Welcome back to the CCSK Bootcamp

Michael J Shannon

CISSP, CCSP, CCSK

AWS Security-Specialty

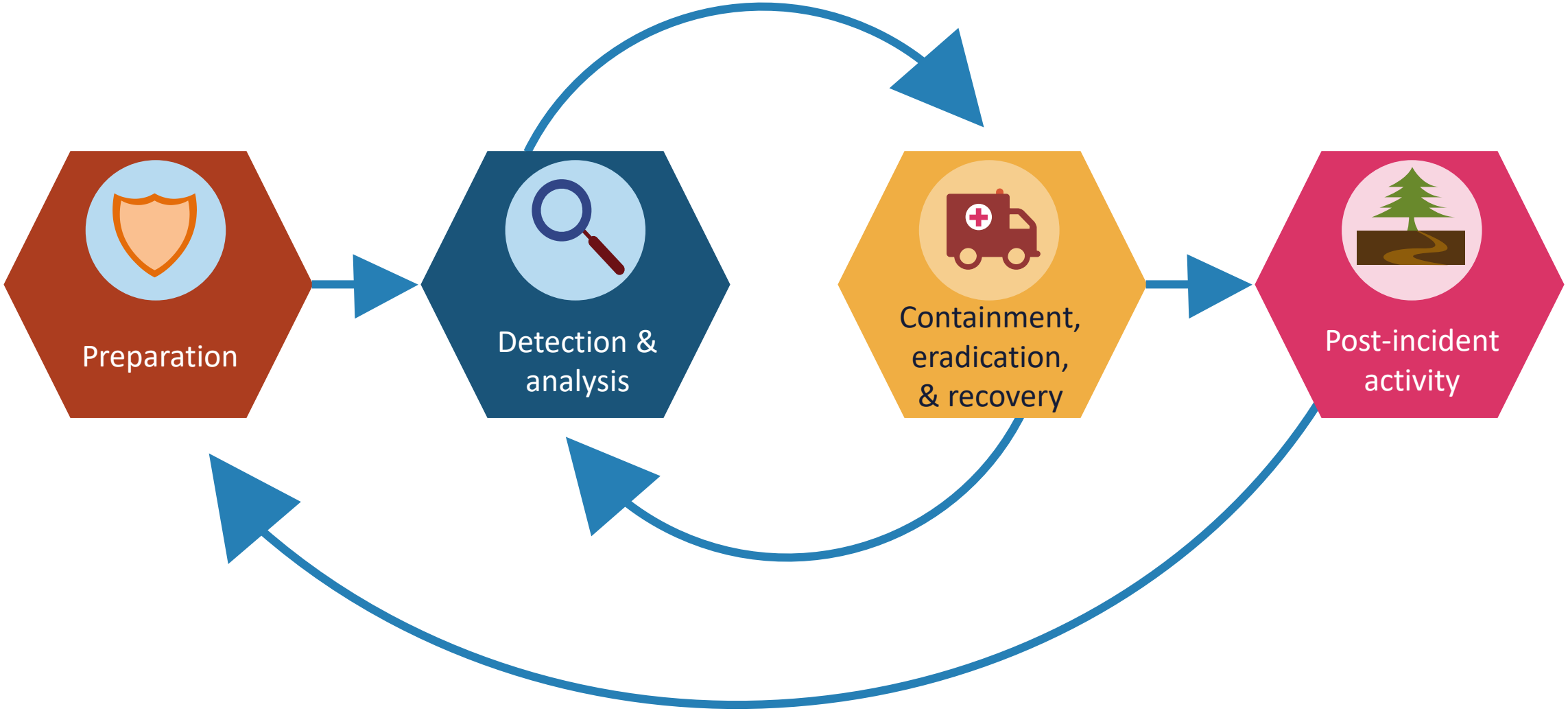
ITIL4 Managing Professional

Class will begin at 10:00 Central Standard Time

Incident Response and IRTs

- 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
- **If a CSIRT is cost-prohibitive then form a “swarm” team**

Incident Response Lifecycle



Security Information and Event Management (SIEM)

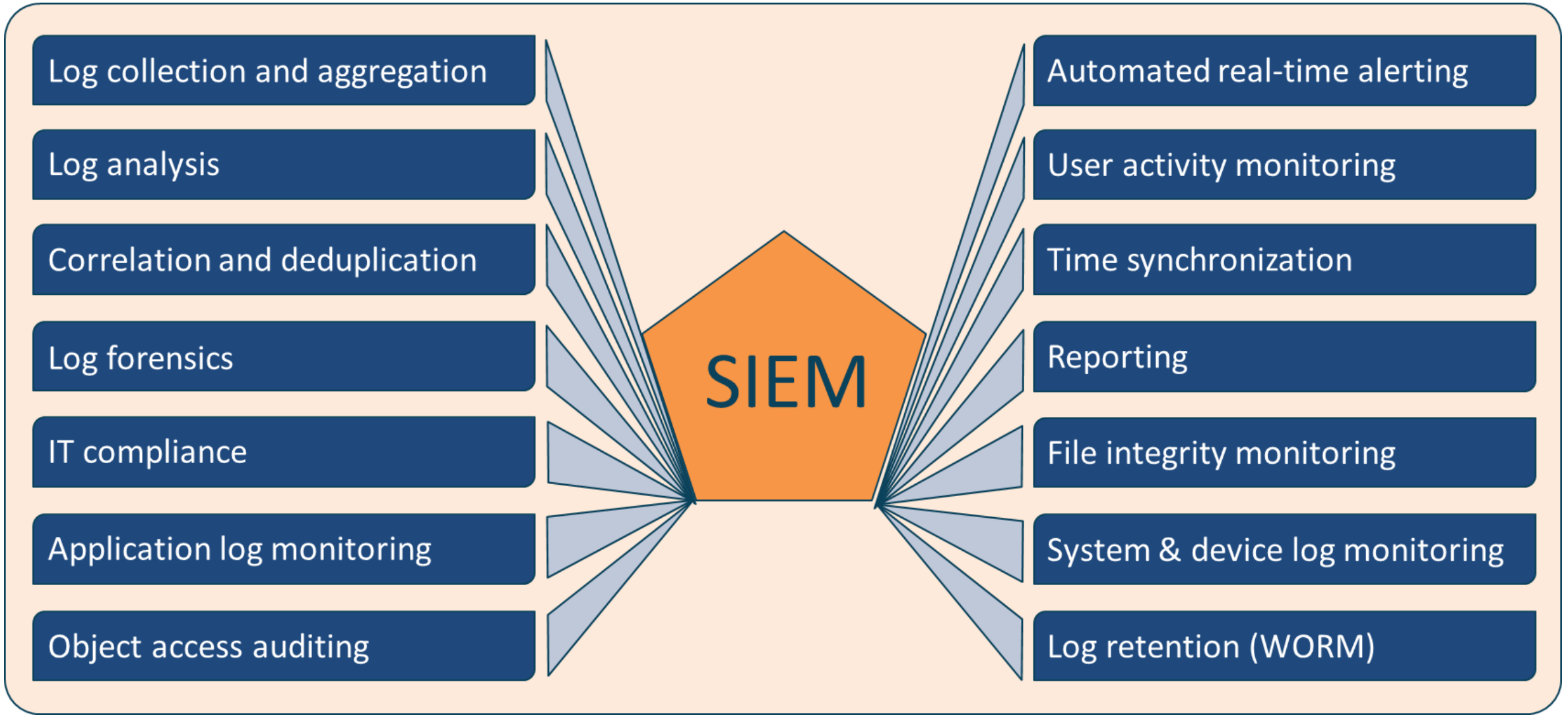
The term SIEM is a combination of security event management (SEM) and security information management (SIM)

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

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

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

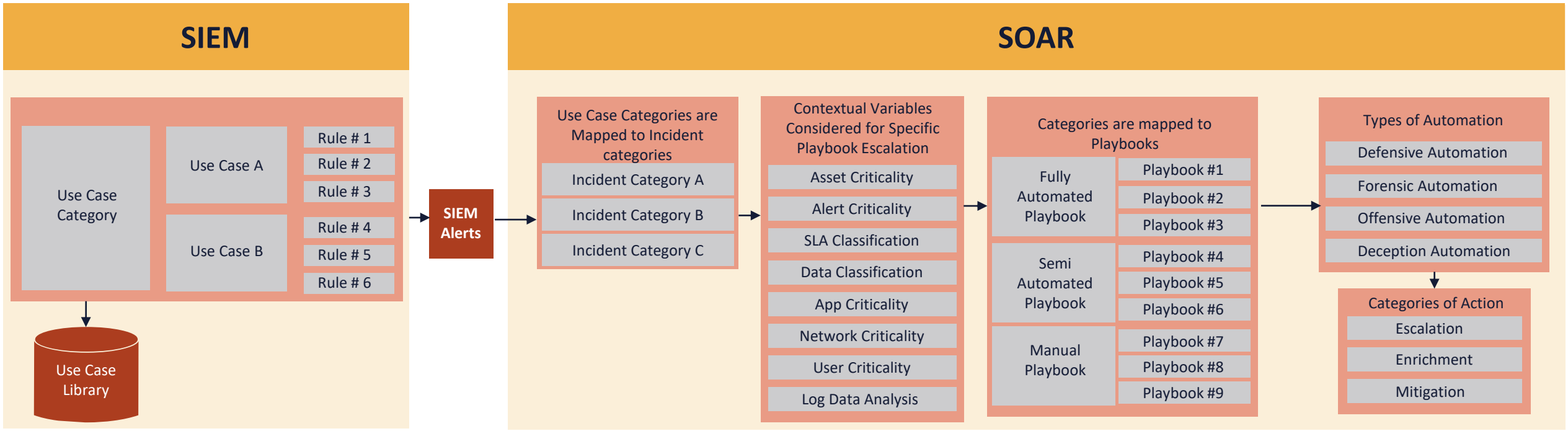
SIEM


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

Security Orchestration, Automation, and Response (SOAR)

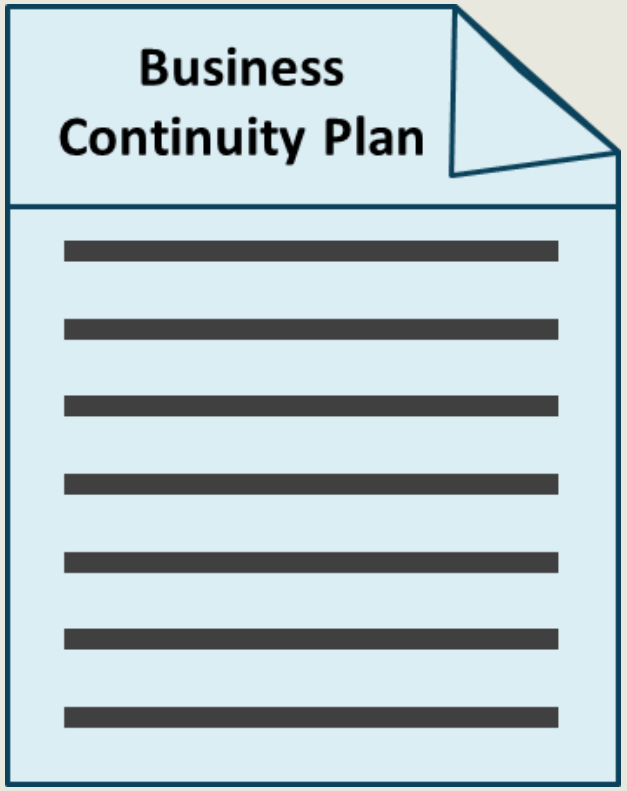
- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas
  - **Threat and vulnerability management**
  - **Incident response**
  - **Security operations automation**
- Security automation involves performing security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

SIEM AND SOAR INTEGRATION (Azure Sentinel)

