(ISC)² Certified Cloud Security Professional (CCSP) Crash Course

Michael J. Shannon

Welcome Back!

Security Operations Centers (SOC)

- For some enterprises, the security operations is an aspect 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)
- The SOC does not have to be physically located in the data center or even on the same campus
- Most CSPs have SOC's that are regional in scope and manage multiple datacenters in zones across a metropolitan area network (MAN) or Wide Area Network (SD-WAN) over high-speed fiber connections

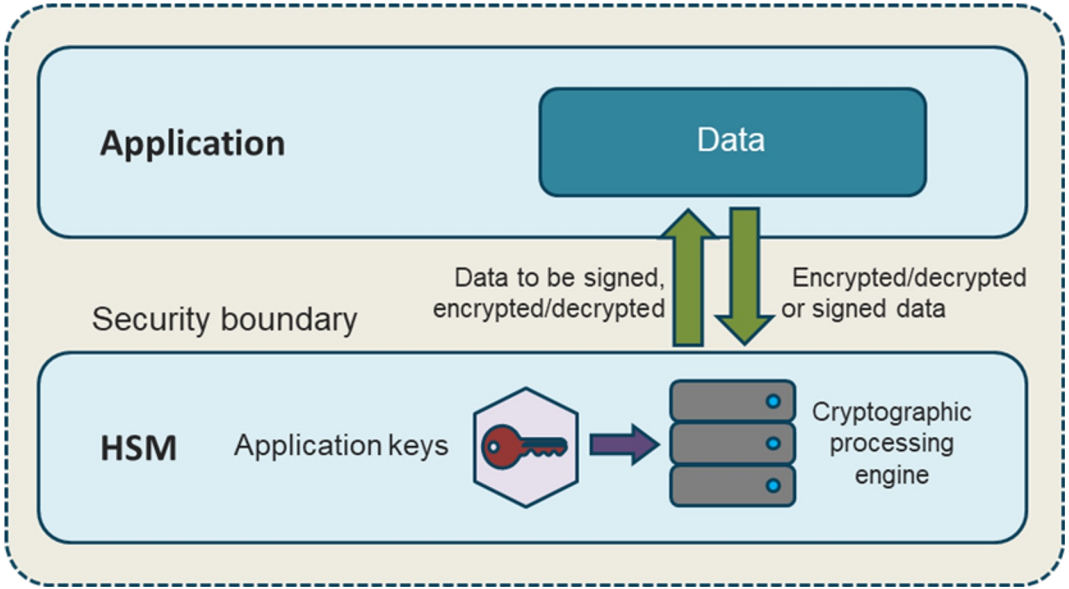
The AWS Cloud Security Triad

- Identity and access management (IAM/IdM)
  - Cloud IAM or Federated SSO (token services)
- Infrastructure security
  - Network design and automated visibility
  - Firewalls (L3/4 stateless, stateful, and WAF)
  - Secure endpoints and policies
  - Secure management access (digitally signing, SSH2, TLS)
  - S2S and P2S VPN services
  - Managed Threat Management (GuardDuty)
- Key Management Services (KMS)
  - Client and server-side

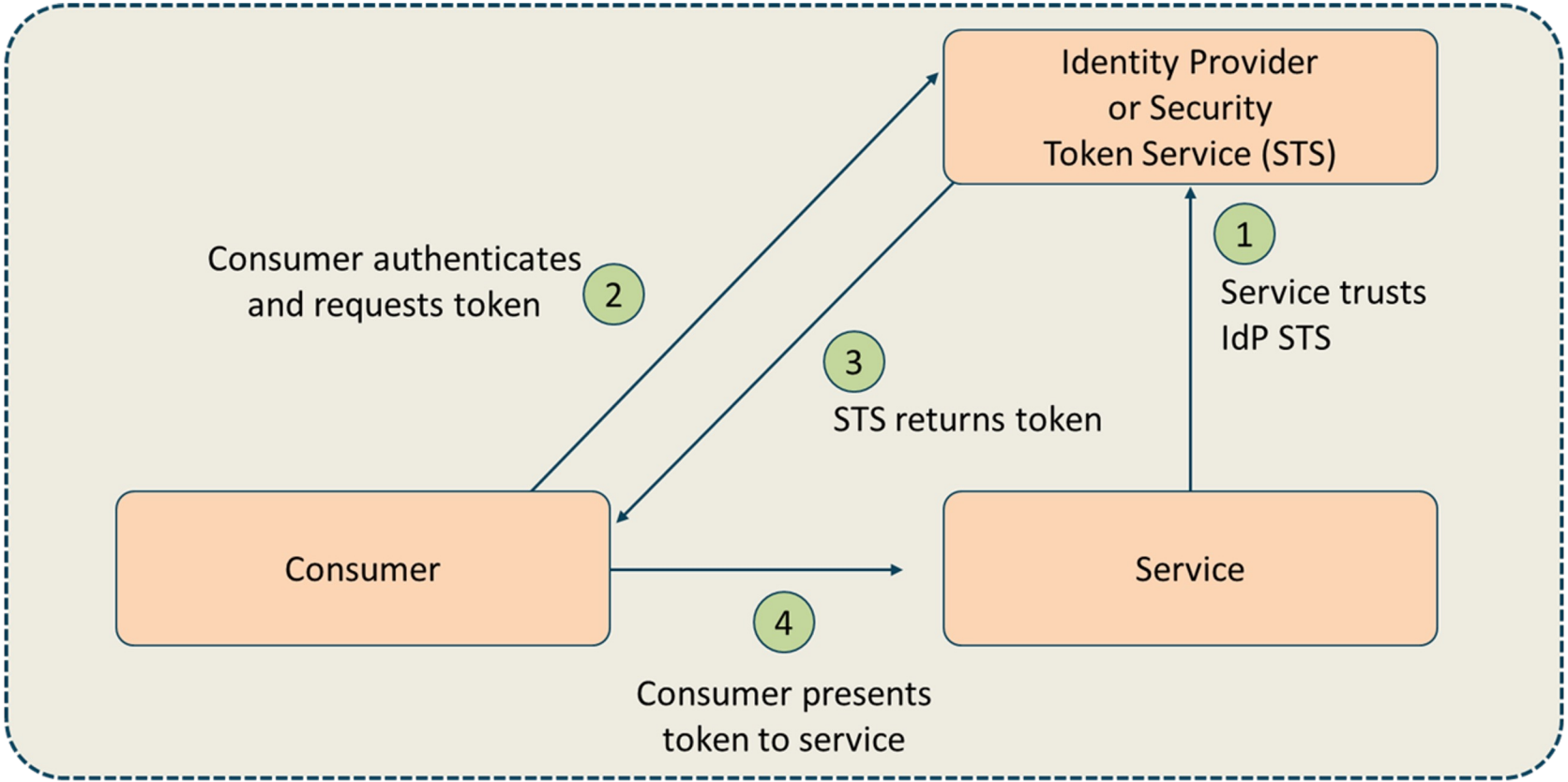
@iconshock.com

Hardware Security Modules (HSM)

- Core technology of Cloud KMS
- Uses tamper-proof, hardened devices
- Conducts crypto processing
- Secures cryptographic keys
- Separates administration and security domains
- Supports key use policies



Federated Identity Providers



Federation Standards

- Manages identities across different enterprises
- Offers single sign-on (SSO) for multiple organizations and service providers
- Provides a Web-of-trust model is where each member of the federation approves the other members
- This is a popular model for the cloud as the identifier can be combined with other services like key management
- Can be outsourced to a Cloud Access Security Broker (CASB) or Managed Security Service Provider (MSSP)

SAML 2.0

- Security Assertion Markup Language
- SAML is an XML-based open-source SSO standard
- **SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet**
- Key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs

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

@iconshock.com

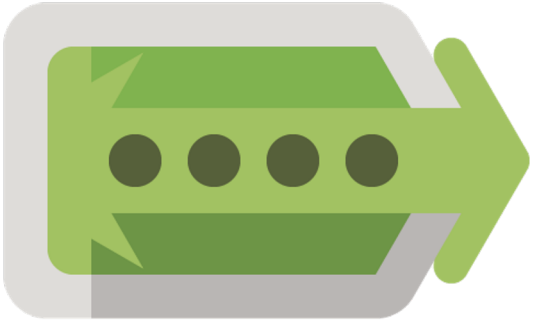
OAUTH

- Intended to work with HTTP(S) and fundamentally 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

@iconshock.com

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



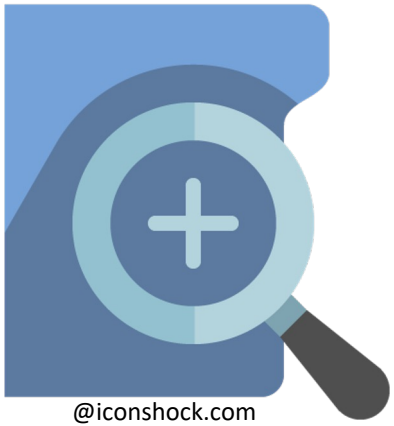
@iconshock.com

Step-Up Authentication

- Confirms that users can access some resources with one set of credentials but will prompt them for additional credentials when access to more sensitive resources is requested
- Users want seamless SSO access to certain assets, but organizations may want to further verify their identities before they grant access to anything more sensitive
- Step-up authentication enables you to provide easy access to one layer of resources and secure access to another layer of resources
- **Often uses Knowledge-based mechanisms (KBA)**

