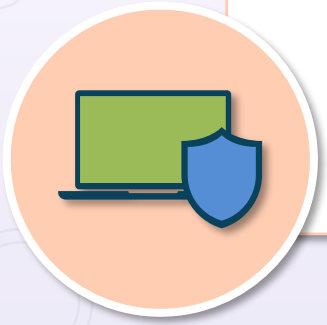


- Device authentication is also commonly referred to as "endpoint authentication"
- It is a security mechanism designed to safeguard authorized devices when connecting to a given LAN, site, or service
- The password response sent from the registered device verifies that the user is connecting from an authorized endpoint
  - The device is usually registered in a directory service or a configuration management database (CMDB)
- In an Active Directory domain, the user and device must be "kerberized" to get a ticket from the Kerberos Key Distribution Center

Azure AD Device Authentication

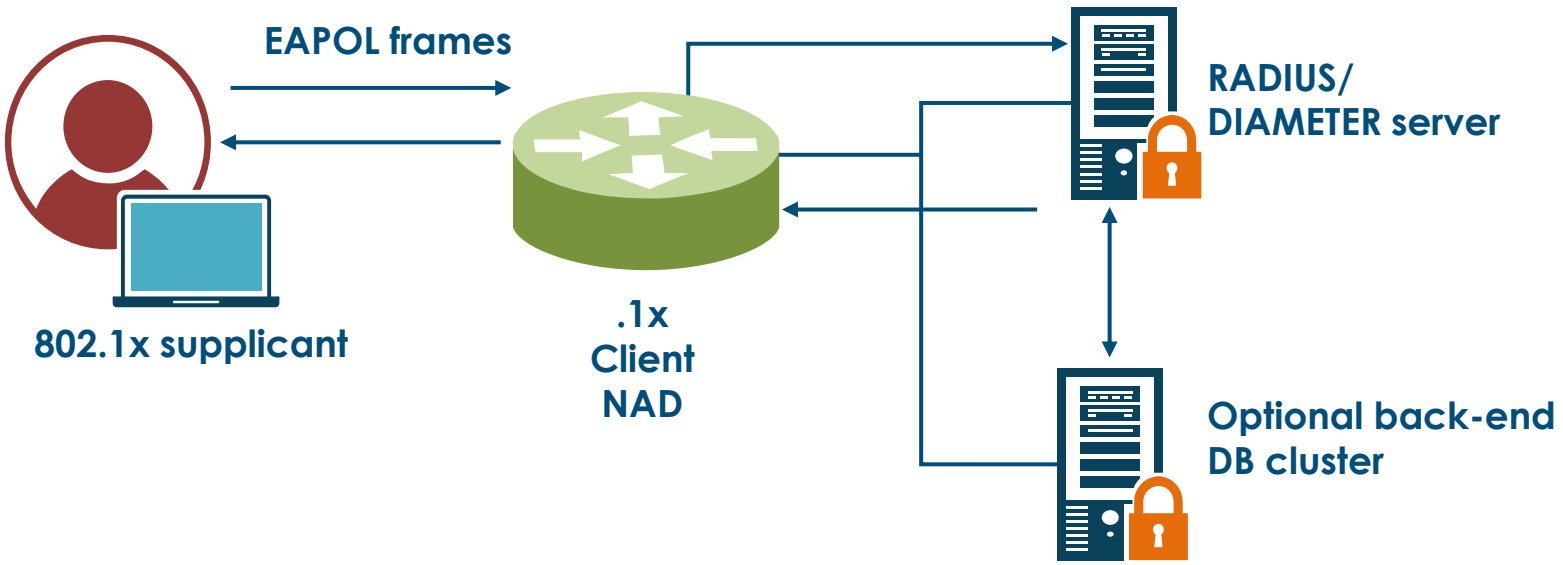


Endpoint Authentication

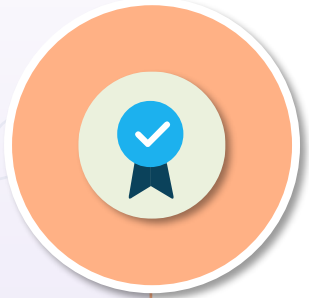


- Other open-source solutions for endpoint authentication will involve installing X509.v3 certificates on the devices and using 802.1X PNAC with EAP-TLS
- Newer solutions may also use 802.11AE MACsec to provide confidentiality, integrity, and origin authentication on the frames sent from supplicant to the switch with AES-GCM-256 and GMAC

802.1X PNAC

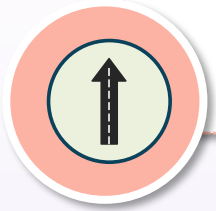

EAPOL frames
802.1x supplicant
.1x
Client
NAD
RADIUS/
DIAMETER server
Optional back-end
DB cluster

Trust Relationships



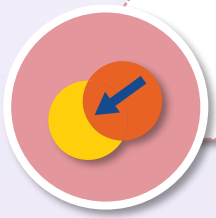
- Trust relationships are an administration and communication link between two domains
- This enables subjects in a domain to be authenticated and authorized to access resources in another domain
- Trust relationships can represent one of the main vulnerabilities in assess control and federated access design
- Administrators must be diligent in the proper configuration
  - This has historically been a difficult and vulnerable aspect of SSO and federation services
  - Using infrastructure as code and other templates is desirable
- Cloud providers will offer various managed services to assist with the trusted federation between identity and service providers

Types of Trusts



1-way (one-way) trusts

2-way (two-way) trusts

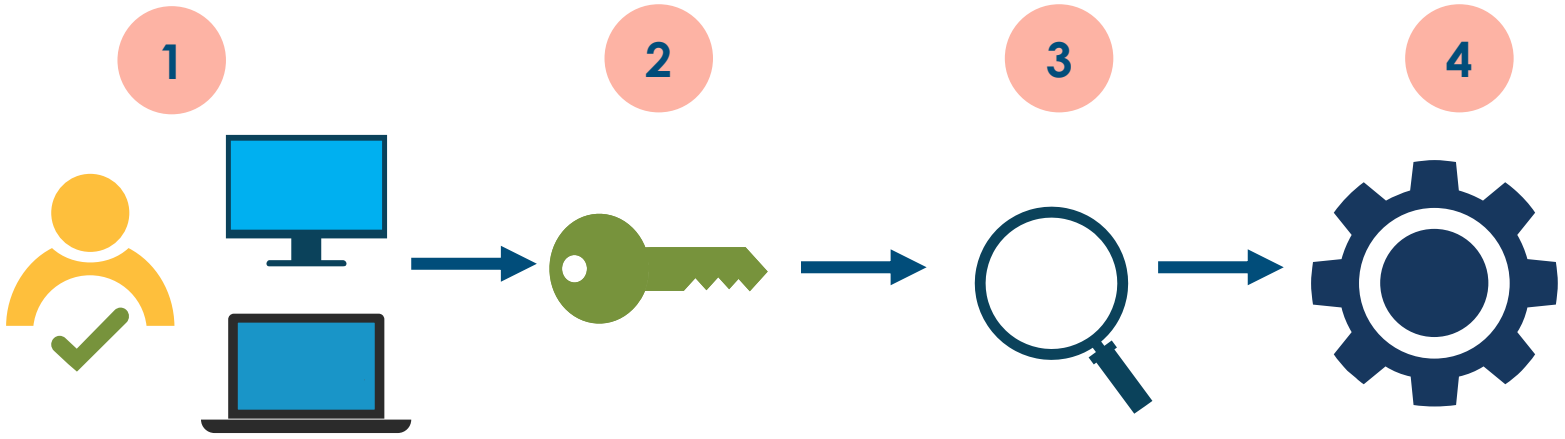


Transitive trusts

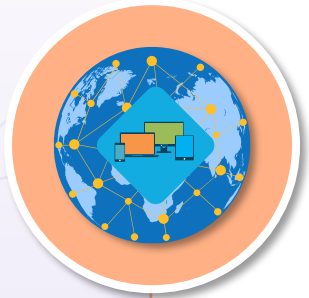
Zero Trust

- Zero Trust is a network security model based on stringent identity verification processes
- The framework demands that only authenticated and authorized users and devices can access applications and data while protecting those entities from advanced Internet threats
- This model was first introduced by an analyst at Forrester Research
- It has rapidly become vital for modern digital transformation, IoT, and embedded devices (SCADA) used on enterprise networks

Zero Trust


1
2
3
4
Never trust, always verify
Least privilege and default deny
Full visibility and inspection
Centralized management

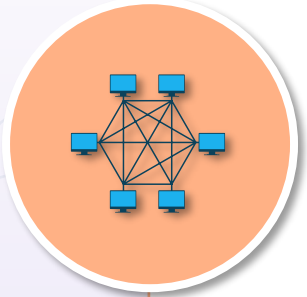
Internet



- According to NIST, the Internet is "The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share (a) the protocol suite specified by the Internet Architecture Board (IAB) and (b) the name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN)."
- The **dark web** is a part of the Internet that is not visible to search engines and involves using anonymizing browsers, such as Tor, the Invisible Internet Project (I2P), and Subgraph OS to be accessed

CSRC Content Editor, “Internet - Glossary,” CSRC, accessed September 2, 2021, https://csrc.nist.gov/glossary/term/internet.

Intranets



- According to NIST, an intranet is "a computer network, especially one based on Internet technology, that an organization uses for its own internal (and usually private) purposes and that is closed to outsiders."
- It is an internal hub (e.g., Microsoft SharePoint) used by enterprises to store vital inside information, communicate with employees, increase stakeholder participation, modernize key processes, and encourage team collaboration
- Intranets can be used to provide employee corporate profiles (internal Facebook), support human resources, coordinate extra-curricular activities and events, and improve corporate morale

CSRC Content Editor, “Intranet - Glossary,” CSRC, accessed September 2, 2021, https://csrc.nist.gov/glossary/term/intranet.

Extranets

- According to NIST, an extranet is "a computer network that an organization uses for application data traffic between the organization and its business partners"
- Several examples of extranets would include
  - communication links to strategic partners
  - links between research partnerships
  - government and military contracts
  - high-speed connections and VPN connections to cloud service providers and Software as a Service (SaaS) offerings
  - community cloud deployments (medical, financial, insurance, industrial supply chain)

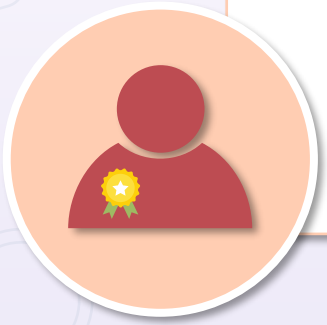
CSRC Content Editor, “Extranet - Glossary,” CSRC, accessed September 2, 2021, https://csrc.nist.gov/glossary/term/extranet.

Systems Security Certified Practitioner (SSCP)

Identity Management and Access Control Models

Identity Authorization

- Authentication must occur even if it is open or anonymous
- Authorization (AuthZ) always follows authentication (AuthN) and is optional, technically speaking
- Authorization is the act of determining that an entity is entitled to access a resource in question



AuthN vs. AuthZ

- Consider a scenario where you ask a friend to care for your pet cat while the family is away on vacation
- That person will likely need
  - **authentication** in the form of a key and an alarm code (dual-factor), allowing them to enter the house and disable the alarm system
  - **authorization** in the form of permission to access the kitchen cupboard that stores the pet food
    - The person does not have permission to go into the master suite for a quick nap and a soak in the jacuzzi tub

Authorization

- Authorization also enforces what an authenticated entity (subject) can do with or to an object
  - OS or DS permissions
  - Acceptable use policies
  - Tokens
  - Firewall rules
  - Security committee or team
  - Physical controls (security guards, entry and exit, mantraps, etc.)

Identity Proofing

- Proofing is a vital aspect of identity management where requirements ensure that the claimed identity is the actual real-life identity of the subject attempting to enroll with the credential service provider (CSP) and not an impostor
- This process must be fully completed before the subject engages in the biometric authentication process or receives other digital tokens or credentials
- It is often a part of step-up authentication where additional knowledge-based authentication (KBA) is performed
  - Subject answers a series of questions from public records

Identity Proofing

- Modern proofing methods enable consumers and end users to access your systems by verifying their identity using the knowledge and data they already possess
  - Reduce risk of fraud in online financial transactions
  - Allow authorized subjects enhanced access to interact with more sensitive data, information, and systems
  - Streamline proof of membership in a defined class or role, like "custodians" or "owners"
  - Verify age requirements for legal compliance
  - Increase the speed of secure digital transactions
  - Provision digital wallets with persistent identity verification

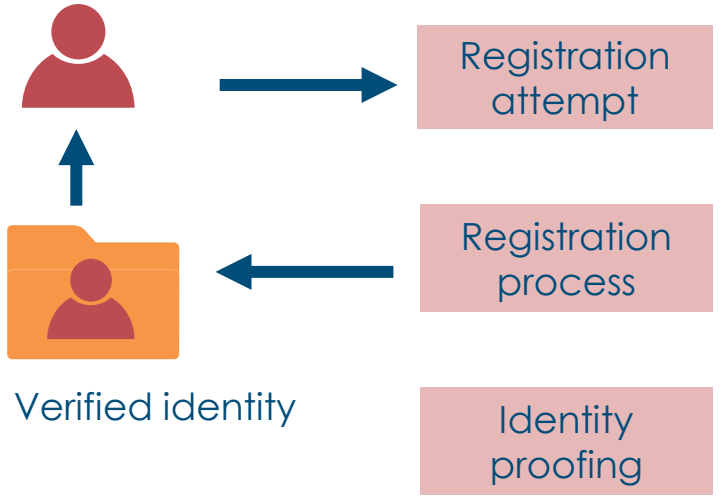
NIST Proofing Requirements

The credential service provider (CSP) shall collect the items below from the applicant

1. One piece of superior or strong evidence if the evidence's issuing source, during its identity proofing event, confirmed the claimed identity by collecting two or more forms of superior or strong evidence and the provider validates the evidence directly with the issuing source; OR

2. Two pieces of strong evidence; OR

3. One piece of strong evidence plus two pieces of fair evidence



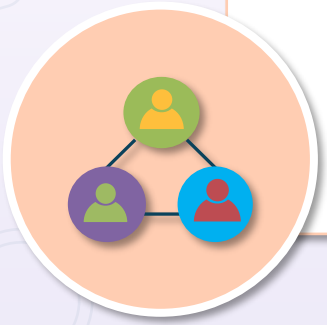
Identity Provisioning

- A digital identity is some unique identification that can be used to identify some person or entity (organization, application, device) in an identity provider, such as a directory service or database
- The unique identifier could be a SID, PIN, employee ID number, code, or credential pair, among others
- Provisioning (or onboarding) involves the assignment of this object to a subject

Identity Provisioning

- Simply put, identity provisioning is the process of creating, managing, and deleting (de-provisioning) digital identities in a computer system
- Typically, a new hire will automatically have an account created that is populated with attributes and granted permissions directly or based on some group membership or sensitivity level
- From here, they will log in to all authorized applications, systems, and databases, including external trusting service providers

Automated Provisioning



- Automated identity configuration and provisioning should enable the creation, modification, and deletion of user and system accounts across a wide variety of services and applications
- Examples: Microsoft Active Directory, Microsoft Office 365, Azure, SAP, and Salesforce