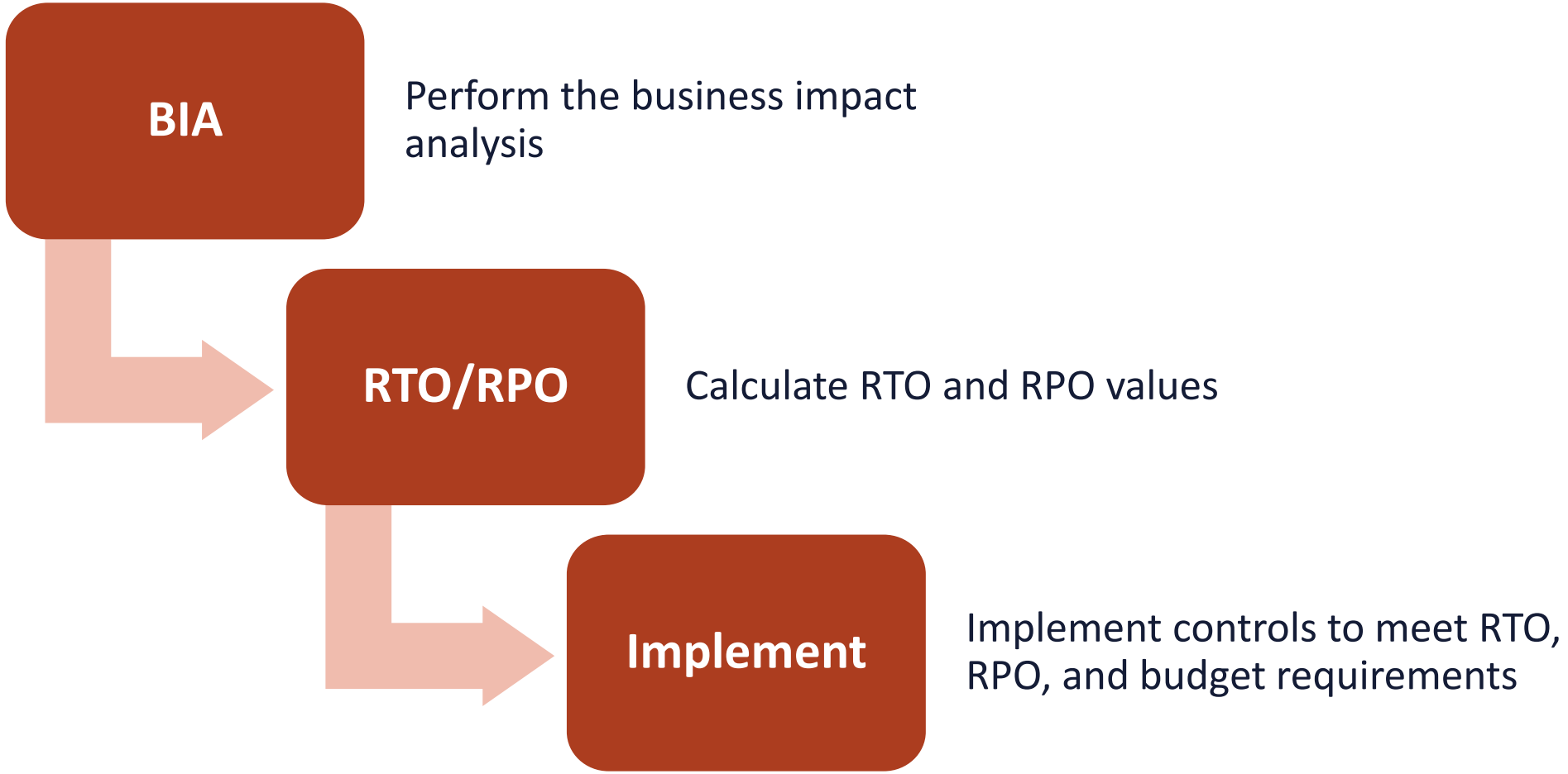


BCP/COOP

- 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



BCP Lifecycle

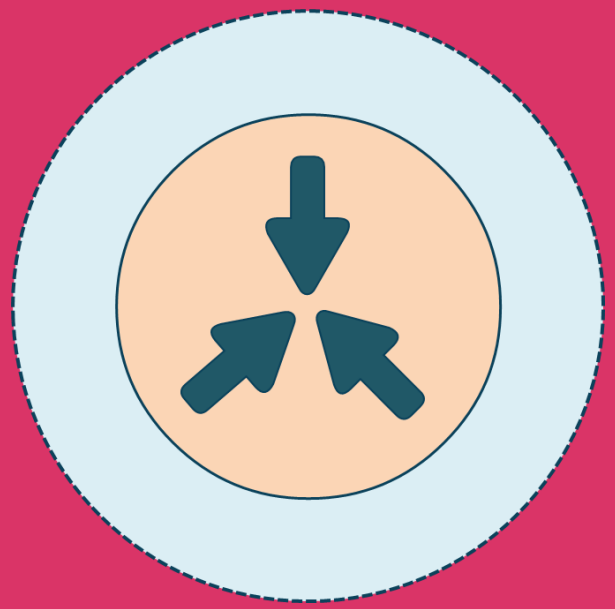


NIST SP 800-34, Revision 1

BCP according to NIST

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

BCP from Ready.gov

Business Impact Analysis

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

Recovery strategies

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

Plan development

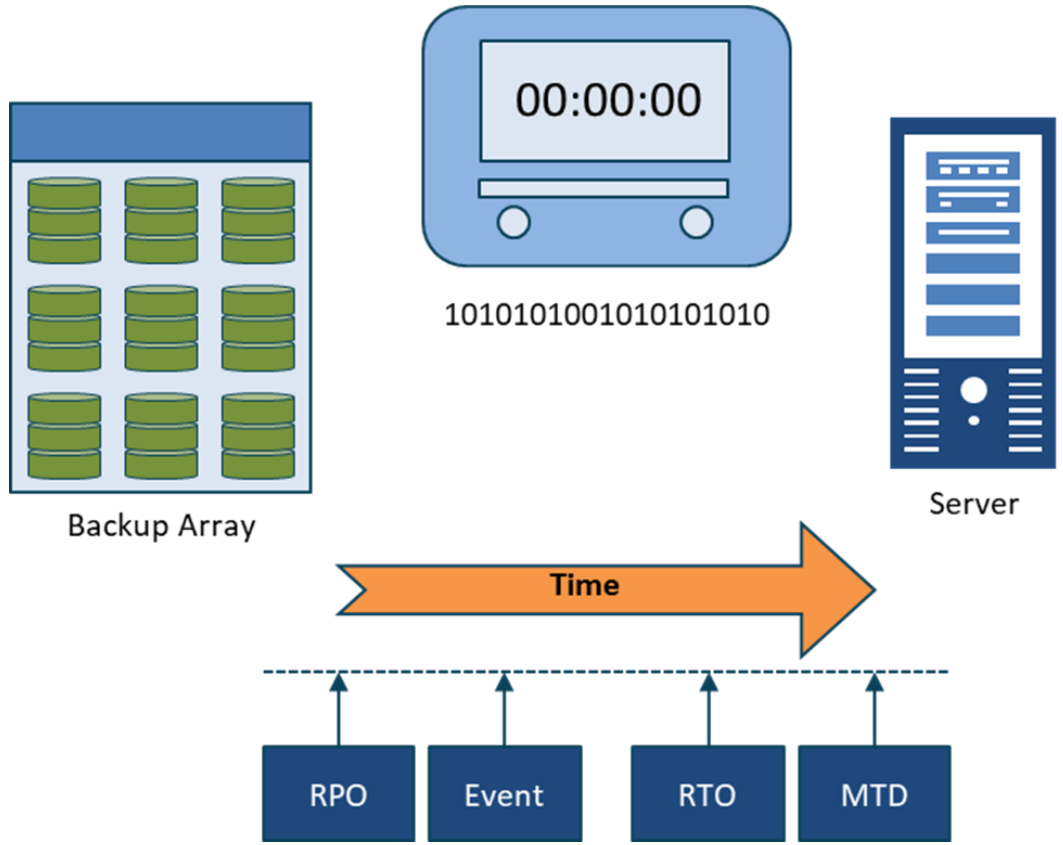
- Develop plan framework
- Organize recovery teams
- Develop relocation plans
- Write business continuity and IT disaster recovery procedure
- Document manual workarounds
- Assemble plan
- Validate and gain management approval

Testing & exercises

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

Recovery Time Objective (RTO)

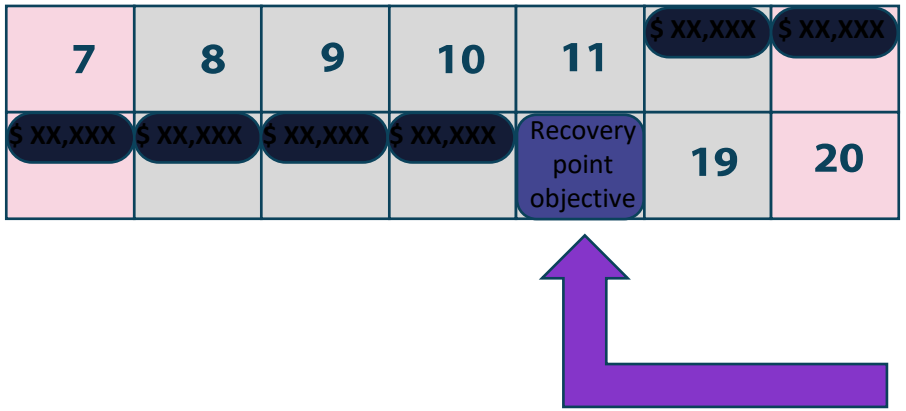
- The amount of time available to recover the resource, service, and function
- **Must be equal to or less than Maximum Tolerable Downtime (MTD)** which is the absolute maximum amount of time that a resource, service, or function can be unavailable before we start to experience a loss



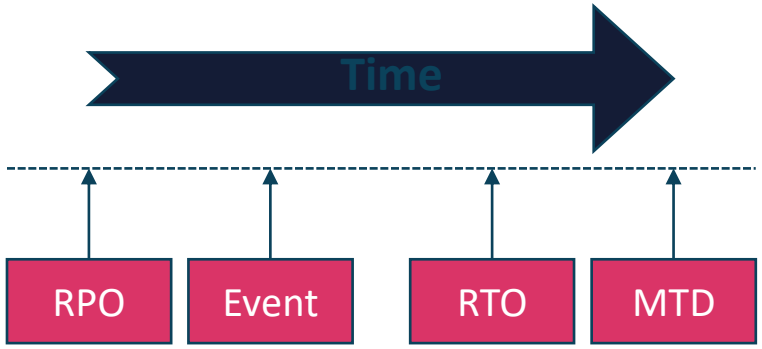
Recovery Point Objective (RPO)

The point, relative to a disaster, where the recovery process or activity begins

- Database transaction logs and snapshots
- System state last known good configuration
- Recovery volume point



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



Mean Time Between Failures (MTBF)

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

Mean Time To Repair or Replace (MTTR)

- How long does it take to repair or replace?
  - Measures time to fix or obtain the replacement or install the hot spare
  - Average value predicted based on experience and documentation
  - **Heavily affected by supply chain disruptions**

Disaster Recovery Planning (DRP)

- Ensuring that the company can recover to an established baseline of continuity after any kind of high-level incident
- The tasks and processes that will be conducted when a disaster or catastrophe strikes
- Incident can affect a single drive, an entire server, a VLAN, an area of the facility, an entire floor or building, or the entire site or campus

Disaster Recovery Planning (DRP)

- Outlines the technical aspects involved for restoration **(should have physical copies)**
  - 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

Disaster Recovery Site Strategies

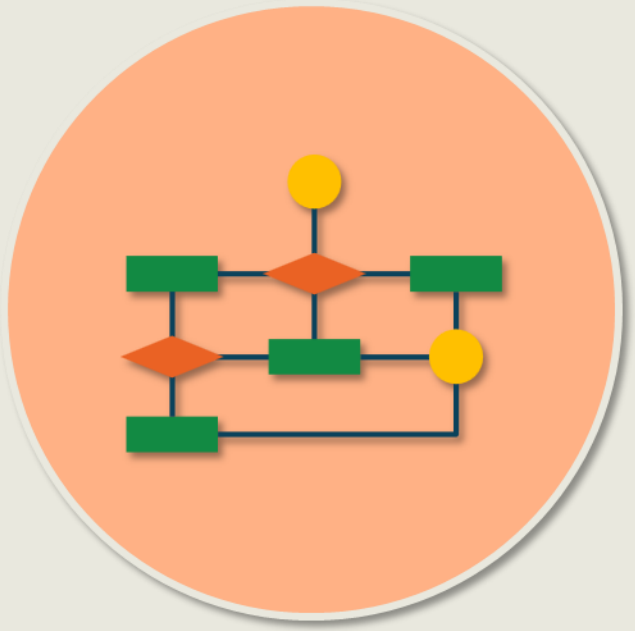
Recovery strategy	Recovery time	Advantages	Disadvantages
Commercial hot site	0 to 24 hours	• Fastest recovery time • Smoothest deployment, as facility, equipment, application software, data, and OS are installed and running • Easy to test when necessary • The optimal solution for recovering on-going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

Test Disaster Recovery Plans

Read-through testing

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

Test Disaster Recovery Plans



Tabletop testing

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

Test Disaster Recovery Plans

Walkthrough testing

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

Test Disaster Recovery Plans

Simulation testing

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

Test Disaster Recovery Plans

Parallel testing

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

Test Disaster Recovery Plans

Full interruption testing

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

Lessons Learned

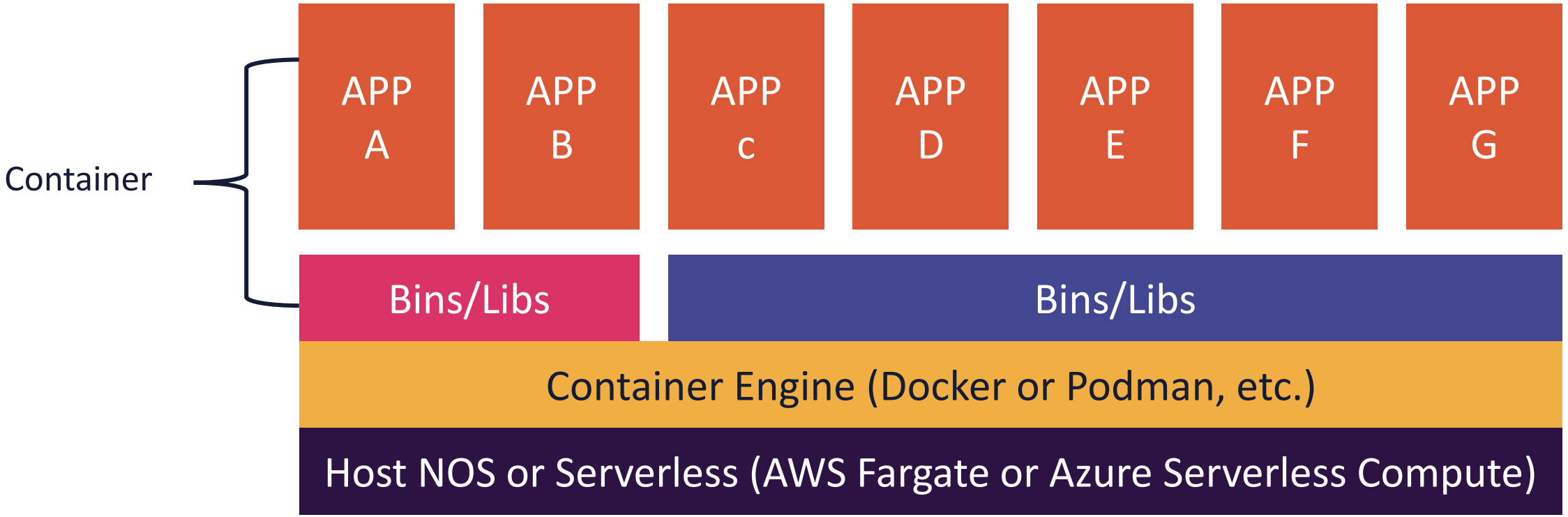
From the After-Action Reporting

- 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

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
- 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

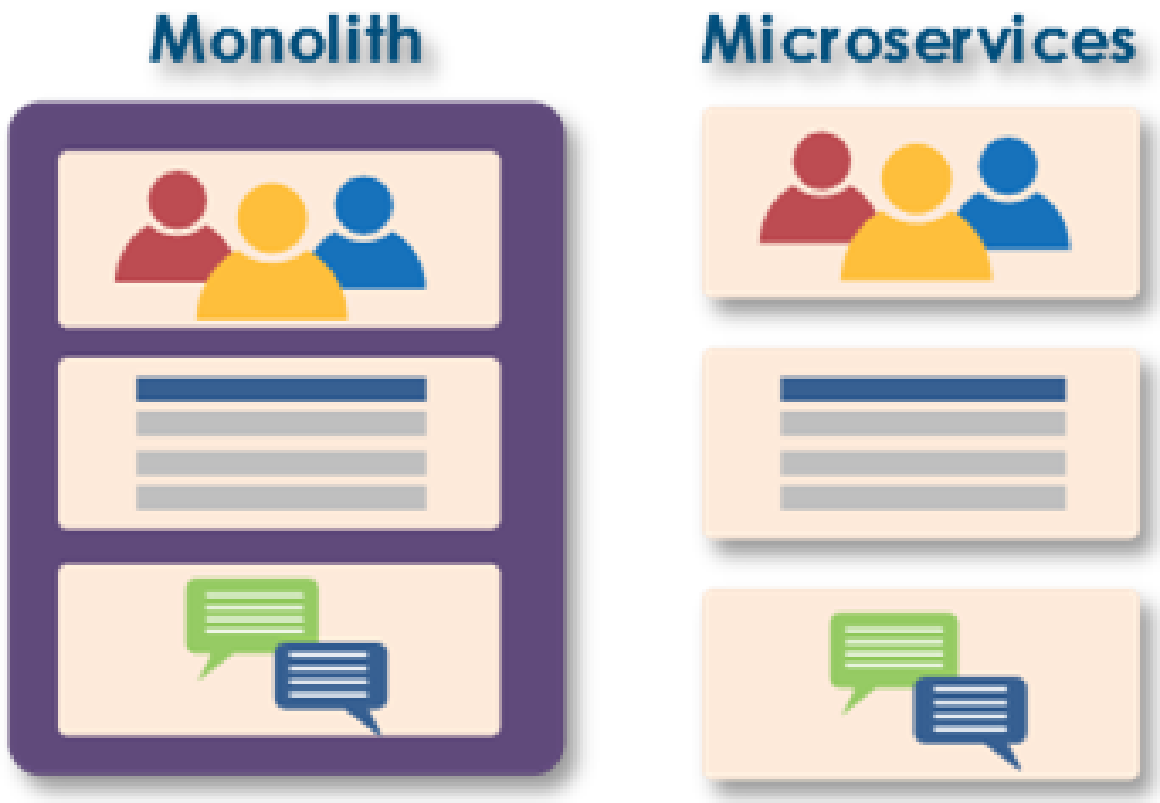


Microservices

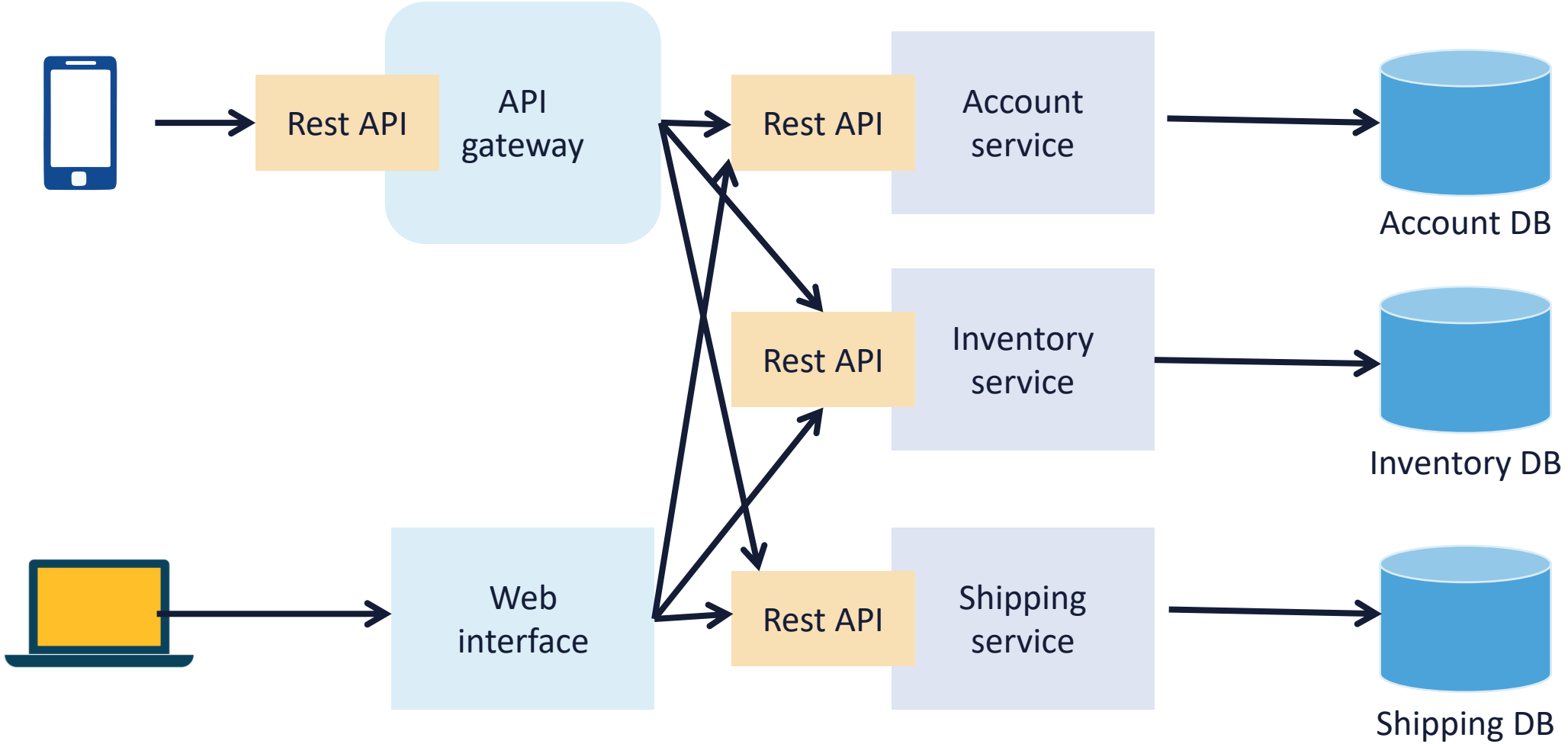
- Microservices are specific service-oriented application components
- An architectural approach to software development where the results are made up of small independent services that communicate over well-defined APIs
- These services are typically maintained by small, self-contained teams of developers
- 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