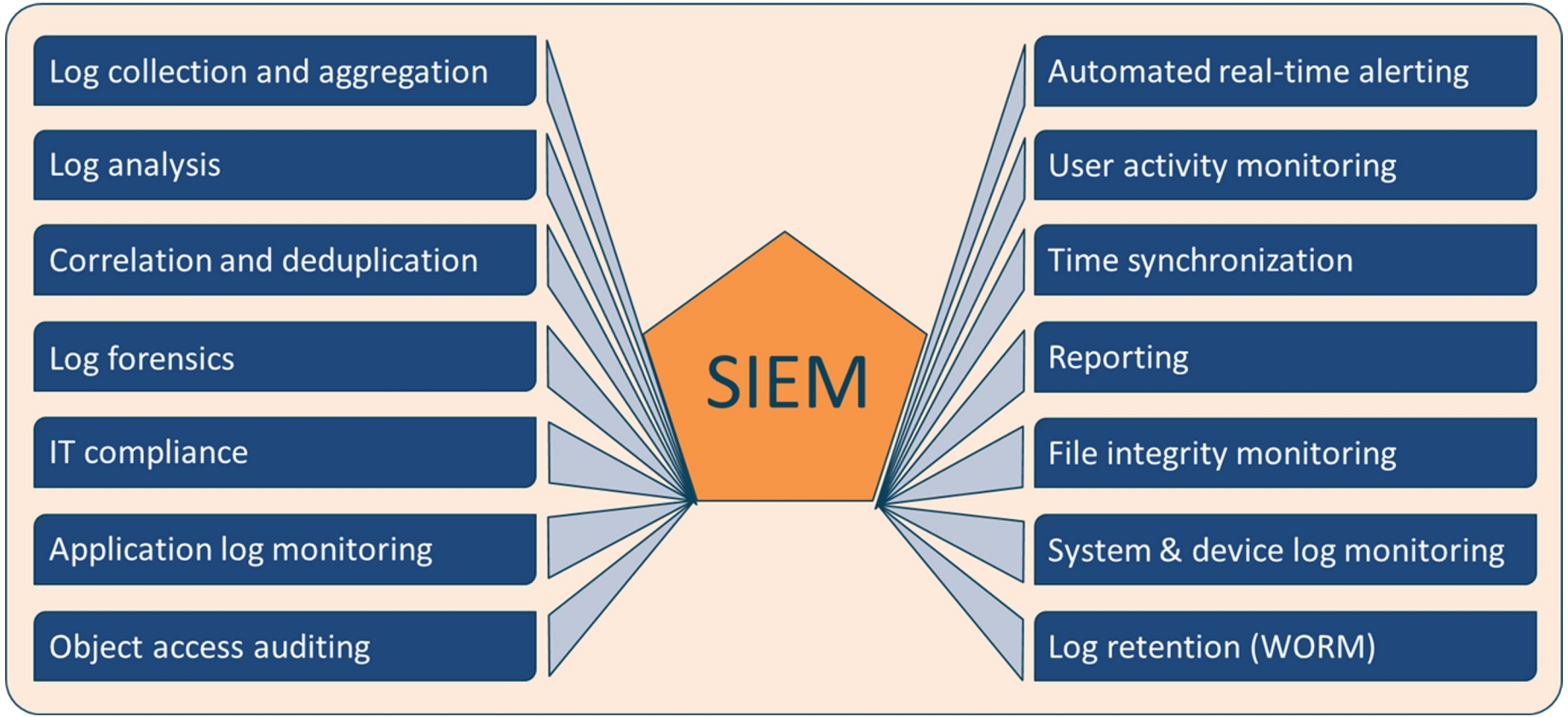
SIEM systems

- NIST: An application that collects security data from information system components and presents that data as actionable information via a single interface
- A combination of security information and event management
  - Various logs (system, application, firewall, etc.)
  - SNMPv2c and 3 traps and informs
  - NetFlow v5 and v9 collections
  - Next-Gen IPS and firewall alerts and logs
  - Output from various proxies



@iconshock.com

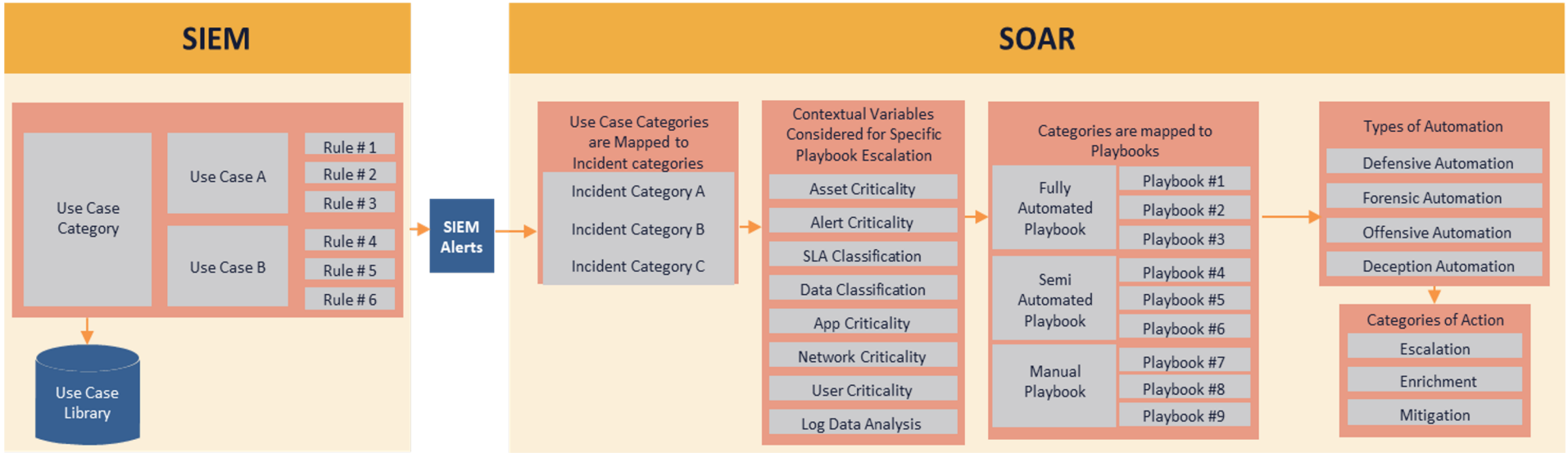
SIEM


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)

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**
  - **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

SIEM AND SOAR



Cloud Development Basics

- Entails Integrated Development Environments (IDEs), application lifecycle management initiatives, and application security testing
- Developers should ask several questions for “Cloud-friendliness”
  - What would the impact be if the data or information crossed geographic boundaries?
  - What if an employee of the cloud provider accessed the data or application?
  - What if the program failed to meet the planned results?
  - What if the app is manipulated by a corporate outsider?
  - What if the data or application were modified unexpectedly?
  - What if the application were subject to downtime?

SOAP vs. REST

- **Simple Object Access Protocol (SOAP)** uses an envelope then HTTP (or FTP/SMTP) to transfer data; only supports XML format; slower; no caching, scalability can be complex; Used when REST is not feasible
- **Representational State Transfer (REST)** uses simple HTTP protocol and supports many different data formats like JSON, YAML, XML; Restful APIs are widely used; Performance and scalability are good, and it uses caching as well

OWASP Top 10 Web Vulnerabilities

- **A01:2021 -** Broken Access Control moves up from the fifth position; 94% of applications were tested for some form of broken access control. The 34 Common Weakness Enumerations (CWEs) mapped to Broken Access Control had more occurrences in applications than any other category.
- **A02:2021 -** Cryptographic Failures shifts up one position to #2, previously known as Sensitive Data Exposure, which was broad symptom rather than a root cause. The renewed focus here is on failures related to cryptography which often leads to sensitive data exposure or system compromise.

OWASP Top 10 Web Vulnerabilities

- **A03:2021 -** Injection slides down to the third position. 94% of the applications were tested for some form of injection, and the 33 CWEs mapped into this category have the second most occurrences in applications. Cross-site Scripting is now part of this category in this edition.
- **A04:2021 -** Insecure Design is a new category for 2021, with a focus on risks related to design flaws. If we genuinely want to “move left” as an industry, it calls for more use of threat modeling, secure design patterns and principles, and reference architectures.

OWASP Top 10 Web Vulnerabilities

- **A05:2021 -** Security Misconfiguration moves up from #6 in the previous edition; 90% of applications were tested for some form of misconfiguration. With more shifts into highly configurable software, it's not surprising to see this category move up. The former category for XML External Entities (XXE) is now part of this category.
- **A06:2021 -** Vulnerable and Outdated Components was previously titled Using Components with Known Vulnerabilities and is #2 in the Top 10 community survey, but also had enough data to make the Top 10 via data analysis.

