Functional vs. Non-Functional Testing

Criteria	Functional	Non-Functional
Definition	The application is tested against the functional requirements/ specifications	Is tested against requirements like usability, performance, security and compliance
Foundation	Based on client's **requirements**, for example, a client might need that a financial report be generated	Based on client's **expectations**, for example, the client may expect that the financial report be generated within ten seconds
Concentration	It tests **WHAT** the software does	It tests **HOW** the software does
Process	Test execution is usually manual	Test execution is usually automated
Levels	Performed during all levels of Testing: Unit, Integration, System and Acceptance.	Performed normally during System and Acceptance Testing levels
Methodology	Normally, Black Box Testing method is used	Normally, White Box Testing method is used

White Box vs. Black Box Software Testing

- **Black** box testing is also known as Behavioral Testing
- It is a software testing method in which the internal structure, design, and implementation is not known to the tester
- Procedures to derive and/or choose test cases are based on an analysis of the specification of a component without reference to its internal structure
- These tests can be functional or non-functional, though usually functional

- **White** box testing is also known as Clear Box Testing, Open Box Testing, Glass Box Testing, Transparent Box Testing, Code-Based Testing or Structural Testing
- It is a software testing method in which the internal structure, design, and implementation is known to the tester
- Based on an analysis of the internal structure of the component or application
- **Gray** box testing is a compromise between White and Black box

SAST

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 lifecycle**
- 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

DAST

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

IAST

Interactive Application Security Testing

- **IAST combines the advantages of a SAST and a DAST solution**
  - **The benefits of a static view, because they can see the source code**
  - **The benefits of a web scanner approach, since they see the execution flow of the application during runtime**
- Can detect ~100% of OWASP benchmark in real-time with no false positives
- Can flexibly be used in QA and production environments, analyzing dependencies as well as legacy components
- No need to scan or attack the application
- Continuous detection – DevOps-friendly
- Integrates and communicates with task management systems to create unified workflows

Abuse Case Testing

- An Abuse Case test is a technique for using a particular software feature in a way that was not expected by the implementer
- This tests the ability of an attacker to influence a feature (or outcome of use of the feature) based on the attacker action or input
- Misuse and abuse cases define how users misuse or exploit the weaknesses of controls in software features to attack an application
- A direct attack against business functionalities can lead to tangible negative business impact

Quality Assurance with SCA

Security Control Assessment (SCA)

- 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

Quality Assurance with SCA

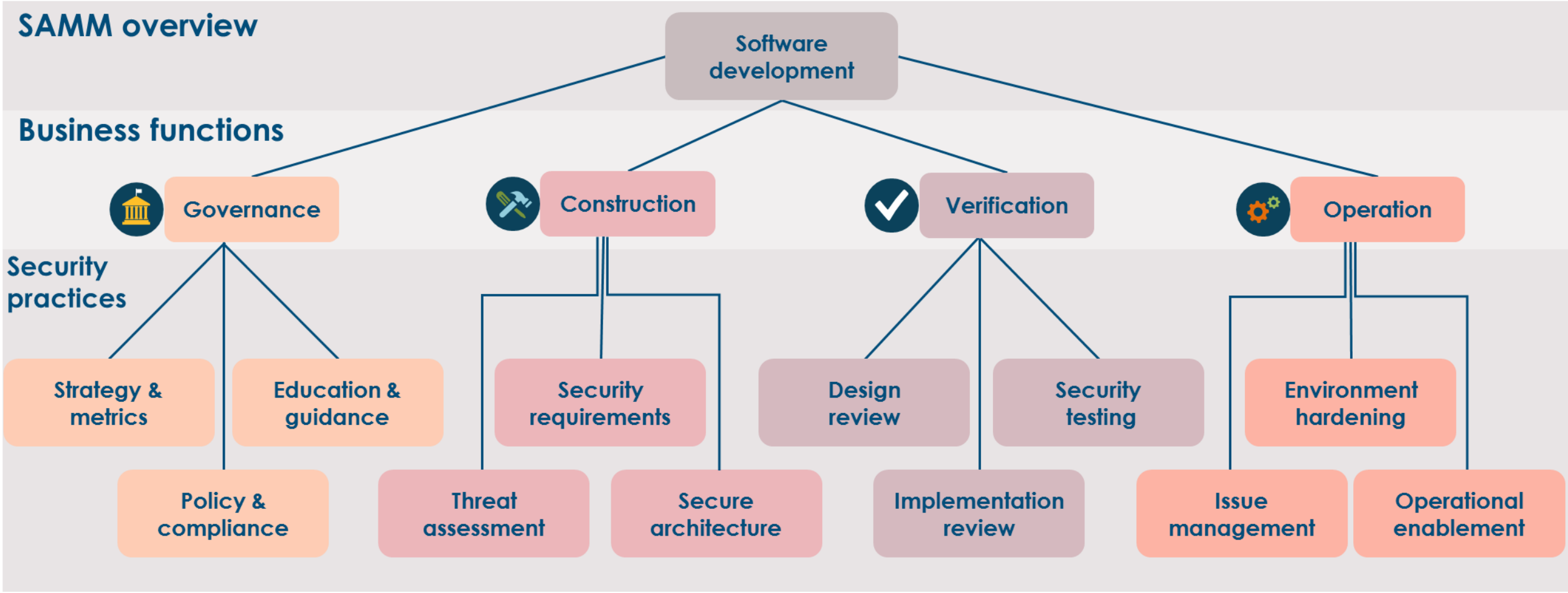
Security Test and Evaluation (ST&E)

- SCA and ST&E will appraise the operational plan (or planned implementation) of controls
- Results are 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

Software Assurance Maturity Model (SAMM)

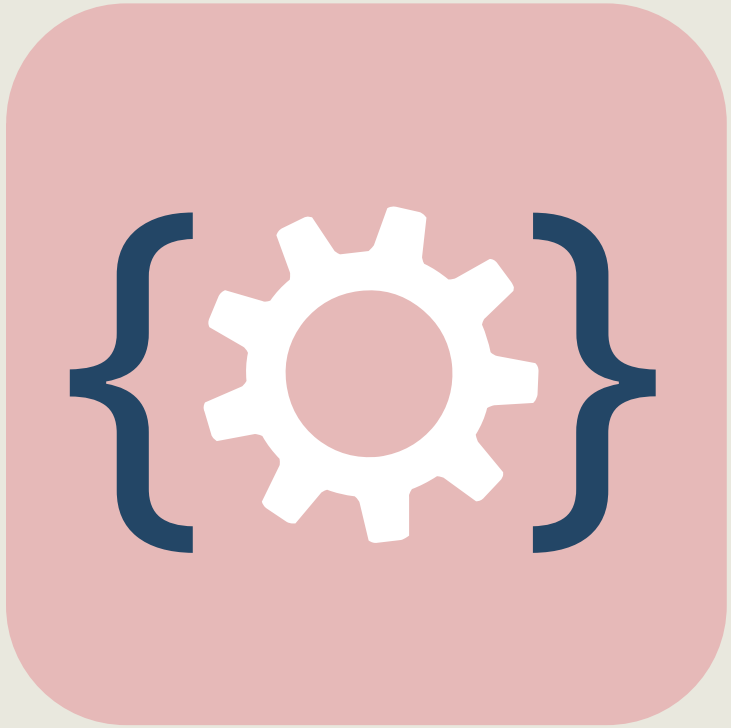
- The Software Assurance Maturity Model (SAMM) is an open framework from OWASP to assist organizations in developing and deploying a secure software delivery strategy that is focused on the detailed risks facing the enterprise. The resources offered by SAMM will assist in:
  - Appraising the organization's 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
  - Defining and gauging security-related tasks throughout the enterprise

Software Assurance Maturity Model (SAMM)



"Software Assurance Maturity Model." OWASP.org. Accessed June 8, 2021. https://owasp.org/www-pdf-archive/SAMM_Core_V1-5_FINAL.pdf.

OWASP API Top Ten



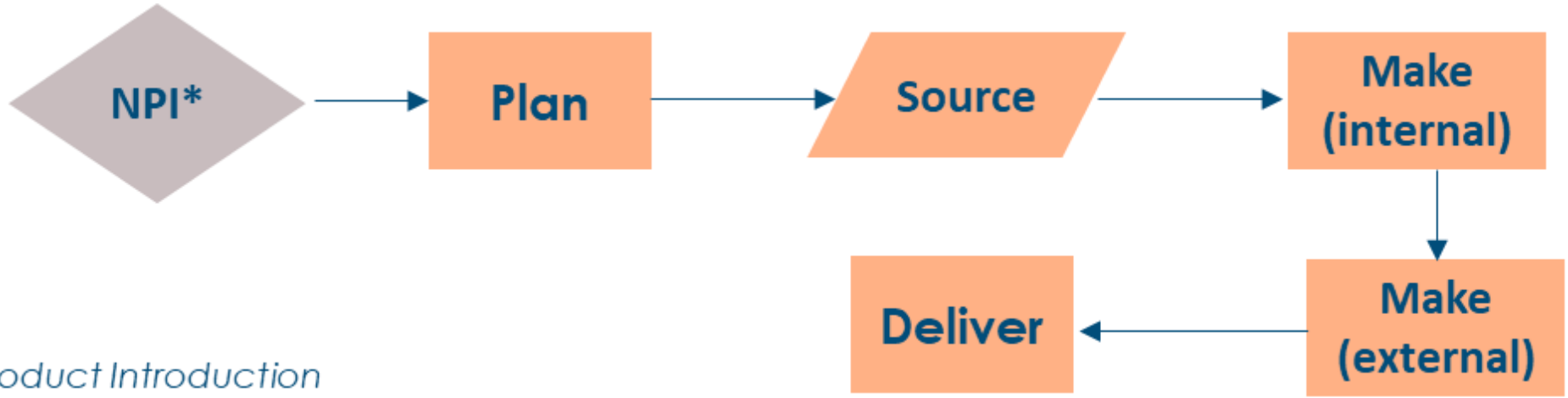
- API1:2019 Broken Object Level Authorization
- API2:2019 Broken User Authentication
- API3:2019 Excessive Data Exposure
- API4:2019 Lack of Resources & Rate Limiting
- API5:2019 Broken Function Level Authorization
- API6:2019 Mass Assignment
- API7:2019 Security Misconfiguration
- API8:2019 Injection
- API9:2019 Improper Assets Management
- API10:2019 Insufficient Logging & Monitoring

Supply Chain Management

- Many risks exist because vendors' employees can introduce cybersecurity vulnerabilities with hardware, software, and services
- Some tiers of the supply chain may be considered proprietary so that a lack of visibility impedes the security lifecycle, and this can make third-party assessment and monitoring more difficult
- Delivering meaningful metrics and analysis related to specific supply chain exposures such as:
  - Cargo disruption trends and exposure of transit modalities
  - Threats posed by terrorist/activist groups and criminal elements
  - Country risk variables, such as the rule of law and the effectiveness of local law enforcement
- **Exam: The CSA combined Cloud Controls Matrix (CCM) v4 and the Consensus Assessment Initiative Questionnaire (CAIQ) for cloud vendor assessment**

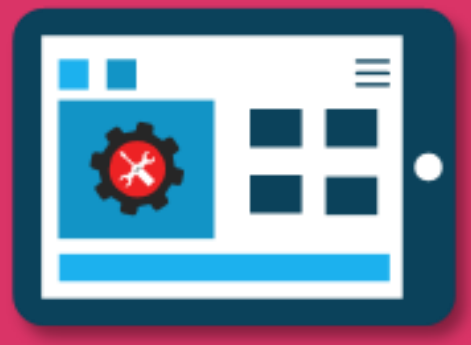
Supply Chain Risk Management

1. Identify and document risks
2. Create a supply-chain risk management framework
3. Monitor risk using customized tools
4. Implement governance and regular audits
5. Manage unknown risks by building strong defense-in-depth in a security-aware culture



*New Product Introduction

Commercial Off-the-shelf (COTS)



- A common commercial off-the-shelf as-is solution
- COTS products are intended to be easily installed and to interoperate tightly with existing system components
- Almost all software bought by the public computer user fits into the COTS category (operating systems, office product suites, word processing, and e-mail programs)
- One of the major advantages of mass-produced COTS software is that it is relatively low cost
- **A key security issue is proper licensing management and visibility into Ghost (or Shadow) IT combined with Information Rights Management (IRM)**

Validate Open-Source Software

Secure Code Reviews

- Directing an informal or formal secure code review is another approach to assessing code for appropriate security controls
- An informal code review may involve a software engineer evaluating sections of code, looking for vulnerabilities
- A formal code review may involve the use of trained teams of reviewers that are assigned specific roles as part of the review process, as well as the use of a tracking system to report on vulnerabilities found
- The integration of a code review process into the SDLC can improve the quality and security of the code being used or developed

Open-Source Vulnerabilities

- 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

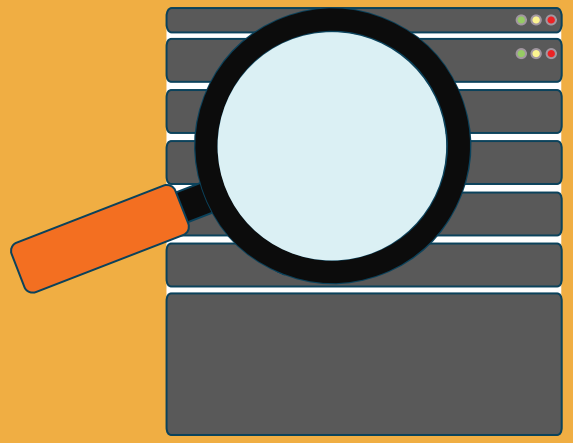
Open-Source Vulnerabilities

- 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

Web Application Firewalls (WAF)

- An appliance, server plugin, or CSP service that applies a set of rules to an HTTP/S connection
- The AWS WAF runs on an Application Elastic Load Balancer (with TLS Listener enabled), a CloudFront CDN distribution, or the API Gateway
- WebACLs filter for common attacks, such as:
  - Cross-site scripting (XSS)
  - SQL injection
  - Cross-site request forgery (CSRF)
  - Buffer overflows
  - DDoS and botnets
  - Custom WebACL rules

Database Activity Monitoring (DAM)



- A suite of cross-platform tools or enterprise services used to identify and report on fraudulent, illegal, or other undesirable behavior concerning data
- A DAM system should have minimal or no impact on user operations and productivity
- Modern solutions deploy a comprehensive toolkit for:
  - Visibility, discovery and classification
  - Vulnerability protection
  - Application-level analysis and intrusion prevention
  - Support for unstructured data security
  - Identity and access management integration
  - Risk management support