Microservices Architecture

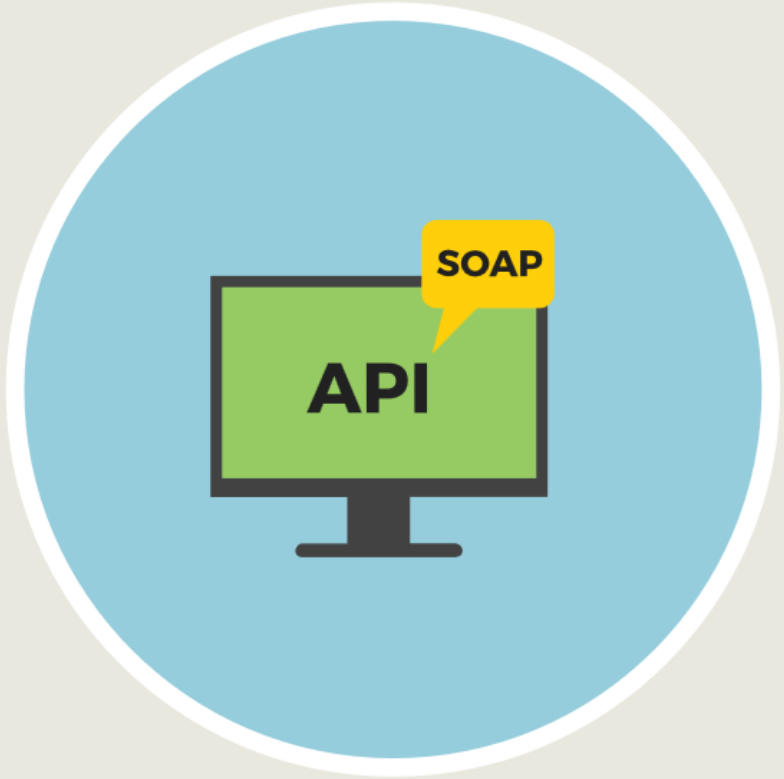


Containers vs. Microservices

- The line is blurred since containers can contain microservices and vice-versa
  - Containers and microservices can both be used collaboratively or in isolation
- A container is simply an isolated modular process represented by a collection of segmented resources and application functions to do one specific thing
  - It is literally a “container” filled with all the code, dependencies, and a runtime environment required to perform a process
- A microservice is a distinct micro-function that forms a singular part of a larger collection of functions and are better defined by how they fit into a collection rather than as a singular entity
- Microservices provide for more extensible and scalable solutions, as each service can move fluidly across different segments and platforms
  - This also means that microservices can be very lightweight compared to other solutions

Understanding APIs

SOAP vs. REST-based APIs

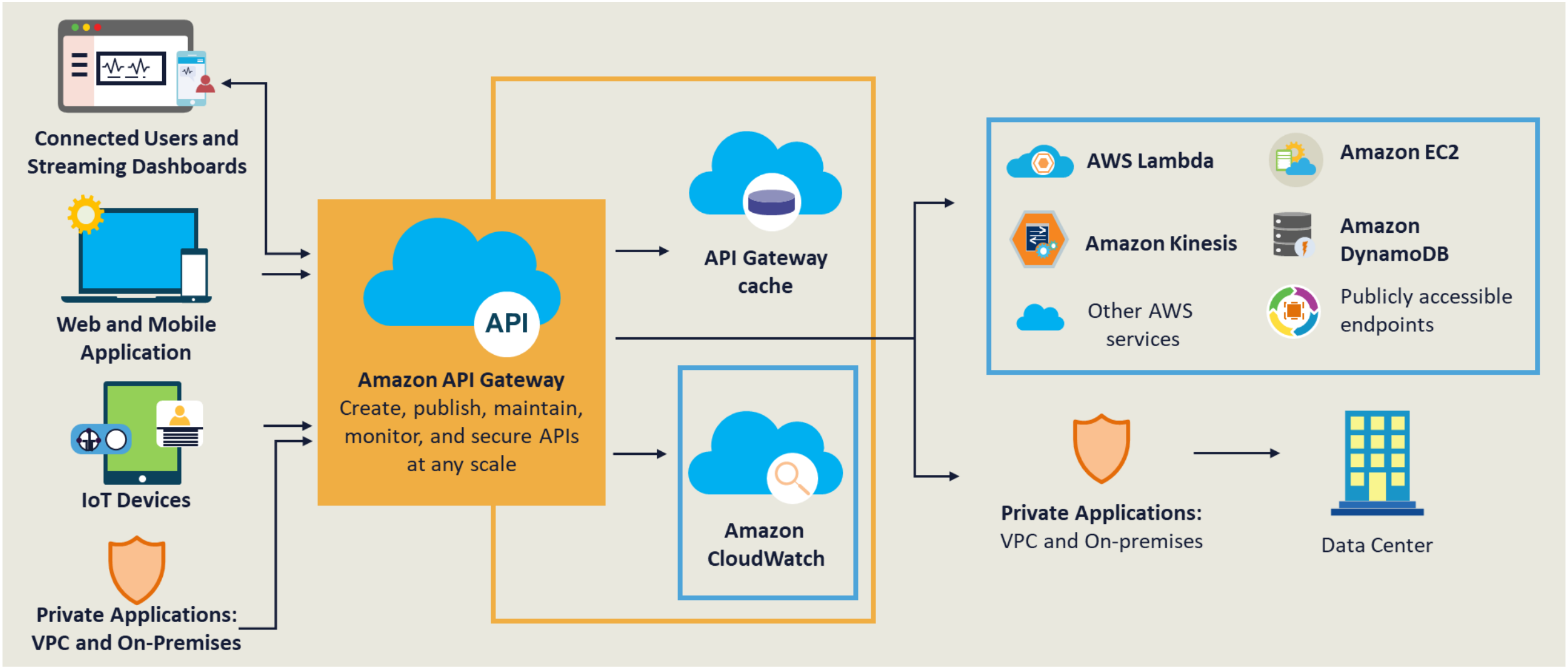


- It is important for developers to understand that in most cloud deployments, access is acquired through the means of an Application Programming Interface (API)
- These APIs will utilize tokens instead of traditional usernames and password credentials
- **Simple Object Access Protocol (SOAP)** uses 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

API Gateways

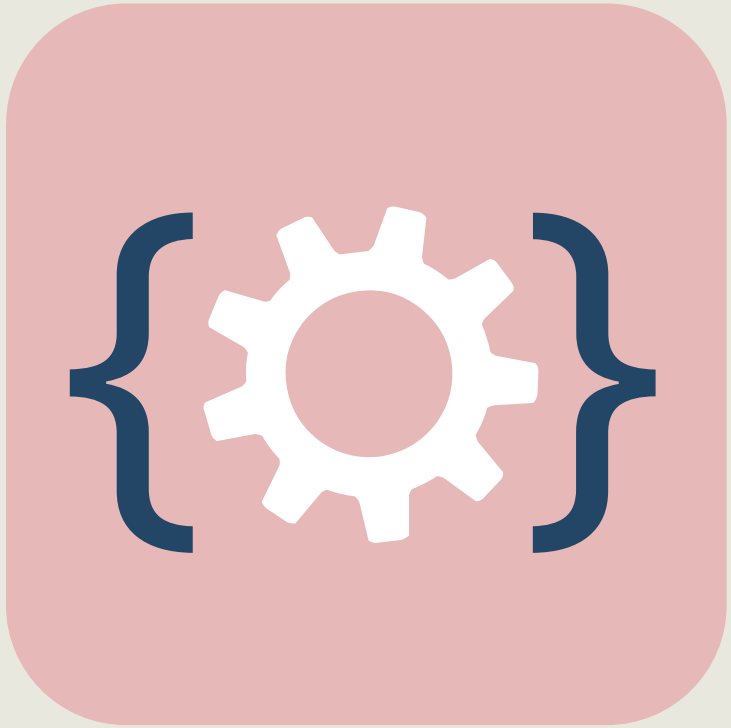
- An API Gateway is usually a fully managed cloud service that enables developers to create, publish, maintain, monitor, and secure APIs at any scale
- APIs act as the "front door" for applications to access data, business logic, or functionality from backend services
- AWS supports RESTful APIs and 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 Gateways



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

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

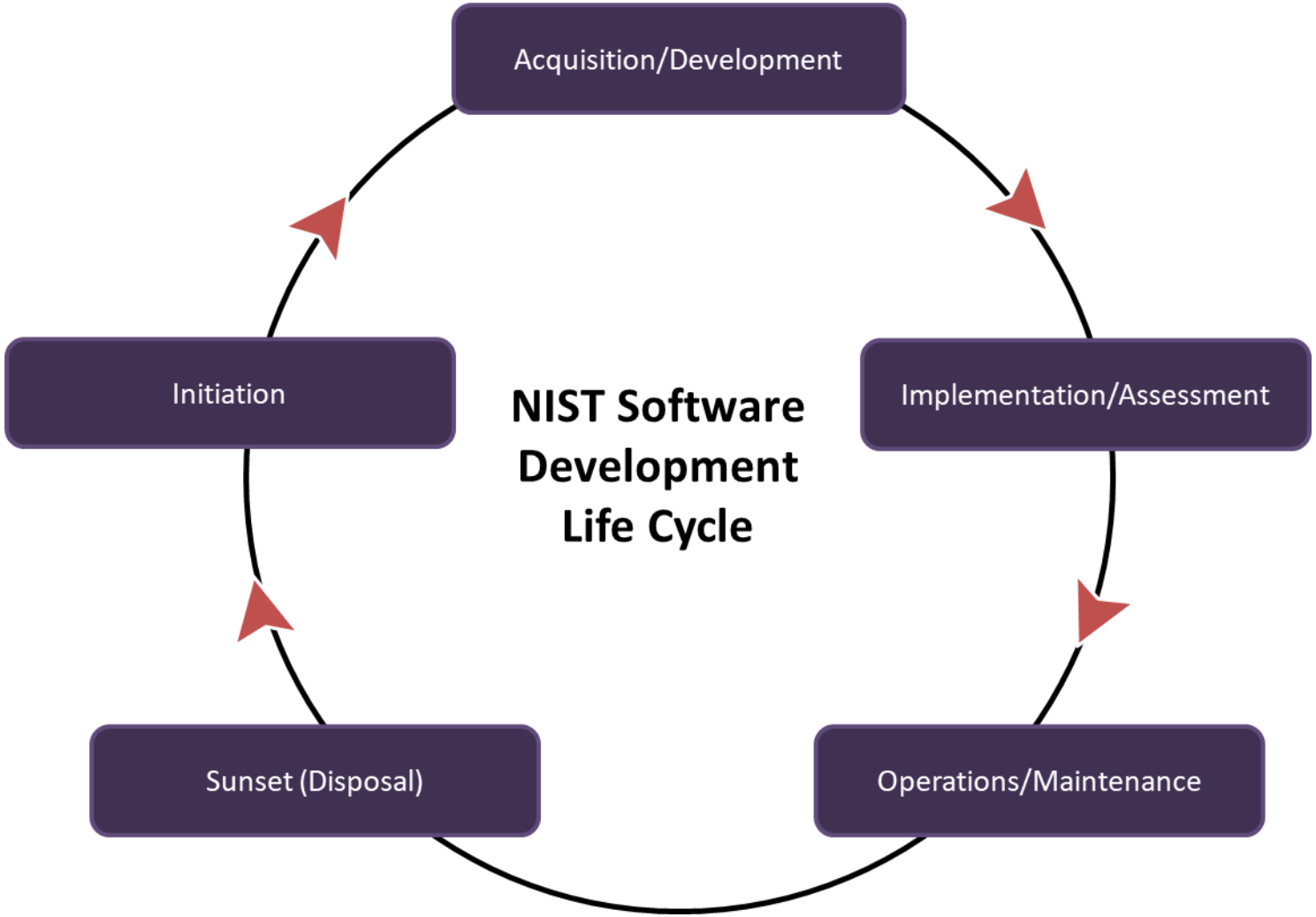
Common Web Vulnerabilities – OWASP Top 10

1. A1—Injection: Injection flaws like SQL, OS, and LDAP happen when untrusted data is sent to an interpreter as part of a command or query then the attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization
2. A2—Broken Authentication and Session Management: Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities
3. A3—Cross-Site Scripting (XSS): XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping allowing attackers to execute scripts in the victim's browser, which can hijack user sessions, deface websites, or redirect the user to malicious sites
4. A4—Insecure Direct Object References: A direct object reference happens when a developer exposes a reference to an internal implementation object like a file, directory, or database key - without an access control check or other protection, attackers can manipulate these references to access unauthorized data
5. **Security Misconfiguration: inactive virtual images and disks that have not been updated or patched**

Common Web Vulnerabilities – OWASP Top 10

6. A6—Sensitive Data Exposure: Many web applications do not properly protect sensitive data (credit cards, tax IDs) so attackers may steal or modify such weakly protected data to conduct fraud or identity theft
7. A7—Missing Function Level Access Control: Most web apps verify function-level access rights before making the functionality visible in the UI; However, applications must conduct the same access control checks on the server when each function is accessed
8. A8—Cross-Site Request Forgery (CSRF): This attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application
9. A9—Using Components with Known Vulnerabilities: Components, such as libraries, frameworks, and other software modules, almost always run with full privileges
10. Unvalidated Redirects and Forwards: Web applications frequently redirect and forward users to other pages and websites using untrusted data to determine the destination pages - without proper validation, attackers can redirect victims to phishing or malware sites

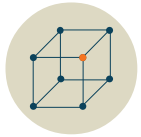
NIST Software/System Development Lifecycle



Secure DevOps Lifecycle

Training

- Secure coding practices
- Writing security tests
- Provider/ platform technical training