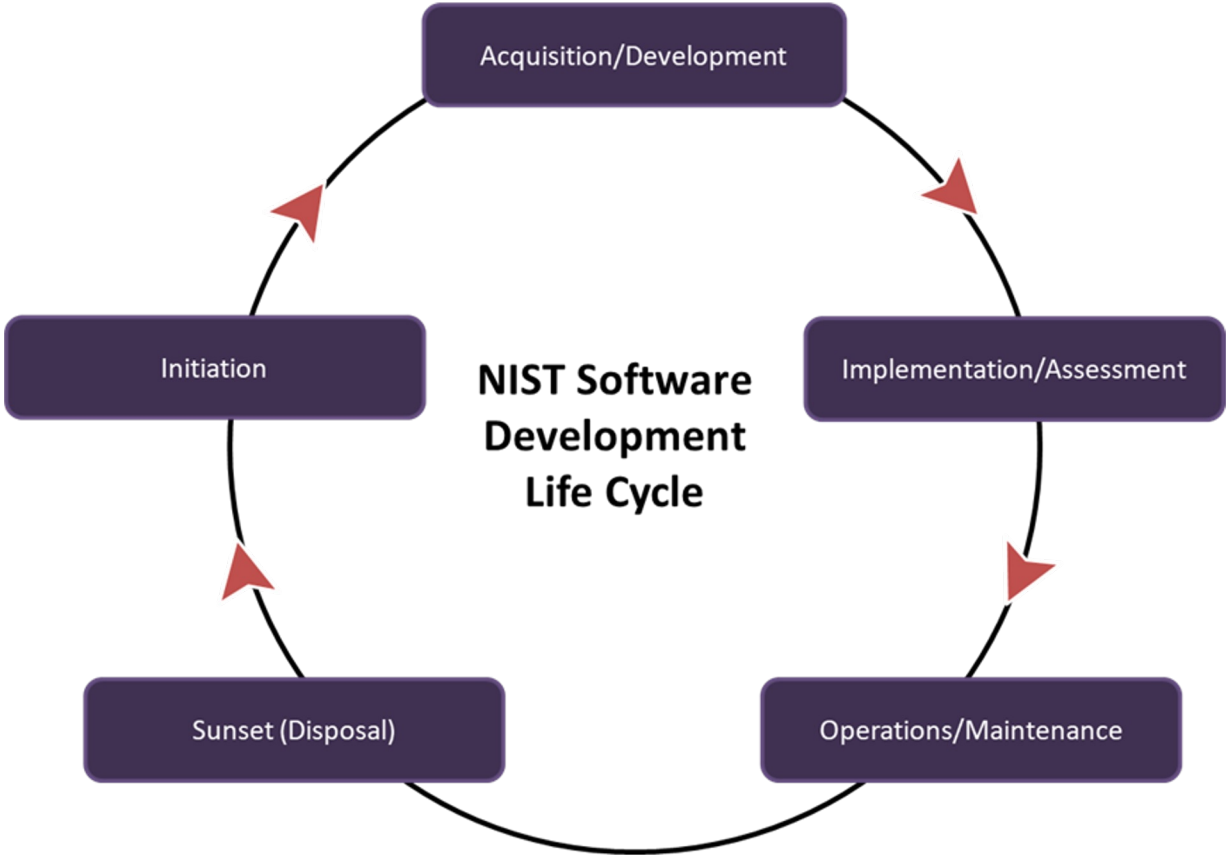
OWASP Top 10 Web Vulnerabilities

- **A07:2021 -** Identification and Authentication Failures was previously Broken Authentication and is sliding down from the second position, and now includes CWEs that are more related to identification failures. This category is still an integral part of the Top 10, but the increased availability of standardized frameworks has helped.
- **A08:2021** - Software and Data Integrity Failures is a new category for 2021, focusing on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity. One of the highest weighted impacts CVE/CVSS data mapped to the 10 CWEs in this category.

OWASP Top 10 Web Vulnerabilities

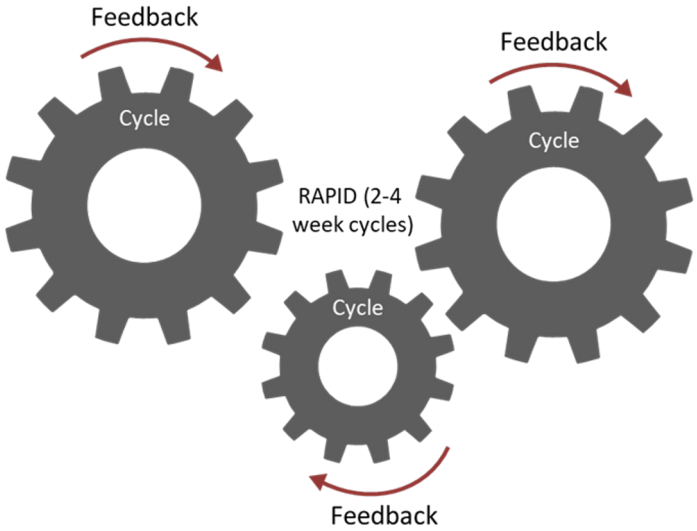
- **A09:2021 -** Security Logging and Monitoring Failures was previously Insufficient Logging & Monitoring and is added from the industry survey (#3), moving up from #10 previously. This is expanded to include more types of failures, is challenging to test for, and isn't well represented in the CVE/CVSS data. However, failures in this category can directly impact visibility, incident alerting, and forensics.
- **A10:2021 -** Server-Side Request Forgery is added from the Top 10 community survey (#1). This category represents the scenario where the security community members are telling us this is important, even though it's not illustrated in the data at this time.

NIST Software Development Lifecycle



Agile Development Lifecycle

- Excellent for smaller and quick projects
- An evolutionary approach – measured in weeks
- Collaboration of cross-functional teams
- Flexible, adjustable, not predictable, testing done during development
- High level of customer involvement throughout the project
- Works tightly with Agile Project Management



CI/CD

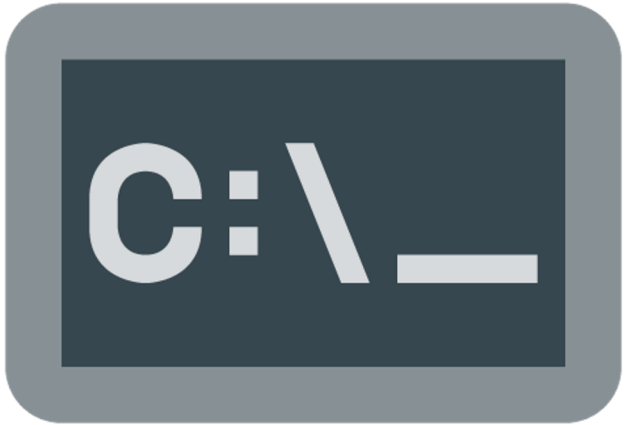
- Continuous Integration/Continuous Deployment (CI/CD)
- Development technique that forces developers to integrate code into a shared repository several times a day
- Each check-in is then verified by an automated build, allowing teams to detect problems early
- The goal is to detect and locate bugs and security flaws quickly
- Very popular method at AWS and GCP for developing traditional apps as well as containers and microservices

DevSecOps

- DevOps is a clipped compound referring to a set of practices that accentuate the collaboration and communication of both software developers and IT professionals that automate the software delivery process
- DevOps is a methodology for building software quickly by linking development and operations
- **DevSecOps** involves considering application and infrastructure security from the start and automating some security gates to keep the DevOps workflow from slowing down
- Choosing the right tools to integrate security continuously is critical

Common Programming Weaknesses

- Poor error handling
- Poor exception handling
- Improper input validation
- Not relying on stored procedures
  - Precompiled groups of code, statements, and commands that can be called later
- Unsecure usage of code repositories
- Leaving inoperative dead code
- Redundancy in the code (no normalization)



@iconshock.com

Source Code Weakness

- Code vulnerabilities exist because solid secure development is quite difficult
- Most organizations do not have a clearly defined policy to confirm that developers wanting to use a section of software code go through an authorization process
- Since open-source components exist in almost all codebases, keeping up with open-source components in your software is an overwhelming task – including tracking the forks, versions, and state of updates to the code

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)
- **Many enterprises and products (90% by some estimates) use at least one open-source component, often without being aware of it**

@iconshock.com

Open-Source Vulnerabilities

- Software is typically built using public community collaboration and is preserved and updated on a voluntary basis
- Open-source 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**

@iconshock.com

Open-Source Vulnerabilities

- Open-source software often includes the use of vulnerable third-party libraries which can involve intellectual property challenges
- Characterized by lax integrations oversight and control
  - Teams often have non-existent review processes for open-source components
  - Operational inadequacies can drive additional work for proper DevSecOps
  - 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

Validate Open-Source Software

- Another approach to assessing code for proper security controls involves directing an informal or formal secure code review
  - 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

Threat Modeling: STRIDE

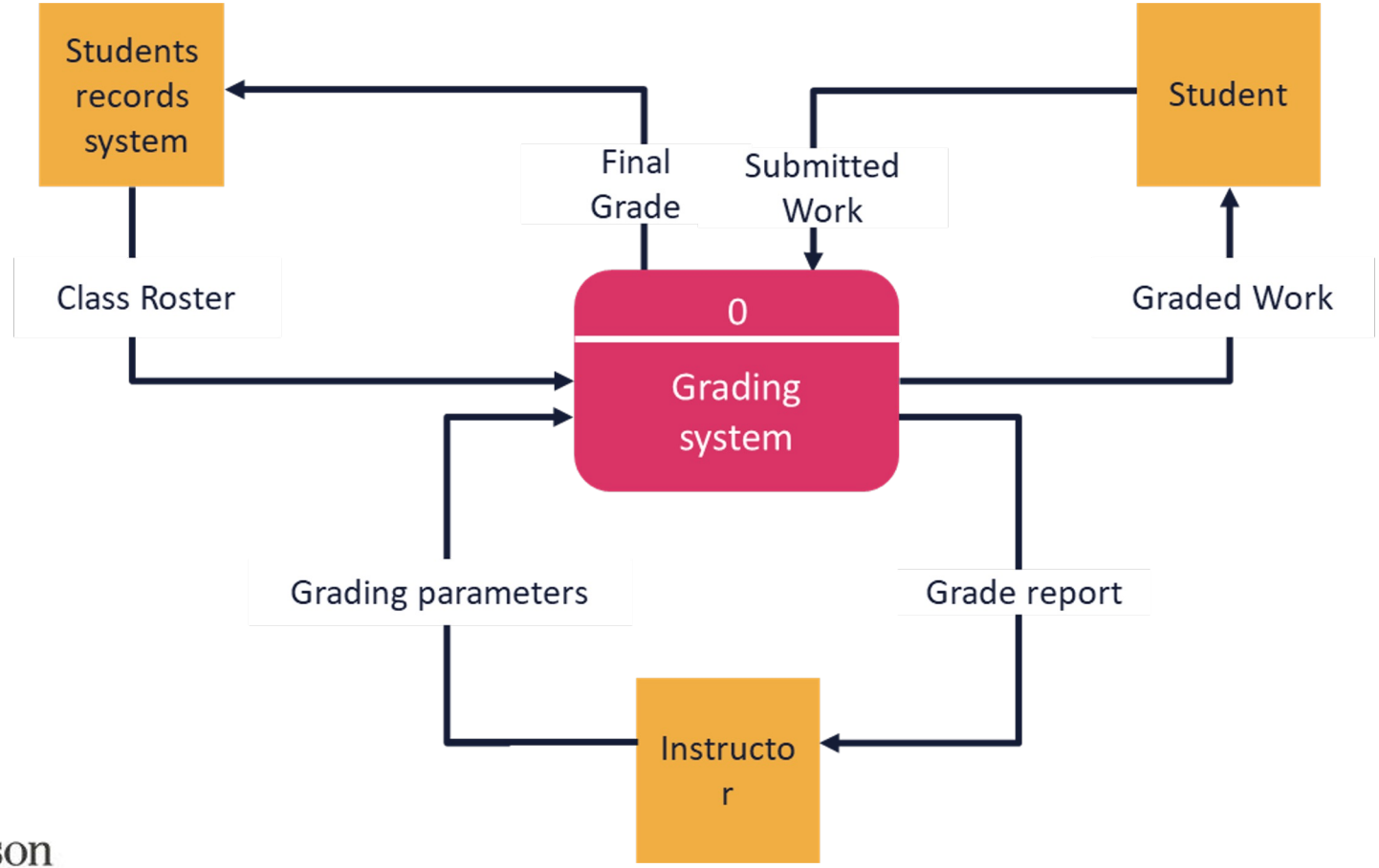
- **Spoofing Tampering Repudiation Information Message Disclosure Denial of Service and Elevation of Privilege** is a developer-focused threat modeling tool
- Emphasis is on ensuring that Microsoft's Windows software developers think about security during the design phase
- Goal is to get an application to meet the security properties of CIA along with authentication, authorization, and non-repudiation
- Once the security SME builds the Data Flow Document (DFD)-based threat model, system engineers or other experts check the application against the STRIDE threat model classification scheme

S.T.R.I.D.E.