De-provisioning

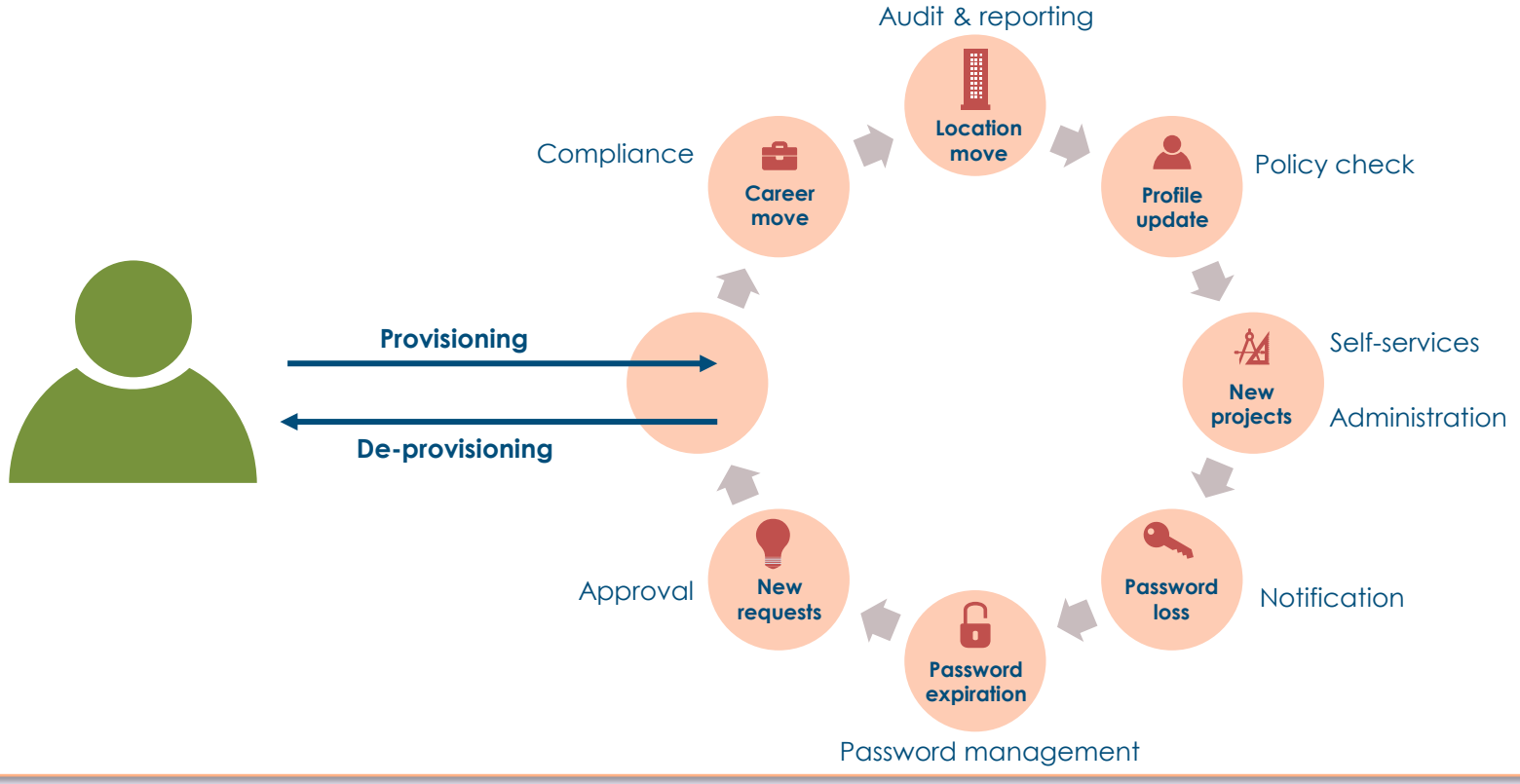
Offboarding

- De-provisioning does not merely involve the proper deletion of identity accounts
- The system should also be able to handle changes such as
  - transfers to other divisions or units
  - promotions and demotions
  - temporary suspension of account
  - changes due to mergers and acquisitions, and
  - changes with service providers

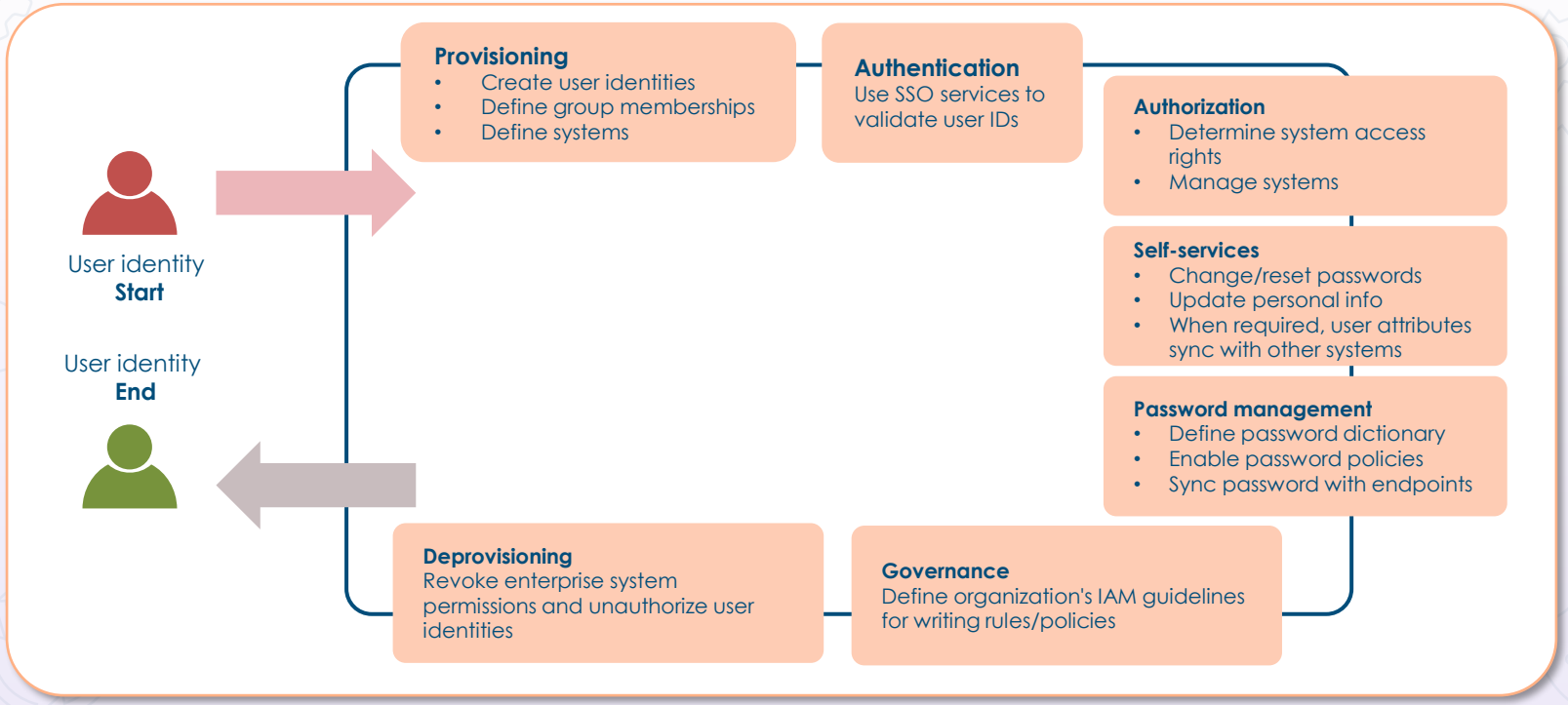
Identity Maintenance

- Maintenance usually involves establishing automatic connectors to new service providers and trusted federation scenarios
- Visibility tools and assessments should be used to discover "scope creep" and "privilege creep"
- Maintaining an identity management solution involves continual improvement initiatives

Sample 1: Identity Management Lifecycle



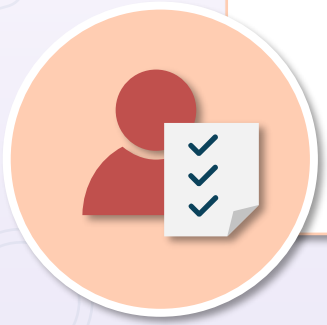
Sample 2: Identity Management Lifecycle



Identity Entitlement

- It helps to think of an entitlement as a form of permission slip with assertions added
- For example, if you want a new employee to be given an Active Directory account when they are added to your human resources system, the user must have a permission slip, or entitlement, for the Active Directory account

Identity Entitlement



- Identity entitlement often involves the temporary granting of privilege escalation (elevation) to data, applications, or services
- This may entail obtaining a temporary "clearance" to access a file (read-up) in a mandatory access model
- In most automated systems, a service desk ticket, workflow, and approval are often involved

MAC According to NIST

"MAC is an access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is **constrained** from doing any of the following:

(i) passing the information to unauthorized subjects or objects

(ii) granting its privileges to other subjects

(iii) changing one or more security attributes on subjects, objects, the information system, or system components

(iv) choosing the security attributes to be associated with newly-created or modified objects, or

(v) changing the rules governing access control"

CSRC Content Editor, "Mandatory Access Control (MAC) - Glossary," CSRC, accessed Sept 6, 2021, https://csrc.nist.gov/glossary/term/mandatory_access_control.

Mandatory Access Controls

- A Mandatory Access Control (MAC) model uses a strict set of established sensitivity levels and access controls for integrity and confidentiality based on classifications
- These are mathematical models used in high-security environments, like military, government agencies, and enterprises involved with sensitive data and activities
- Typically, state machine and information flow models are designed by a security team or steering committee as opposed to an administrator or asset owner

Discretionary Access Controls (DAC)

- The DAC policy is enforced over all entities so that a subject being granted access can
  - pass the information to other subjects or objects
  - grant its privileges to other subjects
  - change security attributes on subjects, objects, information systems, or system components
  - choose the security attributes to be associated with newly-created or revised objects; or
  - change the rules governing access control
- Discretionary Access Control (DAC) models involve control and management by the owner/creator of the object
- DAC leaves a certain amount of access control to the discretion of the object's owner – or anyone else who is authorized to control the object's access
- The opposite of a MAC model in that the owner can determine who should have access rights to an object and what those rights should be

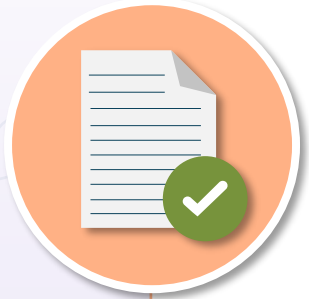
Role-based Access Controls (RBAC)

NIST: "Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role).

Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals."

CSRC Content Editor, "RBAC - Glossary," CSRC, accessed Sept 6, 2021, https://csrc.nist.gov/glossary/term//rbac.

Rule-based Access Controls

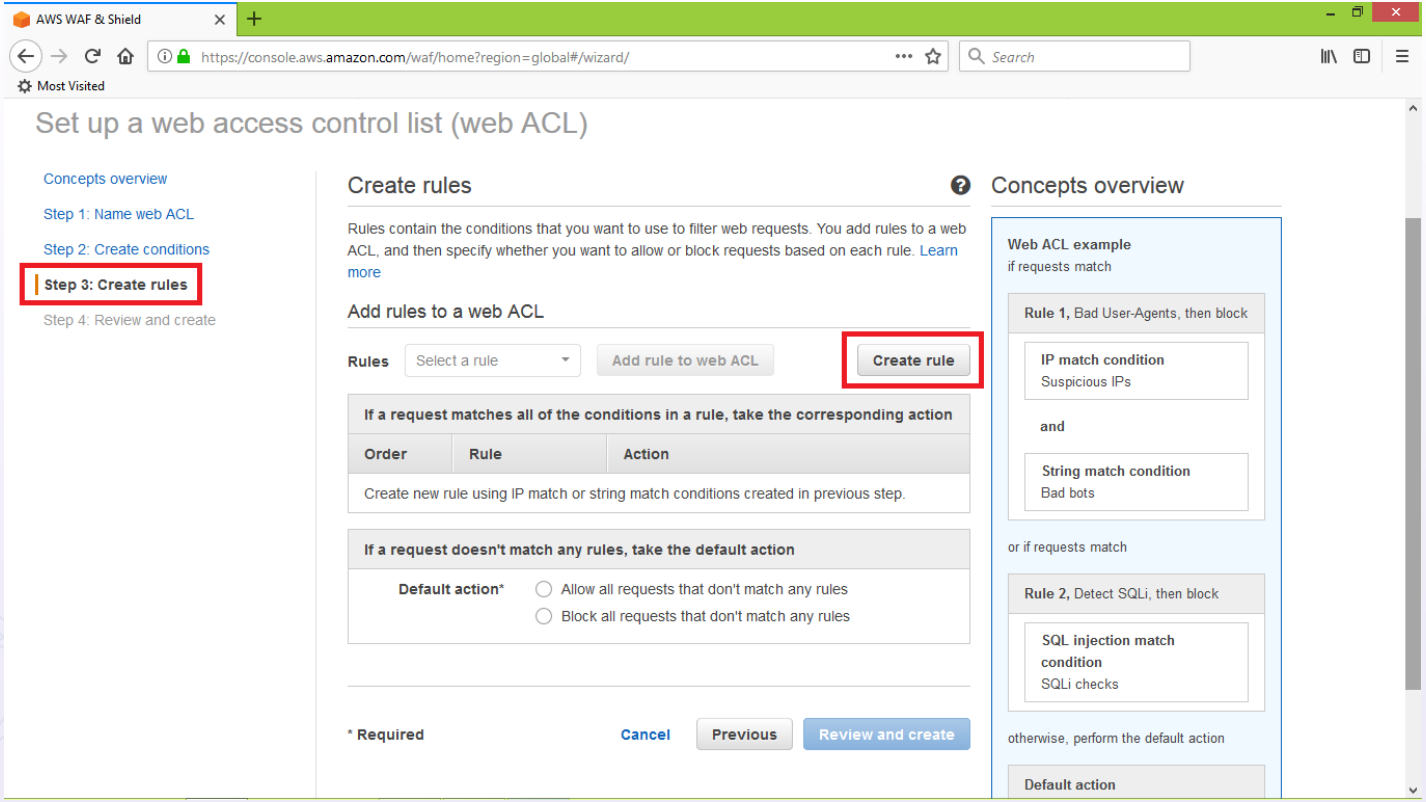


- With Rule-based (or Rules-based) Access Control, access is permitted or denied to resource objects based on a set of rules defined by a system or network administrator
- As with DAC, access properties are stored in Access Control Lists (ACLs) associated with each resource object
- When a certain group or user account attempts to access a resource, the operating system checks the rules contained in the ACL for that object
- Examples of Rules-based Access Controls are time-based ACLs, router infrastructure ACLs, static (stateless) firewalls, and AWS network ACLs

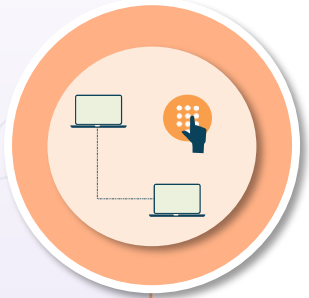
Sample Inbound Access Rule

Protocol	Port	Source	Destination	Name	Action
UDP	53	Any	192.16.10.200	Allow DNS queries	Allow
TCP	80,443	Any	192.168.10.201	Allow HTTP and HTTPS	Allow
TCP	3,389	IT_Admin_IP_Range	Any	Allow RDP	Allow
Any	Any	Any	Any	Default	Deny