Define

- Code standards
- Security functional requirements

Design

- Threat modeling
- Secure design

Develop

- Code review
- Unit testing
- Static analysis
- Dynamic analysis

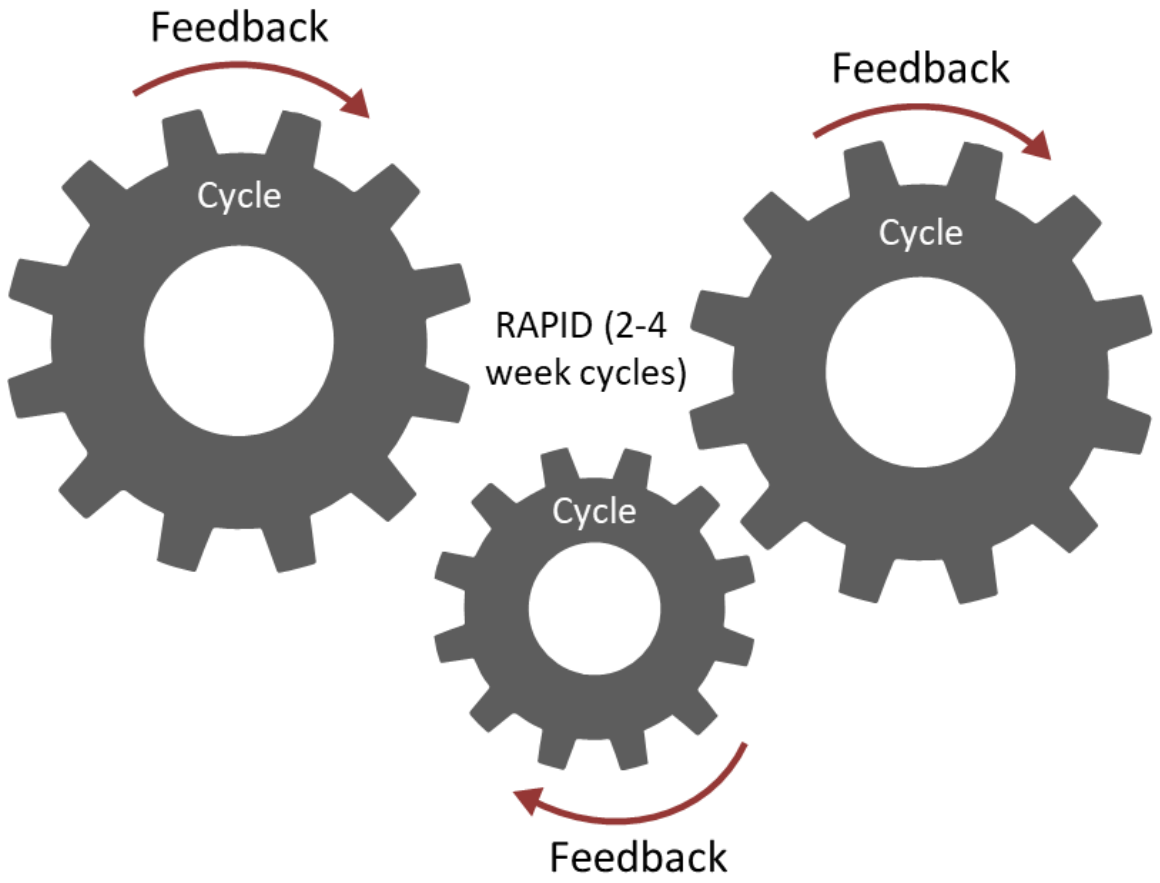
Test

- Vulnerability
- Assessment
- Dynamic analysis
- Functional tests
- QA

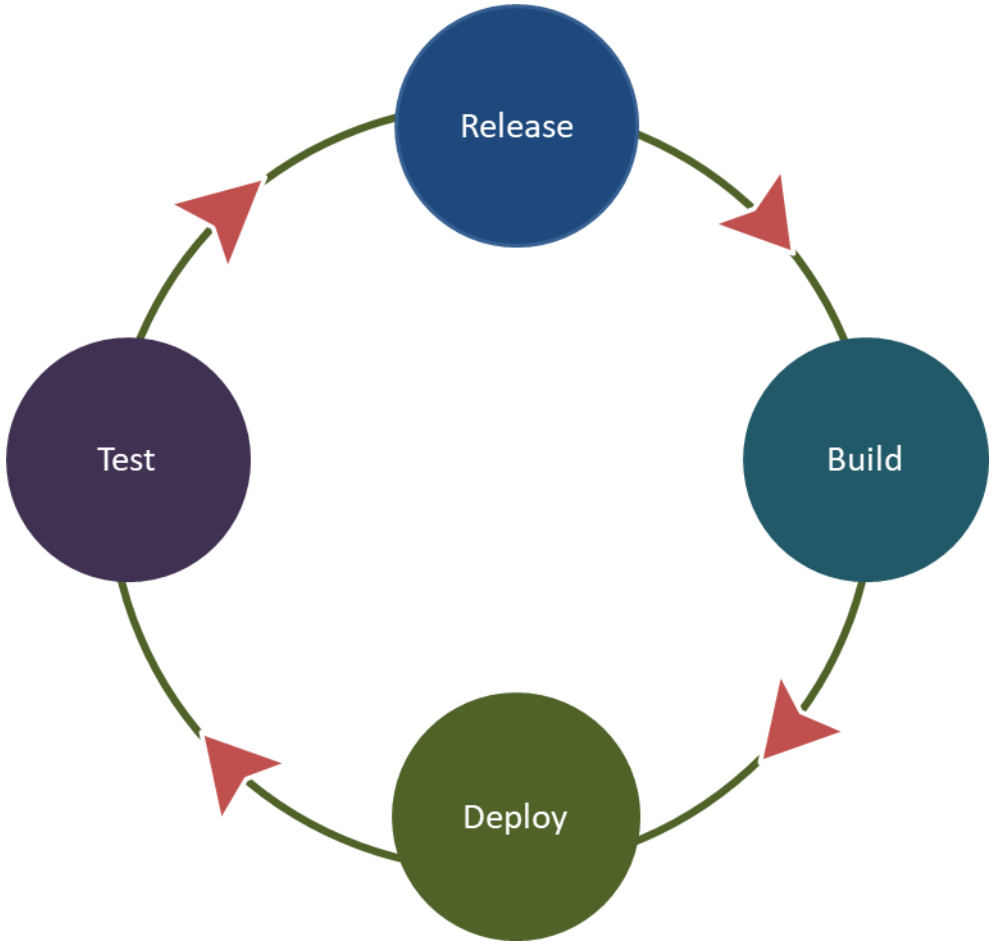
Agile Software Development

Excellent for smaller projects

- Evolutionary approach – measured in weeks
- Collaboration of cross-functional teams
- Very flexible, adaptable, not predictable, testing done during development
- Very high level of customer involvement throughout the project
- Works tightly with Agile Project Management

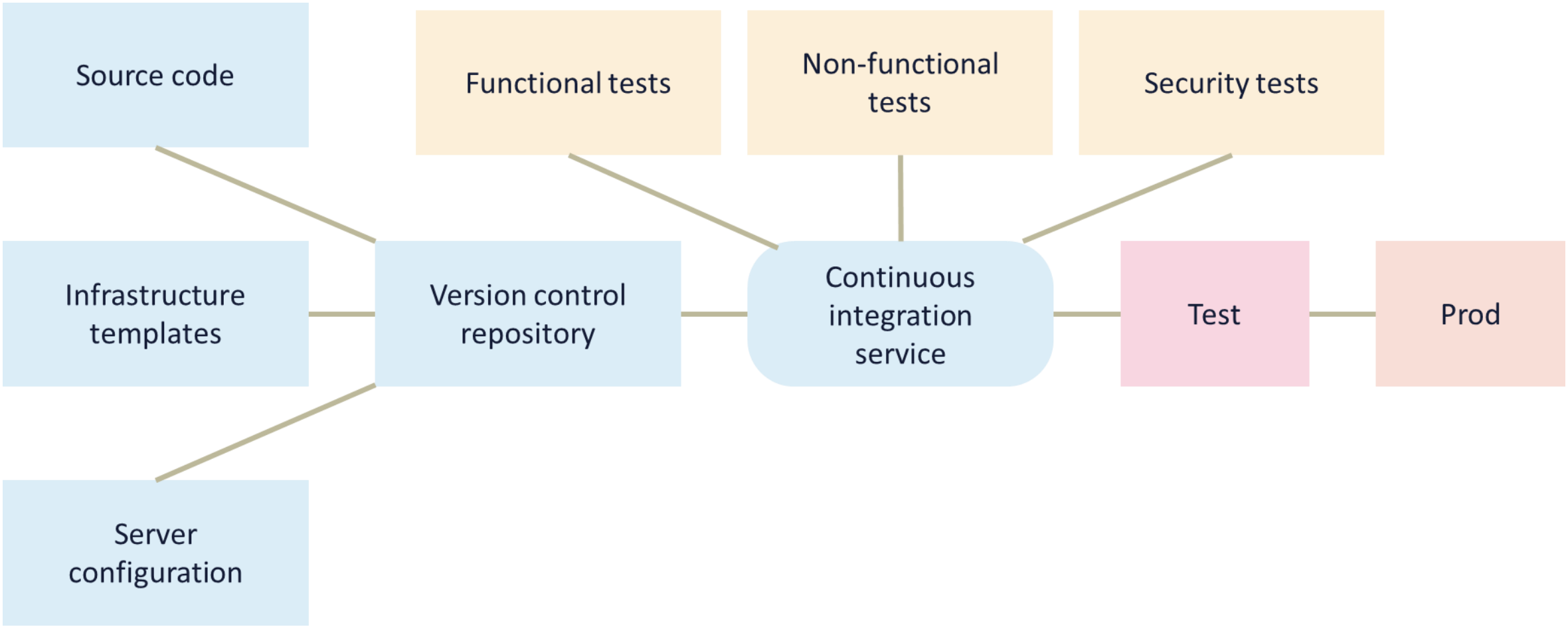


Continuous Integration – Continuous Deployment (CI/CD)



- Continuous Integration (CI) is a 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

Continuous Deployment Pipeline



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

STRIDE Threat Modeling

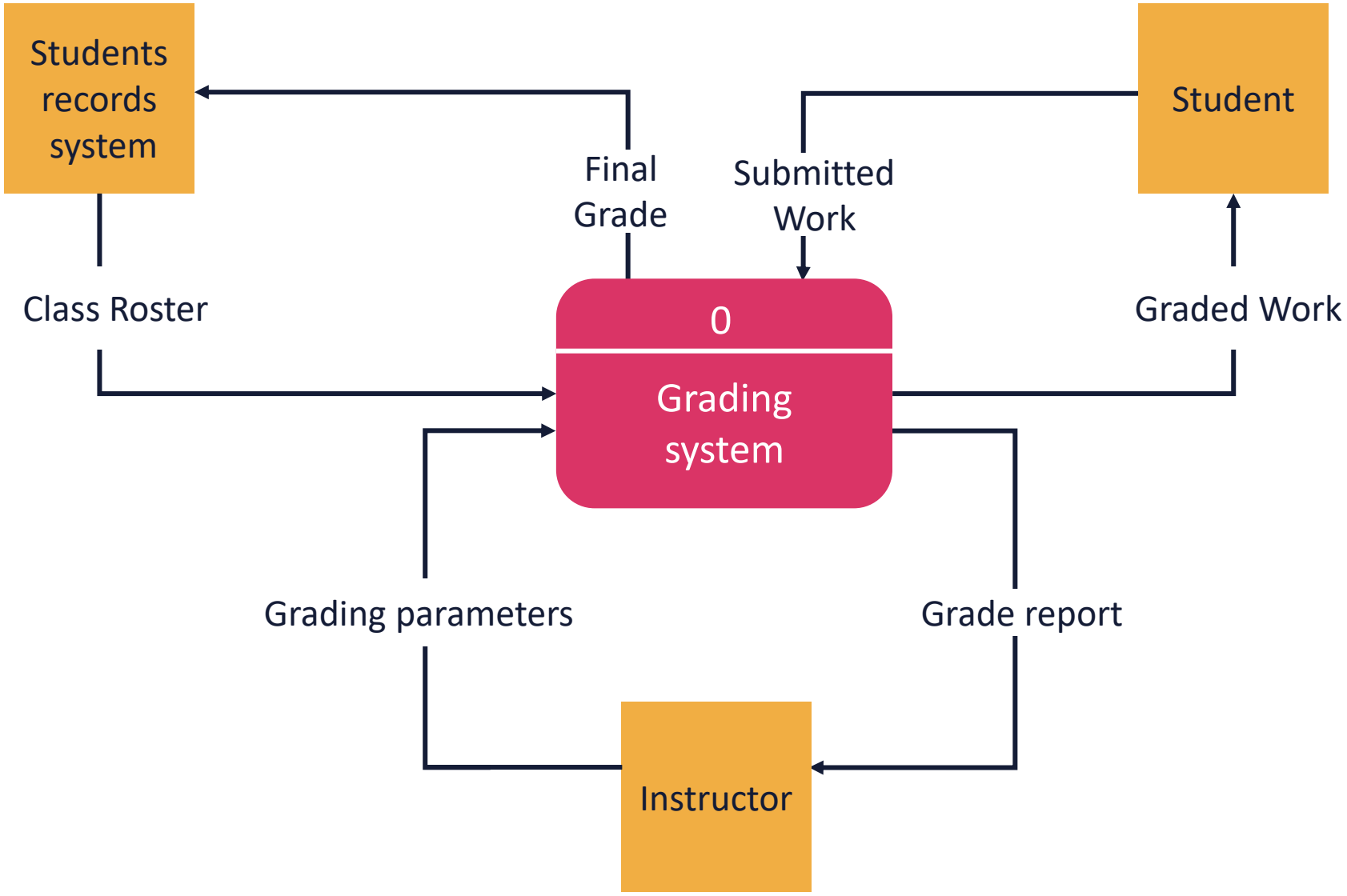
- STRIDE is a developer-focused threat modeling tool
- Microsoft threat modeling methodology that aligns with their Trustworthy Computing directive of January 2002
- Focus is to help ensure that Microsoft's Windows software developers think about security during the design phase
- Goal is to get an application to meet the security properties of CIA along with authentication, authorization, and non-repudiation
- Once the security SME builds the DFD-based threat model, system engineers or other experts check the application against the STRIDE threat model classification scheme

STRIDE

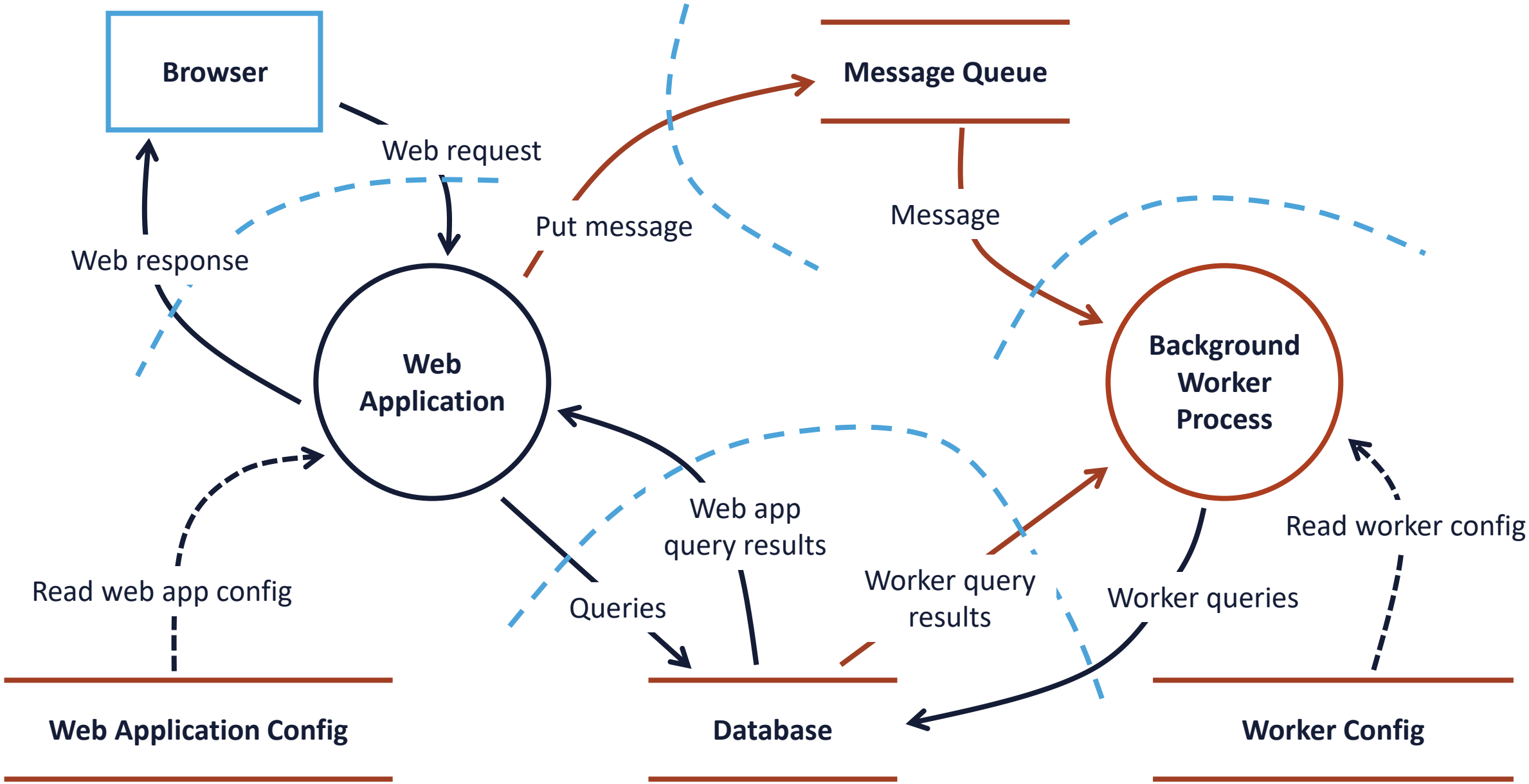
Threat	Definition	Property	Example
Spoofing	Pretending to be someone else	Authentication	Hack victim's email and to send messages as the victim
Tampering	Changing data or code	Integrity	Software executive file is tampered with by hackers
Repudiation	Claiming not to do a particular action	Non-repudiation	"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