Threat	Definition	Property	Example
Spoofing	Pretending to be someone else	Authentication	Hack victim's email and to send messages as the victim
Tampering	Changing data or code	Integrity	Software executive file is tampered with by hackers
Repudiation	Claiming not to do a particular action	Non-repudiation	"I have not sent an email to users"
Information Disclosure	Leaking sensitive information	Confidentially	Making credit card information available on the internet
Denial of Service	Non-availability of service	Availability	Web application not responding to user requests
Elevation of privilege	Ability to perform unauthorized action	Authorization	Normal user can delete admin account

Admin. "STRIDE: Acronym of Threat Modeling System." All About Testing, February 21, 2019. https://allabouttesting.org/stride-acronym-of-threat-modeling-system/.

Sample Data Flow Diagram (DFD): basic



DREAD

- A risk assessment model that can be used to prioritize security threats
- Like the STRIDE model, it was created by Microsoft
- Each risk factor for a given threat can be given a score (for example, 1 to 5 or 1 to 10)
- The sum of all the factors divided by the number of factors represents the overall level of risk for the threat
- A higher score implies a higher risk level and would normally be given a higher priority when determining which threats get the most initial attention

DREAD

DAMAGE	Impact of an Attack
REPRODUCIBILITY	How Easily the Attack can be Reproduced?
EXPLOITABILITY	How Easy it is to Launch the Attack
AFFECTED USERS	How Many Users will be Impacted
DISCOVERABILITY	How easily the vulnerability can be found

PASTA

- Process for Attack Simulation and Threat Analysis (PASTA) is a relatively new application threat modeling approach
- Offers a seven-step platform-independent process for risk analysis
- Goal is to **align business objectives** with technical requirements, while considering business impact analysis and compliance requirements
- Combines an attacker-centric perspective on potential threats with **asset-centric risk and impact analysis**
- Works best for organizations that need to align threat modeling with strategic objectives as it integrates business impact analysis as an integral part of the process

ASATM

- Applied Security Architecture and Threat Models (ASATM) covers all types of systems, from the simplest applications to complex, enterprise-grade, hybrid cloud architectures
- It describes the many factors and essential information that can impact an assessment such as:
  - When should the security architect begin the analysis?
  - At what points can a security architect add the most value?
  - What are the activities the architect must execute?
  - How are these activities delivered?
  - What is the set of knowledge domains applied to the analysis?

Comparing Threat Modeling Methods

	OCTAVE	Trike	P.A.S.T.A	Microsoft	VAST
Implement application security at design time	✓	✓	✓	✓	✓
Identify relevant mitigating controls	✓	✓	✓	✓	✓
Directly contributes to risk management	✓	✓	✓		✓
Prioritize threat mitigation efforts	✓	✓	✓		✓
Encourage collaboration among all stakeholders	✓	✓			✓
Outputs for stakeholders across the organization	✓				✓
Consistent repeatability		✓			✓
Automation of threat modeling process		✓			✓
Integrates into an Agile DevOps Environment					✓
Ability to scale across thousands of threat models					✓

"Threat Modeling Methodologies." ThreatModeler Software, Inc. Accessed June 7, 2021. https://threatmodeler.com/threat-modeling-methodologies-/.

Vulnerability Assessment

- Vulnerability assessment adds value to supporting security of applications and systems prior to going into production
- Vulnerability scans and tests attempt to identify and report on known vulnerabilities in a system
- Automated and manual scheduled scanning results should map to an established risk ledger (log) and risk ratings 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

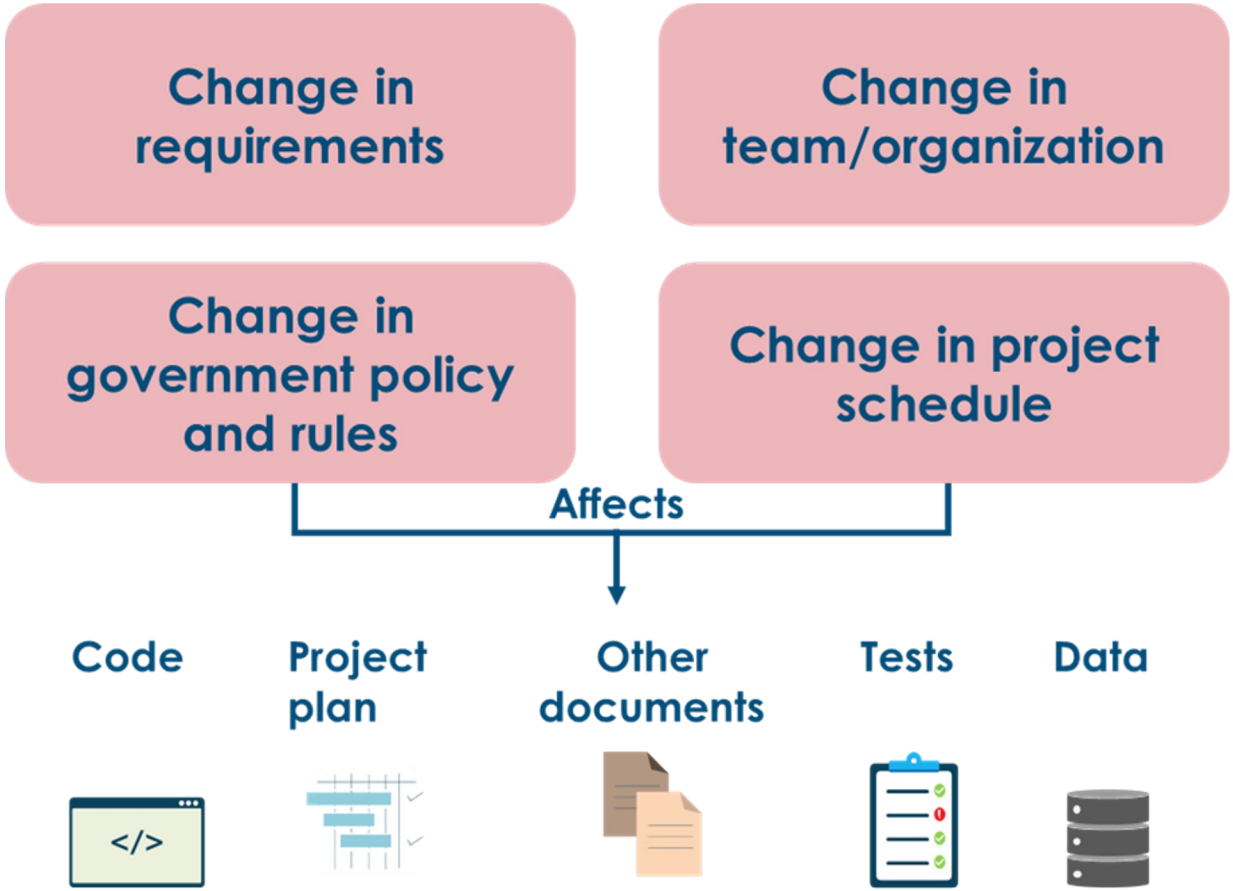
- Penetration testing is a process used to collect information and actively expose vulnerabilities in an application or system by conducting actual exploits and red team attacks
- Penetration testing is often a black or gray box test, where the tester assumes the attacker role with little or no knowledge of the application and must discover any security issues
- Some CSPs demand that customers seek permission of complete documentation before testing is performed

Software Configuration Management

- Software configuration management (SCM) is a software engineering process to systematically manage, consolidate, and control the changes in the documents, codes, and other artifacts during the software development life cycle
- The primary goal is to boost efficiency and reduce errors
- SCM is part of the cross-disciplinary field of configuration management (integrated product teams – IPT)

@iconshock.com

Software Configuration Management



Code Repository Security

1. Choose a repository you trust
2. Consider the exposure and customer base of your repository
3. Protect all access credentials
4. Separate secret credentials from source code
5. Revoke repository access quickly when compromised or no longer needed

@iconshock.com

Code Repository Security

6. Include open code in your risk model
7. Assess all code changes in a peer review environment
8. Realize that external code changes may be malicious
9. Protect your identity if using a publicly accessible repository
10. Ensure that your code is backed up (CSP availability zones)