AWS WebACL


AWS WAF & Shield
https://console.aws.amazon.com/waf/home?region=global#/wizard/
Search
Most Visited
Set up a web access control list (web ACL)
Concepts overview
Step 1: Name web ACL
Step 2: Create conditions
Step 3: Create rules
Step 4: Review and create
Create rules
Rules contain the conditions that you want to use to filter web requests. You add rules to a web ACL, and then specify whether you want to allow or block requests based on each rule. Learn more
Add rules to a web ACL
Rules
Select a rule
Add rule to web ACL
Create rule
If a request matches all of the conditions in a rule, take the corresponding action
Order
Rule
Action
Create new rule using IP match or string match conditions created in previous step.
If a request doesn't match any rules, take the default action
Default action*
Allow all requests that don't match any rules
Block all requests that don't match any rules
* Required
Cancel
Previous
Review and create
Concepts overview
Web ACL example
if requests match
Rule 1, Bad User-Agents, then block
IP match condition
Suspicious IPs
and
String match condition
Bad bots
or if requests match
Rule 2, Detect SQLi, then block
SQL injection match condition
SQLi checks
otherwise, perform the default action
Default action

Bell-LaPadula



- The Bell–LaPadula Model is a state machine methodology developed by David Elliott Bell and Leonard J. LaPadula
- It is used for imposing access control in military and government agency systems and applications
- It was originally used to formalize the U.S. Department of Defense (DOD) multilevel security policy
- All Mandatory Access Control (MAC) systems are based on the Bell-LaPadula model because of its multilevel security – and it's been adopted by most government agencies

Bell-LaPadula

The model focuses on ensuring that subjects with different clearances are appropriately authenticated by having the required security clearance, need-to-know, and formal access approval before accessing an object under different classification levels

The Bell-LaPadula Ruleset

Simple Security rule: a subject at a given security level cannot read data that resides at a higher security level (no read-up rule)

Strong Star Property rule: a subject who has read and write capabilities can only perform those functions at the same security level – nothing higher and nothing lower

Bell-LaPadula Confidentiality

Tranquility principle: subject and objects cannot change their security levels once they have been instantiated (created)

Star Property (*) rule: a subject at a given security level cannot write information to a lower security level (no write-down rule)

Biba

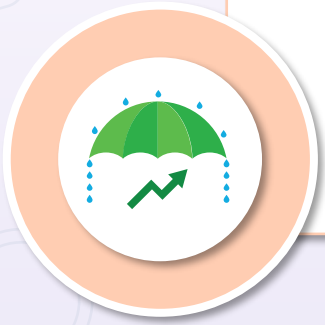
Integrity Model

- Biba was developed after Bell-LaPadula and uses a lattice of integrity levels (unlike Bell-LaPadula)
- It's also an information flow model, as it is most concerned with data flowing between levels
  - Simple integrity rule (no read-down): states that a subject cannot read data from a lower integrity level
  - Star integrity rule (no write-up): states that a subject cannot write data to an object at a higher integrity level
  - Invocation property: states that a subject cannot invoke (call upon) a subject at a higher integrity level

Systems Security Certified Practitioner (SSCP)

The Risk Management Process

Defining Risk



- Inherent (total) risk
  - Risk the organization faces if safeguard is not implemented
- Residual risk
  - Risk that remains once safeguard is in place
- Residual = inherent risk − safeguards (controls)

Structured vs. Unstructured Threats

Structured

- Planned
- Organized
- Persistent
- Multi-phased
- Can be internal or external
- Exploit kits, zero-days, modules, and ransomware

Unstructured

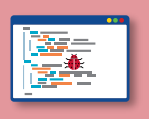
- Accidental
- Non-malicious
- Drive-by web surfing
- No AUP
- Poor awareness
- Email and webmail
- USBs and personal electronics

Indicators of Compromise (IoC)

These are network or host-based cyber observables

Forensic artifacts of an incursion or disturbance

A measurable event or stateful property in the cyber domain



Registry entries, compressed and encrypted files on disk and in-memory, etc.

Risk Matrix

		Event type								
		Accidental Leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Intent	**Nonhostile**									
	Reckless insider	X			X			X		
	Untrained/distracted insider	X			X			X		
	Outward sympathizer	X			X					
	Unknown (nonhostile or hostile)									
	Supplier	X	X	X	X	X		X		
	Partner	X	X	X	X	X		X		
	Hostile									
	Irrational individual	X			X		X		X	X
	Thief		X	X		X	X			
	Disgruntled insider	X	X	X	X	X	X	X	X	X
	Activist		X		X	X	X	X	X	
	Terrorist						X		X	X
	Organized crime		X	X		X	X	X		
	Competitor		X			X		X	X	
	Nation state		X			X		X	X	

Tim Casey, "A Field Guide To Insider Threat," https://www.nationalinsiderthreatsig.org/itrmresources/Intel%20Insider%20Threat%20Field%20Guide.pdf, (2015).

Creating a Risk Ledger (Register or Log)

- A compilation of information related to vulnerabilities, risks, and countermeasures
  - Repository of identified risks, impact, scenarios, and potential responses
- Populated from after-action reporting, lessons learned, case studies, and assessments
- Often represented as a scatter plot/table from a database or spreadsheet
- Fulfills regulatory compliance

Identified Risks	Root Causes	Probability and Impact	Ranking	Categories	Priorities	Time and Cost Objectives	Potential Responses	Risk Owners	Assumptions

Risk Assessment Document

- Record the processes used to identify probable threats and propose subsequent action plans if the hazard occurs
- Document assets at risk (people, buildings, information technology, utility systems, machinery, raw materials, and finished goods)
- Many templates and prototypes available online

Risk Assessment Document Inputs

Hazard identification

Hazards

- Fire
- Explosion
- Natural hazards
- Hazardous materials spill or release
- Terrorism
- Workplace violence
- Pandemic disease
- Utility outage
- Mechanical breakdown
- Supplier failure
- Cyber attack

Property & magnitude

Vulnerability assessment

Assets at risk

- People
- Property, including buildings and critical infrastructure
- Supply chain
- System and equipment
- Information technology
- Business operations
- Reputation of or confidence in entity
- Regulatory and contractual obligations
- Environment

Vulnerability

Impact analysis

Impacts

- Casualties
- Property damage
- Business interruption
- Loss of customers
- Financial loss
- Environmental contamination
- Loss of confidence in the organization
- Fines and penalties
- Lawsuits

Assessing Vulnerability

Begins with the definition

- It should be quantified as a percentage of probability and not just a vague list of "scary things"
- The likelihood that a threat agent's actions will result in a loss (frequency and magnitude)
- It can be a derived value from the threat capability of actors combined with the resistance of existing security controls

Assessing Vulnerability

Asset assessment and labeling

- All client and server operating systems and versions/builds
- Posture of patches, updates, and security fixes
- Browsers and types of endpoints
- Methods of access – wired, wireless, VPN, and remote teleworkers
- Control types and categories
- Access control methodologies (2FA)

Vulnerability Information Gathering

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps
- NetFlow collection
- Security information and event management (SIEM) systems
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based visibility tools
- Machine learning and artificial intelligence data analysis

Vulnerability Databases

- A collection and distribution of information about exposed computer security vulnerabilities
- Typically, it categorizes and defines an identified vulnerability (and variants) with a timeline and coding
- The database usually assesses the potential impact on affected systems based on a qualitative scale (1-5)
- May also provide mitigations, workarounds, and updates

Vulnerability Databases

These are two of the most used resources

Common Vulnerabilities and Exposures (CVE)

- A list of entities from MITRE.org that represents publicly known cybersecurity vulnerabilities
- Consists of an ID number, description, and public references
- Used by the National Vulnerability Database (NVD)

Common Vulnerability Scoring System (CVSS)

- Open standard for weighing the severity of computer system vulnerabilities
- Uses a uniform and consistent scoring method ranging from 0 to 10, with 10 being the highest severity

Vulnerability Databases

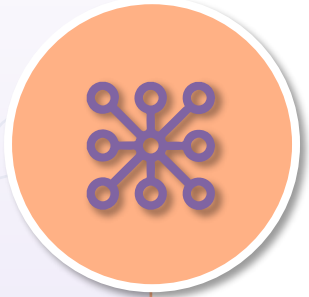
- Common Vulnerabilities and Exposures (CVE) with MITRE
- National Vulnerability Database with NIST
- ISS X-Force database
- Symantec/SecurityFocus BID database
- @Risk from SANS.ORG

Vulnerability Scanning

HTTP/S is the most common traffic

- Web application vulnerability scanners are most common due to heavy usage of HTTP (e.g., Burp Suite and OWASP ZAP)
- Automated tools can scan web applications and look for these security vulnerabilities:
  - cross-site scripting
  - cross-site request forgery
  - SQL and command injection
  - path traversal, and
  - insecure server configuration

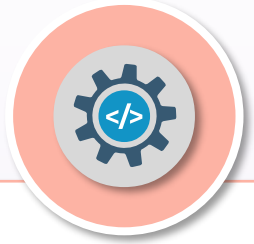
Open-source Intelligence (OSINT)



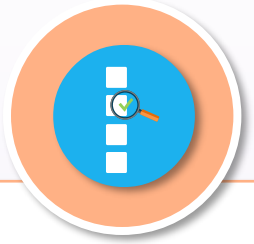
- OSINT is any data or information concerning an individual or organization that can be collected legally from free public sources
- Usually information found on the Internet but can be sourced from books or reports in a public library, articles in a newspaper/magazine, statements in a press release, and FOIA reports
- Can be gathered using tools such as Maltego, sharing centers, and code repositories, such as GitHub, among others

Threat Intelligence Sources

Automated Indicator Sharing (AIS) – Cybersecurity and Infrastructure Security Agency (CISA) capability, enables the real-time exchange of machine-readable cyber threat indicators



Structured Threat Information Exchange (STIX) – standardized language developed by MITRE (in a collaborative way) to represent structured information about cyber threats

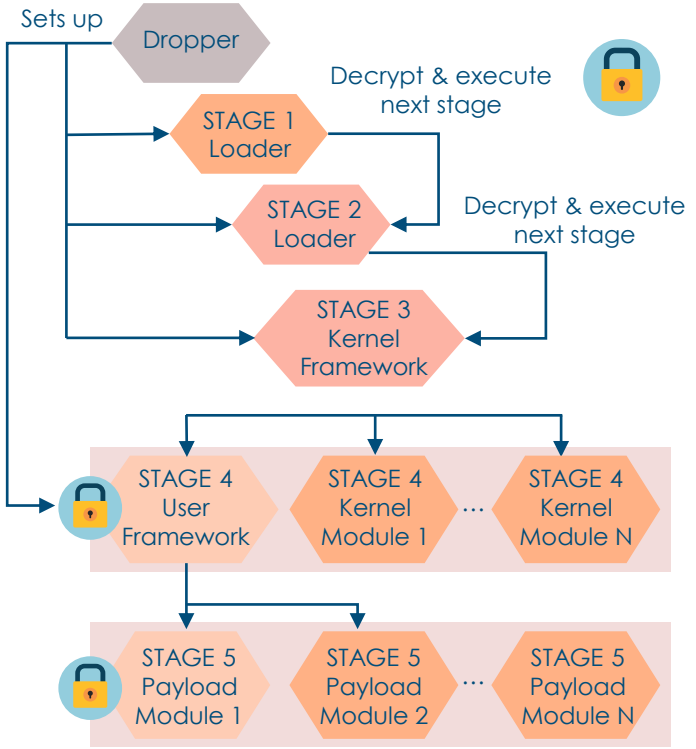


Trusted Automated eXchange of Indicator Information (TAXII) – transport vehicle for services and message exchanges to allow sharing of information about cyber threats

Predictive analysis and threat maps – use cutting-edge machine learning engines and artificial intelligence tools to predict future threats

Threat Modeling

- Involves creating an abstraction of a system to identify risk and probable threats (private cloud/sandboxing)
- When cyberthreat modeling is applied to systems being developed, it can lower vulnerabilities and risk
- With the widespread adoption of threat intelligence technologies, most enterprises are trying to adopt a threat-focused approach to risk management
- Provides visibility, increased security awareness and prioritization, and understanding of posture



Threat Modeling Methodologies

STRIDE and PASTA are common threat modeling methods

STRIDE stands for: Spoofing of user identity, Tampering, Repudiation, Information disclosure, Denial of service, and Elevation

It is a threat model initially developed by Microsoft in 1999 that classifies the attacker's prevalent goals

PASTA stands for Process for Attack Simulation & Threat Analysis

It is a risk-oriented method that endeavors to link business objectives to technical requirements

PASTA has seven stages, with the goal of delivering a dynamic process ranging from identification and enumeration to scoring

Threat Modeling Methodologies

Trike and VAST are two other common modeling solutions along with DREAD

Trike is a technique frequently used as a risk management tool during security audits

It is a unique, open-source threat modeling method focused on enhancing the security auditing process from a cyber risk management perspective

VAST is Visual, Agile, & Simple Threat Modeling

It attempts to address the limitations of other threat methodologies by using a more practical approach

Founding principle is that, in order to be effective, threat modeling must scale across the infrastructure and entire DevOps portfolio

It has separate operational and application models

Qualitative Risk Analysis

- The most common method used in risk and security
- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels
  - Expert judgement
  - Best practices
  - Experience
  - Intuition
- Often involves interviewing people (Delphi) regarding assets, known risks, known vulnerabilities, common threats, and historical impacts

Qualitative Heat Map

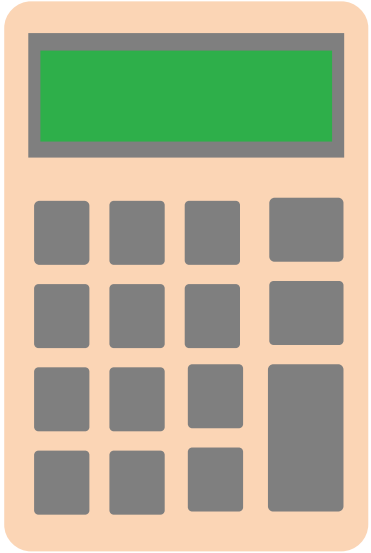
			Impact				
Likelihood			Negligible	Minor	Moderate	Critical	Disastrous
			1	2	3	4	5
	Frequent	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

Quantitative Risk Analysis

- Scientific/mathematical approach to getting monetary and numeric results based on the following:
  - asset values, and
  - impact and magnitude
    - severity of incident
- Probability and likelihood of occurrence
  - Threat frequency
- Costs and effectiveness of safeguards
- Probabilities based on percentages and calibrated estimation
- A semi-quantitative approach is preferable to qualitative

Classic Quantitative Analysis (Whitman)

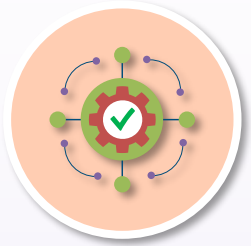
- **AV (asset value)**
  - Value of the asset according to the organization
- **EF (exposure factor)**
  - Percentage of asset loss caused by identified threat
- **SLE (single loss expectancy)**
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- **ARO (annualized rate of occurrence)**
  - Estimated frequency the threat will occur within a single year
- **ALE (annualized loss expectancy) = (SLE * ARO)**



Classic Quantitative Analysis (Whitman)

Risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15,000	100%	$15,000	0.1	$1,500
SRV_2	Fire	$20,000	100%	$20,000	0.1	$2,000
SRV_1	Flood	$15,000	100%	$15,000	0.0001	$1.5
SRV_2	Flood	$20,000	100%	$20,000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15,000	10%	$1,500	365	$547,500
SRV_1	Virus (with AV software)	$15,000	10%	$1,500	1	$1,500

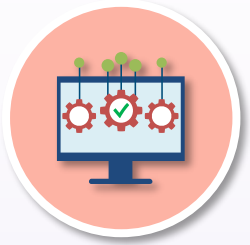
Security Control Frameworks



ISO/IEC 27000

Very broad, flexible, and mature framework focused on information security

The security equivalent of the more widely known ISO 9000 quality standards for manufacturers



NIST Special Publication 800-53 Revision 4

Has evolved over 20 years and could be seen as the "father figure" for others

Mature and comprehensive and can be aligned to other ISO standards, such as ISO 9000 quality management