Sample Data Flow Diagram (DFD): complex

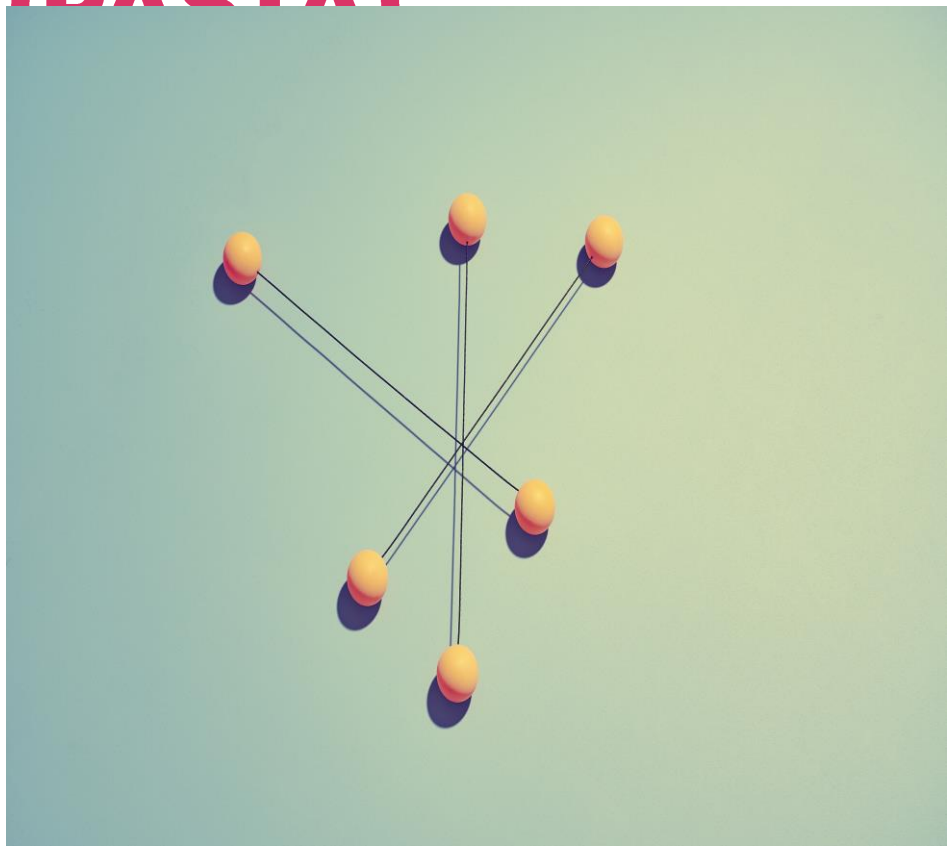


DREAD

- DREAD is 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

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

Process for Attack Simulation and Threat Analysis (PASTA)



- 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 and magnifies cybersecurity responsibilities beyond the IT department

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-/.

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?
  - What are the outputs?
  - What are the tips and tricks that make security architecture risk assessment easier?

Software Assurance

- The key objective of the Software Assurance Program is to shift the security paradigm from patch management to software assurance
- Encourage developers to raise overall software quality and security from the start
- Emphasize the usage of tested standard libraries and modules
- Employ industry-accepted approaches that recognize that software security is fundamentally a software engineering issue that must be addressed systematically throughout the software development life cycle

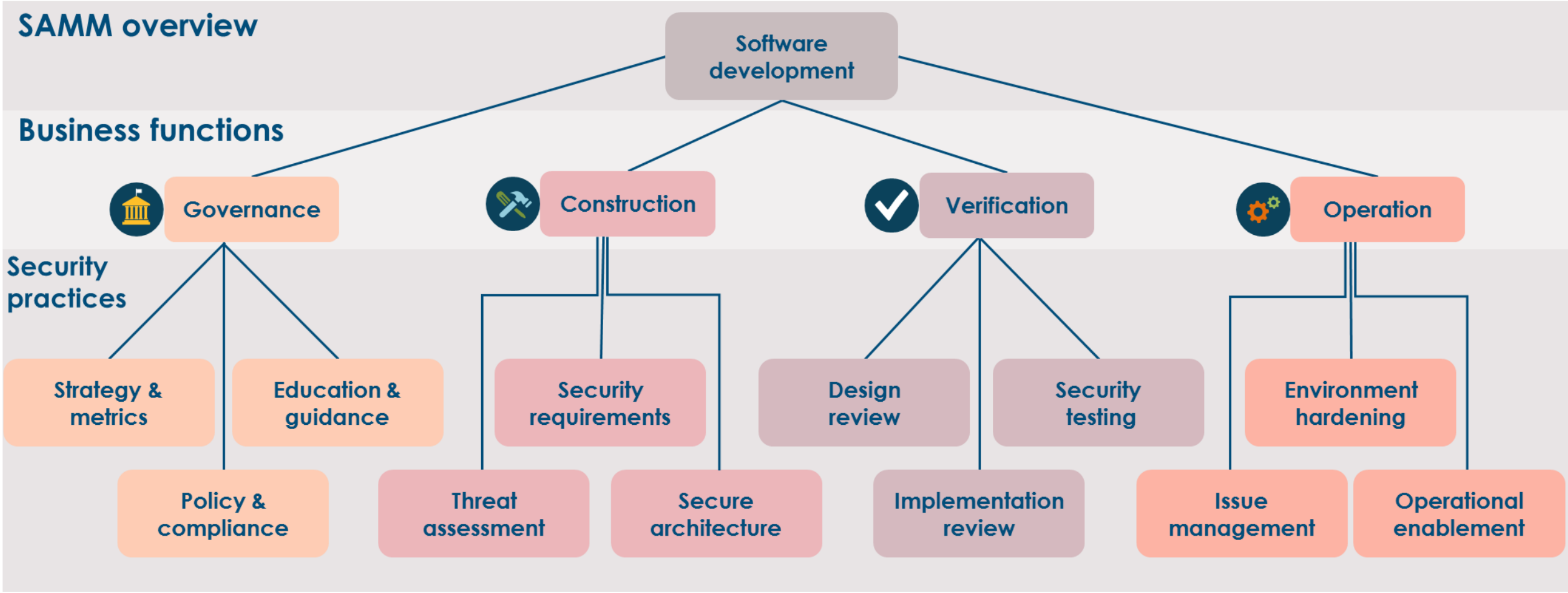
OWASP Application Security Verification Standard (ASVS)

- 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 were developed to be used:
  - As a meaningful metric
  - As secure development guidance
  - During the procurement process

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.

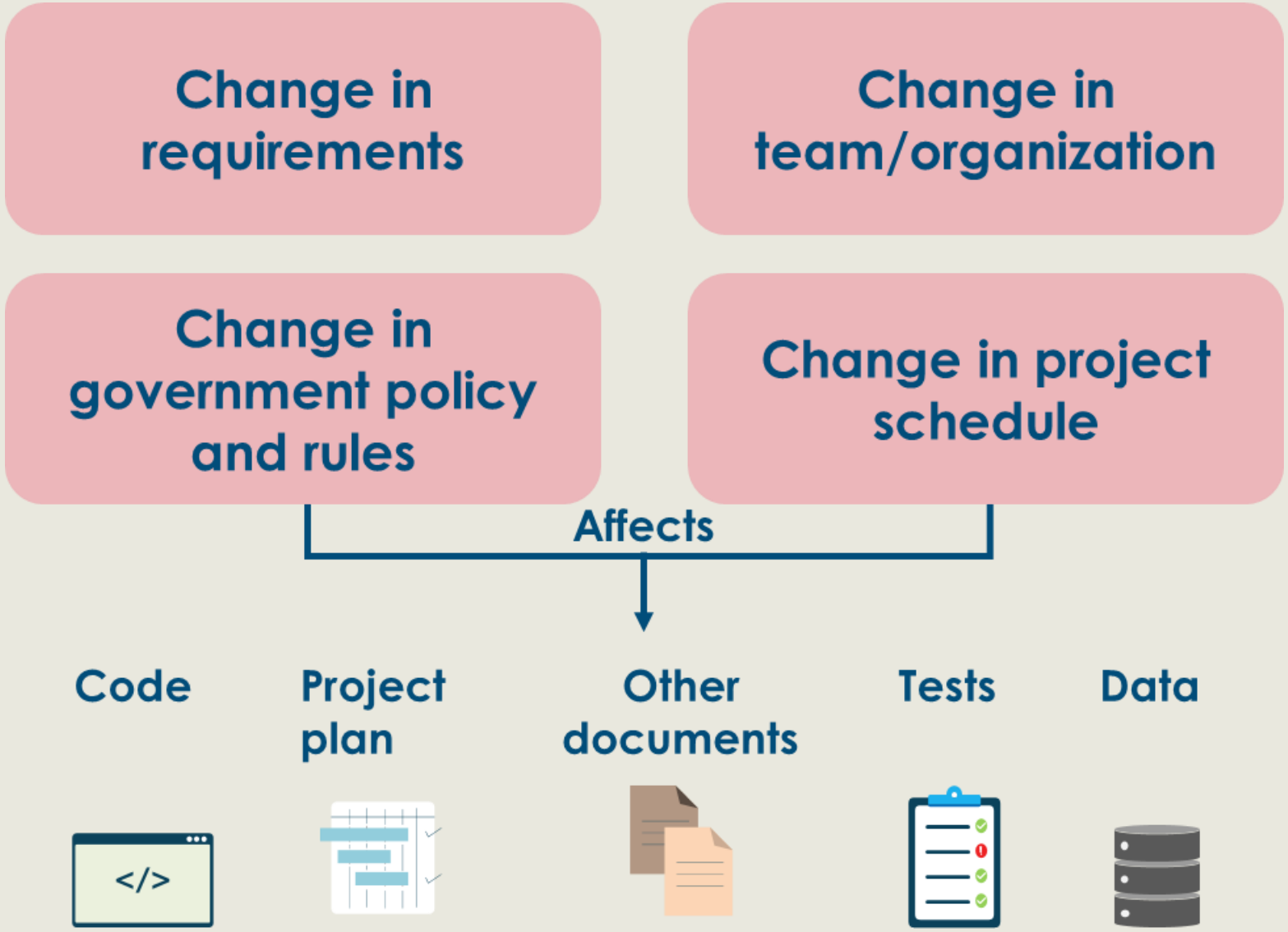
SAFECode

- SAFECode is 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
- They publish the “SAFECode Fundamental Practices for Secure Software Development” to help the industry start or advance their own software assurance programs and encourage secure development practices

Software Configuration Management (SCM)

- Software configuration management (SCM) is a software engineering process to systematically manage, organize, and control the changes in the documents, codes, and other artifacts during the software development life cycle
- The primary goal is to enhance productivity and minimize errors
- SCM is part of the cross-disciplinary field of configuration management (integrated product teams – IPT) and can correctly determine the revision history

Software Configuration Management (SCM)



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 without the need to scan or attack the application
- Continuous detection – DevOps-friendly
- Integrates and communicates with task management systems to create unified workflows

RASP

Runtime application self-protection (RASP)

- RASP tools block possibly malicious actions while an application is in production
- RASP observes the app or application at runtime, analyzing its behavior as well as the context in which the behavior occurs
- If it discovers a security event (such as an attempt to run a shell, open a file, or call a database) it will automatically attempt to terminate that action
- RASP can mitigate main types of web application attacks such as XSS, SQLi, and other zero-day exploits
  - It can also be beneficial to businesses with lean security resources since it can automatically block attacks on the spot without human intervention

Data Structures

- **Structured** data follows a pre-defined data model and is therefore straightforward to analyze since it conforms to a tabular format with relationship between the different rows and columns (Excel files or SQL databases)
- **Unstructured** data – information that does not have a predefined data model or is not organized in a pre-defined way (audio, video files or No-SQL databases)
- **Semi-structured data** - does not conform with the formal structure of data models associated with relational databases or other forms of data tables, but nonetheless contain tags or other markers to separate semantic elements and enforce hierarchies of records and fields within the data (JSON, YAML, XML)
- **Metadata** – data about data that supports Big Data analysis and big data solutions to provides deeper analysis regarding a specific set of data

Data Discovery

- Data discovery is a methodology that often serves two goals:
  - The enterprise is performing an initial asset assessment and inventory of data ownership
  - The organization is performing e-discovery as part of a digital forensic investigation
- There are three main forms of data discovery
  - **Content-based** – dataset contents such as terms and pattern-matching
  - **Label-based** – discovery is based on existing labels an/or tagging that is applied to physical and logical assets both on-prem and in the cloud
  - **Metadata-based** – leveraging the extensible metadata available on data stored as objects – i.e., using APIs against data in AWS S3, Google Cloud Storage, Azure Blob storage

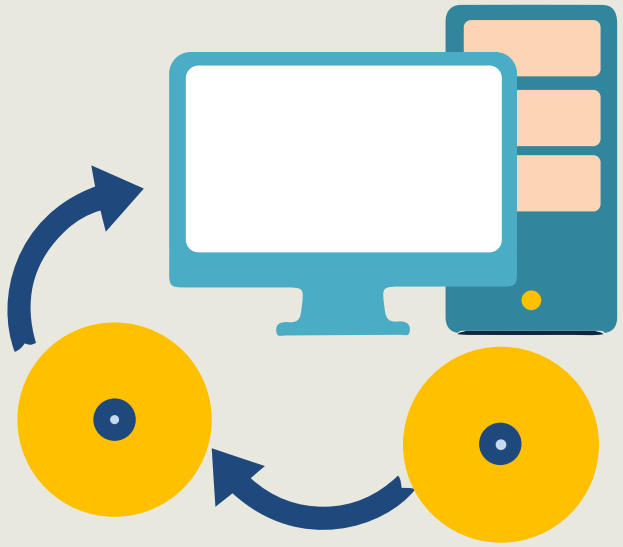
Cloud Data Life Cycle Phases

Phase 1: Create

- Data is either generated from scratch, inputted, or modified into another format either locally or in the cloud
- If created locally it may need to be sent over IPsec or TLS VPN (S2S or P2S) or the customer can perform client-side encryption and send over a clear channel
- The data owner is identified in the create phase
- Other key activities of phase one include:
  - Data discovery
  - Data categorization
  - Data classification
  - Data mapping
  - Data labeling (tagging)

Cloud Data Life Cycle Phases

Phase 2: Store



- After the Create phase, the data is put into a volume (block)/object storage system or into one of several types of database systems
- This phase relates to transactional, near-term usage data as **opposed to long-term cold data storage**
- It also includes files and spreadsheets, typically done at during or at the end of the Create phase
- **Activities of this phase can also occur simultaneously when the data is generated in phase one**
- Protection of data at rest and data in transit will often occur in this phase unless default encryption is implemented in the Create phase

Cloud Data Life Cycle Phases

Phase 3: Use

- Data is utilized by people, applications, and tools as well as being changed from the original state
- Raw data becomes information
- If data is used remotely then protection mechanisms must be in place (VPN, secure endpoints, digitally signed API calls)
- The systems that “use” the data must be secured as well; for example, endpoint detection and response (EDR) or host-based IPS agents (Palo Alto Traps)
- Technologies like VPN, Identity Rights Management (IRM), and Data Loss Prevention (DLP) engines may be introduced
- Assistance can come form a Managed Security Service Provider (MSSP) or Cloud Access Security Broker (CASB)