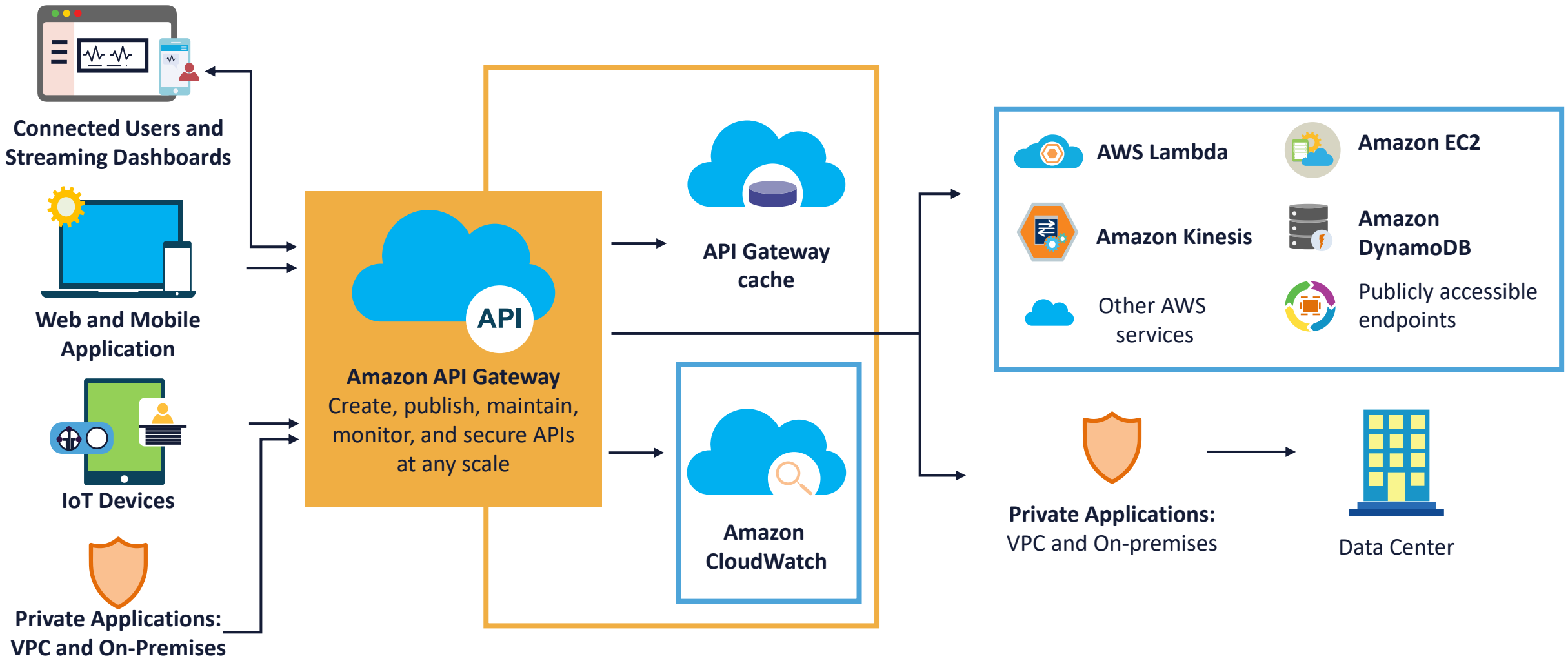
XML Firewalls

- An XML Firewall processes XML requests and responses over HTTP/S and contains a processing policy with a set of request, response, two-way, and error rules
  - Processing can include AAA, transformations, schema validation, logging, and cryptographic operations
- Through the processing policy, the XML Firewall can apply all processing actions to the request and response message, regardless of format
- Although an XML Firewall processes XML documents of all types, including SOAP-formatted messages, it can accept unprocessed (text or binary) documents

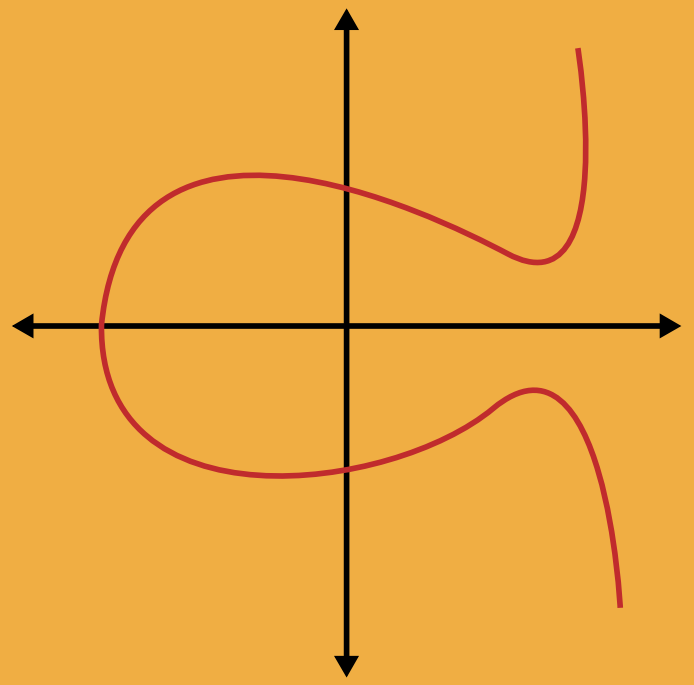
API Gateways

- An API Gateway is usually a fully managed cloud service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale
- APIs act as the "front door" for applications to access data, business logic, or functionality from backend services
- AWS supports RESTful APIs and WebSocket APIs to enable real-time two-way communication applications
- API Gateways will now support containerized and serverless workloads, as well as web applications.

API Gateway at Amazon Web Services



Cryptographic Best Practices



- Gravitate towards elliptic curve (ECDSA) and ephemeral protocol suites (IKEv2) when protecting data in transit
- Digitally sign all external API calls to cloud resources
- Never embed cryptographic keys or credentials in the API or in a code repository
- Always use the most recent TLS instead of SSL
- Consider DNSSEC and HSTS on web servers
- Leverage managed Key Management Services for better control and compliance (CloudHSM)
- AES-GCM-256 is an Authenticated Encryptor with Associated Data (AEAD) that does not need a separate HMAC
- Homomorphic encryption to protect data-in-use

HTTP Strict-Transport-Security (HSTS)

- If a web site accepts an HTTP connection and redirects it to HTTPS, users may initially access the non-encrypted version of the site before being redirected
- This creates a vulnerability to man-in-the-middle attacks, as the redirect can be exploited to direct users to a malicious site instead of the secure version of the original site
- HTTP Strict-Transport-Security (HSTS) allows a TLS web site to instruct browsers that it should only be accessed using HTTPS, instead of using HTTP
- The web server employs the HTTP Strict-Transport-Security header

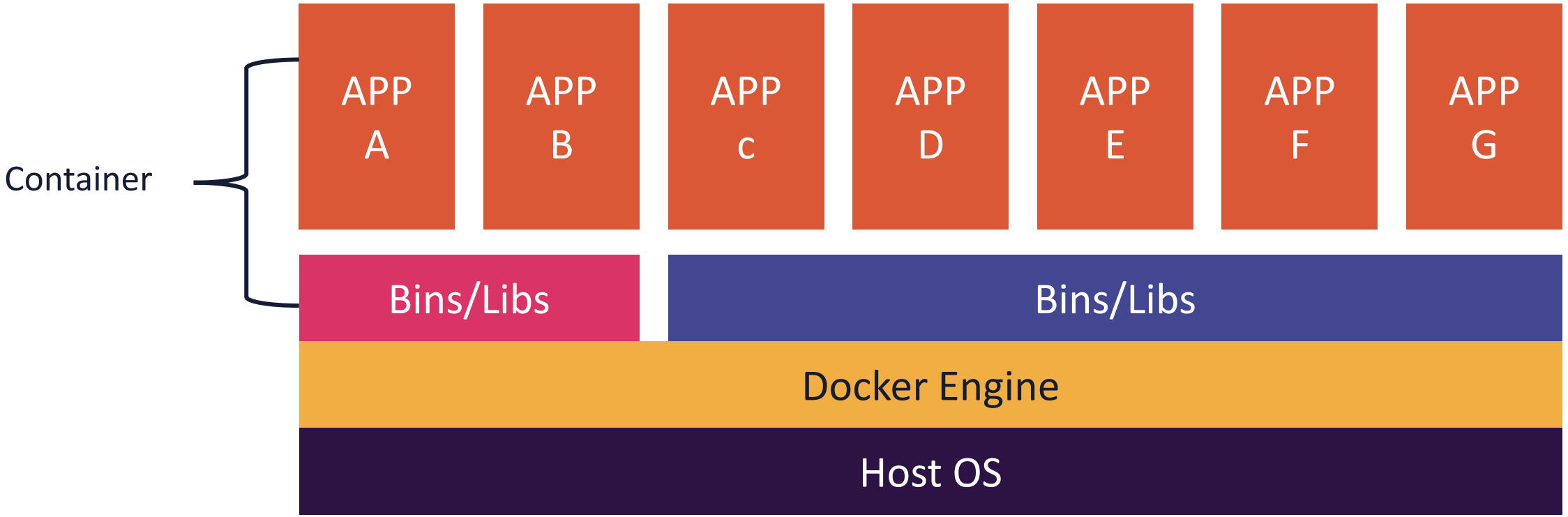
Containers

- Application container technologies, also known as containers, are a form of operating system virtualization combined with application software packaging
- Containers provide a portable, reusable, and automatable way to package and run applications

Containers

- DevSecOps should adapt the organization's operational culture and technical processes to support the new way of developing, running, and supporting applications made possible by containers
- Use container-specific host OSs instead of general-purpose ones to reduce attack surfaces
- Adopt container-specific vulnerability management tools and processes for images to prevent compromises

APPLICATION CONTAINERS

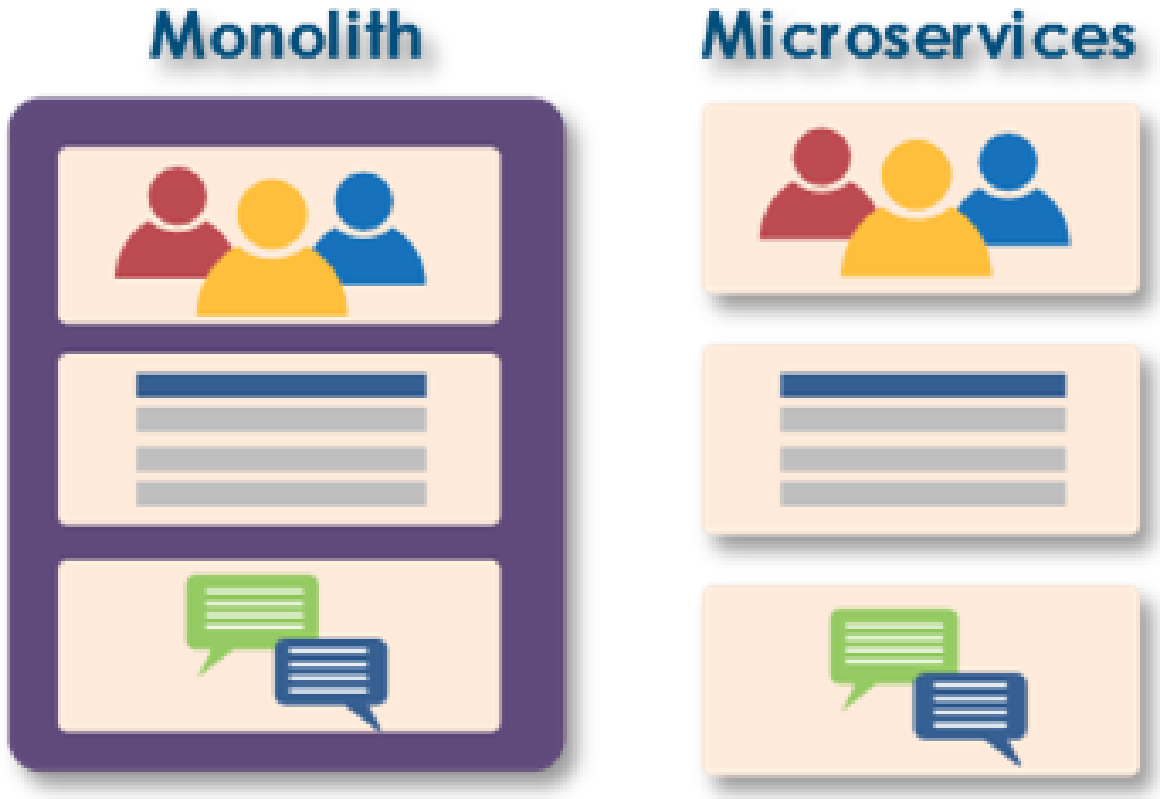


Microservices

- Microservices are specific service-oriented application components
- An architectural approach to software development where the results are made up of small independent services that communicate over well-defined APIs
- These services are typically maintained by small, self-contained teams of developers
- Microservices architectures make applications faster to develop and easier to scale
- They enable innovation and fast-tracked delivery of new application features

Microservices

- Tightly scoped but loosely coupled
- Thoroughly modular and encapsulated
- Independently deployable
- Freely scalable
- Communicate using notification and queueing services



More about CASB

- One of the first companies to introduce a product labeled as a “CASB” was Sky High Networks acquired by McAfee in January 2018
- The Cloud Access Broker is also called a Cloud Access Gateway
- They are API-based (AWS PrivateLink partners) or Proxy-based (Palo Alto Aperture)
- The 4 Pillars of CASB are:
  - Visibility
  - Compliance
  - Data Security
  - Threat Protection

Cloud Secrets Management

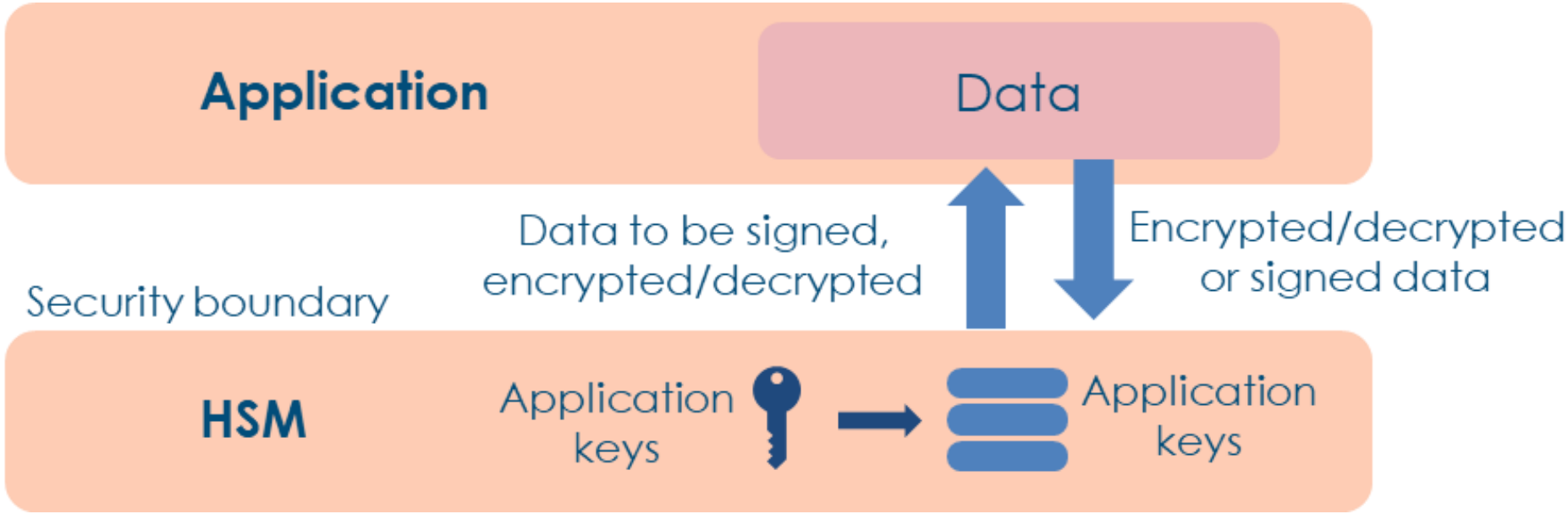
- Secrets management makes it easy to rotate, manage, and retrieve database credentials, API keys, and other secrets during their lifecycle
- Users and applications retrieve secrets with a call to secrets manager APIs, removing the requirement to hardcode sensitive information
- The service is also extensible to other types of secrets, including API keys and OAuth tokens
- One can control access to secrets using fine-grained permissions and audit secret rotation centrally for resources in the cloud, third-party services, and on-premises

Domain 5

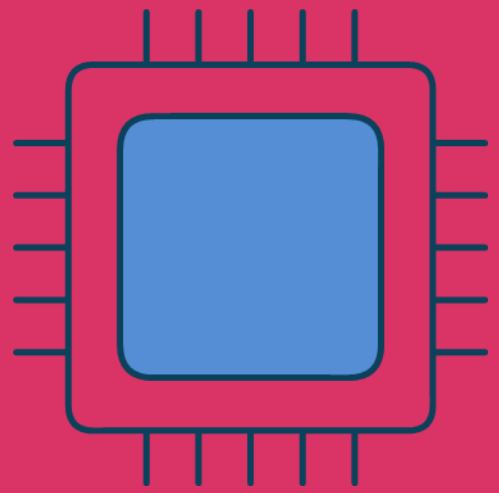
Cloud Security Operations

Hardware Security Modules (HSM)