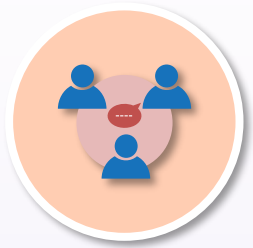
Is very good for large businesses, as well as those with a US connection

COBIT 5

Control Objectives for Information and Related Technology (COBIT) was created by the Information Systems Audit and Control Association (ISACA)

A framework and supporting tool set that allows managers to bridge the gap between control requirements, technical issues, and business risks

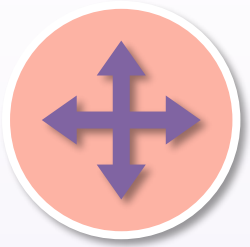
Security Control Frameworks



AGATE

Atelier de Gestion de l'ArchiTEcture des systèmes d'information et de communication (AGATE)

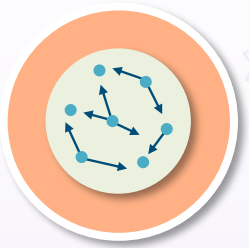
A framework for modeling computer or communication systems architecture



IDABC

Interoperable Delivery of European eGovernment Services to Public Administrations, Businesses and Citizens (IDABC)

An EU program launched in 2004 that promotes the correct use of information and communication technologies (ICT) for cross-border services in Europe



OBASHI

OBASHI provides a method for capturing, illustrating, and modeling the relationships, dependencies, and data flows between business and information technology assets and resources in a business context

NIST Cybersecurity Framework

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset management • Business environment • Governance • Risk assessment • Risk management strategy	• Awareness control • Awareness and training • Data security • Info protection and procedures • Maintenance • Protective technology	• Anomalies and events • Security continuous monitoring • Detection process • Communications	• Response planning • Communications • Analysis • Mitigation • Improvements	• Recovery planning • Improvements • Communication

Center for Internet Security (CIS)

- Repository for cybersecurity best practices, tools, and threat assessment and awareness
- CIS leverages the power of a global IT community to defend public and private organizations against various cyber threats with
  - CIS Benchmarks™ – consensus-created secure configuration guidelines for hardening data, systems, and applications
  - CIS Controls® – a strict, ordered, and simplified set of cybersecurity best practices and guidelines
  - CIS SecureSuite® - membership program that offers an automated combination of CIS Benchmarks, CIS Controls, and CIS-CAT Pro into a commanding and efficient cybersecurity resource
    - CIS-CAT Pro allows users to evaluate conformance to best practices and expand compliance scores on an ongoing basis

Cloud Security Alliance (CSA)

- An organization committed to defining and raising awareness of guidance for organizations of all types and sizes to guarantee a secure cloud computing experience
- Offers the Cloud Control Matrix (CCM) Version 4 to ensure handling of requirements stemming from
  - new cloud technologies
  - new controls and security responsibilities
  - necessary auditability of controls, and
  - interoperability and compatibility with other standards

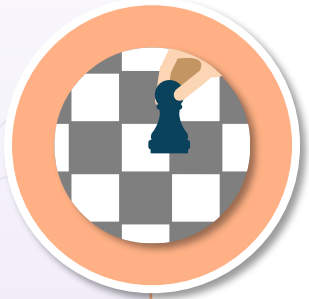
Benchmarks

- Improves an organization's information security management by establishing a standard
- CIS Benchmarks™ are best practices to securely configure various systems and are available for more than 140 technologies
- Established using a special method constructed from an accord of global cybersecurity experts from across the globe
- CIS Benchmarks™ are security configuration guides created by government, business, industry, and academia

Risk Treatment: Accept

- Risk acceptance
  - Do not implement any safeguards
  - Justification in writing is often required
- This can also be the process of "ignoring" the risk
- Examples include
  - only having one supplier or vendor for hardware or services based on their uptime reputation
  - leasing a facility in a 100-year flood zone, and
  - deciding not to add a cyber security rider to your existing business insurance policy

Risk Treatment: Transfer



- Risk transference is also referred to as risk sharing
- Involves passing off risk to a third-party or shared party
- Examples include
  - purchasing an insurance policy or additional cyber insurance
  - using a shared responsibility model with a cloud service provider, and
  - leasing a warm/cold disaster recovery facility with another similar business that is several miles away

Risk Treatment: Mitigate

- Risk mitigation involves the strategic and tactical implementation and deployment of an array of technical, administrative, and physical controls to reduce risk to an accepted level
- Enterprises will Implement safeguards that will eliminate or reduce risk exposure – risk may exist, but impact is reduced
- Examples include
  - implementing endpoint protections, such as Palo Alto Traps
  - upgrading the edge firewall appliance
  - using a threat management service from a cloud provider or managed security service provider (MSSP), such as Fortinet, and
  - hiring armed security guards

Risk Treatment: Avoid

- Risk avoidance involves deciding not to undertake actions or engage in activities that introduce or increase risk
- Examples include
  - not processing and storing credit card information of customers on premises
  - using a NoSQL database solution instead of Microsoft SQL for the web service back end
  - not using any clear-text protocols, such as HTTP, LDAP, FTP, SMTP, or telnet, and
  - not storing sensitive data in a personal cloud service, such as Dropbox

Regulatory Issues

Regulatory

- HIPAA
- SOX
- PCI-DSS
- General Data Protection Regulation (GDPR)

Non-regulatory

- NIST
- ITIL 4
- ISO/IEC
- COBIT5
- CIS
- ISACA

Legal Agreements

- **BPA – business partners agreement**
  - Agreement between partners for business purposes
  - Purpose of business
  - Contributions of each partner
  - Rights/responsibilities of each partner
- **SLA – service-level agreement**
  - Official commitment between provider and consumer
  - Defines quality, availability levels, responsibilities, support, and conflict resolution
- **OLA – organizational-level agreement**
  - The internal version of SLA

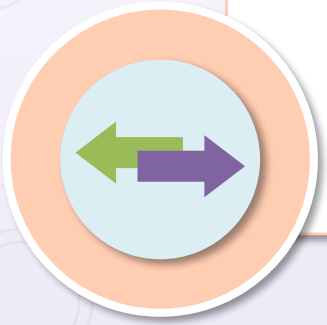
Legal Agreements

- **ISA – interconnection security agreement**
  - Documents and formalizes the connections between two organizations
  - Defines security and safeguards for the connections
  - Examples: AWS Direct Connect and Azure ExpressRoute
- **MOU/A – memorandum of understanding or agreement**
  - Defines pre-agreement parameters and commitments between two parties
  - Generally non-binding declaration of intent or responsibilities of each party

Licensing Issues

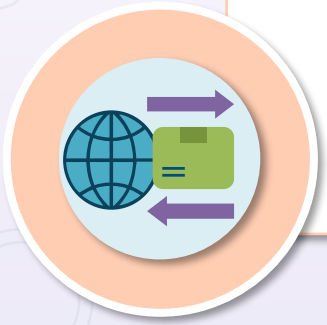
- Contractual license agreements
  - Written contracts and digitally-signed
- Shrink-wrap license agreements
  - Written on packaging
- Click-through license agreements
  - During install
- Cloud service provider license agreements
  - Depends on managed service

Import and Export Issues



- Mandates began during the Cold War to control transborder flow
  - The International Traffic in Arms Regulations (ITAR) control the export of items that are specifically designated as military and defense items
  - The Export Administration Regulations (EAR) cover a broader set of items
- Supply chain security is critical when engaged in import/export activities

Import and Export Issues



- Cybersecurity-related trade conflict is an emerging global phenomenon
  - Countries can do nothing, develop import trade barriers, restrict procurement, develop norms, or escalate conflict
  - Companies can make recommendations, comply, avoid, collaborate, or compromise based on the situation
- Encryption export controls are a key issue
  - The Department of Commerce's Bureau of Industry and Security sets forth regulations on the export of encryption products outside the United States

Security Awareness and Training

- CBT and streaming webinars
- Email bulletin reminders
- Classroom sessions
- Phishing campaigns
- Gamification of training
- Capture the flag exercises
- Self-enabled interactive websites
- Posters, coffee mugs, and mouse pads

Security Awareness and Training

- Organization mission, charter, and vision
  - All applicable policies and procedures
  - Example security topics:
    - password and badge policy (MFA)
    - tailgating/piggybacking
    - social engineering and phishing awareness
    - data loss prevention, and
    - governance and regulations

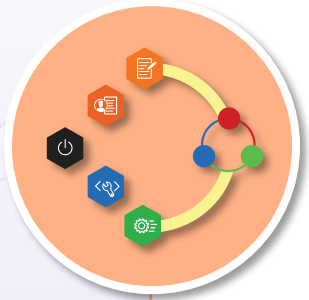
Role-based Security Training

- General endpoint users
- Data/system owners
- Data/system custodians and stewards
  - Custodians = technical
  - Stewards = business
- Administrators
- Privileged users
- Executive users
  - Executive management
  - C-suite or C-team
  - Board of directors

Systems Security Certified Practitioner (SSCP)

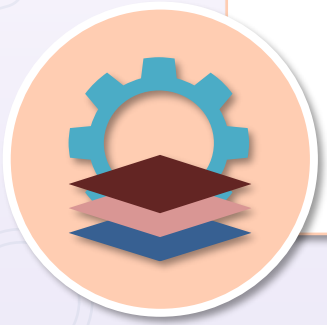
Security and Vulnerability Assessment

Security Testing with SCA and ST&E



- Security testing attempts to verify that an implementation protects data and maintains functionality as intended
- Security Control Assessment (SCA) is a formal evaluation of a system against a pre-defined set of controls
- Performed with, or independently of, a full security test and evaluation (ST&E), which is carried out as part of an official security authorization
- Often conducted as part of an official accreditation or certification process

Security Testing with SCA and ST&E



- SCA and ST&E will appraise the operational plan (or planned implementation) of controls
- Results in a risk assessment report that represents a gap analysis, documenting the system, application, or data risk
- Tests conducted should include audits, security reviews, vulnerability scanning, and penetration testing

Security Testing, Validation, and Measurement (STVM)

- At NIST, the Security Testing, Validation, and Measurement (STVM) Group's testing-focused activities include
  - validating cryptographic algorithm implementations, cryptographic modules, and Security Content Automation Protocol (SCAP)-compliant products
  - developing test suites and test methods
  - providing implementation guidance and technical support to industry forums, and
  - conducting education, training, and outreach programs

Static Application Security Testing (SAST)

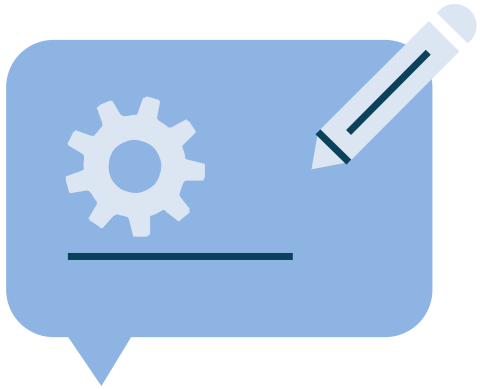
- SAST is commonly defined as a white-box test, where an analysis of the application source code, byte code, and binaries is carried out by the application test without executing the code
- It is used to find coding errors and omissions that are symptomatic of security vulnerabilities
- SAST is often used as a test method when the tool is under development – earlier in the development life cycle
- It can be used to find SQL injection attacks, cross-site scripting errors, buffer overflows, unhandled error conditions, and probable back doors into the application

Dynamic Application Security Testing (DAST)

- Due to the nature of SAST being a white-box test tool, SAST typically delivers more comprehensive results than those found using DAST
- DAST is considered a black-box test, where the tool must find distinct execution paths in the application being analyzed
- Unlike SAST, which analyzes code that is not running, DAST is used against applications in their running state
- It is primarily considered effective when testing exposed HTTP and HTML interfaces of web applications
- Static and dynamic application tests work in concert to improve the reliability of applications being built and bought by organizations

Runtime Application Self Protection (RASP)

- RASP is usually employed to focus on applications that have self-protection capabilities built into their runtime environments, which have full insight into application logic, configuration, and data and event flows
- RASP prevents attacks by "self-protecting" or reconfiguring automatically without human intervention in response to certain conditions (threats, faults, etc.)



Risk Review

- Risk reviews should be conducted on a regular, scheduled basis
- Security practitioners and engineers should use tools and processes with a well-defined scope:
  - internal applications and systems
  - extensible architectures and methodology advancements and updates
  - supplier (supply chain)
  - external vendors, and
  - strategic partners
- The results will be input into the risk ledger (register)

Capability Maturity Model (CMM)

Initial (Chaotic): chaotic, ad hoc, individual heroics

Level 1

Repeatable (Implicit): process is not codified or defined and is still vulnerable to inconsistency

Level 2

Defined (Early Explicit): process is defined and documented as a standard business process

Level 3

Managed (Mature Explicit): process is controlled and can be adjusted and adapted to particular projects without measurable losses in quality

Level 4

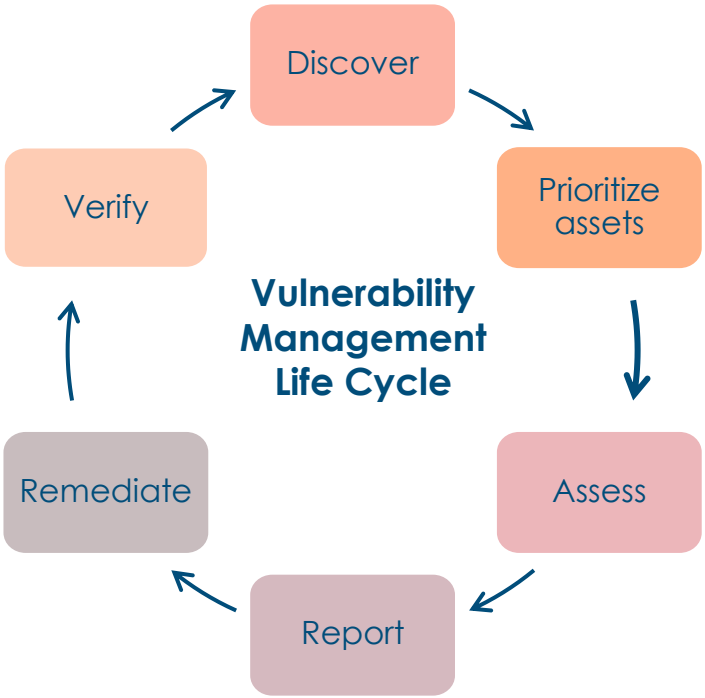
Optimized (Purely Explicit): process management includes deliberate process optimization and improvement