Cloud Data Life Cycle Phases

Phase 4: Share

- Data is visible, analyzed, and apportioned among users, systems, and applications
- Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as IRM and DLP services)
- Stringent Identity and Access Management (IAM) and/or Identity Management (IdM) should be used to enforce the least privilege principle in line with access control model (DAC, RBAC, MAC, ABAC, etc.)
- It may be beneficial to implement egress DLP on the email message transfer agents (MTA) to and from the cloud provider and partners using the same CSP

Cloud Data Life Cycle Phases

Phase 5: Archive

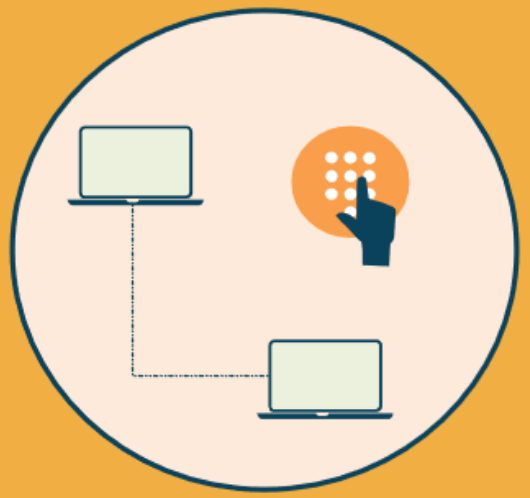
- Data is stored for long-term and removed from active usage
- It can be sanitized based on policy
- Stringent cryptography will be introduced for data at rest – as in AES-GCM-256 AEAD solutions
- Archiving is often automated and based on governance or regulations for example AWS S3 Intelligent Tiering or Storage Gateway management over a Direct Connect link
- Factors in choosing long-term storage:
  - Location
  - Media format
  - Staffing
  - Operating procedures

Cloud Data Life Cycle Phases

Phase 6: Destroy

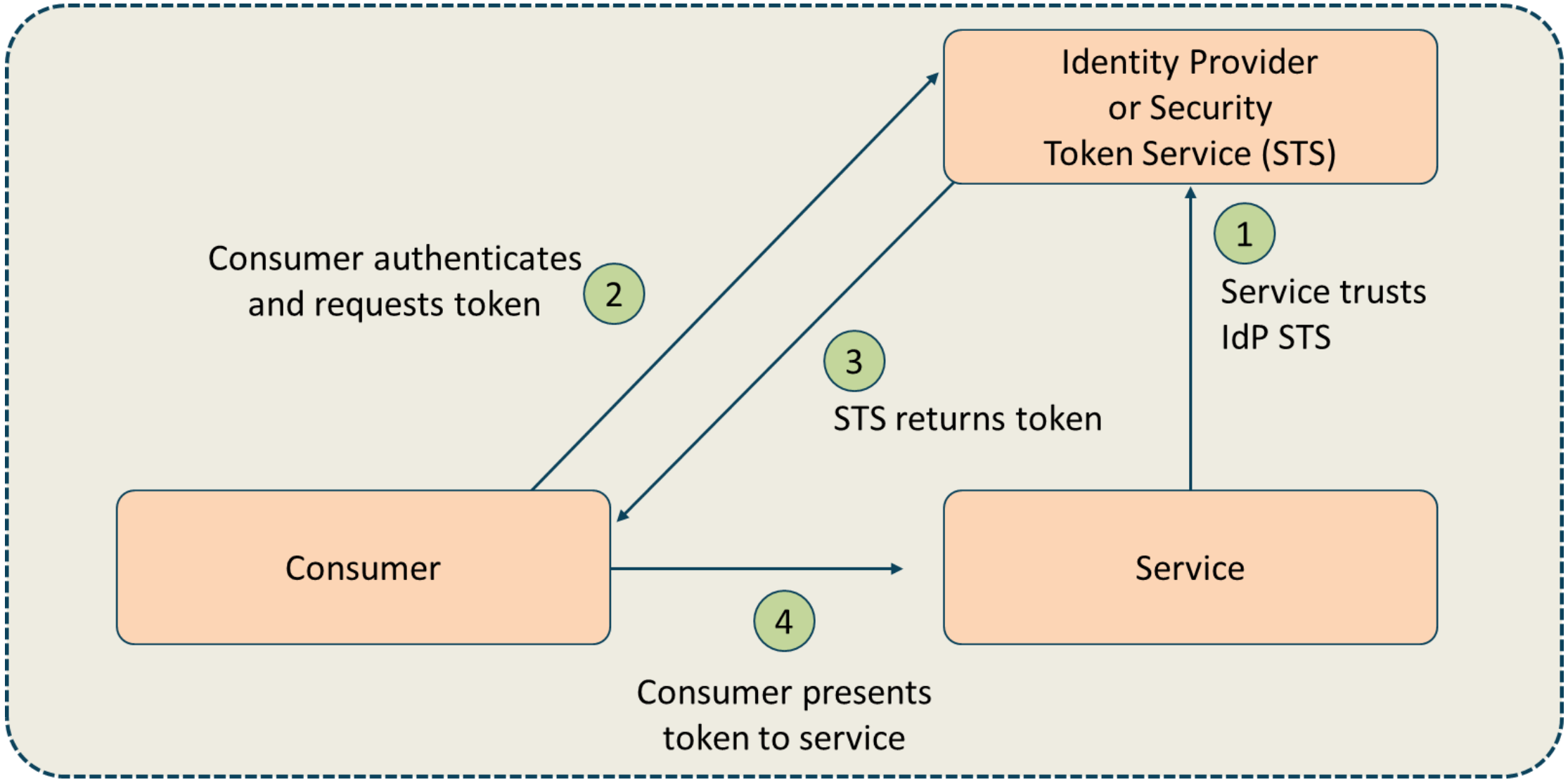
- Data is no longer accessible or usable based on lifetime, utility, policy, governance, and/or regulations
- Although data can be disposed of using a variety of methods, when storing data at a CSP, cryptoshredding (cryptographic erasure) is the only practical and comprehensive solution
- The provider will have their own established methods for disposal of data and media, often using military grade programs or physical destruction

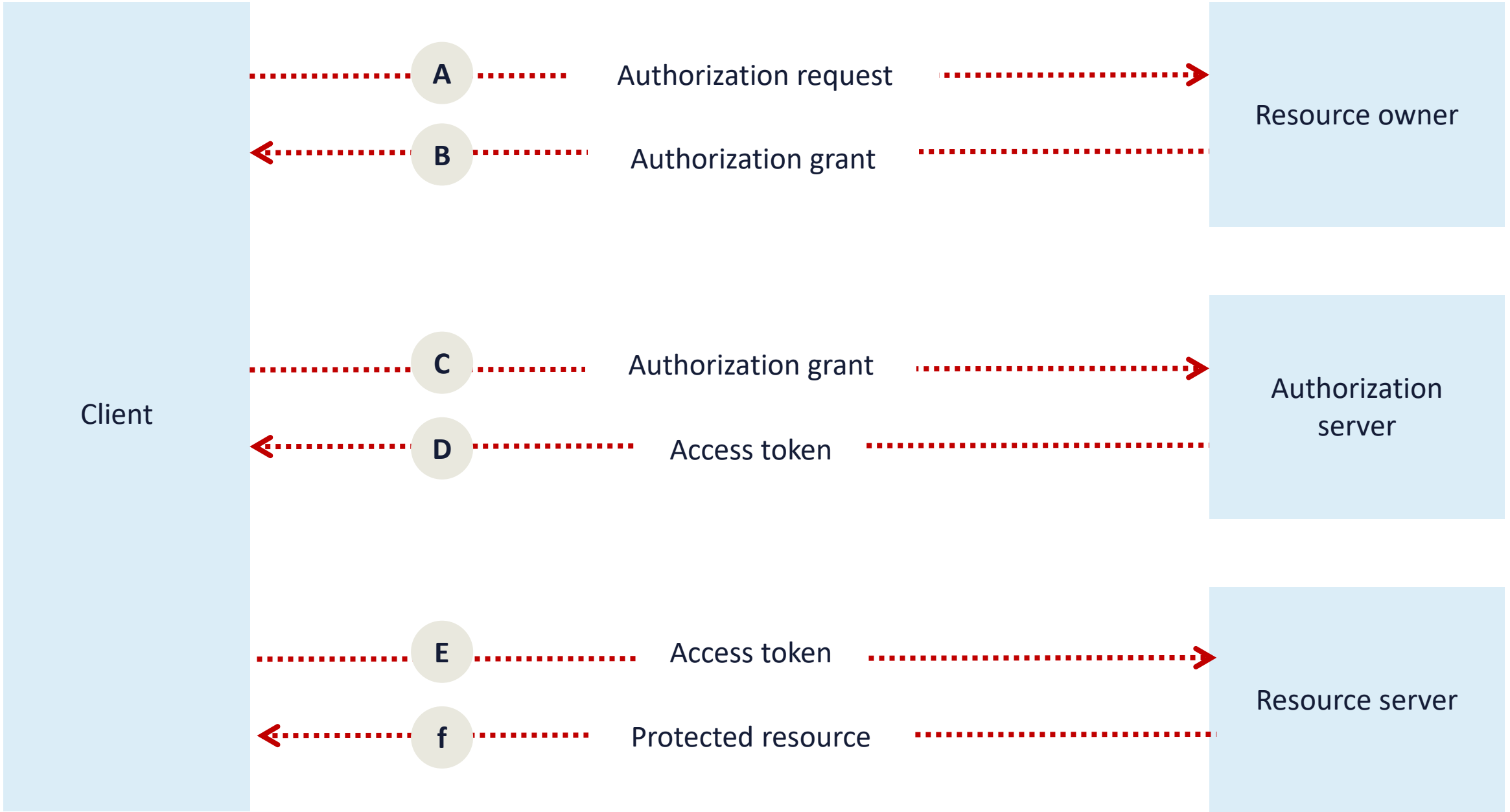
Identity and Access Management (IdM)



- As a customer of a cloud service provider there are two main identity management (AAA) options:
  - **Cloud-based IAM managed services**
    - Role-based access control (groups, users, roles, and persistent permissions)
    - AzureAD
  - **Single Sign-on with federated access**
    - Session-based with token, assertion, or ticket
    - Single (multi-factor authenticated) credential provides access to possible many services and service providers

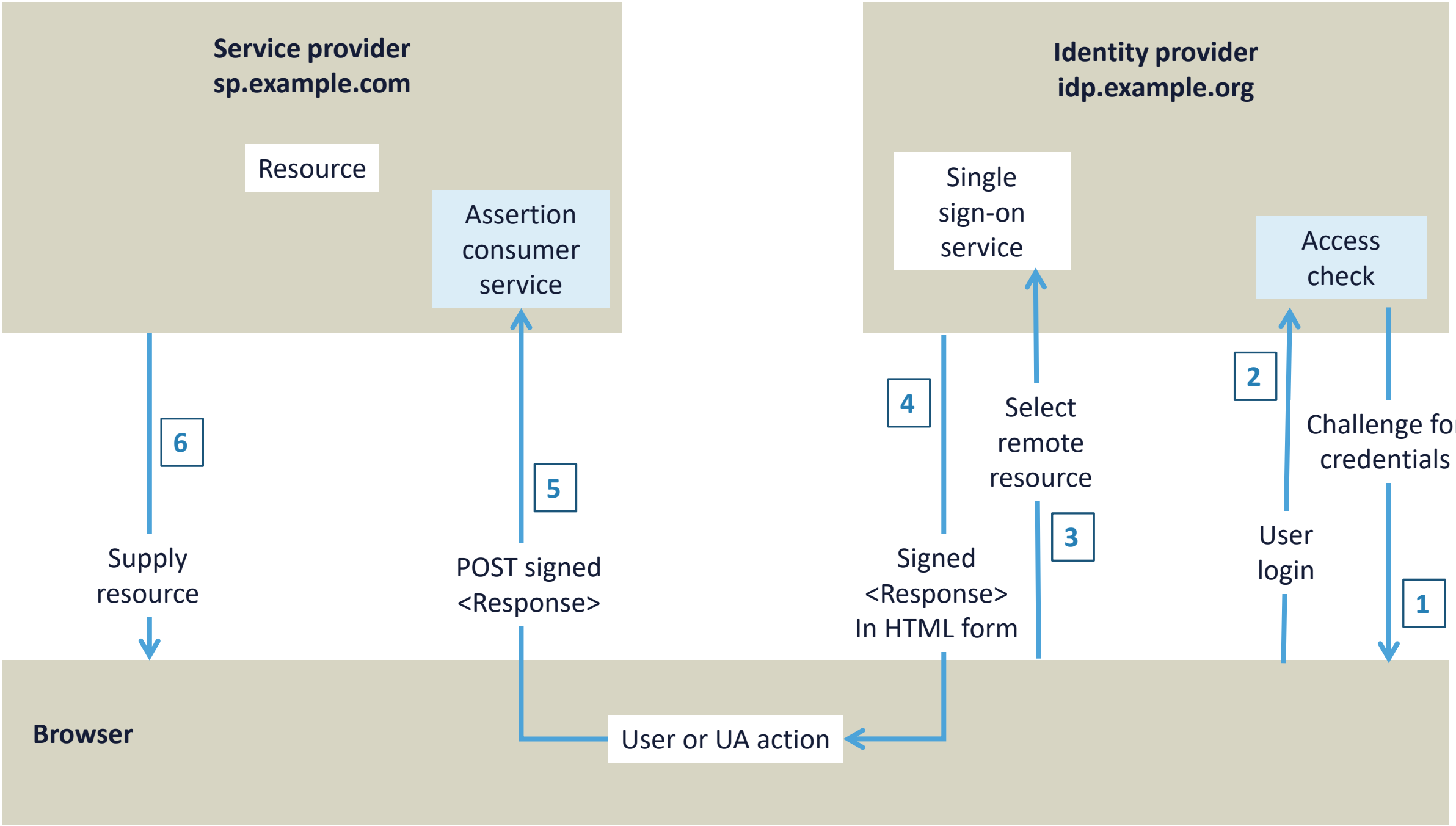
Federated Identity Providers

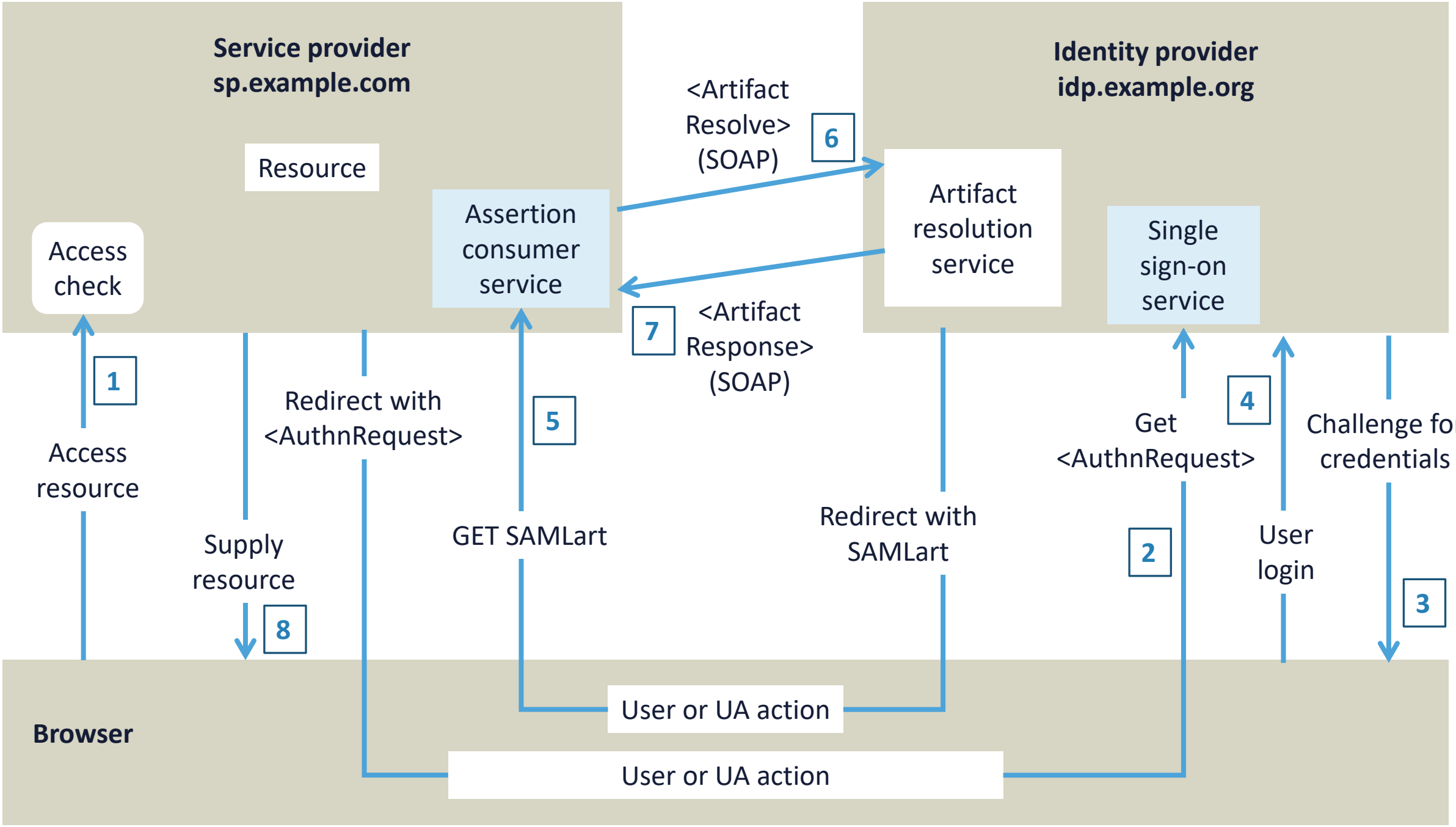



Client
A
Authorization request
Resource owner
B
Authorization grant
C
Authorization grant
Authorization server
D
Access token
E
Access token
Resource server
f
Protected resource