- Uses tamper-proof, hardened devices to provide crypto processing and protection of cryptographic keys and functions
- Involves partitioned administration and security domains
- Applies corporate key use policies
- Can be used in place of software crypto libraries and accelerators



Boot Integrity

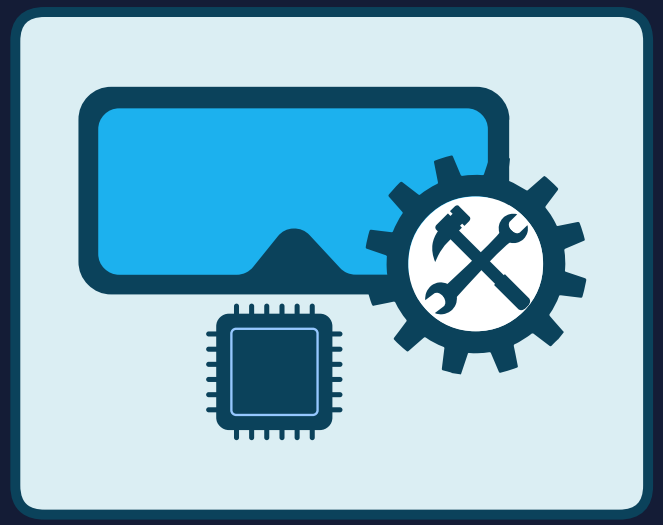


- **UEFI – Unified Extensible Firmware Interface** replaces legacy BIOS (basic input/output system)
  - Low-level software for booting the device
  - Tests the hardware components (POST)
  - Gets the OS up and running
- Offers the ability to protect the device at a lower level with passwords

Boot Integrity

- Computer chip (microcontroller)
  - Installed on the device or built into PCs, tablets, and phones
  - Tamper-resistant security chip
  - Stores info needed to authenticate the platform
  - Passwords, certificates, and encryption keys
- Provides confidentiality, integrity, authentication

Hardware Root of Trust



- Hardware root of trust
  - Anchoring the trustworthiness of a system to hardware not software
  - Hardware solutions are more secure than software solutions
  - Less susceptible to attacks since security solutions are on-chip
- Foundations of a Trusted Execution Environments (TEE) or Trusted Computing (TC):
  - TPM – module embedded in a system
  - SED – self-encrypting drives
  - HSM – dedicated crypto processor

Cloud Host Servers: Best Practices

- Secure build: To implement fully, follow the specific recommendations of the vendor to securely deploy their operating system
- Secure initial configuration: Depends on different variables, such as OS vendor, operating environment, business requirements, regulatory requirements, risk assessment, risk appetite, and hosted workload(s)
- Host hardening and patching: The more automated the better

Cloud Host Servers: Best Practice (Continued)

- Host lock-down: Implement host-specific security measures including:
  - Blocking of non-root access to the host under most circumstances
  - Only allowing the use of secure communication protocols/tools
  - Configuration and use of host-based firewall
  - Use of role-based access controls
- Secure ongoing configuration maintenance: Achieved through the following:
  - Patch management of hosts, guest OSs, and application workloads
  - Periodic vulnerability assessment scanning
  - Periodic penetration testing of hosts and guest operating systems

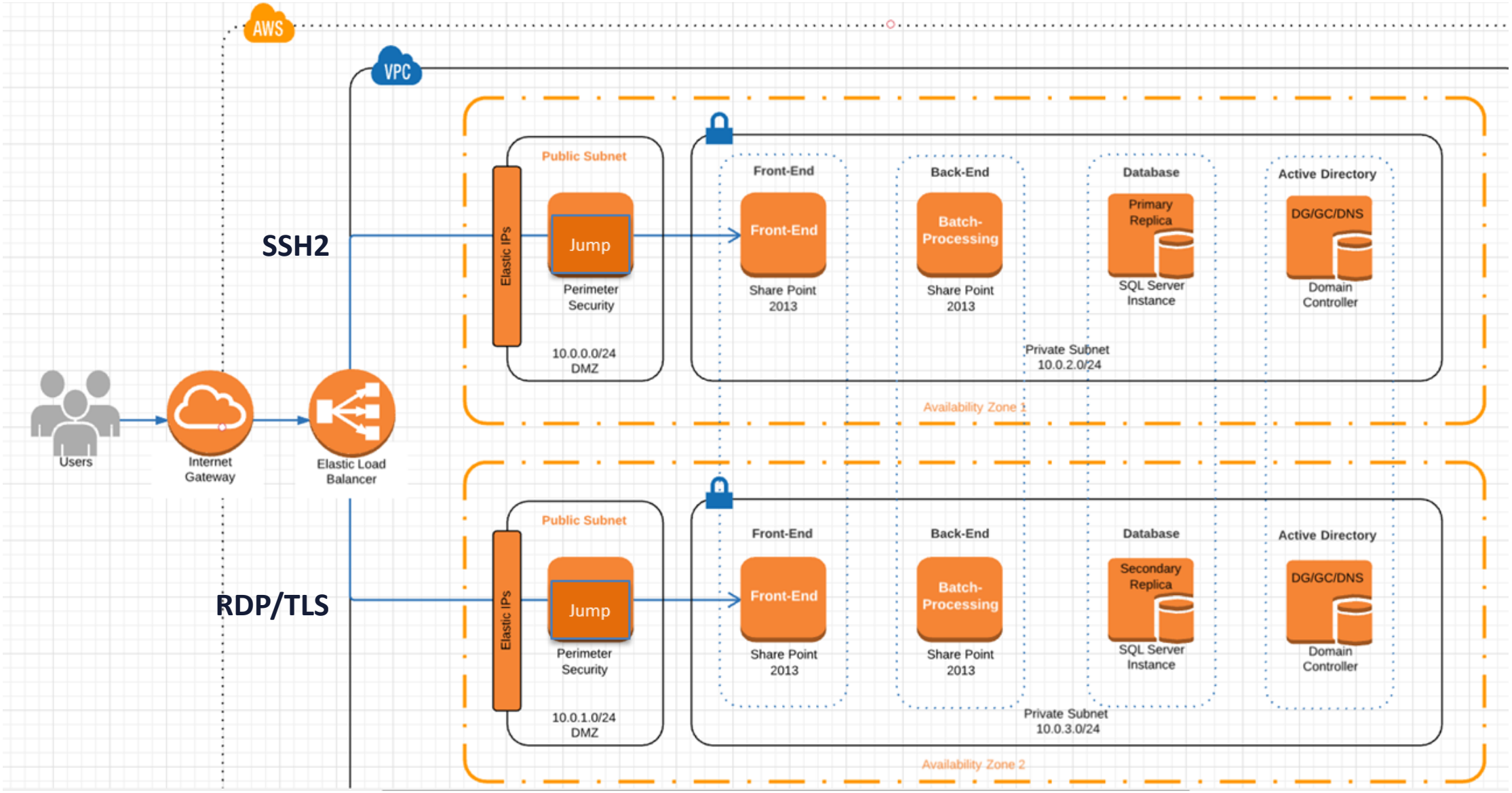
Storage and Network Controllers: Best Practices

- **Storage controllers may be in use for iSCSI, Fiber Channel (FC), or Fiber Channel over Ethernet (FCoE) – uses initiators and targets**
- Prevent oversubscription with a dedicated LAN for iSCSI traffic
- Do not share the storage network with other network traffic such as management, fault tolerance or vMotion/Live Migration
- Use encryption mechanisms such as IPsec AH or 802.11AE MACsec

Storage and Network Controllers: Best Practices (Continued)

- iSCSI can use several authentication mechanisms: Kerberos, Secure Remote Password (SRP), or SPKM1/2 (Simple Public-Key Mechanism)
- The key to virtual network security is isolation and compartmentalization using VXLAN, SDS, and PVLAN implementations
- When using internal and external networks, always create a separate isolated virtual switch with its own physical network interface cards and do not mix internal and external traffic on the virtual switches

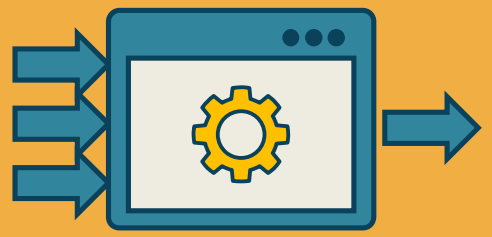
Using Bastion (Jump) Hosts



AWS Systems Manager

- Systems Manager enables you to manage servers running on AWS and in your on-premises data center through a single interface
- It securely communicates with a lightweight agent installed on your servers to execute management tasks
- This helps you manage resources for Windows and Linux operating systems running on Amazon EC2 or on-premises
- With **Session Manager**, you can easily and securely access your instances through an interactive one-click browser-based shell or through the AWS CLI without having to open inbound ports, maintain bastion hosts, or manage SSH keys

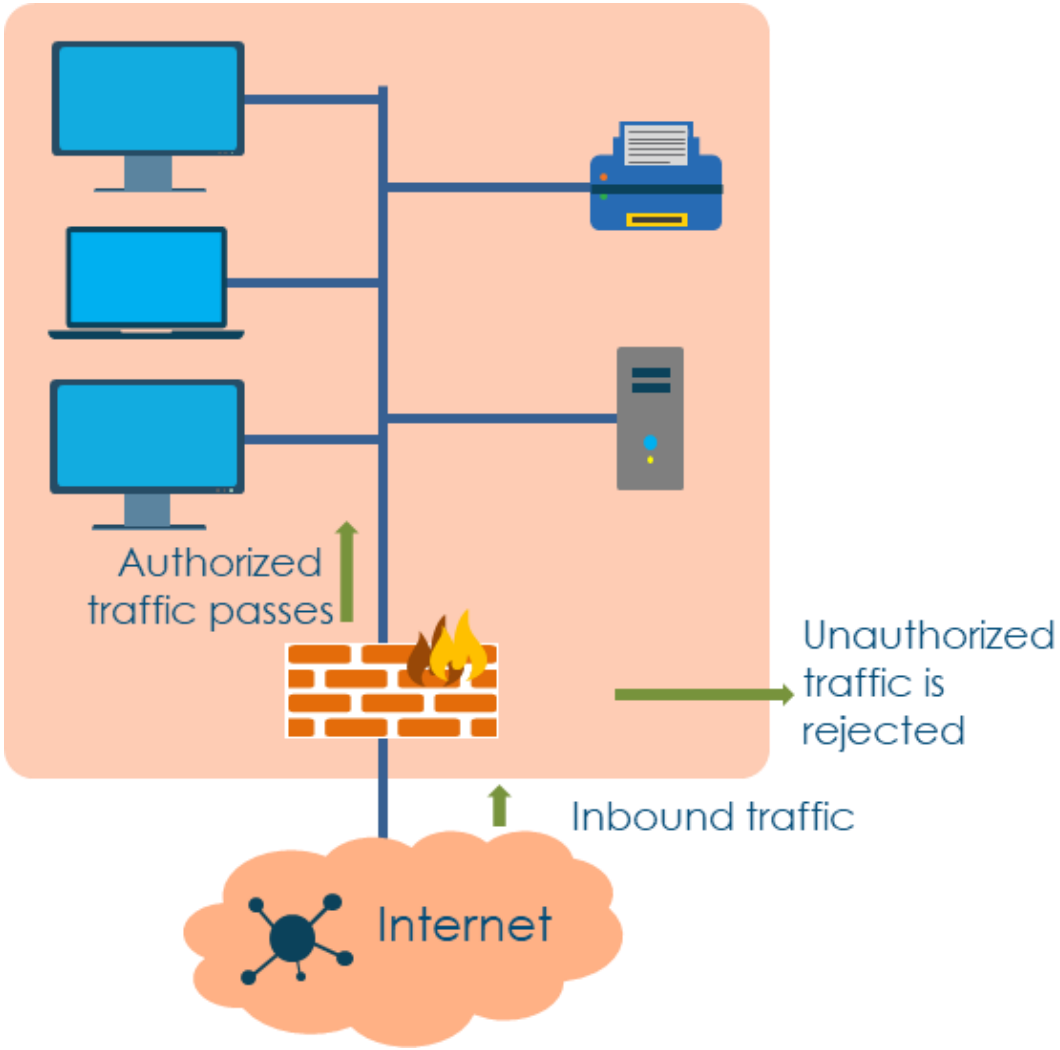
AWS AppStream



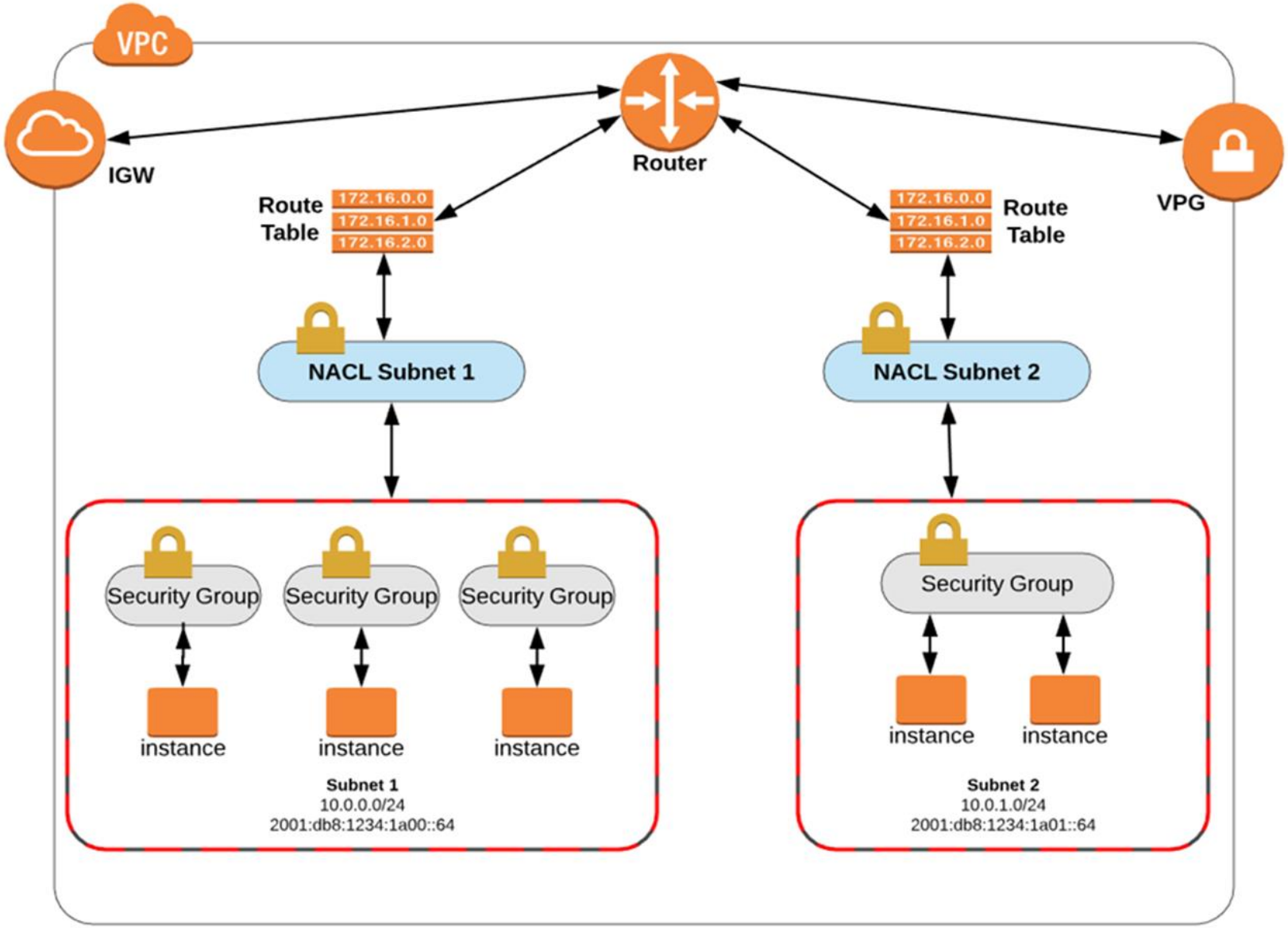
- An SSO dynamic bastion solution to allow your administrators to manage their environment without giving them a full (possibly unsecure) bastion/jump host
- AppStream spins-up fresh instances each time a user requests access, a compromised instance will only last for the duration of a user session
- As soon as the session closes and the Disconnect Timeout period is reached, AppStream terminates the instance
- You will also potentially reduce your costs because AppStream 2.0 has built-in auto-scaling to increase and decrease capacity based on user demand