Level 5

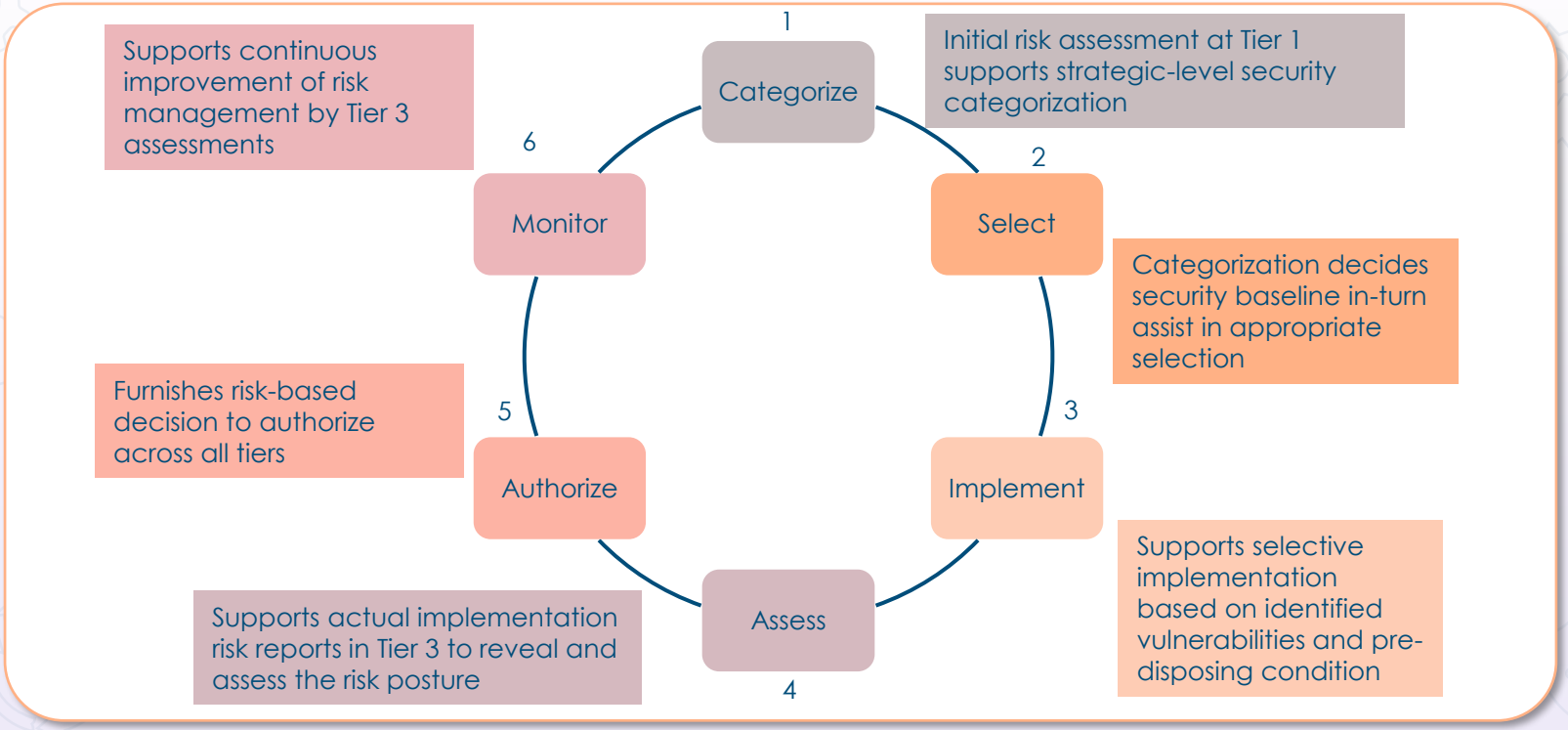
Software Assurance Maturity Model (SAMM)

- The Software Assurance Maturity Model (SAMM) is an open framework from OWASP to assist organizations in developing and deploying a secure software delivery strategy that is focused on the detailed risks facing the enterprise. The resources offered by SAMM will assist in
  - appraising the organization's current software security initiatives
  - constructing a well-adjusted software security assurance program using established iterative processes
  - establishing tangible continual improvement methodologies to a software security assurance program, and
  - defining and gauging security-related tasks throughout the enterprise

Vulnerability Management Life Cycle



NIST Risk Management Framework (RMF) Life Cycle



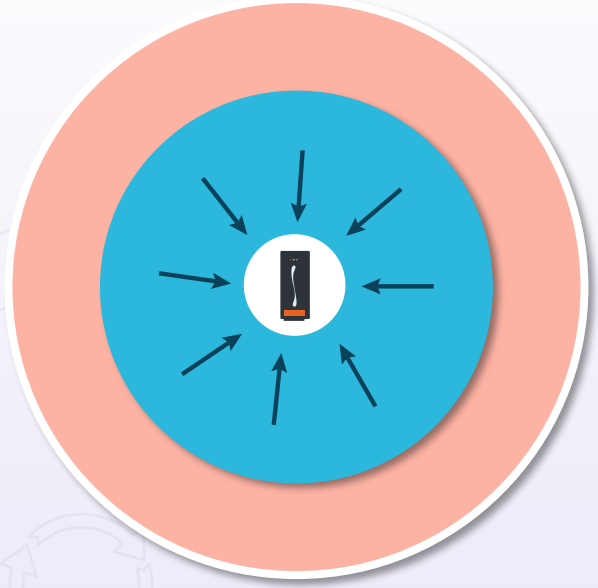
Vulnerability and Penetration Testing

- Vulnerability assessment and penetration testing both add value to supporting application and system security prior to going into production
- Vulnerability scans and tests attempt to identify and report on known vulnerabilities in a system
- Automated and manually scheduled scanning results should map to an established risk ledger (log) and risk rating combined with potential exposures and countermeasures
- Most often, vulnerability assessments are performed as white box tests, where the tester knows the application and has complete knowledge of the running environment
- Penetration testing is a process used to collect information and actively expose vulnerabilities in an application or system by conducting actual exploits and red team attacks
- Penetration testing is often a black or gray box test, where the tester assumes the attacker role with little or no knowledge of the application and must discover any security issues

Penetration Testing Frameworks

- SSAF – framework provided by Open Information Systems Security Group (OISSG), a not-for-profit organization based in London
- OSSTMM – open-source security testing created by ISECOM (Institute for Security and Open Methodologies)
- OWASP – popular methodology used widely by security professionals, created by a non-profit organization focused on advancing software security

Penetration Testing Frameworks



- PTES – Penetration Testing Execution Standard (PTES) methodology was developed to cover the key parts of a penetration test
- NIST – National Institute of Standards and Technology (NIST) provides a manual that is best suited to improve the overall cybersecurity of an organization

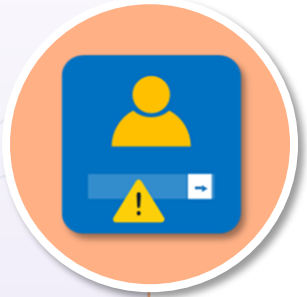
Common Web Vulnerabilities – OWASP Top 10

- A01:2021 - Broken Access Control
- A02:2021 - Cryptographic Failures
- A03:2021 - Injection
- A04:2021 - Insecure Design
- A05:2021 - Security Misconfiguration

Common Web Vulnerabilities – OWASP Top 10

- A06:2021 - Vulnerable and Outdated Components
- A07:2021 - Authentication and Identity Failures
- A08:2021 - Software and Data Integrity Failures
- A09:2021 - Security Logging and Monitoring Failures
- A10:2021 – Server-Side Request Forgery (SSRF)

Disadvantages of Open-source Software



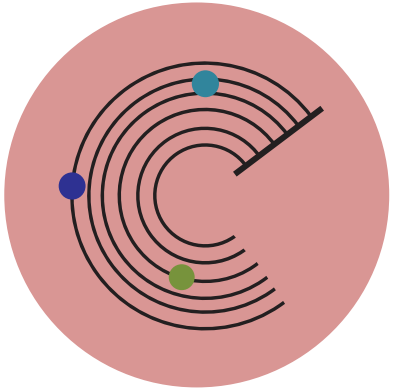
- Many enterprises and products (90% by some estimates) use at least one open-source component, often without being aware of it
- Normally, this software is built using public community collaboration and is preserved and updated on a voluntary basis
- Open-source software can be used according to a diversity of licenses, depending on what the developers have implemented
- There are over 200 types of licenses that can be used with open-source software
- Lack of warranty for its security, support, or content
- No claims or obligations to be secure

Open-source Vulnerabilities

- Open-source software often includes or demands the use of vulnerable third-party libraries, which can involve intellectual property challenges
- Lax integrations oversight and control
- Dev teams often have non-existent review processes for open-source components
- Operational inadequacies requiring additional work for proper DevSecOps
- Poor development practices and procedures
- Risks increase as developers commonly copy and paste chunks of code from open-source software
- Developers often transfer components through email or use poor repository security practices

Monitoring Source Systems and Events

- Various logs (system, application, firewall, etc.)
- Simple Network Management Protocol (SNMP) traps and informs
- NetFlow v5 and v9 collections
- Security information and event management (SIEM) systems
- Security Orchestration, Automation, and Response (SOAR)
- Next-Generation Intrusion Prevention System (NGIPS) alerts and logs
- Cloud-based ML and AI visibility/analysis
- Output from endpoint detection and response agents (Cisco AnyConnect Mobility Client, Palo Alto Traps)



Monitoring Source Systems and Events

- **Events of interest:**
  - anomalies
  - intrusions
  - indicators of compromise, such as encrypted or compressed files, registry entries, code in memory, and more
  - indicators of action of threat actor kill chain
  - unauthorized change, and
  - compliance monitoring and audit results
- Log management
- Event aggregation and correlation with SIEM and SOAR systems

SIEM

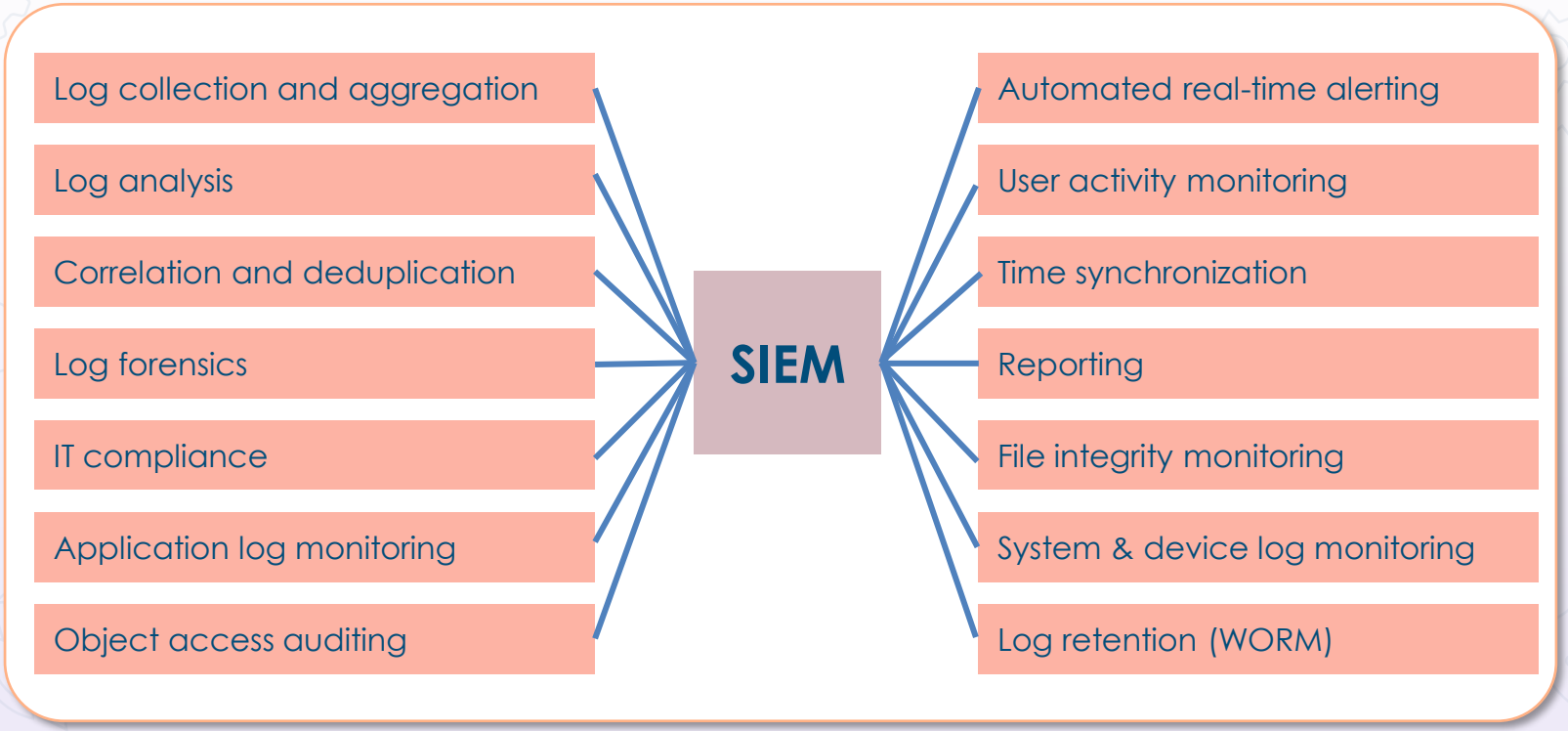
The term SIEM is a combination of security event management (SEM) and security information management (SIM)

Centralize the storage and analysis of logs and other security-related documentation to perform near real-time analysis

Send filtered data to mining, big query, and data warehousing servers in a data center or at a cloud service provider

Allow security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents

SIEM


Log collection and aggregation
Log analysis
Correlation and deduplication
Log forensics
IT compliance
Application log monitoring
Object access auditing
SIEM
Automated real-time alerting
User activity monitoring
Time synchronization
Reporting
File integrity monitoring
System & device log monitoring
Log retention (WORM)

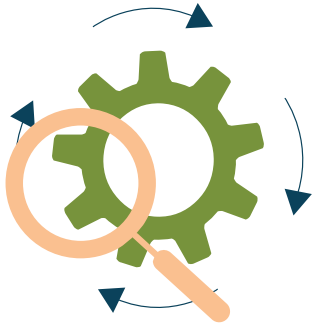
Security Orchestration, Automation, and Response (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas:
  - threat and vulnerability management
  - incident response, and
  - security operations automation
- Security automation involves performing security-related tasks without the need for human intervention
- Can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing
- You should automate if the process is routine, monotonous, and time-intensive

SOAR Components

1. SIEM use cases, categories, and rules are mapped to incident categories; these categories are then mapped to playbooks

2. Three types of playbooks:
    - Manual playbooks (series of manual tasks)
    - Semi-automated playbooks (hybrid of automated and manual subtasks)
    - Fully-automated playbooks (completely automated)



SOAR Components

3. Four types of automation
    - Defensive automation (anything that tries to prevent the threat or risk)
    - Forensic automation (anything that tries to retrieve additional evidence)
    - Offensive automation (anything pro-active that tries to investigate an asset)
    - Deception automation (anything that retrieves or adjusts deception tools)

4. Three different categories of action
    - Enrichment (adding additional CMDB or environment data)
    - Escalation (email, ticket escalation, SNS, chat/messaging communication)
    - Mitigation (the modification of device configuration)

Analysis of Monitoring Results

- Generate and utilize security baselines
- Analyze anomalies, findings, and indicators of compromise and action
- Create visualizations, metrics, and trends (e.g., notifications, dashboards, timelines)
- Perform event and incident data analysis
- Document and communicate findings through robust reporting

Generating Reports

Meaningful metrics

- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- To help understand components of visual communications
    - avoid three-dimensional representation
    - use a palette of sequential colors, and
    - avoid pie charts for scatterplots, bar and bubble charts, histograms, density plots, and boxplots

Generating Reports

Utilize tools that deliver meaningful and digestible results

- CSP tools – CloudWatch, CloudTrail, Operations Insights
- Dashboards for visibility created with R programming and Python
- Automated system reports
- Written PDF summaries
- Engaging charts and graphs
- After-action reports including "lessons learned" sections

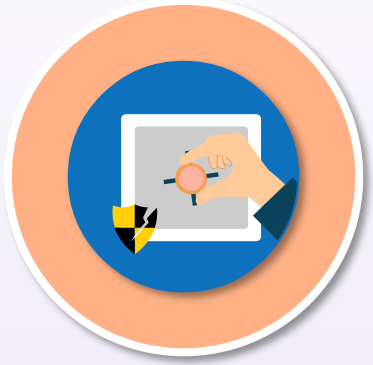
Systems Security Certified Practitioner (SSCP)

Incident response and forensics

Incident Response

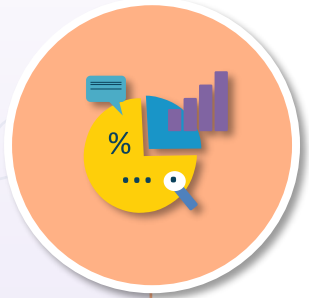
- The classification of the incident will determine action
  - Is it an event or an incident?
  - What is the immediate impact on operations?
  - What is the scope of impact?
  - How prioritized or critical is the target?
  - Can root cause analysis be performed quickly and easily?
  - Does the incident trigger disaster recovery escalation?