@iconshock.com

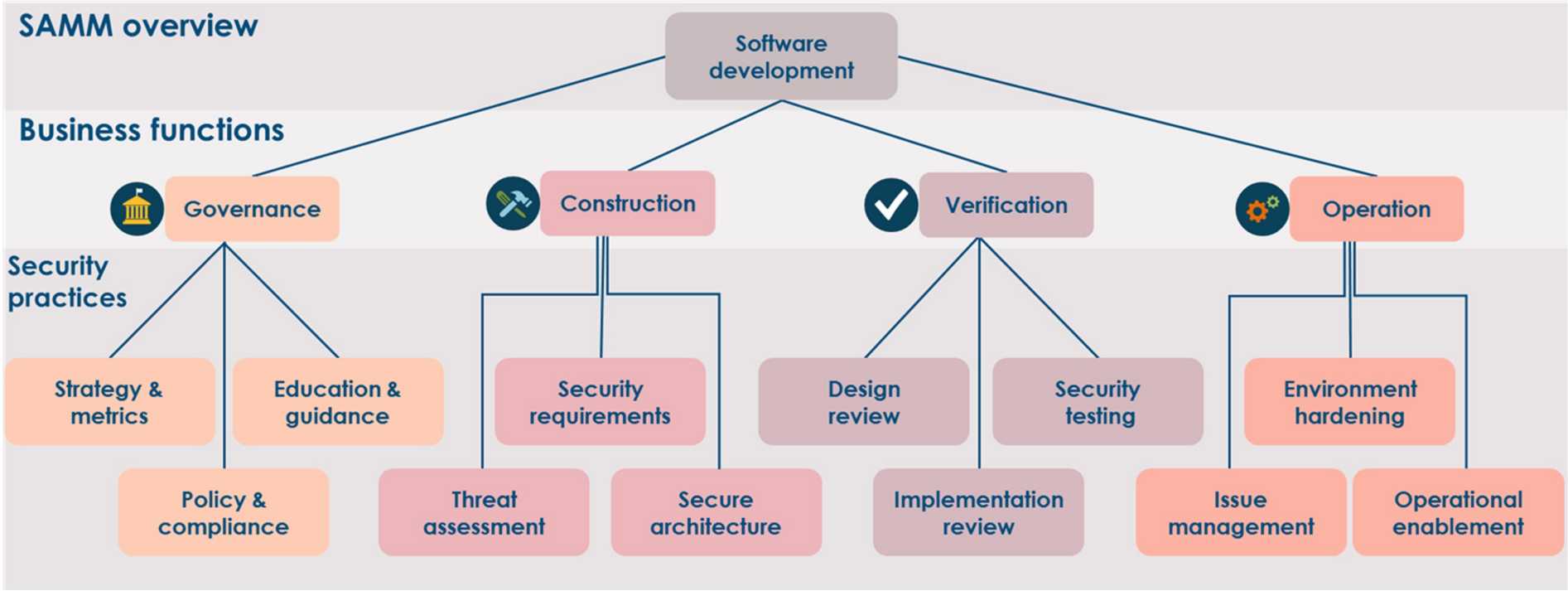
Software Assurance

- The main objective is to shift the security paradigm from patch management to software assurance
- Embolden developers and programmers to elevate overall software quality and security from the start
- Accentuate the usage of tested standard libraries and modules
- Employ industry-accepted tactics that identify that software security is essentially a software engineering issue that must be addressed systematically during the software development life cycle

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)



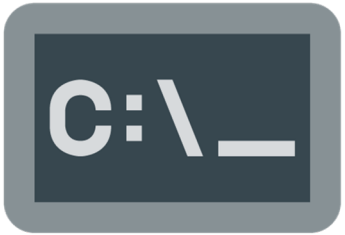
"Software Assurance Maturity Model." OWASP.org. Accessed June 8, 2021. https://owasp.org/www-pdf-archive/SAMM_Core_V1-5_FINAL.pdf.

OWASP Application Security Verification Standard (ASVS)

- This project gives developers a list of requirements for secure development
- The standard provides a basis for testing application technical security controls, as well as any technical security controls in the environment, that used to mitigate attacks such as Cross-Site Scripting (XSS) and SQL injection
- The requirements are to be used:
  - As a meaningful metric
  - As secure development guidance
  - During the procurement process

SAFECode

- A global nonprofit organization that brings business and technical leaders together to exchange insights on creating, refining and promoting effective and scalable software development
- Software assurance involves developing and employing processes for ensuring that software is:
  - Functioning as intended
  - Free of design defects
  - Without implementation flaws



- Publishes the “SAFECode Fundamental Practices for Secure Software Development” to help the industry advance software assurance

Software Diversity

- Application development methodology where two or more functionally duplicate are developed from the same specification
- The process uses different developers or programming teams
- Better error detection, consistency, and fewer programming errors
- Automated software diversity uses randomization to significantly increase the difficulty of exploiting the huge amounts of low-level code in existence
- Diversity-based defenses are motivated by the assumption that a single attack will fail against multiple targets with unique attack surfaces

SAST

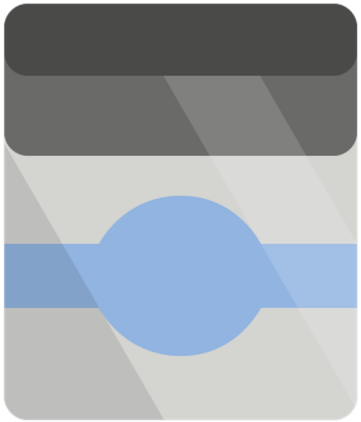
- Static Application Security Testing (SAST)
- Commonly defined as a **white-box test**, where an analysis of the application source code, byte code, and binaries is carried out by the application test **without executing the code**
- It is used to find coding errors and omissions that are symptomatic of security vulnerabilities
- Often used as a test method when the tool is under development - **earlier in the development lifecycle**
- Can be used to find SQL injection attacks, cross-site scripting errors, buffer overflows, and unhandled error conditions

DAST

- Dynamic AST is considered a black-box test finding 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
- **Due to the nature of SAST being a white-box test tool, SAST typically delivers more comprehensive results than those found using DAST**

RASP

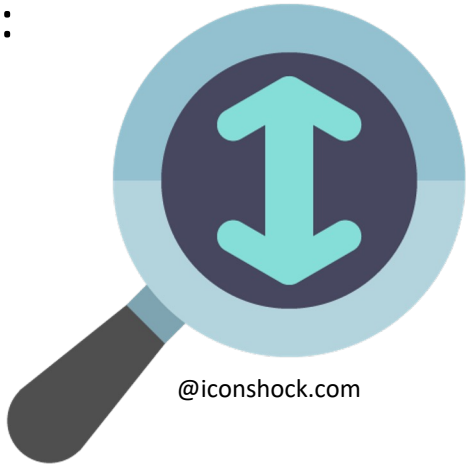
- Runtime Application Self Protection (RASP)
- Typically geared towards applications that have self-protection capabilities built into their runtime environments
  - Have full insight into application logic, configuration, and data and event flows
- Prevents attacks by “self-protecting” or reconfiguring automatically without human intervention in response to certain conditions (threats, faults, etc.)



@iconshock.com

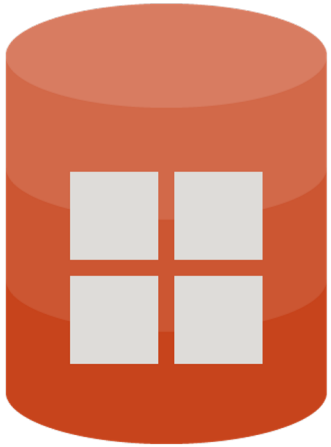
Web Application Firewalls (WAF)

- An CSP service, appliance, or plugin, that applies a WebACL ruleset) to an HTTP/S connection
- The AWS WAF runs on an Application Elastic Load Balancer (with TLS Listener enabled), a CDN distribution, or 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 data behavior
- Should be transparent to activities and users
- Modern solutions deploy a comprehensive toolkit for:
  - Visibility, discovery and classification
  - Vulnerability protection
  - Application-level analysis and IPS
  - Support for unstructured data security
  - Identity and access management integration
  - Risk management support



@iconshock.com

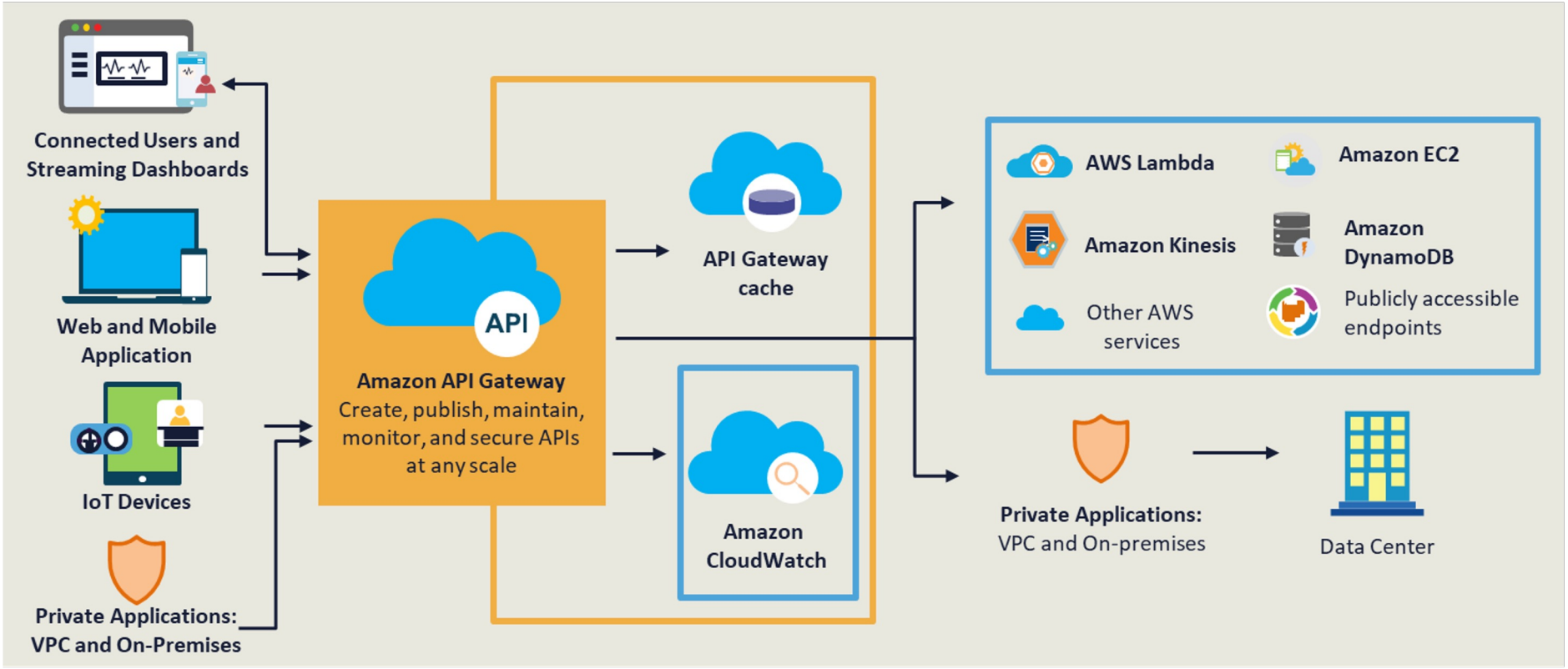
XML Firewalls

- Special firewall that processes XML requests and responses over HTTP/S using a processing policy
  - A set of request, response, two-way, and error rules
  - AAA rules, transformations, schema validation, logging, and cryptographic operations
- With a 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.