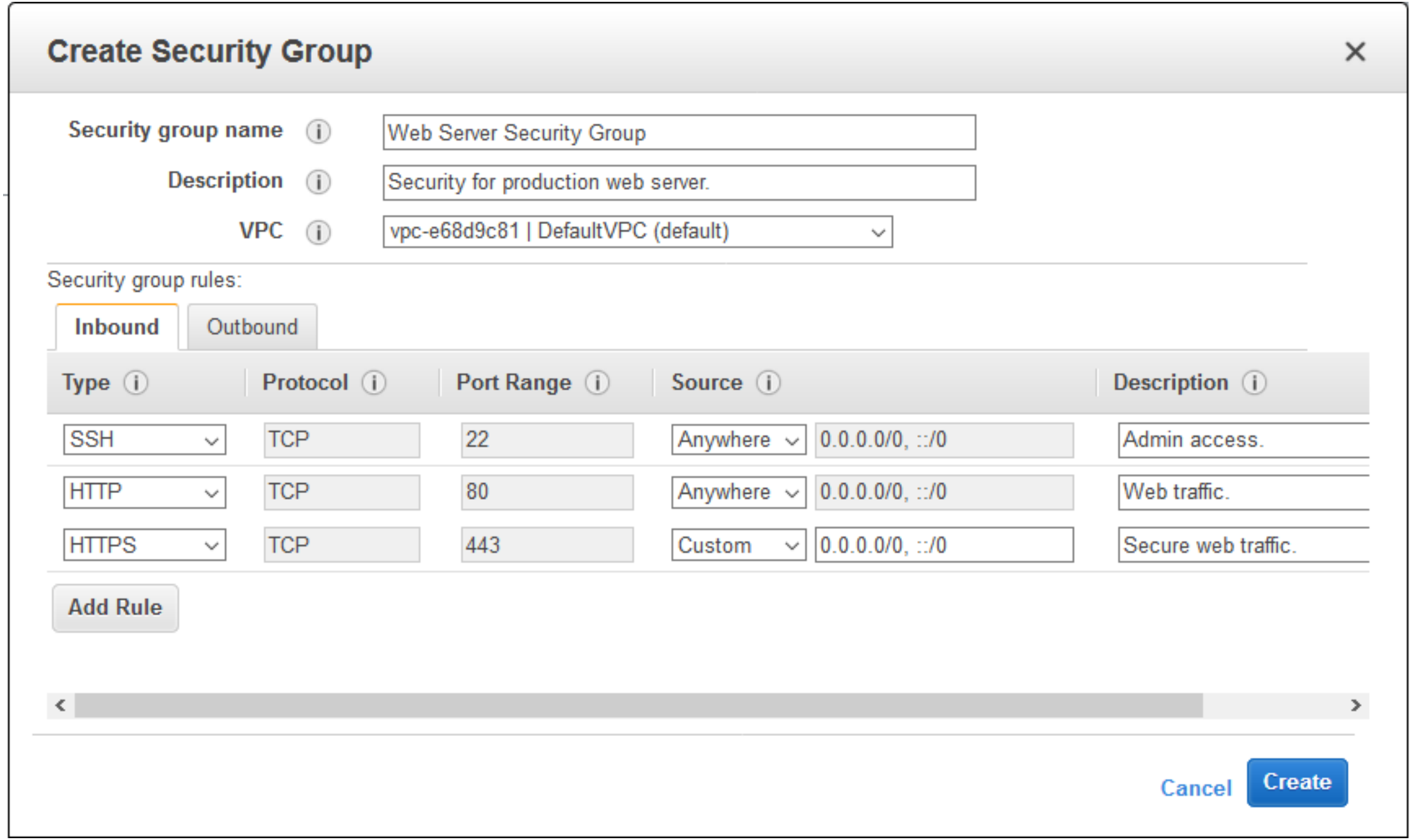
Next Generation Firewalls

- Operate from Layer 2 (transparent) through 7
- Layer 5-7 policies (DPI, AVC), Content security, and Data Loss Prevention engines
- Authentication proxies (Interactive and Transparent
- Identity services (for IdM, ABAC, and Zero Trust)
- Integrated or modular IDS/IPS
- Advanced cloud-based malware prevention
- URL and Botnet filtering

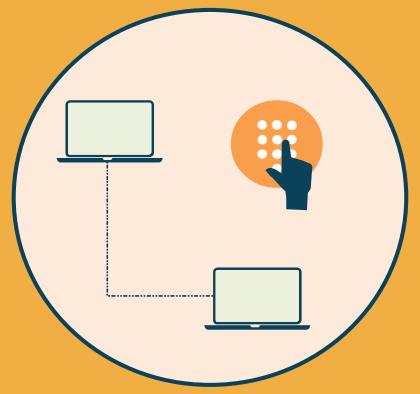


Network Security Groups




Create Security Group
Security group name
Web Server Security Group
Description
Security for production web server.
VPC
vpc-e68d9c81 | DefaultVPC (default)
Security group rules:
Inbound
Outbound
Type
Protocol
Port Range
Source
Description
SSH
TCP
22
Anywhere
0.0.0.0/0, ::/0
Admin access.
HTTP
TCP
80
Anywhere
0.0.0.0/0, ::/0
Web traffic.
HTTPS
TCP
443
Custom
0.0.0.0/0, ::/0
Secure web traffic.
Add Rule
Cancel
Create

Secure KVM



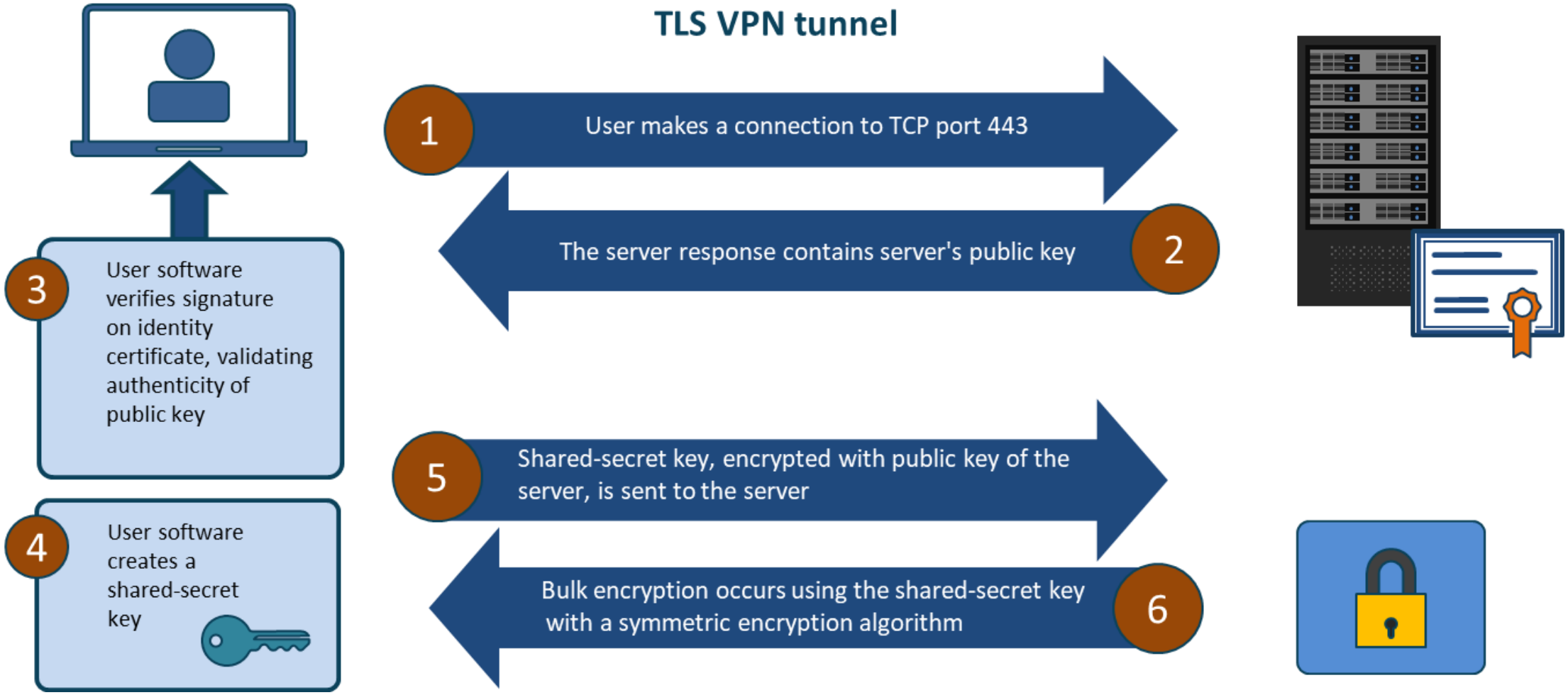
- Access to hosts should be done by secure KVM and access to KVM devices should require a checkout (service desk) process
- Secure KVM will prevent data leakage from the server to the connected computer, as well as preventing unsecure emanations
- According to the Common Criteria, a secure KVM will do the following:
  - Isolated data channels
  - Tamper-warning labels on each side of the KVM
  - Housing intrusion detection
  - Fixed firmware
  - Tamper-proof circuit board
  - Safe buffer design
  - Selective USB access
  - Push-button control

Domain Name System Security Extensions (DNSSEC)

- DNSSEC (DNS Security Extensions) protects users from DNS attacks and forces systems to detect DNS attacks
- It adds a layer of trust on top of DNS by providing authentication while the root DNS name servers help verify domains
- MSSP solutions such as OpenDNS and Cisco Umbrella are also common

- To facilitate signature validation, DNSSEC adds a few new DNS record types:
  - RRSIG – contains a cryptographic signature
  - DNSKEY – contains a public signing key
  - DS – contains the hash of a DNSKEY record
  - NSEC and NSEC3 – for explicit denial-of-existence of a DNS record
  - CDNSKEY and CDS – for a child zone requesting updates to DS record(s) in the parent zone

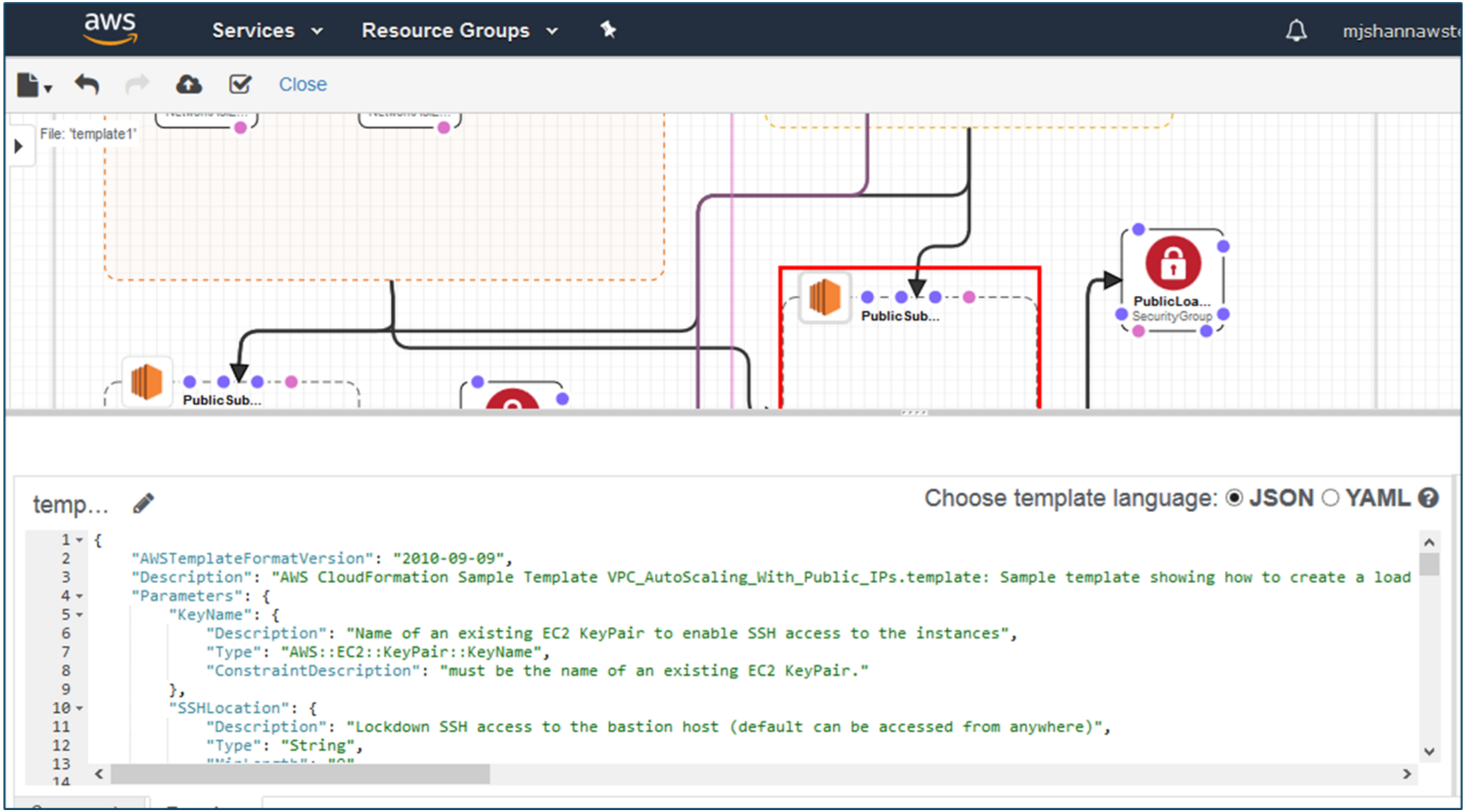
Transport Layer Security (TLS)



TLS Best Practices

- Prevent downgrade attacks from web clients
- Use HTTP Strict Transport Security (HSTS)
- Use the most recent security suites (no RC4 or DES/3DES)
- Do not let vendor-installed code intercept traffic
- Verify encryption
- Perform OCSP stapling from browsers to enforce certificate expirations
- Implement Certificate Pinning to trusted CAs

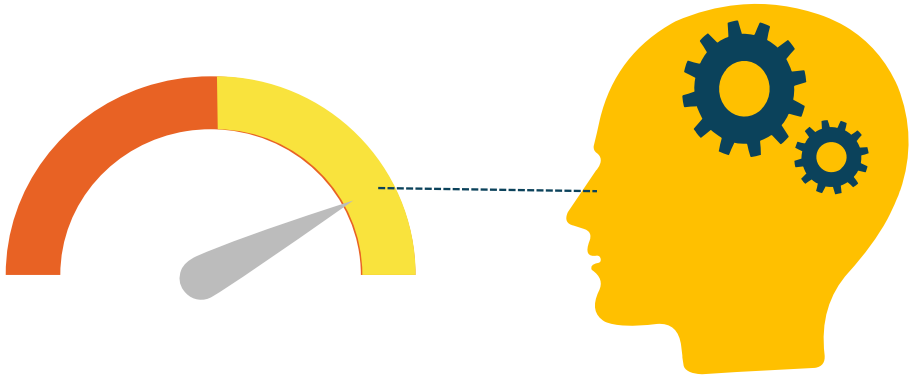
Infrastructure as Code (IaC)



Benchmarks

CIS, CSA, ISO/IEC, DoD

- A technique to improve 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



Distributed Resource Scheduling (DRS)

- DRS continually monitors your cluster utilization to assure that VMs get their resources in the most optimal fashion
- DRS is responsible for keeping the cluster balanced, so the utilization of the ESXi hosts is equal
- DRS also works closely with resource management that guarantee specific resources for your VMs
- DRS constantly monitors a lot of parameters for the peak performance and placement:
  - Host resource capacity
  - Resource reservations
  - Datastore connectivity
  - Actual resource demand from virtual machines
  - Reservations, Shares and Limits (R, L, S)

Dynamic Optimization (DO)

- Dynamic optimization facilitates live migration of VMs and VHDs within a host cluster
- The migration is based on designated settings to improve load balancing among hosts and cluster shared storage, and to correct the placement issues for VMs
  - **Compute Dynamic optimization** is the optimization of hosts in a cluster to optimize performance by migrating VMs across host
  - Host performance thresholds CPU and Memory
  - **Storage Dynamic Optimization** is optimization of disk space and is performed on cluster shared storage (CSV, file shares) to optimize storage space availability by migrating Virtual Hard Disks (VHD) across shared storage
  - You can set free storage space threshold on cluster shared storage

Storage Clusters

- Storage clusters are also referred to as storage pods or Datastore clusters
- A datastore cluster is a collection of datastores with shared resources and a shared management interface
- Datastore clusters are to datastores what clusters are to hosts
- When you create a datastore cluster, you can use a tool like Storage Distributed Resource Scheduling (DRS) to manage storage resources for:
  - Space utilization load balancing
  - I/O latency load balancing
  - Anti-affinity rules

5.4 Implement Operational Controls and Standards (e.g., ITIL 4, ISO/IEC 20000-1)

- Change Management
- Continuity Management
- Information Security Management
- Continual Service Improvement Management
- Incident Management
- Problem Management

5.4 Implement Operational Controls and Standards (cont.)

- Release Management
- Deployment Management
- Configuration Management
- Service level Management
- Availability Management
- Capacity Management

Why Perform Forensic Investigations?