Goals of Incident Response



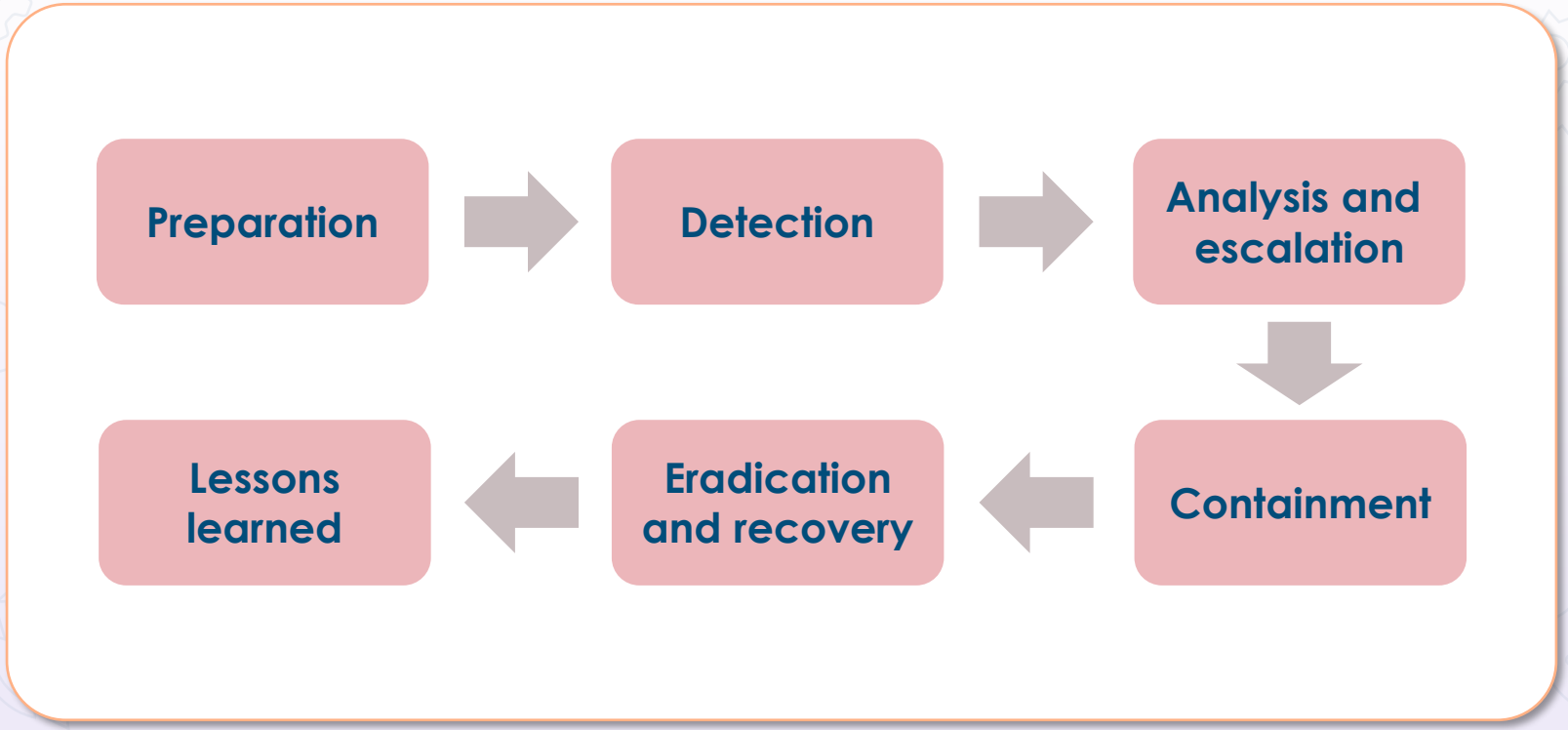
- Reduce the immediate impact and spread
- Protect and maintain enterprise operations
- Support forensics, e-discovery, and continuity of operations
- Provide after-action reports and lessons learned to prevent future occurrences

Incident Response



- To be prepared, you need a plan
  - Documented incident types/category definitions based on risk assessments and BIA (business impact analysis)
  - Know roles and responsibilities of the first responders
  - Reporting requirements/escalation
  - Contact lists, public relations, and legal obligations
- Cyber-incident response teams or computer security incident response teams (CSIRTs)
  - May be outsourced or swarm team
- Best practice is to have pre-performed exercises, drills, and simulations

(ISC)² Incident Response Lifecycle



Incident Detection

- Also referred to as "identification"
- Separate an event from an incident or breach immediately, using pre-defined metrics and experience
- Implement techniques for categorizing and prioritizing the incident based on an established risk register or risk ledger

Incident Response Analysis and Escalation

- This stage is where raw data becomes information in the lifecycle
- Categorize and prioritize the incident based on an established risk register or risk ledger
  - When did it occur and who made the discovery?
  - Are there obvious artifacts and indicators of compromise?
  - Can you discover the actions in the kill chain?
  - Does it qualify for escalation or disaster recovery?
  - Can you quickly identify the root cause?
  - How were you alerted?

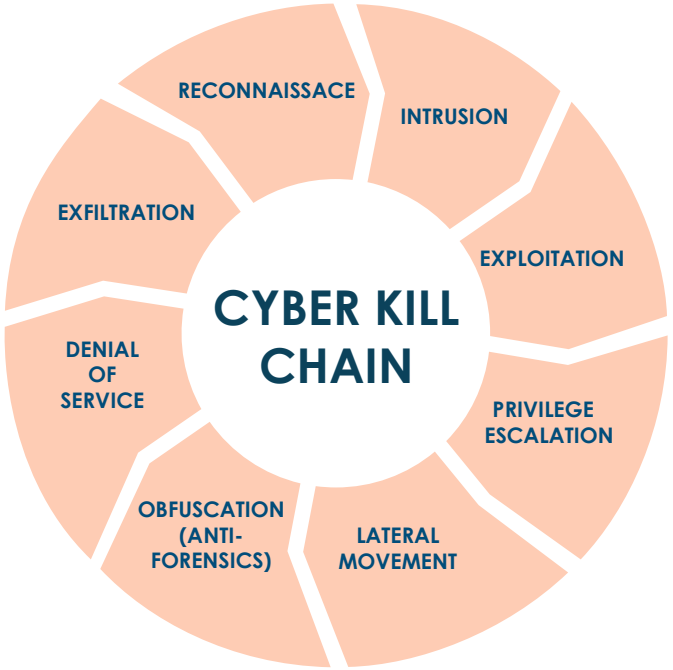
How Were You Alerted?

- Logs, alerts, and feeds
- Phone calls
- Text messages
- Logical and physical alarms
- Interactive monitoring in security operations center (SOC)

Escalation or Elevation

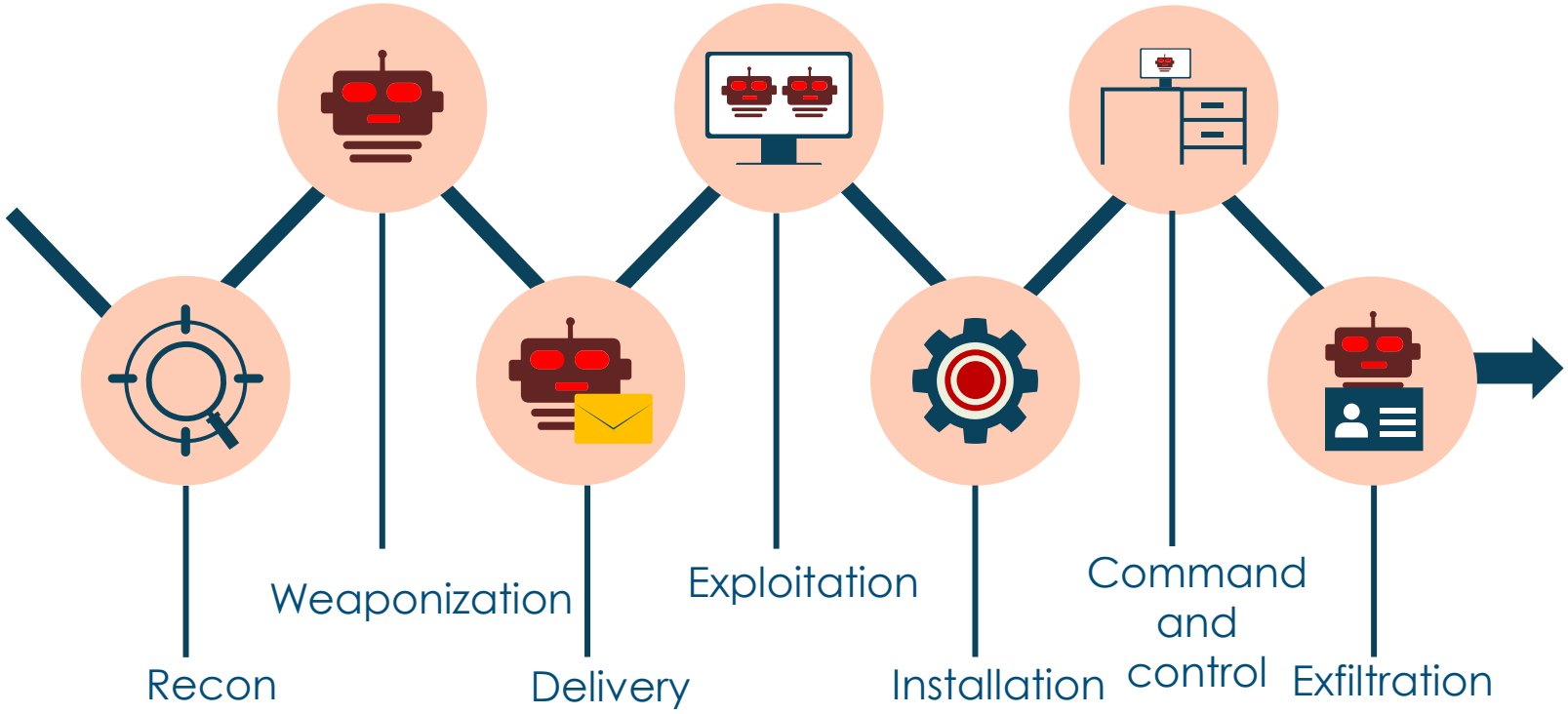
- A pre-established workflow for escalating the incident to a higher service desk tier must be established
- Does the incident need to be passed from the first responders to an incident response team (IRT)?
- Many organizations have a SOC and a service desk along with an emergency change advisory board (CAB)

Cyber Kill Chain



- A succession of steps and phases used during a cyberattack
- Used to better understand malware attacks, such as ransomware, advanced persistent threats (APTs), and distributed denial-of-service (DDoS) attacks – bots
- Originally developed by Lockheed-Martin

7-Step Cyber Kill Chain



8-Phase Cyber Kill Chain

1. Reconnaissance
2. Intrusion
3. Exploitation
4. Privilege escalation
5. Lateral movement
6. Obfuscation/anti-forensics
7. Denial of service
8. Exfiltration

Containment

- Implement short-term processes, such as disconnecting devices from the network
- Malware can be quarantined by anti-virus programs and security suites
- Leverage sandbox locations, detonation chambers, private clouds, and threat modeling environments
- Managed security service providers (MSSPs) can help maintain separation, containment, and segregation

Eradication

- Potential unwanted programs (PUPs) can be eradicated by advanced anti-virus and anti-malware suites
- Some artifacts may need to be moved to detonation chambers for further analysis and machine learning
- All findings should be reported to cloud partners and added to vulnerability repositories and shared reputation databases
- Advanced wiping tools may be needed to completely remove all malware footprints and artifact remanence

Incident Response Recovery and Lessons Learned

- Recovery involves getting back to an acceptable state in order to continue to deliver the value proposition
- Complete remediation may not be possible even for an extended period
- The success of redress and recovery depends on the level of testing and exercises performed

Incident Response Exercises

- Plan review (read-through)
  - Group discussion, plan auditing, and Delphi and brainstorming sessions with stakeholders
- Tabletop
  - Examine documented plans, diagrams, and logical and virtual walkthroughs to eliminate gaps/errors
- Walkthrough (exercise)
  - Planned rehearsals and drills
  - Performed in stages and by department/building only
  - Should find additional gaps to those found during plan review and tabletop exercises

Incident Response Exercises

- Simulation
  - Focuses on specific scenarios and areas
  - Uses real BCP and DRP resources (recovery sites) and teams (swarm simulations)
  - Tests snapshot recovery and hot spares
  - May be the highest-level test that most organizations conduct
- Parallel
  - Real-world drill while still operating business
  - More resource-intensive than simulations
- Full Interruption
  - Real-world drill while ceasing business activities
  - Cost-prohibitive for most organizations

Why Perform Forensic Investigation?