AWS API Gateways



Source: https://aws.amazon.com/api-gateway/

More About CASB's

- One of the first 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**

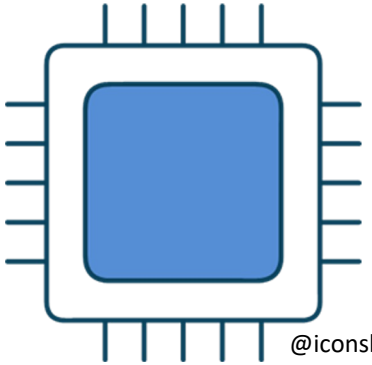
@iconshock.com

Cloud Host Servers: Best Practices

- Secure build: Follow the specific recommendations of vendor or baseline image to securely deploy operating systems
- 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
  - 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

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
  - Restricts people from booting from removable devices
  - Prevents users from changing UEFI settings without permission
  - Prevents users from booting other OSs or installing over current OS



Boot Integrity

- TPM – module embedded in a system
  - Anchoring the trustworthiness of a system to hardware not software
  - Tamper-resistant security chip installed on the device or built into PCs, tablets, and phones
  - Stores passwords, certificates, and encryption keys needed to authenticate the platform
- Contributes to Zero Trust for devices and platforms:
  - Integrity (ensures system has not been altered at a low level)
  - Authentication (ensures system is in fact the correct system)
  - Privacy (ensures system is protected from prying eyes)

Storage & Network Controllers: Best Practices

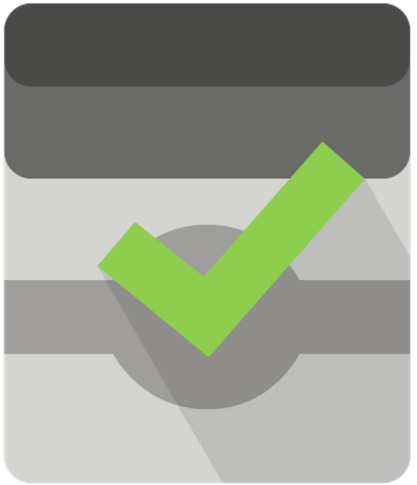
- **Storage controllers may be in use for iSCSI, Fiber Channel (FC), or Fiber Channel over Ethernet (FCoE) – uses initiators and targets**
  - Prevent oversubscription with a dedicated LAN for iSCSI traffic
  - Do not share the storage network with other network traffic such as management, fault tolerance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

Distributed Resource Scheduling (DRS)

- DRS continually monitors your cluster utilization to assure that VMs get their resources in the most optimal fashion
  - Keeps the ESXi host cluster balanced
  - Works closely with resource management that guarantee specific resources for your VMs
- DRS constantly monitors a lot of parameters:
  - 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 expediates live migration of VMs and VHDs within a hypervisor host cluster
- The migration is based on your designated settings to optimize load balancing between hosts and cluster shared storage
- Also corrects any VM placement issues



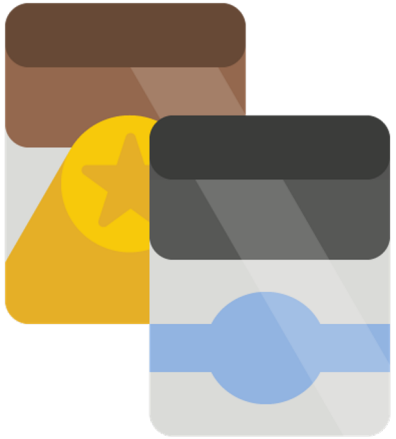
@iconshock.com

Dynamic Optimization (DO)

- **Compute Dynamic Optimization** is the optimization of hosts in a cluster to optimize performance by migrating VMs across host
  - Host performance thresholds you can set are 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

Benchmarks

- 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
  - CIS Benchmarks™ are security configuration guides created by government, business, industry, and academia
  - Established using a special method constructed from an accord of global cybersecurity experts from across the globe



@iconshock.com

Mobile Devices and IoT with the Cloud

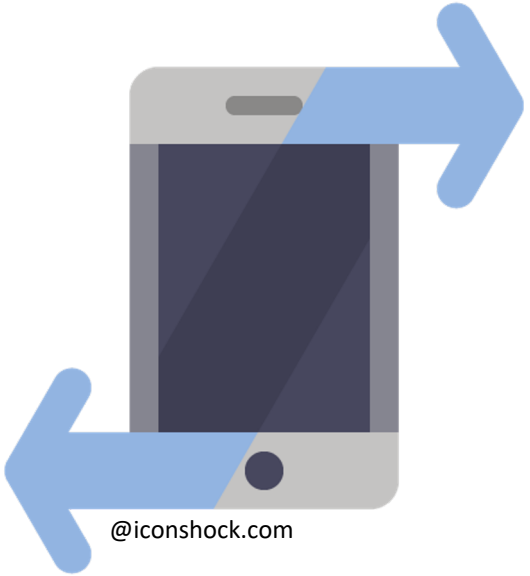
- Cloud-based services will result in many mobile users accessing business data and services without using the corporate network
  - This will increase the need for enterprises to place security controls between mobile users and cloud-based services
  - **Involves Zero Trust initiatives and SSO managed solutions**
- Placing large amounts of sensitive data in a globally accessible cloud leaves organizations open to large, distributed threats
- Attackers no longer must come onto the premises to steal data, and they can find it all in the one “virtual” location

Enterprise Mobility Management (EMM)

- Enterprise mobility management is the combination of mobile device management (MDM) and mobile application management (MAM)
- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used for business
- Solution should reduce risk, so employees are able to access the necessary data from nearly any location, over any network, using a wide variety of mobile devices

Enterprise Mobility Management (EMM)

- 3 basic core EMM competencies:
  - **Visibility**: understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - **Secure access**: the ability for users to securely authenticate and authorize access to apps and data
  - **Data protection**: offering dynamic anti-malware and data loss prevention capabilities to help limit the risk of attacks and data breaches



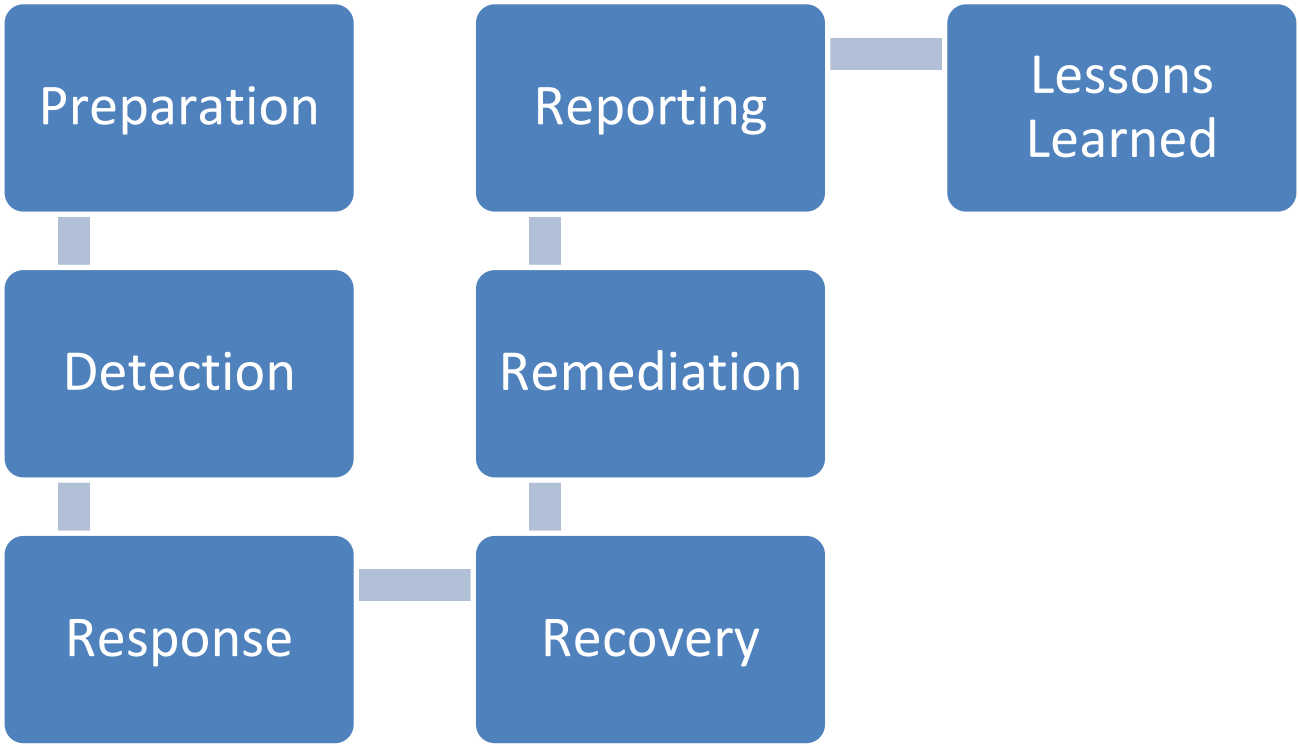
ITIL4 IT Services

- Change Management
- Continuity Management
- Information Security Management
- Continual Service Improvement Management
- Incident Management
- Problem Management
- Release Management
- Deployment Management
- Configuration Management
- Service level Management
- Availability Management
- Capacity Management

Incident Management and Response

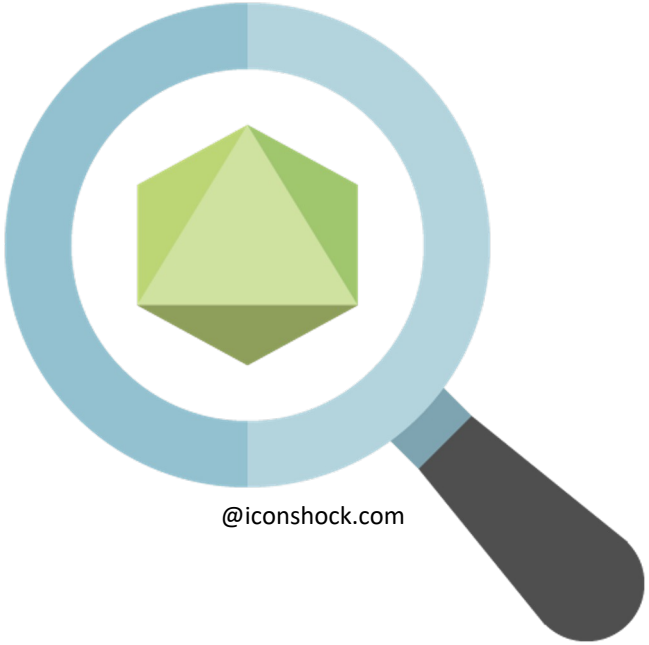
- Steps taken when a negative event disrupts normal operations
- Primary goal is to reduce the immediate impact
- Should have documented incident types/category definitions based on risk assessments, risk registers, and BIA
- Know roles and responsibilities of the first responders, including reporting 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



Why Perform Forensics?