- 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
- Next phase of incident response

Forensic Lifecycle

1. Identification

Detecting the incident

- Once you have determined this is not an event but rather an incident that needs forensics, you will need to identify and classify
- Forensics may not occur until later in the incident response lifecycle (remediation or reporting)
- The notification can come from
  - personal complaint by phone or text
  - monitoring system alarm or alert
  - audit result
  - IDS/IPS/EDR sensor alarm, or
  - notification from trusted or anonymous source

2. Collection

Order of volatility sets the priority

1. CPU, cache, and register content
2. Routing table, ARP cache, process table, and kernel statistics
3. Memory
4. Temporary file system/swap space
5. Data on hard disk
6. Remotely logged data
7. Data on archival media

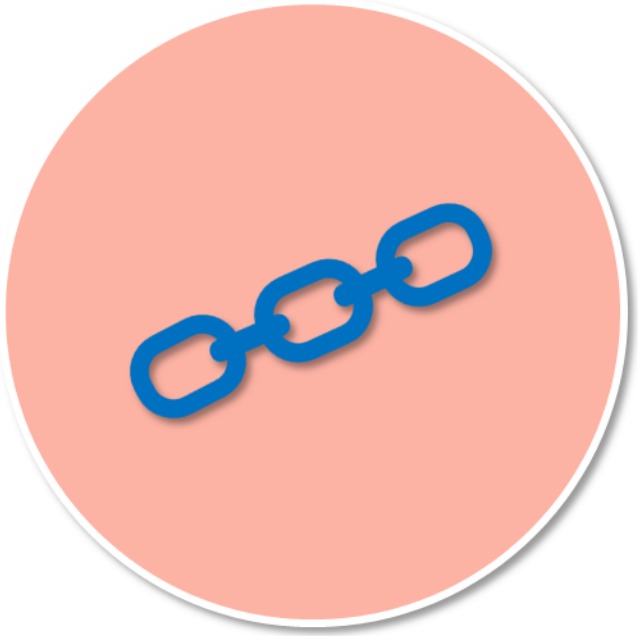
- Forensic toolkits (EnCase from Guidance) and write-blockers

Common utilities include:

- Tcpdump and dd
- nbtstat and netstat
- nc (Netcat)
- memcopy
- tshark
- foremost

2. Collection

Maintain the chain of custody



- Imaging technologies (create copies)
  - Memory dumps from write blockers
  - HDD bit-level copy, sector-by-sector
  - Include deleted files, slack spaces, and unallocated clusters
  - Look for encrypted volumes and files
- Digital pictures and interviews
- Provide a history of the handling of the evidence to maintain integrity, provide accountability, prohibit tampering, and provide assurance through the entire life cycle

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	

2. Collection

Media management

- Should have a software inventory system for configuration items and a category for components removed for investigative and forensic purposes
- Collected media (all types) must be classified and labelled
- Secure storage facilities with dual operators include
  - locked rooms
  - locked cabinets
  - safes, and
  - offsite storage facilities

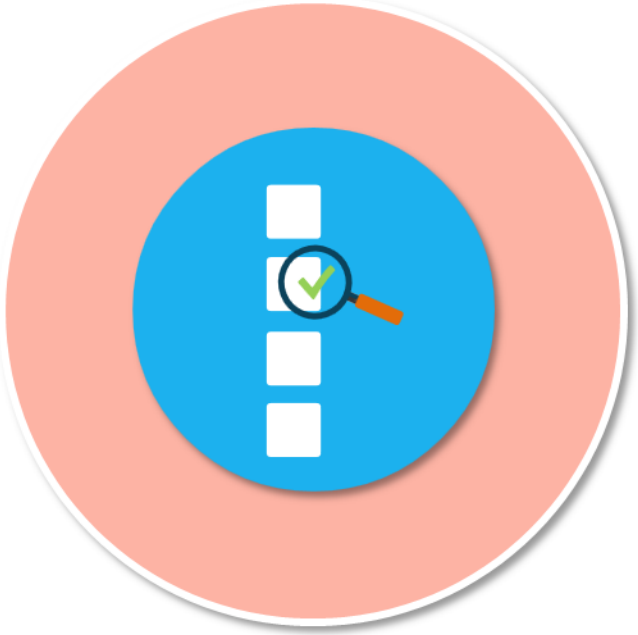
3. Examination

Where data becomes information

- Examination involves finding the relevant data in order to have the proper information to analyze in the next step
- Use tested techniques for
  - validation
  - filtering (i.e., user SIDs)
  - pattern matching
  - tracing
  - hidden data discovery, and
  - data extraction

4. Analysis

Building a solid forensic case



- Operating on the relevant data, facts, and artifacts from collection and examination phases
- May determine that more work should be done in earlier steps
  - If more information is needed, then iterate back to collection and examination
- Answer the 'who, what, where, when, why, and how?'
- Infer motive, opportunity, means
- Is a combination of an art and science that can take years to master
- Use expert judgment of others

5. 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

Non-Disclosure (Confidentiality) Agreements

- Also called "Confidentiality Agreements"
- Legal contract between two or more parties
  - Confidential relationship that is often strictly enforced
  - Business to business/business and employee
- Identifies confidential information they wish to share with each other
  - IP, trade secrets, technologies, campaigns, ideas, new processes, new products, and services
  - Restricts the sharing of that information with others
- Commonly used during interview process and then legally enforced for “leavers”

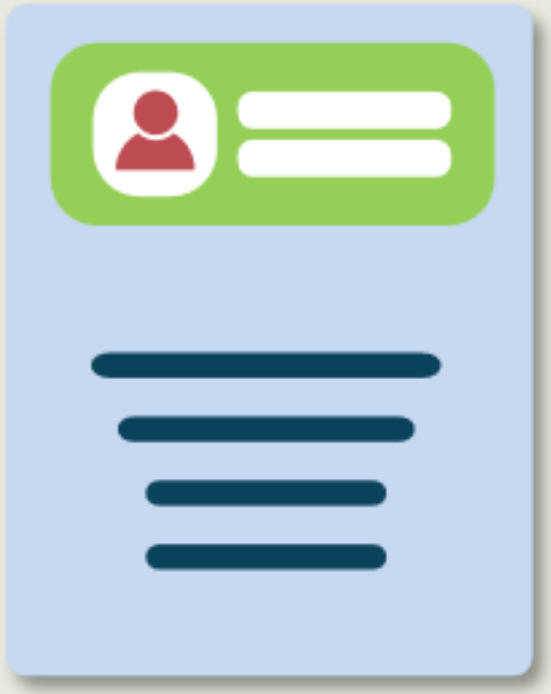
Service Level Agreements (SLA)

- Define the precise responsibilities of the service provider and set customer expectations
- Also clarify the support system (service desk) response to problems or outages for an agreed level of service
- Can be internal between business units or departments, as well as external
- Should be used with new third-party vendors or cloud providers (SaaS, IaaS, PaaS) for 24-hour support

Memorandum of Understanding (MOU)

- Also called a Memorandum of Agreement (MOA) or "letter of intent"
- A formal MOU (or MOA) usually precedes a more formal agreement or contract ISA
- It defines common courses of action and high-level roles and responsibilities in management of a cross-domain connection
- It will usually terminate the customer's provider search process so that subsequent time and resources can be dedicated to the next steps of the formal contract process

Reciprocal Agreements



- A reciprocal agreement is between two organizations with similar infrastructure and technology – often difficult to legally enforce
- The most common goal is that one can be a recovery site for the other in case of a disaster or lengthy outage
- Also seen with data backup and escrow services whereby two departments or organizations agree to store one each other's backup data on their computers

RACI Charts for Mapping Roles

R – Responsible **A** – Accountable **C** – Consulted **I** - Informed

	GRC* Department	Legal Department	Security Team	IT Operations
Establish the provider requirements	R/A	C	C	I
Build the governance scheme	R/A	C	C	I
Assess cloud vendor	A	I	R	R
Build the architecture	I	I	A/R	R
Conduct cloud migration	I	I	C	A/R

**GRC – Governance, Risk, and Compliance*

Security Operations Centers (SOC)

- For some organizations, the security operations is a function of the Network Operations Center (NOC)
- Many data centers have a centralized control center (or control tower) for continuous monitoring and visibility
  - Syslog, SNMPv3, SIEM, SOAR, and more
- The SOC does not have to be physically located in the data center or even on the same campus
- Most Cloud Service Providers have SOC's that are regional in scope and manage multiple zones (availability zones) and datacenters across a metropolitan area network (MAN) or Wide Area Network (SD-WAN) over high-speed fiber connections

4 Key SOAR Elements

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

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

3. Four types of Automation

a. Defensive Automation (anything that tries to prevent the threat or risk)

b. Forensic Automation (anything that tries to retrieve additional evidence)

c. Offensive Automation (anything pro-active that tries to investigate an asset)

d. Deception Automation (anything that retrieves or adjusts deception tools)

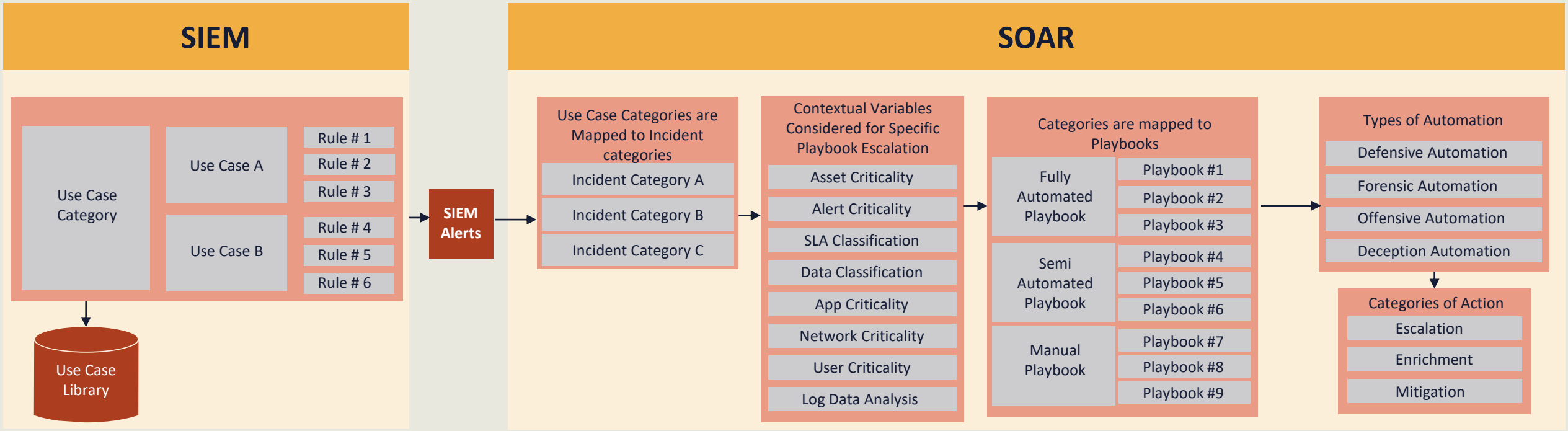
4. Three different categories of action

a. Enrichment (adding additional CMDB or environment data)

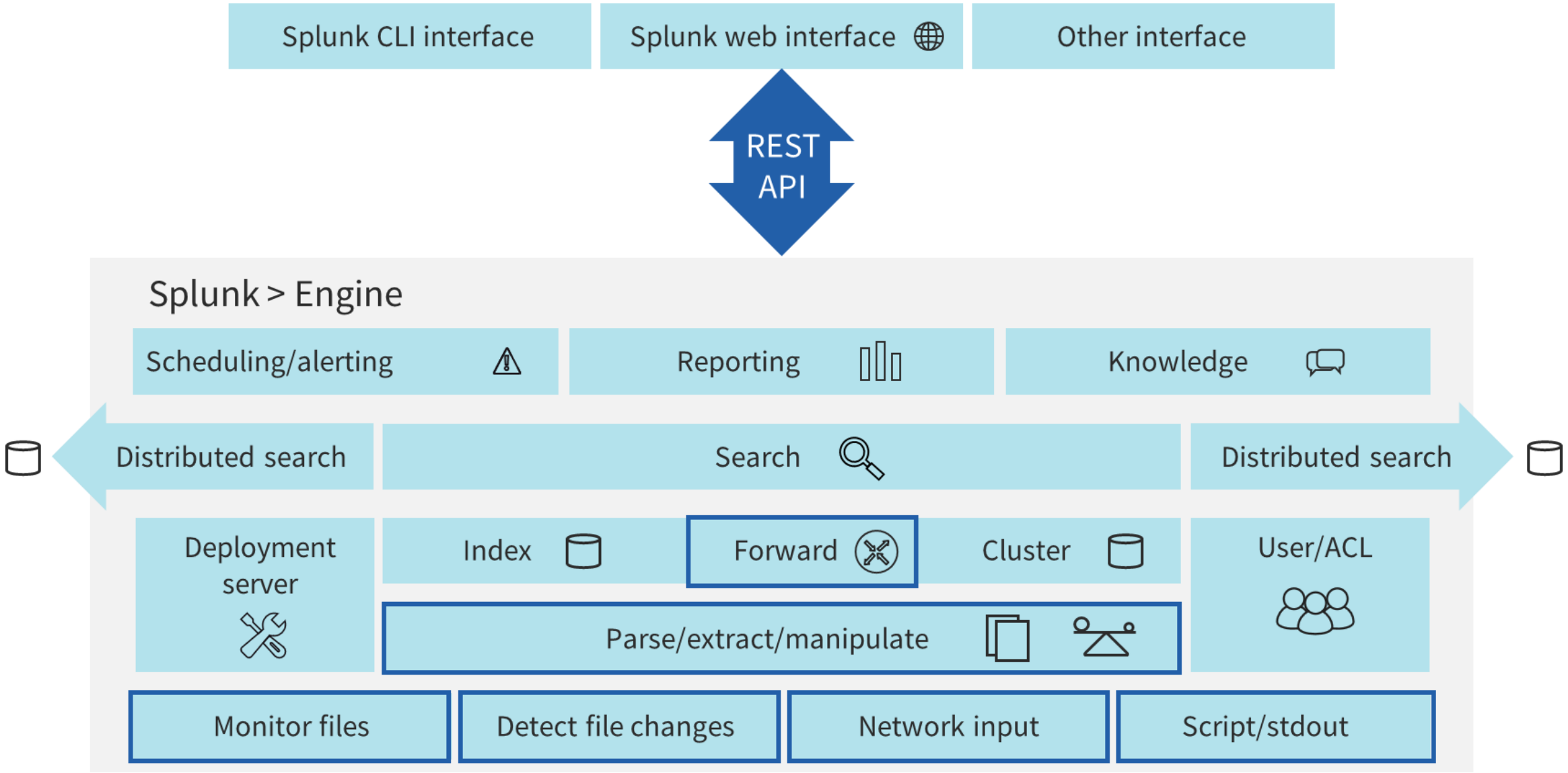
b. Escalation (e-mail, ticket escalation, SNS, chat/messaging communication)

c. Mitigation (the modification of device configuration)