- Laws have been violated
- Organizational policies have been violated
- Systems have been attacked
- Data and identity have been breached
- Intellectual property has been exfiltrated
- Privileged insiders are suspected of crimes
- It's the next incident response phase

Cyber Forensic Investigations

- Involve the scientific investigation of a cyber incident
  - Data breach
  - Insider attack
  - Malware campaign
    - Ransomware
    - Cryptojacking
  - DDoS (distributed denial-of-service)
  - Blackstortion
  - CP files
  - Pirated content
  - Any illegal activities

E-discovery

- Innovative technology that has emerged over the last decade to lower the risks and costs associated with big data, especially in litigation and internal corporate and government investigations
- The e-discovery process includes four phases:
  1. identifying and collecting documents
  2. sorting through data by relevance
  3. creating production sets, and
  4. data management

Cyber Forensics

- Investigations need to be carried out in a standardized manner
  - Identification of the crime
  - Collection of evidence
  - Examination of the evidence
  - Analysis of the evidence
  - Reporting on the findings of the analysis

Legal and Ethical Principles

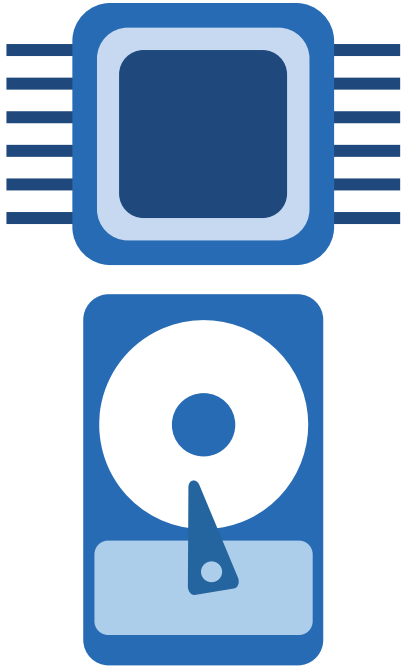
- All SSCP certified candidates must always adhere to the (ISC)^2 code of ethics
- For personal privacy issues, selective filtering may need to be used to isolate activities of certain users – SID (security identifier) filtering
- Responders may need to gain experience working within legal parameters and different layers of law enforcement
- Activities may need to involve legal departments or law firms
- Proper gathering of evidence and chain of custody must be maintained for further presentation in a court case

Handling Evidence

- Capture any hash system images and memory dumps using write-blockers
- Employ forensic kits and laptops
- Collect network traffic and various logs
- Document timeline of event sequence
- Record time offsets
- Take pictures
- Create screenshots
- Conduct witness interviews

Order of Volatility

1. CPU and its cache
2. Kernel statistics, tables, and caches
3. Memory (RAM)
4. Temporary file systems and swap/slack space
5. Disk drives and volumes
6. Attached removable drives
7. Logged data to a remote location
8. Copies of data to archived media/cloud



Processing Forensic Evidence

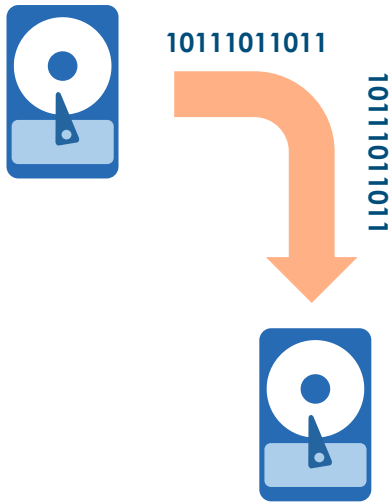
- Encrypted volume detection
- Validation and pattern matching
  - Regular expressions and metacharacters in forensic kits
- Filtering suspected user data
  - Filtering SIDs on shared systems for privacy reasons

Processing Forensic Evidence

- Performing discovery of hidden data in slack space
- Extraction of only meaningful data
- Conducting traces and calibrated estimates to determine suspect
  - Motives
  - Opportunity
  - Means

Chain of Custody

- Follows evidence through entire lifecycle until possible court date
- Involves strict procedures for collecting, handling, and tagging evidence
- Provides a history and timeline of evidence handling
  - Maintains evidence integrity
  - Provides accountability
  - Prohibits tampering
- Anticipates any admissibility issues, such as legal holds



Chain of Custody Documentation

Chain of custody				
Registered mail	Date/Time	Released by	Received by	Reason
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	

Reporting and Visualization Best Practices

- Reports should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Dashboards are very effective (R programming)
- Understand components of visual communications
  - Avoid three-dimensional representation
  - Use a palette of sequential colors
  - Avoid pie charts for scatterplots, bars and bubble charts, histograms, density plots, and boxplots

Forensic Reporting

Communicate results effectively

- Track people-hours and expenses in case software
- Provide electronic and physical documents of all findings
- Meet with proper authorities and possibly prepare to offer expert testimony
- Provide any needed clarification
- Identify overall impact on business and recommend any countermeasures
- Who, what, when, and how? – important for court and other proceedings

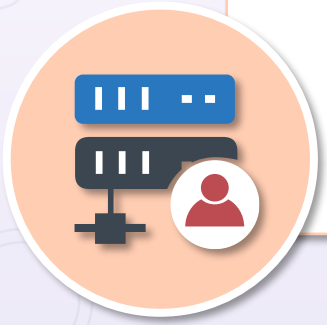
Lessons Learned

- Knowledge gained from the process of conducting the program
- Sessions usually held at the investigation close-out
- To share and use knowledge derived from an experience
- Endorse the recurrence of positive outcomes
- Prevent the recurrence of negative outcomes

Systems Security Certified Practitioner (SSCP)

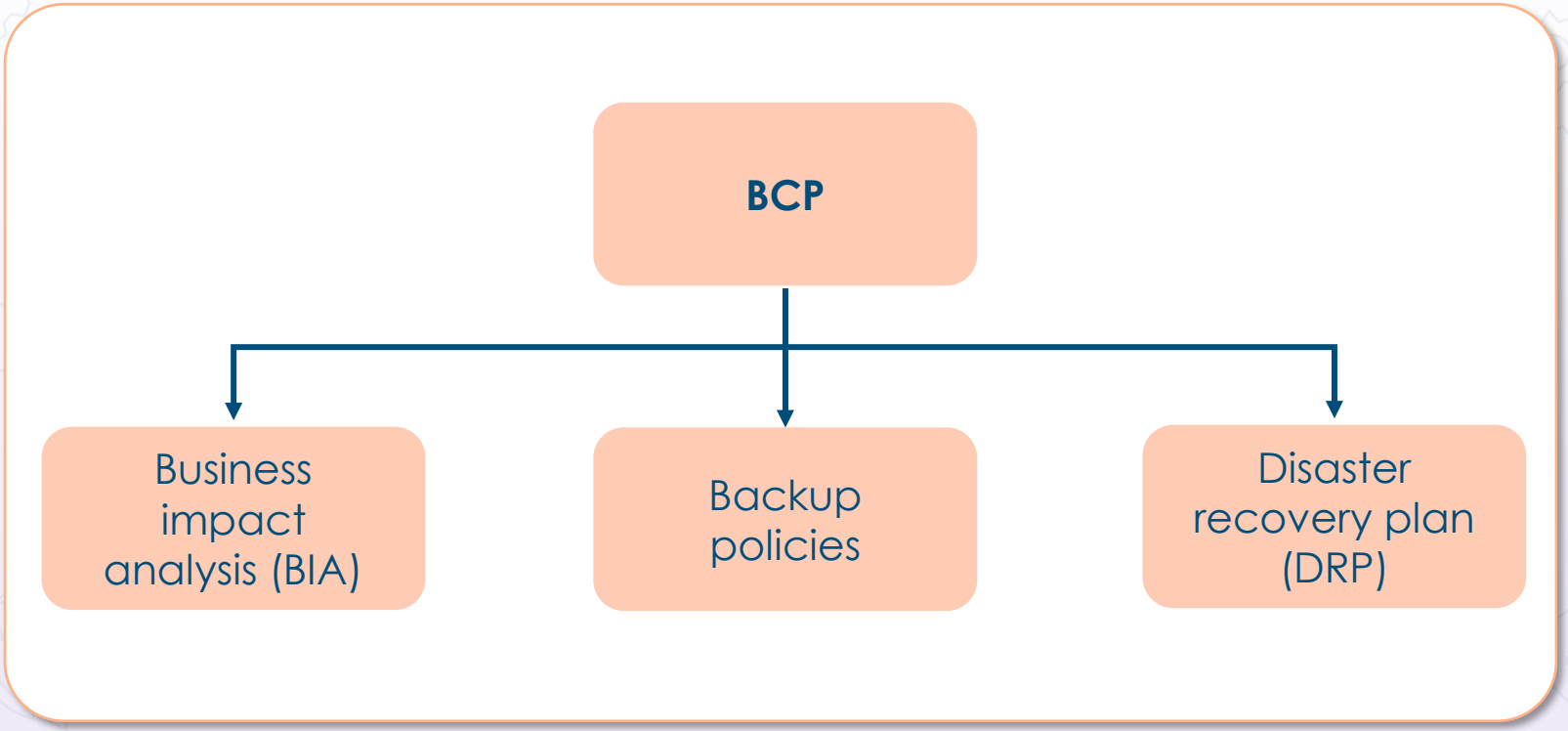
Business Continuity Planning

Business Continuity Planning (BCP)



- BCP involves the preparation of all activities and procedures deployed to avert the loss of critical business functions and services for a pre-determined acceptable amount of time
- For government agencies and other non-commercial entities, the term "Continuity of Operations Planning" (COOP) is often used instead

Business Continuity Planning (BCP)



Disasters Affecting Continuity

Environmental

- Earthquakes
- Wildfires
- Flooding
- Snow
- Tsunamis
- Hurricanes
- Tornadoes
- Landslides
- Asteroids

Man-made intentional

- Arson
- Terrorist
- Political
- Break-ins
- Theft
- Damage
- File destruction
- Information disclosure

Man-made unintentional

- Mistakes
- Power outage
- Illness
- Epidemics
- Information disclosure
- Damage
- File destruction
- Coding errors

BCP from Ready.gov

Business impact analysis

- Develop questionnaire
- Conduct workshop to instruct business function and process managers how to complete BIA
- Receive complete BIA questionnaire forms
- Review BIA questionnaire
- Conduct follow-up interviews to validate information and fill any gaps

Recovery strategies

- Identify and document resource requirements based on BIAs
- Conduct gap analysis to determine gaps between recovery requirements and current capabilities
- Explore recovery strategy options
- Select recovery strategies with management approval
- Implement strategies

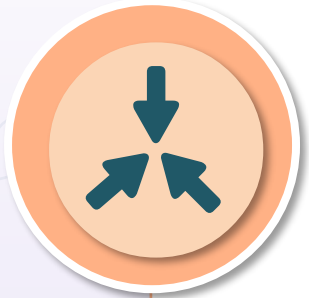
Plan development

- Develop plan framework
- Organize recovery teams
- Develop relocation plans
- Write business continuity and IT disaster recovery procedure
- Document manual workarounds
- Assemble plan
- Validate and gain management approval

Testing and exercises

- Develop testing, exercise, and maintenance requirements
- Conduct training for business continuity team
- Conduct orientation exercises
- Conduct testing and document test results
- Update plan to incorporate lessons learned from testing and exercises

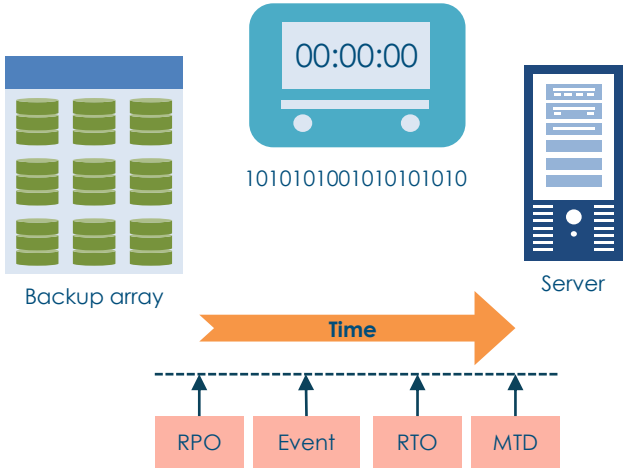
Business Impact Analysis (BIA)



- The risk assessment aspect of BCP
  - Identify critical functions to the business and prioritize them based on need for survival
- Identify the risks associated with the critical functions
  - The probability of the risk occurring (likelihood)
  - The impact the risk will have (magnitude)
- Identify how to eliminate the risk or reduce the risk
- Involves collecting data, meaningful metrics, and key performance indicators (KPIs)

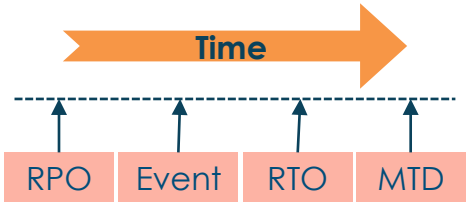
Recovery Time Objective (RTO)

- The amount of time available to recover the resource, service, and function
  - **Must be equal to or less than MTD**
- Any solutions must be accomplished within this time frame, or it is considered a loss
  - Add physical security
  - Add redundancy
  - Purchase insurance
  - Invest in backup generators
  - Invest in faster solutions and processes
  - Safeguard media off-site



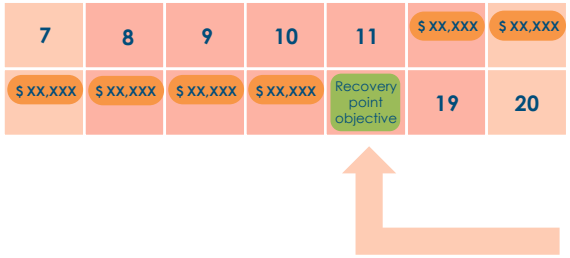
Maximum Tolerable Downtime (MTD)

- Absolute maximum amount of time that a resource, service, or function can be unavailable before we start to experience a loss
- Factors to consider include
  - finances
  - life/safety
  - regulatory
  - legal/contracts
  - reputation, and
  - property

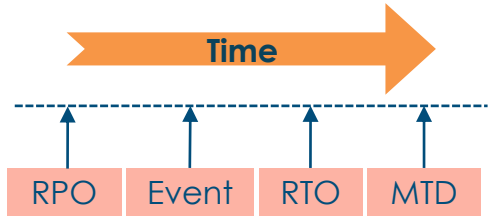


Recovery Point Objective (RPO)

- The point in time, relative to a disaster, where the recovery process begins
  - How much work can be lost if a disruption occurs?
  - What impact will it have?
  - How do we make sure we don't lose more than "X" amount of information?



SUN	MON	TUE	WED	THU	FRI	SAT
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31			



Mean Time Between Failures (MTBF)

- A measure of how reliable a hardware system or component is
- For most devices, the measure is in thousands or tens of thousands of hours between failures
- For example, an SSD drive may have a mean time between failures of 10 years

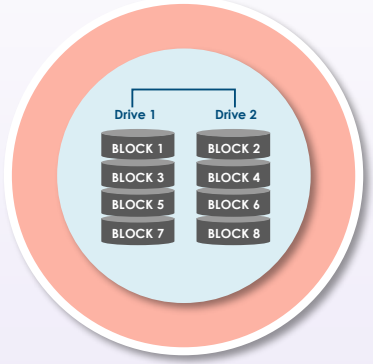
Mean Time To Repair (MTTR)

- How long does it take to repair?
  - Measures time to fix
  - Average value predicted based on experience and documentation
  - (Total down time)/(number of breakdowns)

Redundancy

- Passive redundancy uses additional capacity to reduce the impact of component failures
  - Active/passive failover
  - Hot spares
  - Snapshots
- Active redundancy eliminates performance issues by using simultaneous capacity
  - Active/active failover
  - Hot, mirrored, or parallel sites

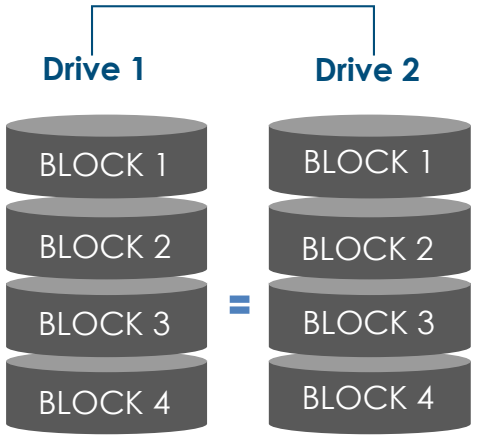
Redundant Array of Independent Disks (RAID 0)



- Data is split up into blocks
- Blocks are written across all array drives
- Uses at least two disks at a time
- Offers fast read and write speeds
- Not redundant = no fault tolerance

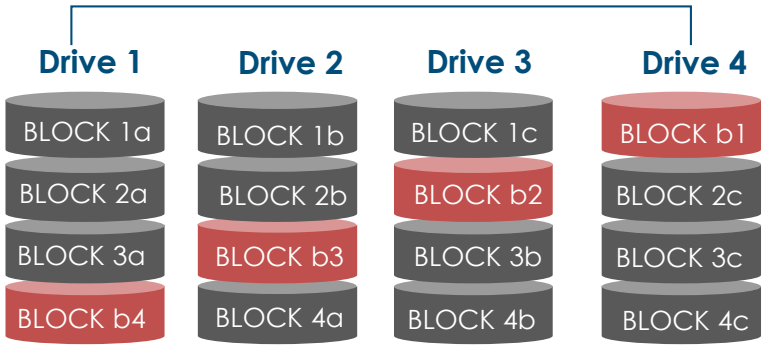
RAID Level 1 (Mirroring)

- Configuration of at least two drives that contain the exact same data
- If one drive fails, the others will still function
- RAID 1 offers high read performance, as data can be read off any of the drives in the array
- Because data needs to be written to all the drives in the array, the write speed is slower than a RAID 0 array