- Violation of laws occur
  - Privileged insiders committing crimes
- Violation of organizational policies
- Systems and applications have been exploited
- Data and/or identity breaches
- Exfiltration of intellectual property
- It is a phase of Incident Response (Problem Management and/or root cause analysis



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

Order of Volatility

1. CPU, cache, and register contents
2. Routing table, ARP cache, process tables, kernel statistics
3. RAM memory and buffers
4. Temporary file system swap files/ slack space
5. Data on hard disks
6. Detachable drives (USB, Firewire, cards)
7. Remotely logged data
8. Data on archival and backup storage media

Document the Chain of Custody

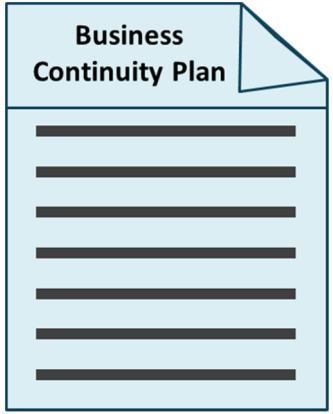
Chain of custody				
Registered mail	Date/Time	Released by	Received by	Reason
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization	
	Time	Signature	Signature	
	Date	Name/Agency/Organization	Name/Agency/Organization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

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**

BCP/COOP

- Ensures business operates a pre-determined level when disaster strikes
  - Documents approved by executive management
- Outlines risk to business
  - Populates risk register/ledger
  - Requirements to mitigate incidents
- Identifies procedures needed to recover from a disaster
  - What is an acceptable amount of time?
  - How to reduce the impact of the disaster



@iconshock.com

BCP using NIST SP 800-34, Revision 1

1. Develop a continuity planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. After-action report
8. Ensure plan maintenance

Business Impact Analysis

- The risk assessment aspect of the Business Continuity Plan (BCP) or (COOP)
- 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

Recovery Time Objective (RTO)

- The amount of time available to recover the resource, service, application and function
- Must be equal to or less than Maximum Tolerable Downtime (MTD)
- Possible methods to lessen the RTO:
  - Add physical security
  - Add redundancy
  - Purchase insurance
  - Invest in backup generators
  - Invest in faster
  - Safeguard media off-site

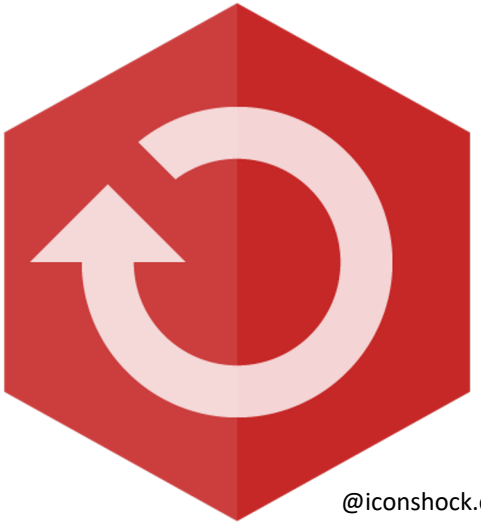
@iconshock.com

Recovery Point Objective (RPO)

- The point in time, relative to a disaster, where the recovery process begins
- In IT systems, it is often the point in time when the last successful backup is performed before the disruptive event occurs
  - Database transaction logs
  - Snapshots of virtual images and block stores
  - Last Known Good Configuration
  - Recovery volumes
  - System and registry states

Maximum Tolerable Downtime (MTD)

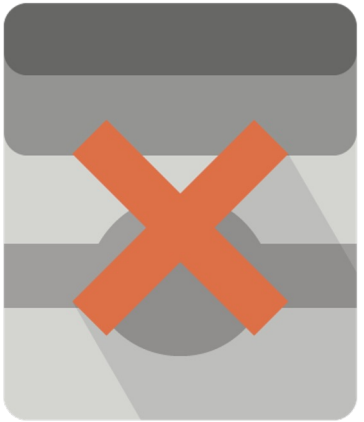
- Absolute maximum amount of time that a resource, service, or function can be unavailable before we start to experience a loss
- Factors to consider include
  - finances
  - supply chain
  - life/safety
  - regulatory
  - legal/contracts
  - reputation
  - property



@iconshock.com

MTBF and MTTR

- Mean Time Between Failure (MTBF) is a measurement hardware resiliency
  - For most devices, the measure is in thousands or tens of thousands of hours between failures
  - Metrics are often provided by vendors or manufacturers
- Mean Time to Repair (MTTR) measures the amount of time it takes to repair or replace
  - Key metric affected by supply chain disruptions



@iconshock.com

Design Resilient

	P1	P2	P3	P4	P5
	Multi-AZ Deployment	Static Stability in Region	Application Portfolio Distribution	Multi-AZ Deployment [Regional DR]	Multi-Region Active-Active Deployment
Design Complexity	Low	Medium	Medium	High	Very High
Cost to Implement	Low	High	Medium	High	High
Operational Effort	Low	Medium	Medium	Medium	Very High
Effort to Secure	Low	Medium	Medium	High	High
Environmental Impact	Low	Medium	Medium	High	High

Uptime Institute

- Standard bearer for digital Infrastructure performance whose Tier Standard has been used in thousands of sites in more than 100 countries
- **Tier 1 - The Basic Site Infrastructure**
  - A simpler and less expensive solution with little or no redundancy - only dedicated space for IT systems, UPS for backup and line conditioning, cooling of critical equipment
  - Problematic personnel activity **WILL** cause downtime
  - **All 4 tiers have at least 12 hours of fuel for generators**

Uptime Institute

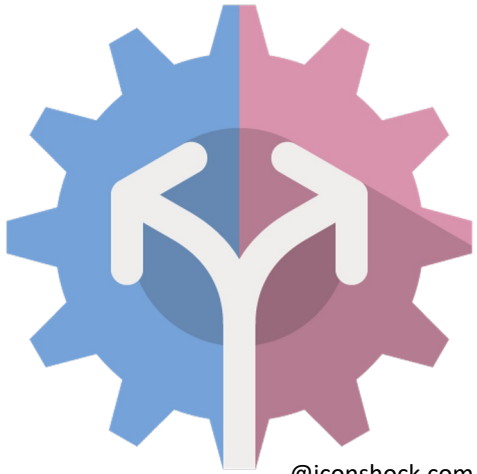
- **Tier 2 - Redundant Site Infrastructure Capacity Component**
  - Has additional feature from Tier 1
  - Critical operation s do not have to be interrupted for scheduled maintenance or replacement
  - The WILL be downtime for any disconnection from power distribution and lines
  - Problematic personnel activity **MAY** cause downtime
  - Unplanned component failure or systems **MAY** cause downtime

Uptime Institute

- **Tier 3 - Concurrently Maintainable Site Infrastructure**
  - Dual power supplies for all systems
  - Critical operations can continue if a single component or power element is down for replacement or scheduled maintenance
  - Unplanned loss of component **MAY** cause downtime; unplanned loss of single system **WILL** cause downtime
- **Tier 4 - Fault-Tolerant Site Infrastructure – the optimal data center**
  - Has features of other tiers included with full redundancy of systems, power, cooling
  - Loss of a single element **WILL NOT** cause downtime
  - Fully automated visibility and response systems with scheduled maintenance performed **without** downtime

Disaster Recovery Planning (DRP)

- Action plans for when an incident is escalated to a potential disaster or critical event with catastrophic results
- Outlines the technical aspects involved for restoration
  - Recovery sites: hot, warm, cold, mobile, cloud, shared
  - Order of restoration (most critical to least critical)
  - Backups, snapshots, and restores
  - Contact information
  - Communication plans
  - Chain of authority
  - Step-by-step instructions
  - Locations of documents, software, and keys



Recovery Sites

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

Disaster Recovery Plan Testing

- Read-through (Checklist)
- Tabletop
- Walkthrough
- Simulation
- Parallel
- Full Interruption