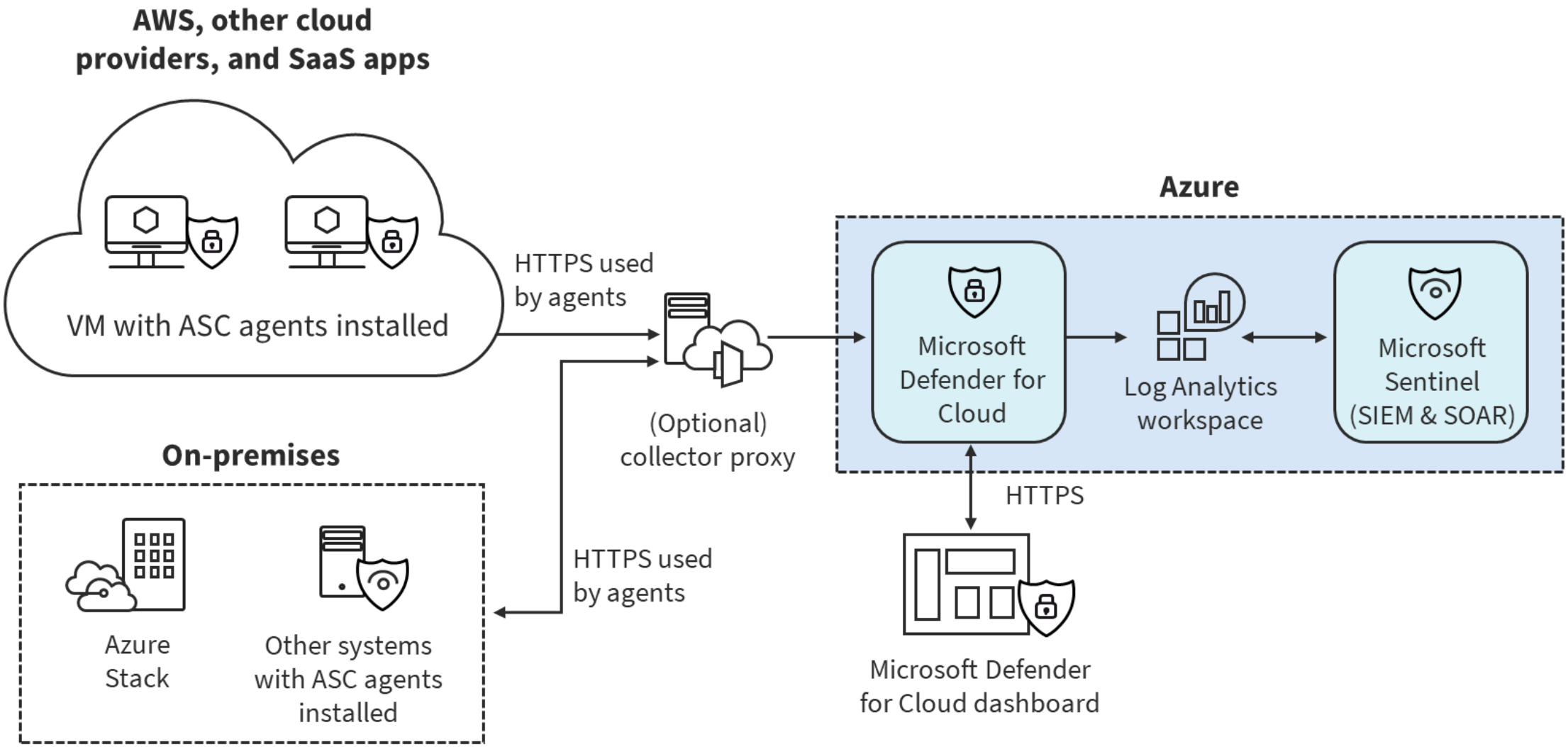
SIEM AND SOAR



Example: Splunk SIEM



Example: Azure Sentinel



Incident Management and Response

- Steps taken when a negative event disrupts normal operations
- Primary goal is to reduce the immediate impact
- Should have documented incident types/category definitions
  based on risk assessments, risk registers, and business impact analysis (BIA)
- Know roles and responsibilities of the first responders, including reporting requirements and escalation processes
- Collect contact lists, public relations people, and legal teams
- Best practice is to have pre-performed exercises, drills, and simulations

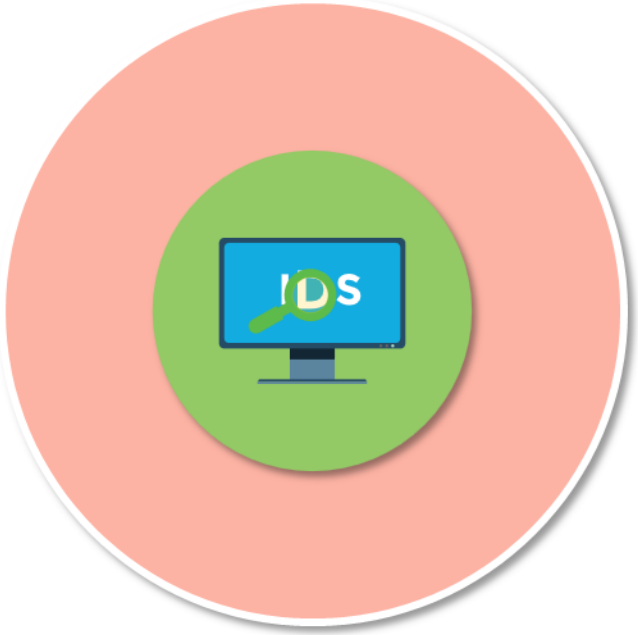
Incident Response Lifecycle

Preparation

- Involves all information gathering, missions, charters, and project initiation tasks
- Get buy-in and funding from executive management in order to know the scope of the response plan
- Establish incident response teams
  - Determine the roles and responsibilities of internal employees on incident response teams
- Establish first responders and processes for communication to relevant stakeholders
- Conduct IR exercises and drills based on budget

Incident Response Lifecycle

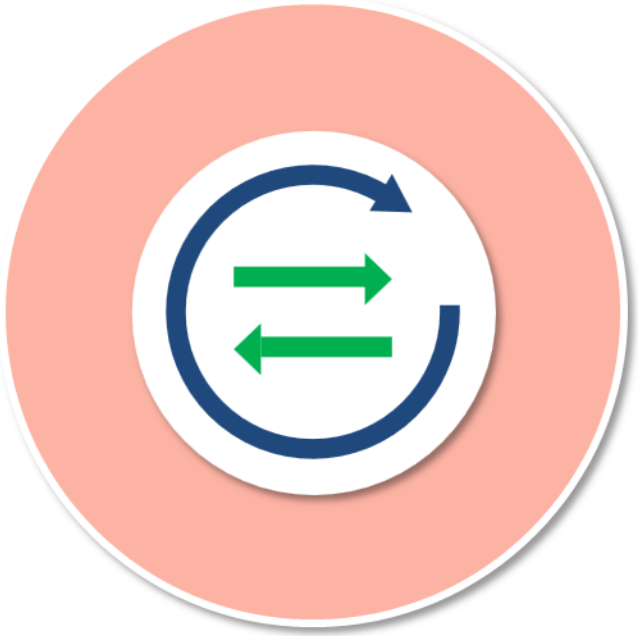
Detection



- Also referred to as "Identification"
- Separate an event from an incident or breach immediately, using pre-defined metrics and experience
- Categorize and prioritize the incident based on an established risk register or risk ledger
    - When did it occur?
    - How were you alerted?
    - Who made the discovery?
    - What is the scope of impact?
    - Does it qualify for escalation or disaster recovery?
    - **Can you quickly identify the root cause?**

Incident Response Lifecycle

Response



- Main goal is containment of the outbreak or malware exploit
- Implement short-term processes, such as disconnecting devices from the network
- Use firewalls, NG-IPS, ML algorithms, and other forensic tools to maintain separation, containment, and segregation
- Evaluate backups and snapshots for future recovery

Incident Response Lifecycle

Mitigation

- This step is also called "eradication" and is often integrated with the previous phase, Containment/Response, as opposed to being a separate action
- Involves determining the root cause of the incident and applying immediate remedies if available
- Involves removing all indicators of compromise and any action, artifacts, remnants, or fingerprints associated with the attack

Incident Response Lifecycle

Recovery

- The process of restoring negatively affected data, applications, systems, and devices to an established baseline performance level or, if possible, the original state
- **This often involves only remediation to a certain operational point and not total recovery**
- During this process, it is vital to establish that you are not in danger of another incident or breach
- Will often involve business impact analysis (BIA) metrics and indicators like RTO, RPO, and MTTR

Incident Response Lifecycle

Remediation

- This is more elaborate than recovery, as it involves a remedy that puts the application or system into a state before the incident occurred
- Remediation may take hours or weeks depending on the fact that the incident may rise to the state of a disaster or catastrophe and business continuity is occurring
- Recovery and remediation are often combined into the same phase or stage of incident response

Incident Response Lifecycle

Reporting

- Reports should be generated from physical, digital, and/or audio notes taken throughout the entire process
- Final reports should meet these requirements:
  - Be concise and comprehensive
  - Generate with different audiences in mind
  - Use newer graphical representation with Python and R programming tools
  - Include recommendations to prevent future incidents
  - Take problem management into consideration

Incident Response Lifecycle

Lessons learned

- Knowledge gained from the process of conducting the program
- Sessions usually held at the response close-out
- To share and use knowledge derived from an experience
- Endorse the recurrence of positive outcomes
- Prevent the recurrence of negative outcomes
- Try to avoid "blamestorming," although someone may be ultimately held accountable if expected due care and diligence were not performed

Vulnerability Assessment Sources and Tools

- Various logs and SNMPv3 traps
- NetFlow and SIEM collection
- Next-Generation IPS and EDR alerts and logs
- Hybrid cloud-based visibility tools using machine learning and artificial intelligence data analysis
- Vulnerability databases (Common Vulnerabilities and Exposures (CVE) with MITRE, NVD, etc.
- Toolkits such as Kali Linux, Parrot, ADHD
- Web application vulnerability scanners are most common due to heavy usage of HTTP (e.g., Burp Suite and OWASP ZAP)

Domain 6

Legal, Risk and Compliance

PROCESS OF SETTING LEGAL AND REGULATORY REQUIREMENTS

1. Understand the law and relevant regulations that apply to the organization
2. Classify data or operations that might require special attention
3. Establish provider contractual negotiation guidelines
4. Set provider evaluation criteria
5. Understand requirements coming from contractual obligations

Evaluation of Legal Risks Specific to Cloud Computing

- Data Privacy and Security (GDPR, PCI-DSS, HIPAA)
- Data Ownership (intellectual property rights and DRM/IRM in various agreements and contracts
- Liability for copyright infringement, data breaches, and privacy violations
- Primary and secondary loss
- Legal issues resulting from counter-attack active defense
- Jurisdictional Issues (import-export, cultural sensitivities)

ISO/IEC 27050

- Information Technology Electronic Discovery Package offers guidance methods on establishing the electronic discovery process
- The ISO/IEC 27050 series enables the user to identify, collect, preserve, process, review, and analyze electronically stored information
- Electronic discovery often serves as a driver for investigations as well as evidence acquisition and handling activities
- **Exam: It is not intended to contradict or supersede local jurisdictional laws and regulations**

The eDiscovery Process

1. **Identification**: electronically stored information (ESI) that is possibly significant to a case is recognized, along with its locations, custodians, sizes/volumes, etc.
2. **Preservation**: the identified, potentially relevant ESI is placed under a legal hold, starting the official forensic process designed to ensure, beyond doubt, that the info is protected
3. **Collection**: ESI is assembled from the original custodian, usually by physically removing the original digital storage media into a safe chain of custody

The eDiscovery Process

4. **Processing**: forensic bit copies are stored in a manner that lets them be searched or analyzed for information and knowledge that is applicable to the case, using appropriate forensic tools and platforms
5. **Review**: forensic bit copies are searched or analyzed for information that is relevant to the case
6. **Analysis**: the information is further scrutinized and evaluated as to its significance, suitability, weight, connotation, implications, etc.
7. **Production**: applicable information from the analysis, plus the original storage media, etc., is officially offered to the court as evidence

Contractual vs. Regulated Private Data

In cloud computing, the legal responsibility for data processing falls to the consumer or user who solicits the services of a CSP

As in all other cases in which a third party is given the task of processing personal data, the user, or data controller, is responsible for ensuring that the relevant requirements for the protection and compliance with requirements for PII and PHI are satisfied or met

- **Contractual PII**
- Where an organization or entity processes, transmits, or stores PII **as part of its business or services**, this information is required to be adequately protected in line with relevant local state, national, regional, federal, or other laws
- The relevant contract should list the applicable rules and requirements from the organization who "owns" the data and the applicable laws to which the provider should adhere

- **Regulated PII**
- The key focus and distinct criteria to which the regulated PII must adhere is required **under law and statutory requirements**, as opposed to the contractual criteria that may be based on best practice or organizational security policies

Trans-border Data and Information Flow

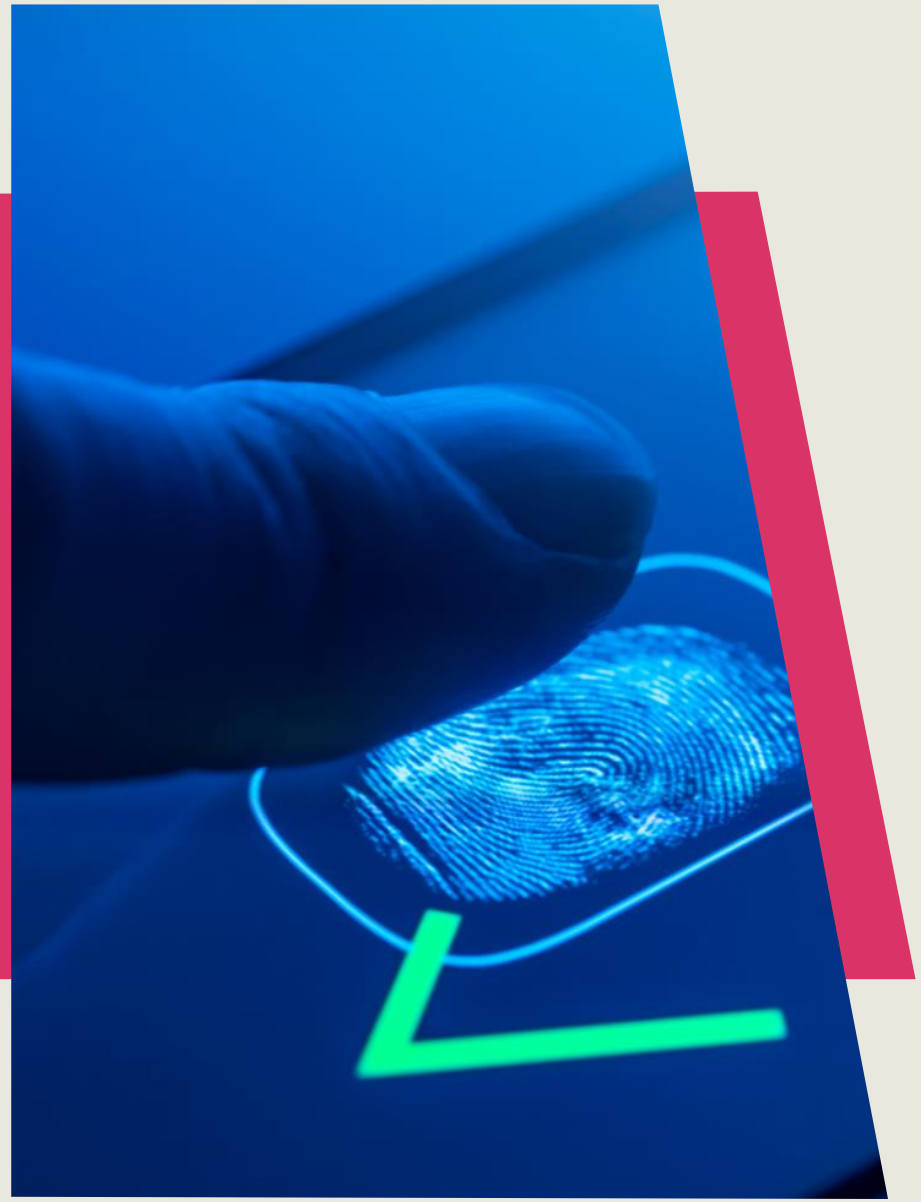
- Considerations should always include the flow of data, information, and goods across international borders and all legal and regulatory implications
  - These issues can change rapidly based on various geo-political factors
- Security initiatives must also consider variances in cultural norms
  - Customs, sensitivities, and behaviors (for example, U.S vs. Arab customs)