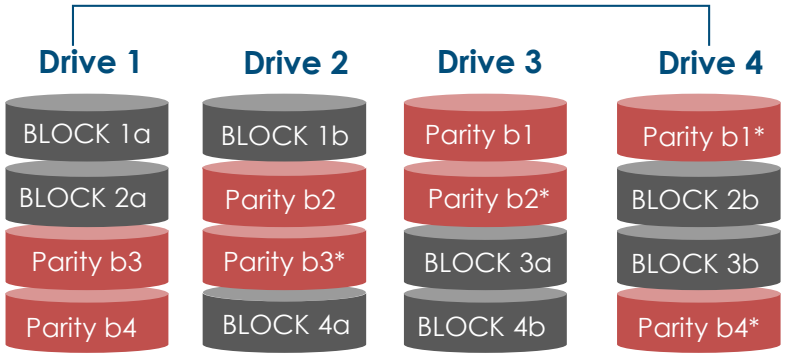
RAID Level 5

- Data is striped across multiple drives like RAID 0, but also has "parity" data distributed across at least 3 required drives
- In the event of a drive failure, data is restored by using the parity information stored across the other drives
- Read times are very fast, but the write speed is slower due to the parity that must be calculated
- The most popular RAID 5 configurations use four drives, which lowers the lost storage space to 25 percent (it can work with up to 16 drives)



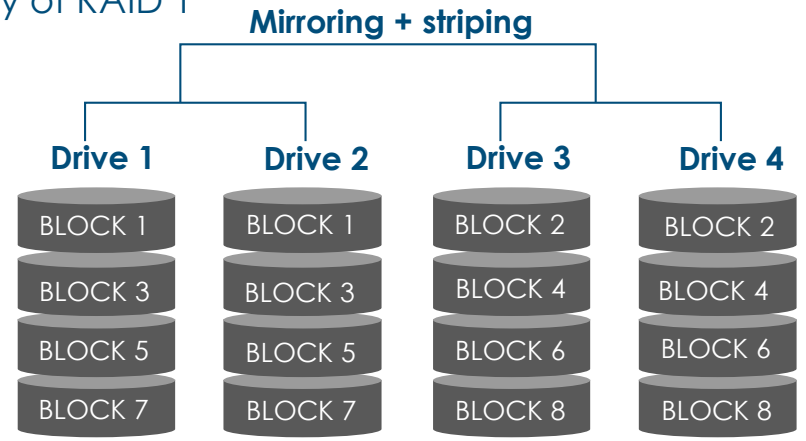
RAID Level 6

- RAID 6 is like RAID 5, but the parity data is written to two drives, so it requires at least four drives
- This solution can survive two drives failing simultaneously
- Read speeds are as fast as RAID 5, but the write speeds are slower than RAID 5 due to the additional parity data that must be calculated



RAID Level 10

- Consists of a minimum of 4 drives and combines the advantages of RAID 0 and RAID 1 into one single system
- Offers security by mirroring all data on secondary drives while using striping across each set of drives to speed up data transfers – the speed of RAID 0 with the redundancy of RAID 1
- Can lose any single drive, and feasibly even a 2nd drive, without losing any data
- Compared to large RAID 5 or RAID 6 arrays, RAID 10 is an expensive way to have redundancy for fast databases, file servers, application servers

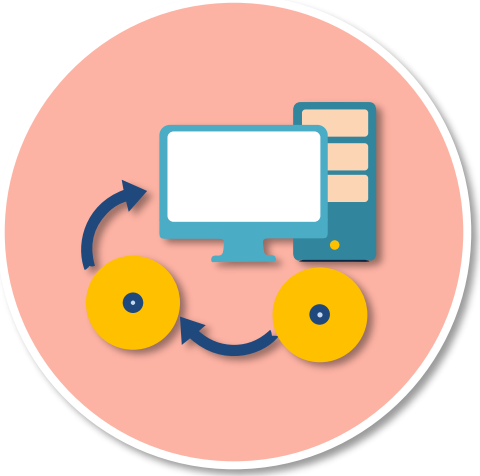


RAID Comparisons

Features	RAID 0	RAID 1	RAID 5	RAID 6	RAID 10
Minimum number of drives	2	2	3	4	4
Fault tolerance	None	Single-drive failure	Single-drive failure	Two-drive failure	Up to one disk failure in each sub-array
Read performance	High	Medium	Low	Low	High
Write performance	High	Medium	Low	Low	Medium
Capacity utilization	100%	50%	67-94%	50-88%	50%

Full Backups

The main ransomware countermeasure



- Backs up everything regardless of archive bit being set or not
- Clears the archive bit once the backup completes
- Takes the longest to back up
  - Depends on how much must be backed up
- Quickest to restore
  - Only the most recent full backup is required

Incremental Backup

Clears the archive bit once the backup completes

- Backs up any new file or any file that has changed since
  - the last full backup, or
  - the last incremental backup
- Subsequent backups only store changes that were made since the previous backup
- The process of restoring lost data from an incremental backup is longer, but the backup process is much quicker
- **Should not be performed manually if possible**

Differential Backup

DOES NOT clear the archive bit when the backup completes

- Backs up any file that has the archive bit set
- Backs up any new file or any file that has changed since the last full backup
- Slow to back up
- Quick to restore
- The last full backup and the most recent differential backup are needed for restoration
- **Not recommended to perform manually**

Snapshots

- Easier and faster backups and restores
- Immediate point-in-time virtual copy of source
- Should be replicated to another medium or cloud storage to be considered a backup
- Time to back up does not increase with amount of data
- Improved RTO and RPO
- Restores are faster
- Less data is lost with an outage

Storage Media Comparisons

Medium	Date of invention	Lifespan	Capacity
HD	1956	5-10 years	From GB to TB
Floppy disk	1971	3-5 years	Hundreds of KB to a few MB
CD/CD-ROM	1979	25-50 years	80 minutes or 700 MB
MD (MiniDisc)	1991	25-50 years	60 minutes or 340 MB
DVD	1994/1995	25-50 years	4.7 GB
SD card	1994	10 years or more	A few MB to tens of GB
USB flash drive	2000	10 years or more	A few MB to tens of GB
SSD	1970-1990	10 years or more	From GB to TB

Daniel Cunha Barbosa, "Types of backup and five backup mistakes to avoid," *WeLiveSecurity*, May 10, 2019, https://www.welivesecurity.com/2019/05/10/types-backup-mistakes-avoid/.

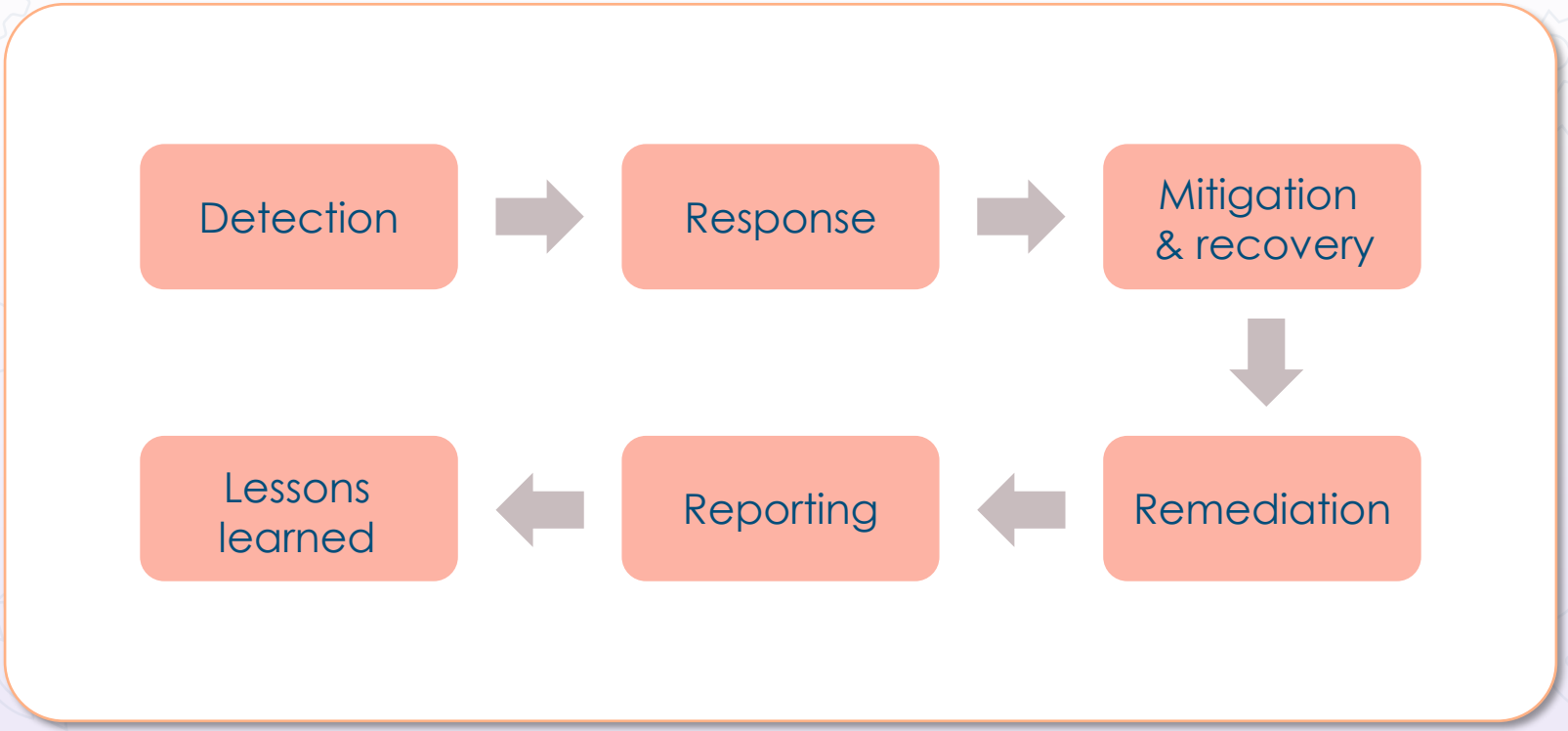
Disaster Recovery Planning (DRP)

- Ensuring that you can help the organization recover **to an acceptable level** from any type of catastrophic event
- A cataclysmic event can be anything from a single drive ransomware attack to an entire facility or campus being put out of action
- The disaster recovery plan (DRP) should contain detailed steps for recovering from any kind of data loss or physical disaster

Disaster Recovery Planning

- Step-by-step instructions on how to recover each aspect of critical systems, applications, and data
- Backup and restore plans with order of restoration
- Contact information for key stakeholders, partners, and vendors
- Contact information for law enforcement, legal, insurance, media outlets
- Order of succession and command
- Location of hot spares, software and CD keys, security access keys and fail-safe passwords, and other valuables
- Site locations and descriptions (cold, warm, hot, cloud)

DRP Lifecycle



Disaster Recovery Site Strategies

Recovery strategy	Recovery time	Advantages	Disadvantages
Commercial hot site	0 to 24 hours	• Fastest recovery time • Smoothest deployment, as facility, equipment, application software, data, and OS are installed and running • Easy to test when necessary • The optimal solution for recovering on-going operations	• The most expensive solutions often need to replicate all equipment and software, including on-going version and patch management issues • Continuous communication costs to duplicate data are very high • Terms of agreement may limit the duration of use especially if part of shared reciprocal agreement • Vendors will often prioritize only the larger customers in a real-world disaster scenario
Warm site	24 to 48 hours	• Moderately priced • A basic infrastructure is in place to support recovery operations – e.g., wireless network only • Allows for some degree of pre-staging of the necessary hardware, application software, OS software, data, and communications	• Not as easy to test • Recovery time is longer than with hot site and is dependent on the time to locate and restore applications • Facility equipment may not be exactly what is needed • Once the recovery begins delays may occur because of equipment, software, or staffing shortfalls
Cold site	72 plus hours	• Lowest cost solution • Basic infrastructure, power, air, and communication are in place and ready • Can rent the facility for a longer term at lower cost • Costs can be lowered even further using reciprocal agreements	• Longest recovery time • All equipment must be ordered, delivered, installed, and made operational • Worst solution for supporting on-going and mission-critical production operations
Cloud	0 to 24 hours	• Could be a lower cost hot/warm solution in the long run based on economy of scale and multitenancy of cloud provider • Data and applications available immediately • Location-independent • Easy to test	• Security may be an issue based on shared responsibility model • May not be feasible due to compliance and regulations • May not allow enough time for a daily cycle processing window

Personnel Safety and Security Concerns

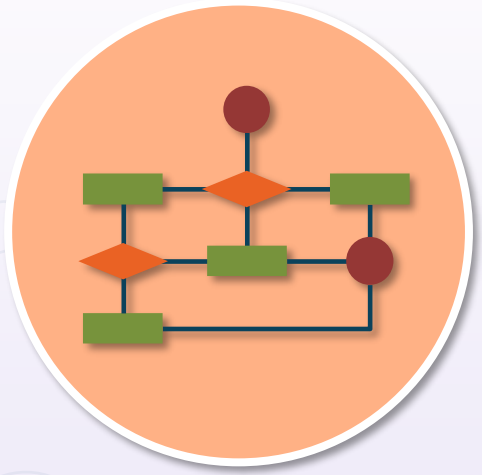
- Most large organizations have a separate department or third-party vendor that handles all employee and contractor travel arrangements
- Company may have fleet of autos or trucks for corporate use and may be assigned to employees on permanent or as-needed basis
- Disaster recovery must be addressed in security training and awareness programs
- May need HR to offer emergency management, counseling, and personal duress assistance

Test Disaster Recovery Plans

Read-through testing

- Read-through (plan review) is where the business continuity plan owner and business continuity team discuss the business continuity plan
- Look for missing elements and inconsistencies within the plan or with the organization
- A type of checklist test is useful to train new members of a team, including the business function owner

Test Disaster Recovery Plans



Tabletop testing

- Participants gather in a room to execute documented plan activities in a stress-free environment
- Can use blueprints, topological diagrams, or computer models to effectively demonstrate whether team members know their duties in an emergency and if they need training
- Documentation errors, missing information, and inconsistencies across business continuity plans can be identified

Test Disaster Recovery Plans

Walkthrough testing

- Planned rehearsal of a possible incident designed to evaluate an organization's capability to manage that incident
- Provides an opportunity to improve the organization's future responses and enhance the relevant competences of those involved
- Often done on a limited basis or by scheduling each department or building separately for fire and active shooter drills

Test Disaster Recovery Plans

Simulation testing

- Desirable to determine if business continuity management procedures and resources work in a realistic situation
- May be the most elaborate test most entities ever conduct
- Uses established business continuity resources, such as the recovery site, backup equipment, services from recovery vendors, and transportation
- May require sending teams to alternate sites to test backup technology as well as business functions

Test Disaster Recovery Plans

Parallel testing

- A parallel test involves bringing the recovery site to a state of operational readiness but maintaining operations at the primary site
- Staff are relocated, backup tapes are transferred, and operational readiness is established in accordance with the disaster recovery plan while operations at the primary site continue normally
- May be the most comprehensive test most entities ever conduct

Test Disaster Recovery Plans

Full interruption testing

- Operations are completely shut down at the primary site to fully emulate the disaster
- Enterprise transfers to the recovery site in accordance with the disaster recovery plan
- A very thorough test, which is also expensive (may be cost-prohibitive)
- Has the capacity to cause a major disruption of operations if the test fails

Lessons Learned

A section of After-Action Report

- Knowledge gained from the process of conducting the program, project, or task included in After-Action Report (AAR)
- Formal sessions usually held at the project close-out, near the completion of the initiative
- Recognized and documented at any point during the life cycle to
  - share and use knowledge derived from an experience
  - endorse the recurrence of positive outcomes
  - prevent the recurrence of negative outcomes