@iconshock.com

Lessons Learned

- 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

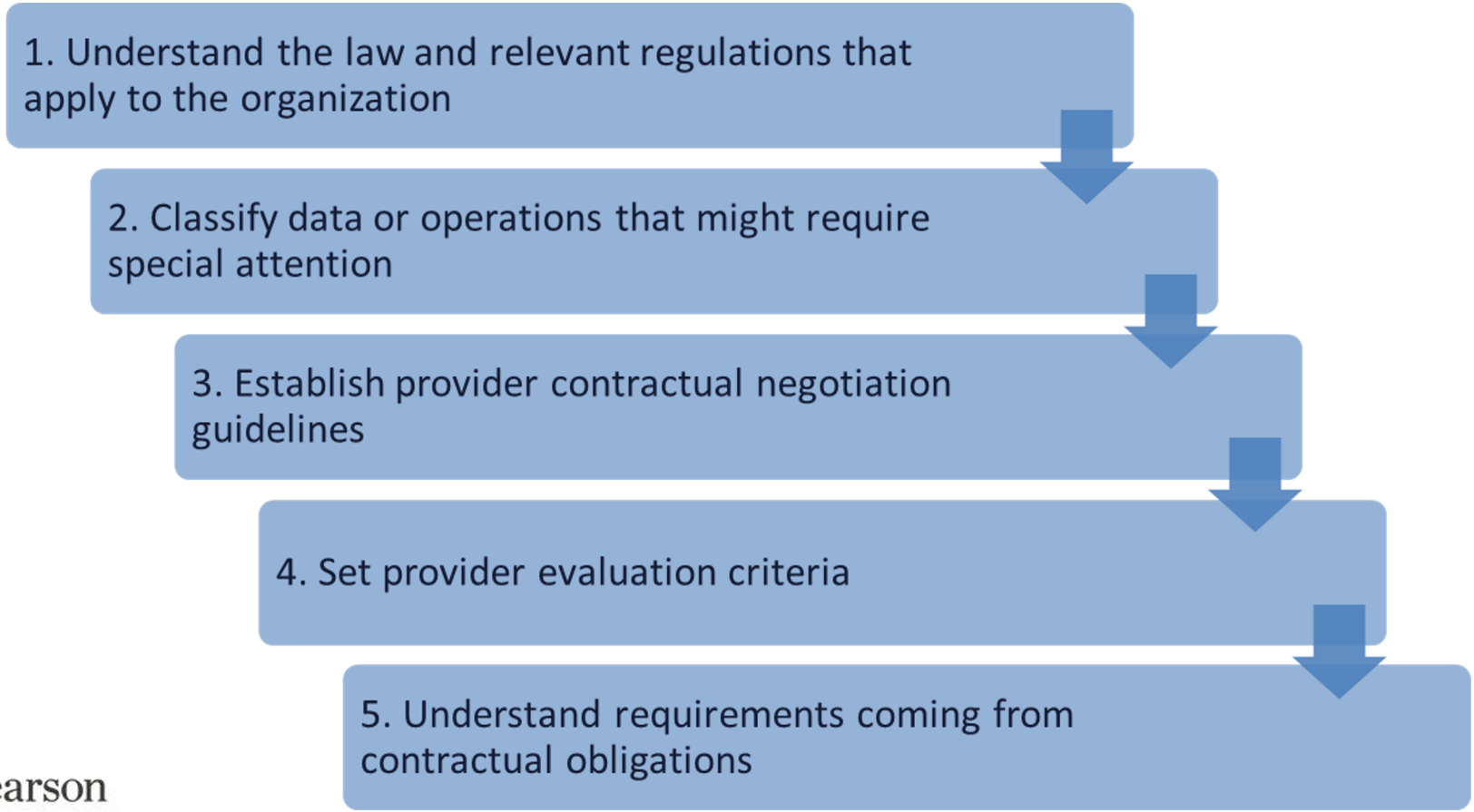
RACI Charts for Mapping Roles

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*

Setting Requirements Process



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

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 program will address privacy responsibilities and risks while enabling current and future business opportunities
- 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

Privacy Impact Assessment (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 and notify the public on
  - What PII DHS is collecting
  - Why the PII is being collected
  - How the PII will be collected, used, accessed, shared, safeguarded, and stored

GDPR

- **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

GDPR

- 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

Actions for U.S. Companies to Consider

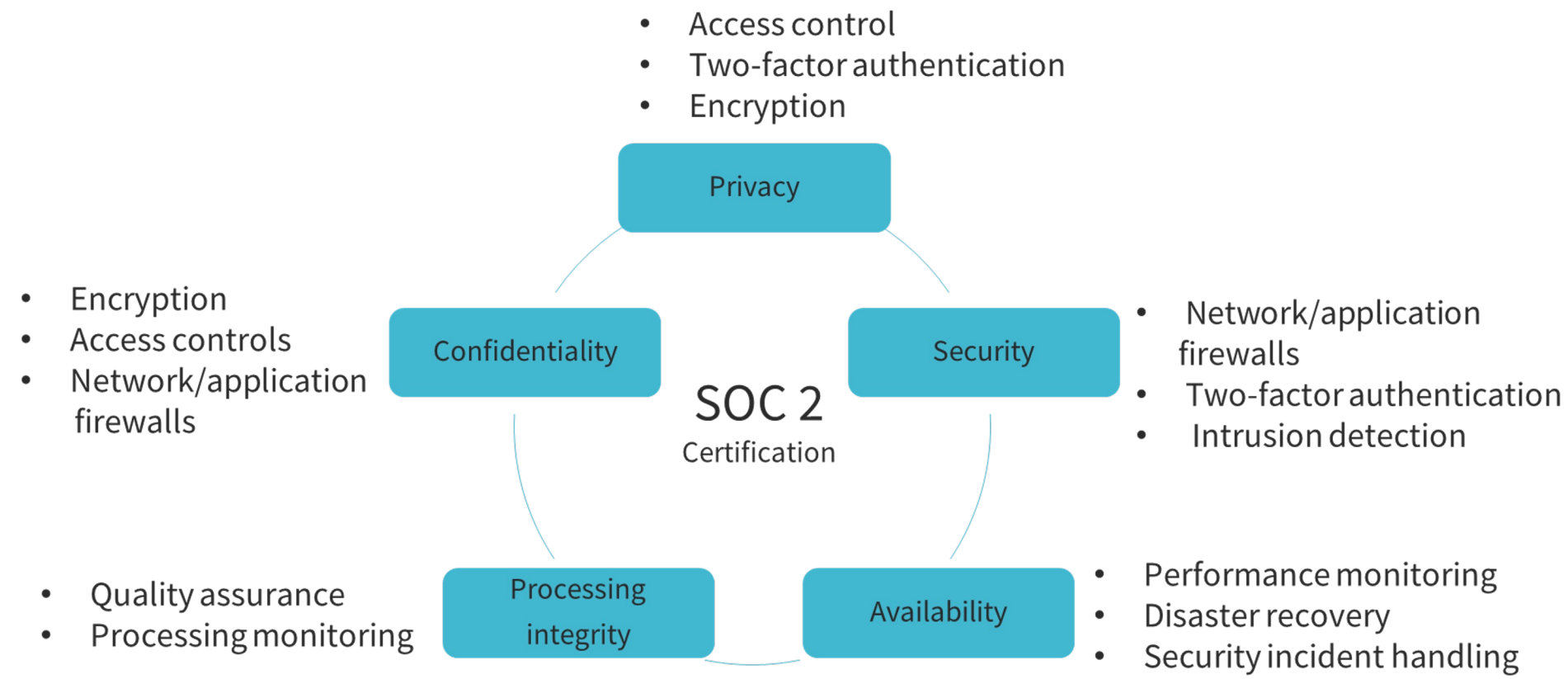
- Assess personal data flows from EU-to-US to define the scope of the cross-border privacy compliance challenge
- Assess model contracts as at least a temporary replacement to Safe Harbor
- Assess readiness to meet model clauses, remediate gaps, and organize audit artifacts of compliance with the clauses
- Conduct a GDPR readiness assessment
- Budget for GDPR remediation

Actions for U.S. Companies to Consider

- Elevate risk and mitigation plans to the Board level
- Enhance EU privacy programs to ensure they can pass an EU regulator audit, or litigation challenge, remediating GDPR gaps along the way
- Conduct EU data-breach notification stress tests
- Monitor changes in EU support for model contracts and binding corporate rules and prepare to shift to the operational adequacy mechanism

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


Access control
Two-factor authentication
Encryption
Privacy
Encryption
Access controls
Network/application firewalls
Confidentiality
SOC 2
Certification
Security
Network/application firewalls
Two-factor authentication
Intrusion detection
Quality assurance
Processing monitoring
Processing integrity
Availability
Performance monitoring
Disaster recovery
Security incident handling

CSA Cloud Controls Matrix

- The CSA Cloud Controls Matrix (CCM) includes 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
- CCM is considered the de facto standard for cloud security assurance and compliance

CCM Domains

- Application and interface security (AIS)
- Audit assurance and compliance (AAC)
- Business continuity management and operational resilience (BCR)
- Change control and configuration management (CCC)
- Data security and information lifecycle management (DSI)
- Datacenter security (DCS)
- Encryption and key management (EKM)
- Governance and risk management (GRM)

CCM Domains

- Human resources (HRS)
- Identity and access management (IAM)
- Infrastructure and virtualization security (IVS)
- Interoperability and portability (IPY)
- Mobile security (MOS)
- Security incident management, eDiscovery, and cloud forensics (SEF)
- Supply chain management, transparency, and accountability (STA)
- Threat and vulnerability management

Consensus Assessment Initiative Questionnaire

- STAR Level 1: Security Questionnaire (Consensus Assessment Initiative Questionnaire v4 / CAIQ v4) offers an industry-accepted way to document what security controls exist in IaaS, PaaS, and SaaS services
- The CAIQ is now combined with the CCM

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: 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

Highly Regulated Industries: PCI/DSS

- 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

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

Service Level Agreement (SLA)

- The CSP must realize that the use of contractual agreements such as hosting/connection agreements and SLAs are used to allocate shared responsibility and risk among both providers and consumers
- An SLA defines the precise responsibilities of the provider, sets customer expectations, and clarifies the support system (service desk) response to problems or outages
- 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)**

Elements of SLA and MSA

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

Statement of Work (SOW)

- An agreement that institutes the expectations for a project or program and aligning the team(s) involved
  - A document of agreement between a client and service or agent defining the scope and details of a project
- Elements should clarify price, cost, timeline, deliverables, process, expectations of requirements, invoicing schedules, and much more, depending on the scope and breadth of the project
- SoW may be the first document you use to establish the framework of a project before entering the planning and execution stages
- **Also: Memorandum of Understanding (or Action) MOU/MOA**

CCSP Crash Course

Michael J. Shannon

Thank You for Attending!