Trans-border Data and Information Flow

- Policies, controls, and procedures can differ based on region
- Countries are typically under different regulations and mandates
  - AGATE, IDABC, OBASHI, ITIL, ISO, or TOGAF
  - The Department of Commerce's Bureau of Industry and Security (BIS) controls nonmilitary cryptographic exports
- Cloud computing is transcending traditional boundaries and jurisdictional barriers and introducing new challenges

ISO/IEC 27002

- Establishes commonly-accepted control objectives and best practices for implementing measures to protect PII in line with the privacy principles in ISO/IEC 29100 for the public cloud computing environment
- Stipulates guidelines based on ISO/IEC 27002, taking into consideration the regulatory requirements for the protection of PII which can apply to a public cloud service provider’s information security risk environment



ISO/IEC 27002

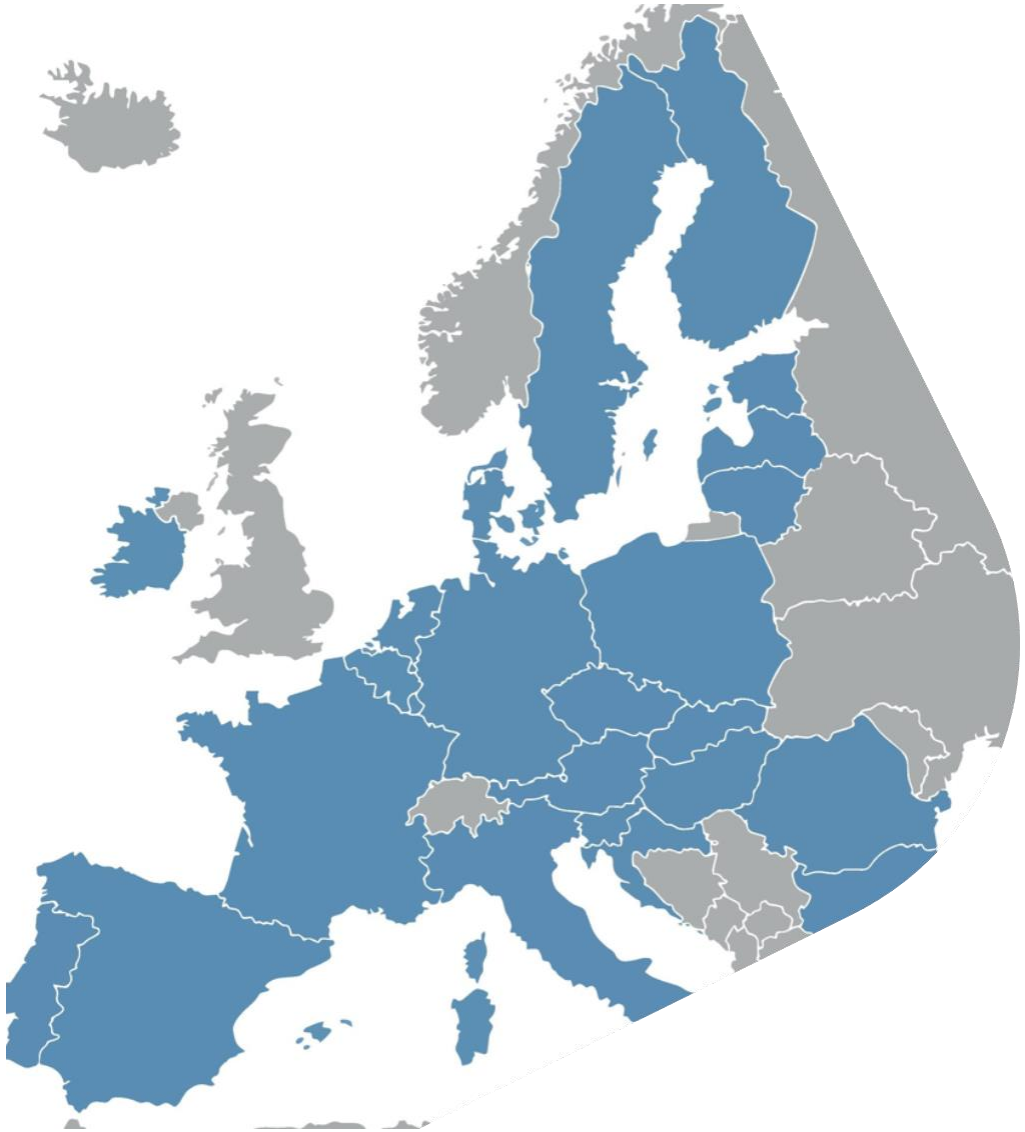
- ISO/IEC 27002 applies to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which provide information processing services as PII processors using contractual cloud computing with other entities
- The guidelines can also apply to enterprises acting as PII controllers
- However, PII controllers can be subject to additional PII protection legislation, regulations and obligations, not applying to PII processors

GAPP and PMF

- The Privacy Management Framework (PMF) is often used as an initial component in launching and operating a comprehensive information privacy initiative
- The PMF was created as an update to the former 2009 Generally Accepted Privacy Principles (GAPP)
- Because of significant changes in technologies and in global, country-specific, local information and data privacy laws and standards, including the publication of the GDPR, the AICPA Privacy Task Force updated the PMF in 2020

General Data Protection Regulation

- General Data Protection Regulation (GDPR) addresses data protection and privacy in the EU and all other areas, citizens, and areas under its jurisdiction, regardless of where the data is created, used, or stored
- It does apply to other countries doing business with EU entities and is very strict
- The European Court of Justice (ECJ) nullified the U.S.-EU Safe Harbor agreement between the EU and the U.S. Department of Commerce in 2015

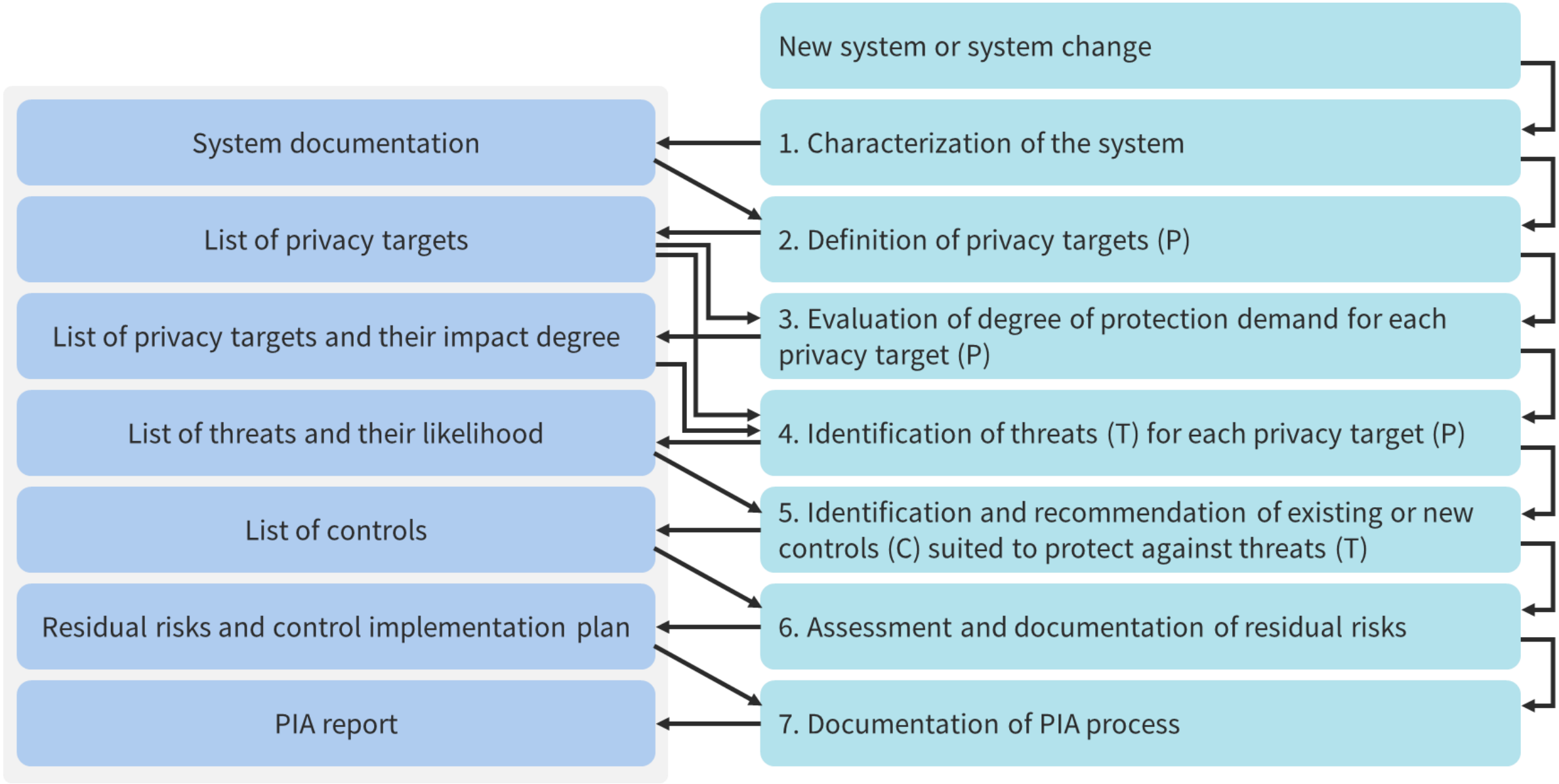


General Data Protection Regulation

- The Privacy Shield Framework then replaced Safe Harbor
- March 25, 2022: The U.S. and European Commission announced an agreement in principle on a new "Trans-Atlantic Data Privacy Framework" to foster trans-Atlantic data flows and address concerns raised by the Court of Justice of the EU in the Schrems II decision of July 2020

Privacy Impact Assessments (PIA)

- A privacy impact assessment (PIA) is an analysis of how personally identifiable information (PII) is treated to maintain compliance with applicable regulations
- It governs the risks associated with information systems or activities, and finds ways to reduce the risks to privacy
- The PIA is a decision tool used by DHS to identify and mitigate privacy risks that notifies the public: What PII DHS is collecting; Why the PII is being collected; and How the PII will be collected, used, accessed, shared, safeguarded and stored


New system or system change
System documentation
1. Characterization of the system
List of privacy targets
2. Definition of privacy targets (P)
List of privacy targets and their impact degree
3. Evaluation of degree of protection demand for each privacy target (P)
List of threats and their likelihood
4. Identification of threats (T) for each privacy target (P)
List of controls
5. Identification and recommendation of existing or new controls (C) suited to protect against threats (T)
Residual risks and control implementation plan
6. Assessment and documentation of residual risks
PIA report
7. Documentation of PIA process

Statement on Standards for Attestation Engagements (SSAE)

- Statement on Standards for Attestation Engagement (SSAE) 18 is an American auditing standard issued by the American Institute of Certified Public Accountants (AIPCA)
- It addresses engagements undertaken by a service auditor for reporting on controls at service organizations that provide services to user entities, for which a service organization's controls are likely to be relevant to a user entities internal control over financial reporting
- The SSAE 18 standard is used to produce three types of System and Organization Controls (SOC) reports - SOC 1, 2 and 3

COMPARING SECURITY AUDITING STANDARDS

Standards applicable to cloud security auditing.			
Standard	**Type**	**Strength**	**Sponsoring organization**
Service Organization Control (SOC) 2	Audit for outsourced services	Technology neutral	American Institute of CPAs
ISO 27001 and 27002	Traditional security audit	Technology neutral	ISO
NIST 800-53 rev, 4	Federal government audit	Technology neutral	National Institute of Standards and Technology
Cloud Security Alliance (CSA)	Cloud-specified audit	Dedicated to cloud security auditing	CSA
Payment Card Industry (PCI) Data Security Standard (DSS)	PCI Qualified Security Assessor cloud supplement	Cloud specific and Provides guidance	PCI DSS

Internal Information Security Management System (ISMS)

- An Information Security Management System defines and demonstrates an organization's approach to information security and privacy
- It assists in the identification and assessment of the threats and opportunities to information and any related assets
- ISMS protects the enterprise from data breaches and defends against the resulting disruptions
- Help you win new business from competitors and enter new sectors
  - Strengthen your relationship with your existing customers
  - Build your organization's brand and reputation
  - Protect your business from security breaches

Risk Treatment

- Risk acceptance (retain)
  - Do not implement any safeguards
  - Justification in writing is often required
- Risk avoidance
  - Choose not to undertake actions that introduce risk
- Risk transference/sharing
  - Pass the risk to a third-party, such as an insurance company or a cloud service provider
- Risk mitigation (modify)
  - Implement safeguards that will eliminate or reduce risk exposure - risk may exist, but impact is reduced

NIST SP 800-30

- NIST Risk Management Guide for Information Technology System:
  - If control would reduce risk more than needed, then see whether a less expensive alternative exists
  - If control would cost more than the risk reduction provided, then find something else
  - If control does not reduce risk sufficiently, then look for more controls or a different control
  - If control provides enough risk reduction and is cost-effective, then use it

Data Ownership

- Owner/Controller – is often the creator of the information/data in DAC model
  - Can categorize and determines classification or sensitivity level
- Custodian – Is the keeper of the information from a technical perspective
  - Ensures that CIA is maintained
- Steward - Manages the data and metadata from a business perspective
  - Ensures compliance (standards/controls) and data quality
- Processor – performs data input and runs batch jobs
- Chief privacy officer - ensures privacy of all data in the entire organization
  - The one accountable (RACI) for due diligence and due care

CSA Cloud Controls Matrix (CCM) and the Consensus Assessment Initiative Questionnaire (CAIQ)

- The CCM is 197 control objectives structured in 17 domains covering all key aspects of cloud technology
- Often used for the systematic assessment of a cloud implementation
- Offers guidance on which security controls should be implemented by which actor within the cloud supply chain
- It is considered the de-facto standard for cloud security assurance and compliance
- The STAR Level 1: Security Questionnaire (CAIQ v4) offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services

Metrics for Risk Management (CCM Domains)