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


Service provider
sp.example.com
Resource
Assertion consumer service
Identity provider
idp.example.org
Single sign-on service
Access check
6
Supply resource
5
POST signed <Response>
4
Signed <Response> In HTML form
Select remote resource
3
2
User login
Challenge for credentials
1
Browser
User or UA action


Service provider
sp.example.com
Identity provider
idp.example.org
Resource
Access check
Assertion consumer service
Artifact resolution service
Single sign-on service
<Artifact Resolve> (SOAP)
6
<Artifact Response> (SOAP)
7
1
Access resource
Supply resource
8
Redirect with <AuthnRequest>
5
GET SAMLart
Redirect with SAMLart
Get <AuthnRequest>
2
4
User login
Challenge for credentials
3
Browser
User or UA action
User or UA action

OAUTH

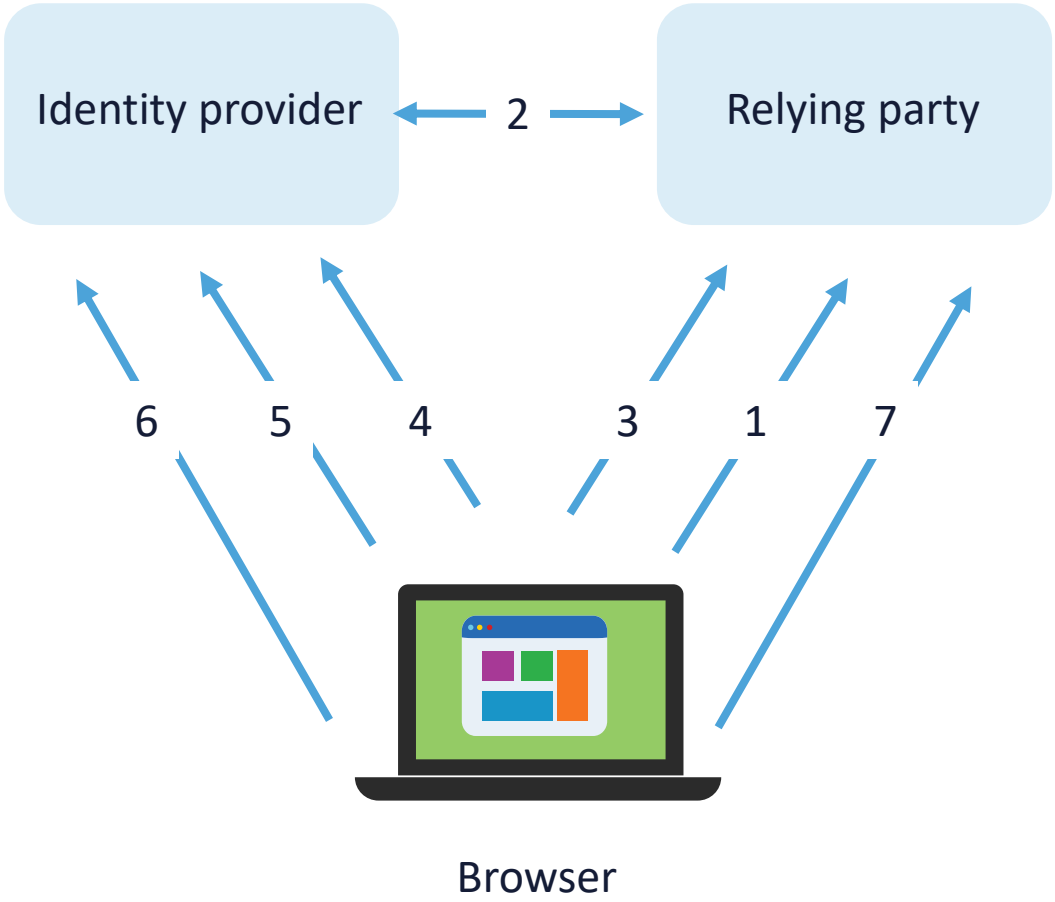
- **OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service**
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OpenID Connect (OIDC)

Should be used for OAUTH Authentication

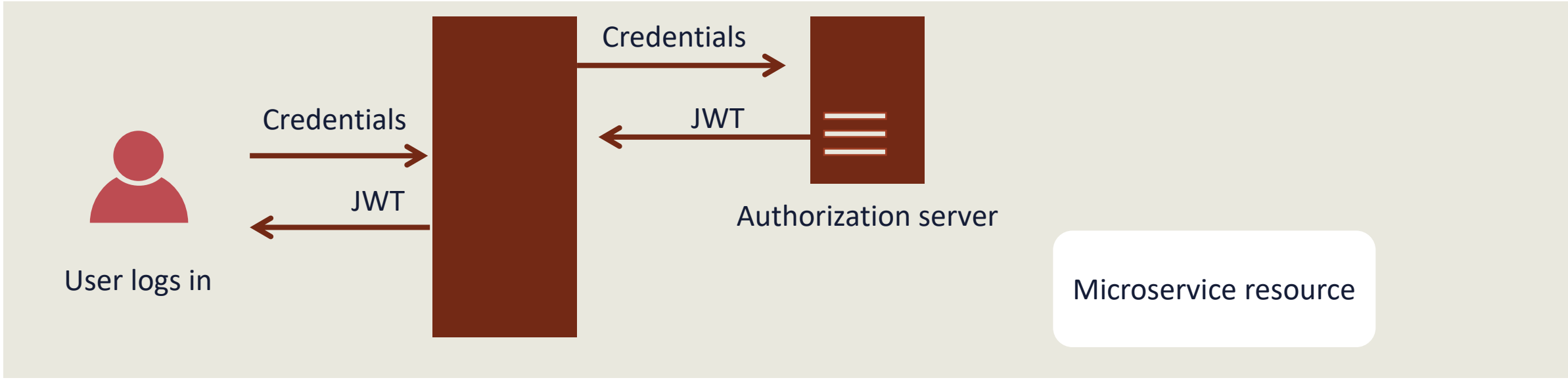
- **OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol**
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients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

Federated Access with OUATH/OIDC

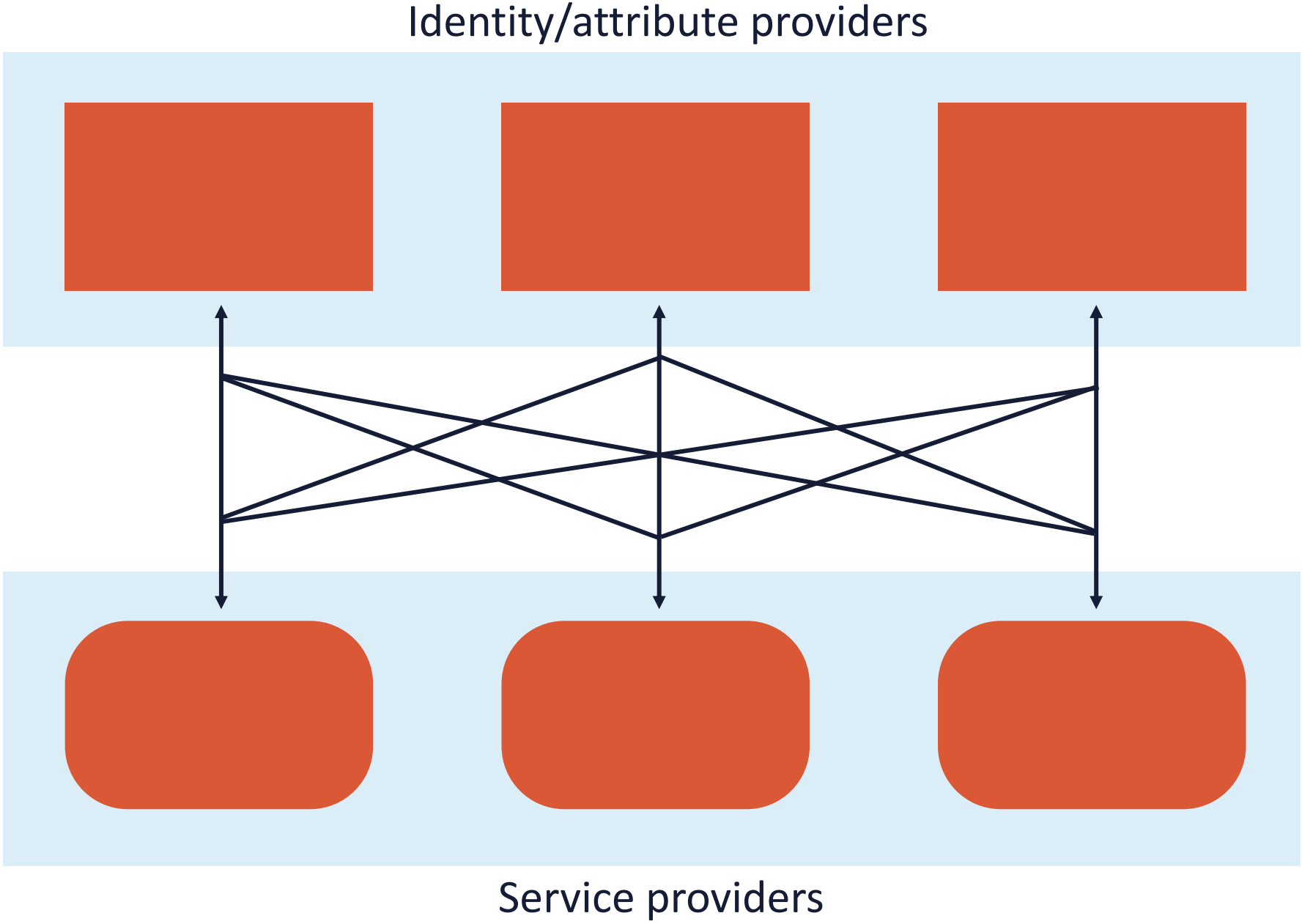


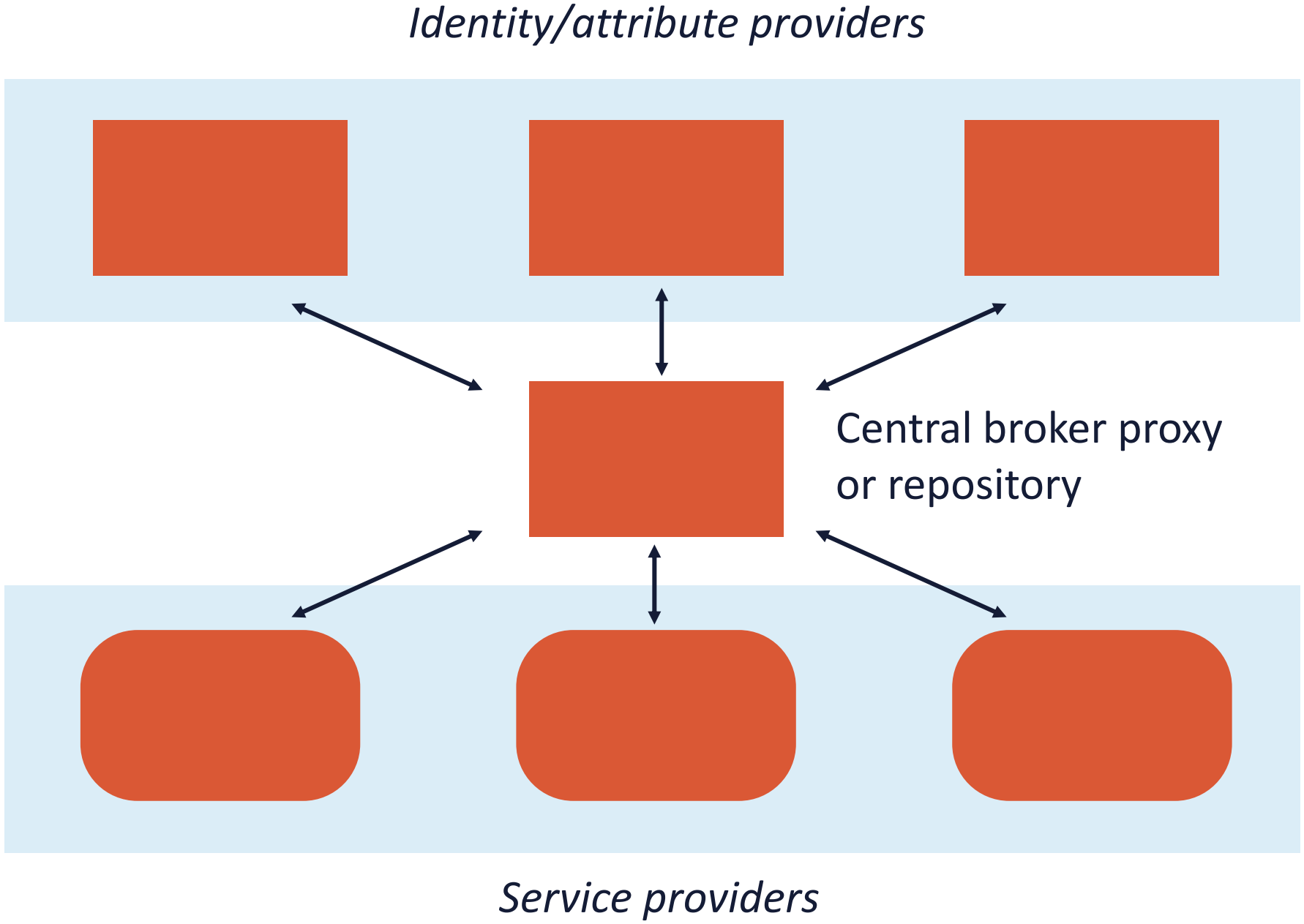
1. User sends their OpenID URL
2. IP and RP set shared secret
3. Browser redirected to ger token from provider
4. Request to IP for token for site
5. Login if needed
6. Token returned to browser
7. Token handed to requesting site

Step1: User logs in and receives JSON Web Token (JWT)