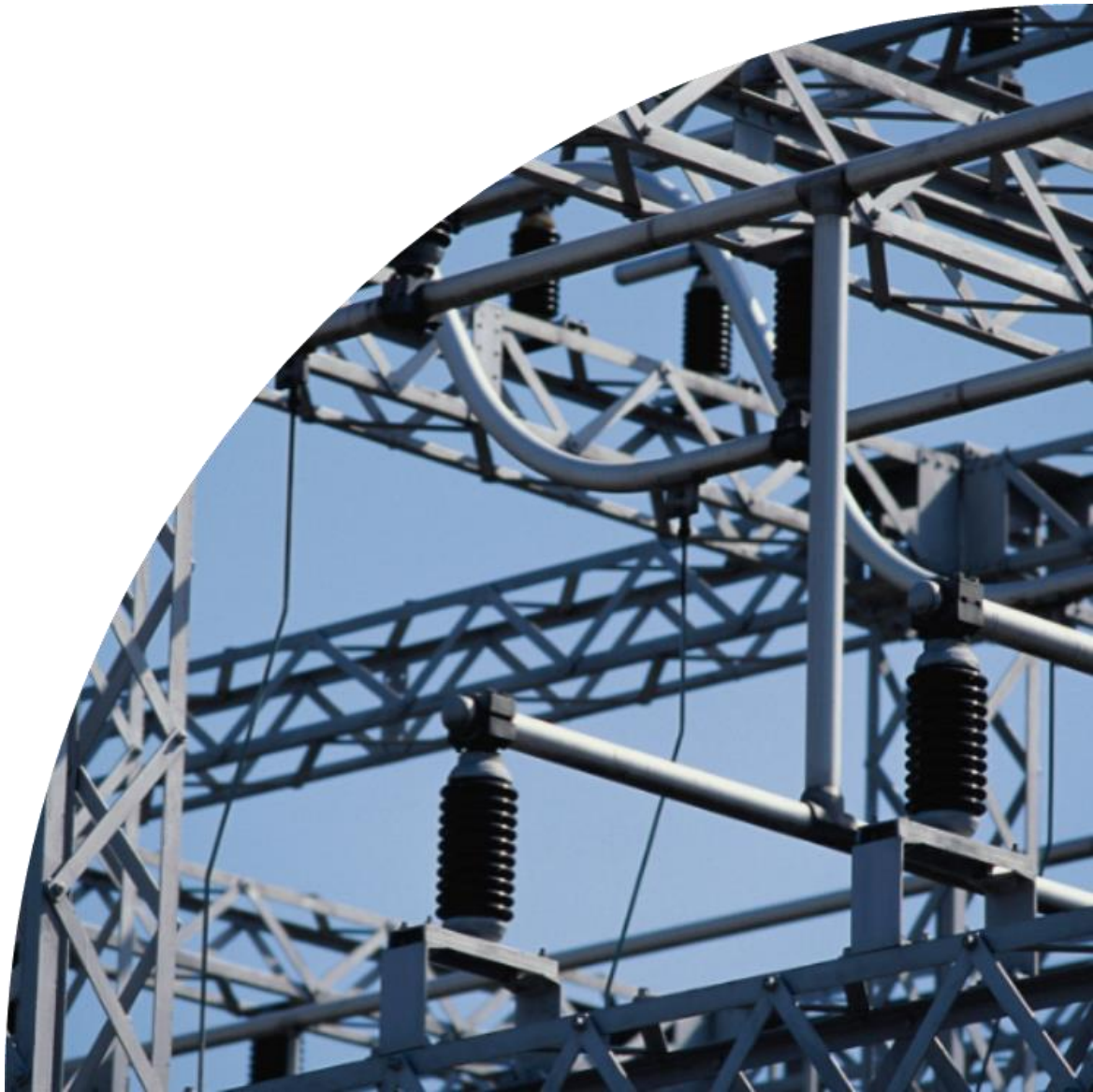
- Application & Interface Security (AIS)
- Audit Assurance & Compliance (AAC)
- Business Continuity Management & Operational Resilience (BCR)
- Change Control & Configuration Management (CCC)
- Data Security & Information Lifecycle Management (DSI)
- Datacenter Security (DCS)
- Encryption & Key Management (EKM)
- Governance & Risk Management (GRM)
- Human Resources (HRS)
- Identity & Access Management (IAM)
- Infrastructure & Virtualization Security (IVS)
- Interoperability & Portability (IPY)
- Mobile Security (MOS)
- Security Incident Management, E-Discovery, & Cloud Forensics (SEF)
- Supply Chain Management, Transparency, and Accountability (STA)
- Threat & Vulnerability Management

Highly Regulated Industries: NERC/CIP

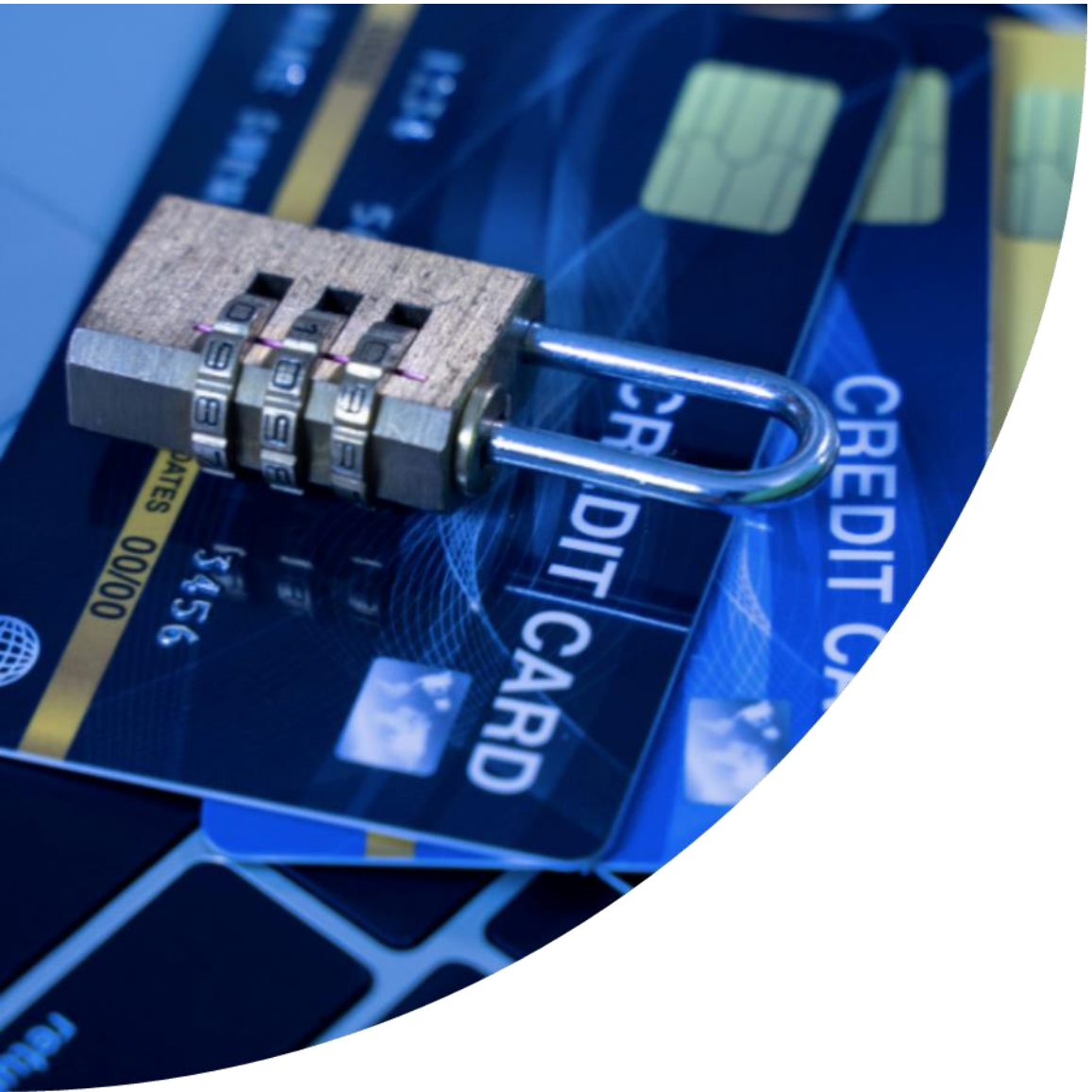
- To fortify the cyber resilience of the U.S., the government created the North American Electric Reliability Corporation (NERC) framework designed to protect a part of the U.S. utility infrastructure
- The NERC Critical Infrastructure Protection (CIP) Standards apply specifically to the cybersecurity aspects of the Bulk Electric System and its efficient and reliable supply
- CIP deals with the pre-planning and groundwork within organizations and agencies to tackle threats to the effective and timely functioning of national and regional critical infrastructure

Ten Areas of NERC/CIP

1. Identification and categorization
2. Security controls
3. Background checks and training
4. Electronic security
5. Physical security
6. System security
7. Incident management
8. Recovery plans
9. Configuration and vulnerabilities
10. Information protection



Highly Regulated Industries: PCI

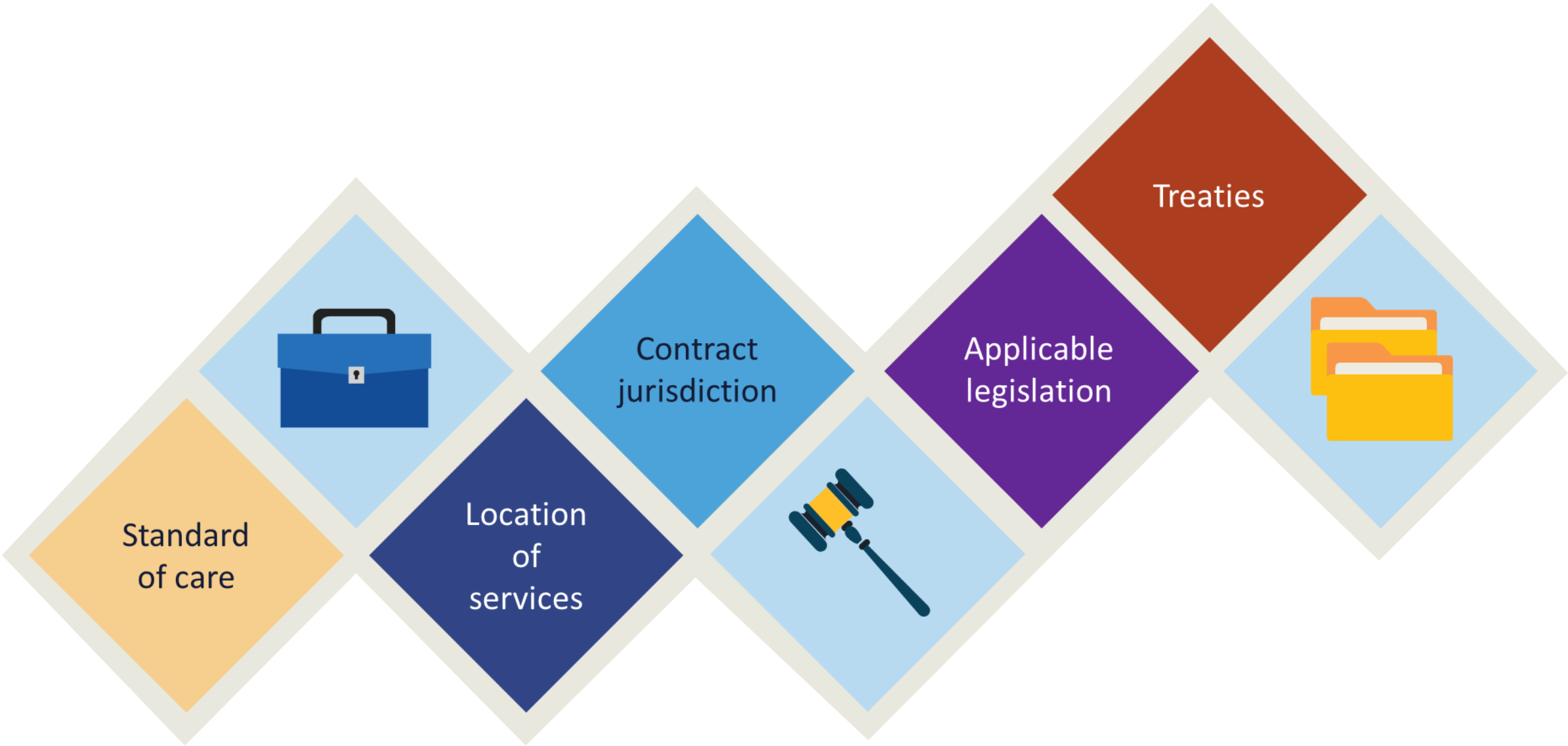


- The Payment Card Industry Data Security Standard (PCI DSS) was formed in 2004 to secure credit and debit card transactions against data theft and fraud
- While the PCI Security Standards Council has no legal authority to compel compliance, the standard is a requirement for any business that processes card transactions
- PCI certification is also considered the best way to safeguard sensitive data and information

Highly Regulated Industries: HIPAA/HITECH

- HIPAA predates the HITECH Act by 13 years and is concerned with the portability of health insurance (ensuring employees do not lose coverage while between jobs), and the privacy/security of health data
- The HITECH Act updated HIPAA and is concerned with promoting the adoption of electronic health records and meaningful use of health information technology, and is part of the American Recovery and Reinvestment Act of 2009

Legal Facets when using Cloud Services



Standard of Care

- The standard of care is a legal term that is applied to determine if a person or company should be held responsible for harming others and thus should be made to compensate victims
- A standard of care exists when people or companies engage in certain activities or provide certain services
- **A common practical example would be a cloud-based healthcare system or community cloud**

Cloud Governance Tools

Contracts

- In addition to bilateral instruments, contracts include (but are not limited to):
  - Awards and notices of awards
  - Job orders or task letters issued under basic ordering agreements
  - Letter contracts
  - Orders, such as purchase orders, under which the contract becomes effective by written acceptance or performance
  - Bilateral contract modifications

Common Contract Documents

- **Terms and Conditions** – Key document that defines service situations, data usage, termination options, warranties, legalities, and more
- **Acceptable Use Policy (AUP)** – states how the services can be utilized
- **Service Terms** – provider-specific contractual agreements
- **SLA/OLAs** – defines performance metrics for external and internal vendors and providers
  - SLA is also called Master Service Agreements (MSA)
- **Specific Clauses**

Service Level Agreements (SLA)

- The CSP must realize that the use of contractual agreements such as hosting/connection agreements and Service Level Agreements (SLAs) are used to allocate shared responsibility and risk among both cloud providers and cloud consumers
- An SLA defines the precise responsibilities of the provider and sets customer expectations
- Also clarifies the support system (service desk) response to problems or outages for an agreed level of service (based on support plan)
- The liability for the failure of one or more controls and the realization of risk can be appropriately documented and understood by all involved parties
- **The SLA is also called a Master Service Agreement (MSA)**

Master Service Agreement (MSA)

- As part of due diligence in your BCP, you should confirm any/all expectations with the candidate service provider and ensure that they are documented in your MSA/SLAs
- A master service agreement (MSA) is a contract two parties enter into during a service transaction
- This agreement details the expectations of both parties
- The goal of a master service agreement is to make the contract process faster
- It also should make future contract agreements simpler

Elements of SLA and MSA

- Confidentiality
- Delivery requirements
- Dispute resolution
- Geographic locations
- Intellectual property rights
- Limitations of liability
- Payment terms
- Venue of law
- Warranties
- Work standards

Statement of Work (SOW)

- A statement of work (SoW) is an agreement that establishes the expectations for a project or program and aligning the team(s) involved
- Details should clarify price, cost, timeline, deliverables, process, expectations of requirements, invoicing schedules, and much more, depending on the scope and breadth of the project
- Basically, a SoW is a document of agreement between a client and service or agent defining the scope and details of a project
- It is among the first documents you will use to establish the framework of a project before entering the planning and execution stages

ISO/IEC 27036

- ISO/IEC 27036 is a multi-part standard offering guidance on the evaluation and treatment of information risks involved in the acquisition of goods and services from suppliers
- The implied context is business-to-business relationships, rather than retailing, and information-related products
- The terms acquisition and acquirer are used rather than purchase and purchasing since the process, information risks and controls are much the same whether the transactions are commercial or not