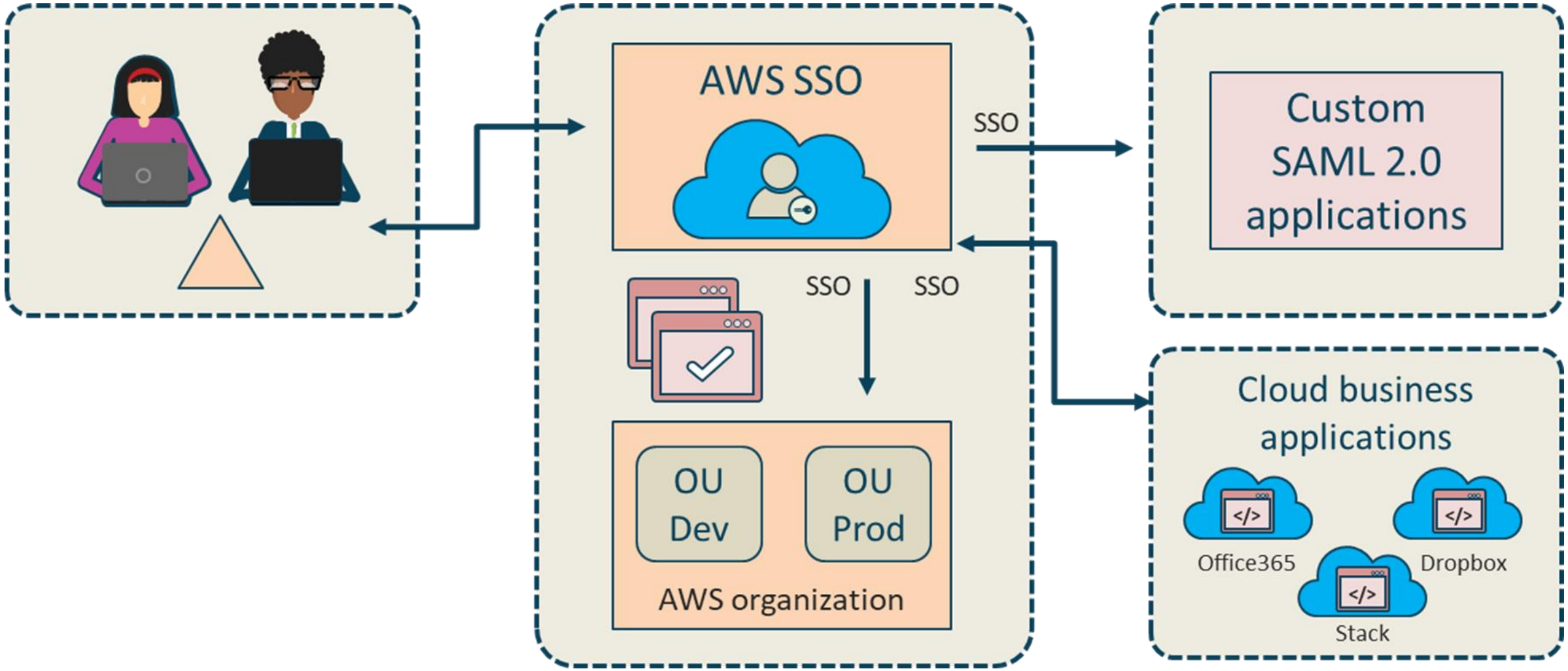


Step2: User requests access to resource with JSON web token (JWT)


Identity/attribute providers
Service providers


Identity/attribute providers
Central broker proxy
or repository
Service providers

AWS Identity Center (formerly SSO)



Step-Up Authentication

- Ensures that users can access some resources with one set of credentials but will prompt them for more credentials when they request more access
  - 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
  - Employees need occasional access to private data that would cause damage if exposed
  - You want to deploy a membership model that limits complete access to your site or service to paying users
- Facilitates easy access to one layer of resources and secure access to another layer of resources **(KBA)**

Cloud Access Security Brokers (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)

Cloud Access Security Brokers (CASB)

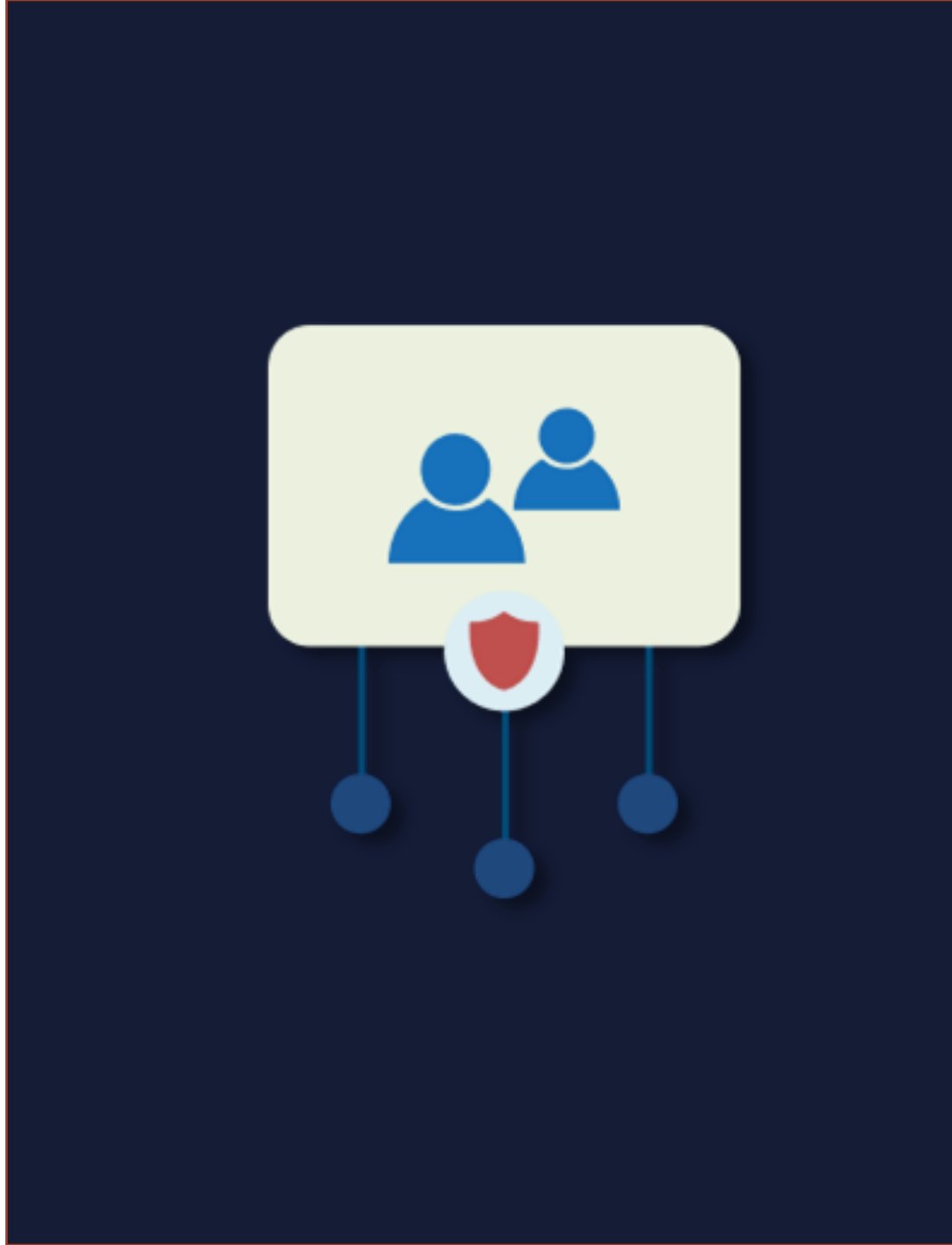
- The 4 Pillars of CASB are:
  - Visibility
  - Compliance
  - Data Security
  - Threat Protection
- The main CASB service offerings are:
  - Enabling and supporting SSO and federated access
  - Multi-SaaS and multi-cloud environments
  - Data loss prevention
  - Information rights management (IRM/DRM)
  - Helping with regulations and compliance

Managed Security Service Providers (MSSP)

- Managed security service providers (MSSP) primarily offer management and outsourced monitoring of systems and security devices
- An MSSP may also handle upgrades, system changes, and modification
- They can serve the role of a security operations center (SOC) for organizations with smaller budgets or lack of qualified personnel

Managed Security Service Providers (MSSP)

- A managed security service provider (MSSP) offers outsourced security monitoring and management for security systems and devices
- Common MSSP services:
  - Managed layer 3-7 firewalls
  - Intrusion detection and prevention (IDS/IPS)
  - Endpoint response and detection
  - Virtual private networking support
  - Vulnerability scanning and anti-viral services



Next-Generation Endpoint Protection

- **Superb example is Palo Alto Networks Cortex XDR**
- Machine-Learning Threat Detection
- User Behavioral Analysis (UBA)
- Incident Management and Host Insights
- Automated Root Cause Analysis
- Deep Forensics
- Next-Generation Antivirus

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
- Access to secrets uses fine-grained permissions and centralized API auditing
- **Service is supported by CSP HSM datacenter clusters**

Amazon GuardDuty

- Amazon GuardDuty is an industry collaborated threat detection service that continuously monitors for malicious or unauthorized activities to help protect accounts and workloads
- It has categories of “findings” that monitor for unusual or unauthorized internal and external behaviors
- GuardDuty also detects potentially compromised instances or reconnaissance by attackers
- It even performs machine-learning “pre-crime” activities to prevent zero days from Internet domains and IP addresses/prefixes

Big Data Cloud Solutions

The 3 “V’s” of Big Data

- **Volume**
  - With big data, you will have to process massive amounts of low-density, unstructured data
  - This can Twitter data feeds, web page clickstreams, mobile app data, or sensor-enabled IoT devices
  - For some enterprises, this might be tens of terabytes to hundreds of petabytes of data
  - CSP solutions might be Google BigQuery, Azure Big Data Analytics, or Amazon Redshift and EMR

Big Data Cloud Solutions

The 3 "V's" of Big Data

- **Velocity**
  - Velocity is the fast rate at which data is received and (often) acted on
  - Typically, the highest velocity of data streams directly into memory (Redis clusters or other serverless solutions) versus being written to disk
  - Some Internet-enabled smart products operate in real time or near real time and will require real-time evaluation and action

Big Data Cloud Solutions

The 3 “V’s” of Big Data

- **Variety**
  - Variety refers to the many types of data that are available
  - Traditional data types were structured and fit neatly in a relational database
  - With the rise of big data, data comes in new unstructured data type
  - Unstructured and semi-structured data types, such as text, audio, and video, require additional preprocessing to derive meaning and support metadata

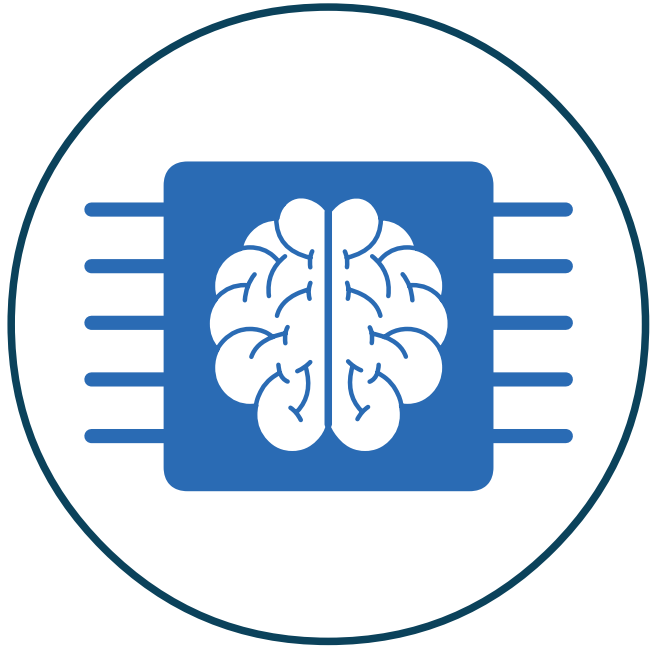
Data Science

- Data discovery and ingestion
- Data lake and data warehouse
- Data preprocessing
- Data analysis and business intelligence
- Machine learning training and serving
- Accountable Artificial Intelligence (AI)
- Orchestration

Machine Learning

Refers to programs and machines acquiring, processing, correlating, and interpreting information

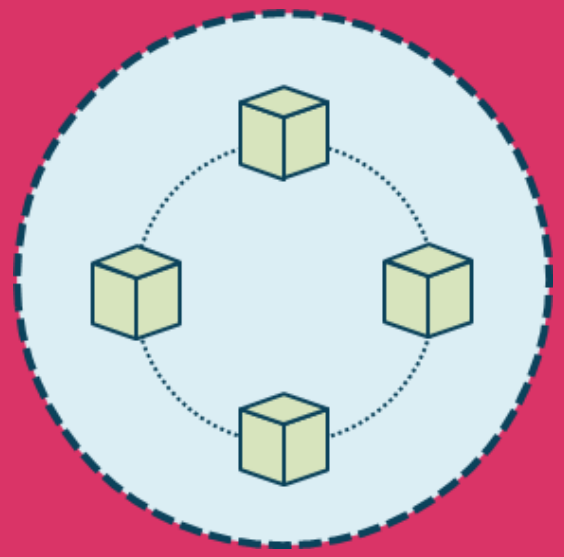
- The results of ML and AI are applied in a myriad number of ways without direct input from programmers or users
- There are a wide variety of cloud services that use machine learning algorithms and services:
  - Security automation
  - Language services
  - Intelligent contact centers and personalization
  - Intelligent search and document processing
  - Fraud detection
  - Media intelligence
  - Business forecasting



Artificial Intelligence (AI)

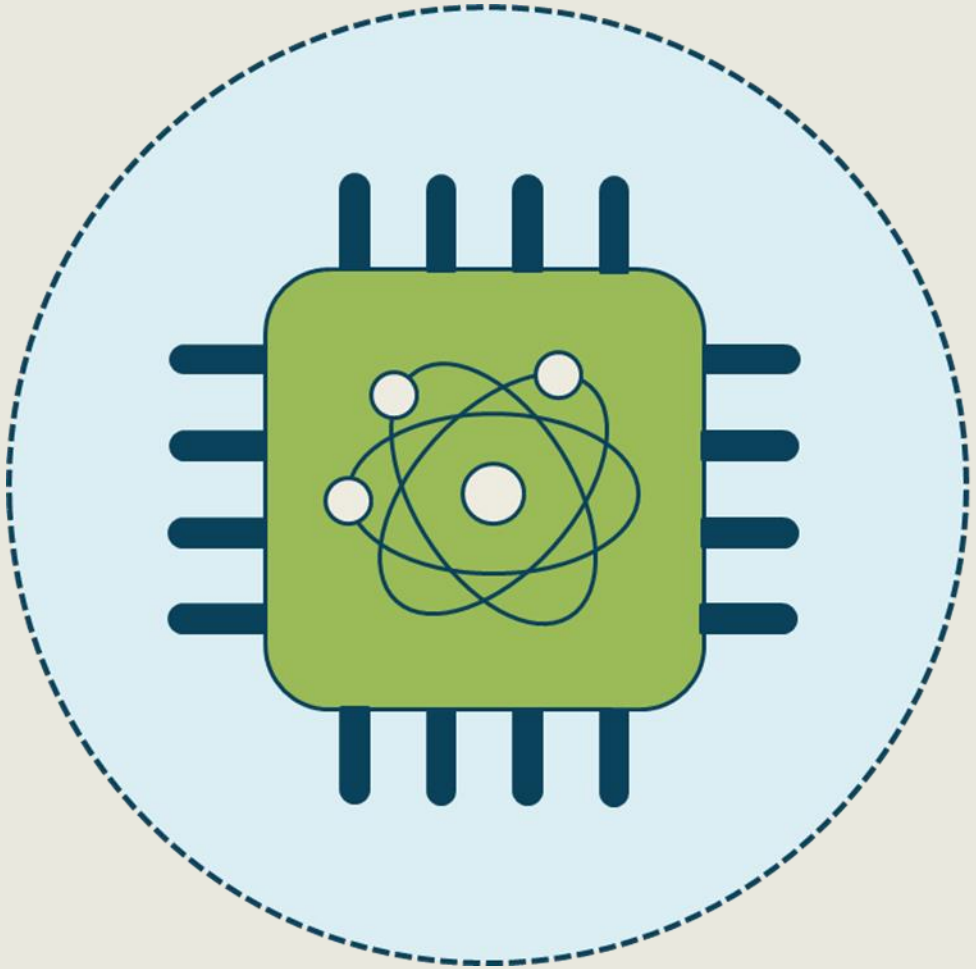
- The goal of Cloud AI is to create a virtual cloud space to emulate the human brain
- AI cloud delivers AI software-as-a-service offering enterprises access to AI tools and enabling them to harness AI capabilities
- AI can automate complex and repetitive tasks to boost productivity, as well as perform data analysis without any human intervention
- IT teams can also use AI to manage and monitor core workflows

Blockchain



- A public ledger consisting of a digital "chain of blocks" storing information
- Data can be read or write but not modified – changes must be made to a subsequent block in the chain
- Transaction data such as date, time, and amount is verified with a consensus mechanism (PoW, PoS, etc.)
- The transaction participants identities are based on digital signatures
- Unique cryptographic hashes are used to distinguish the blocks from each other
- These things must occur for a block to be added
  - A transaction must take place
  - The transaction must be verified (consensus)
  - That transaction must be stored in a block and given a hash

Quantum Computing



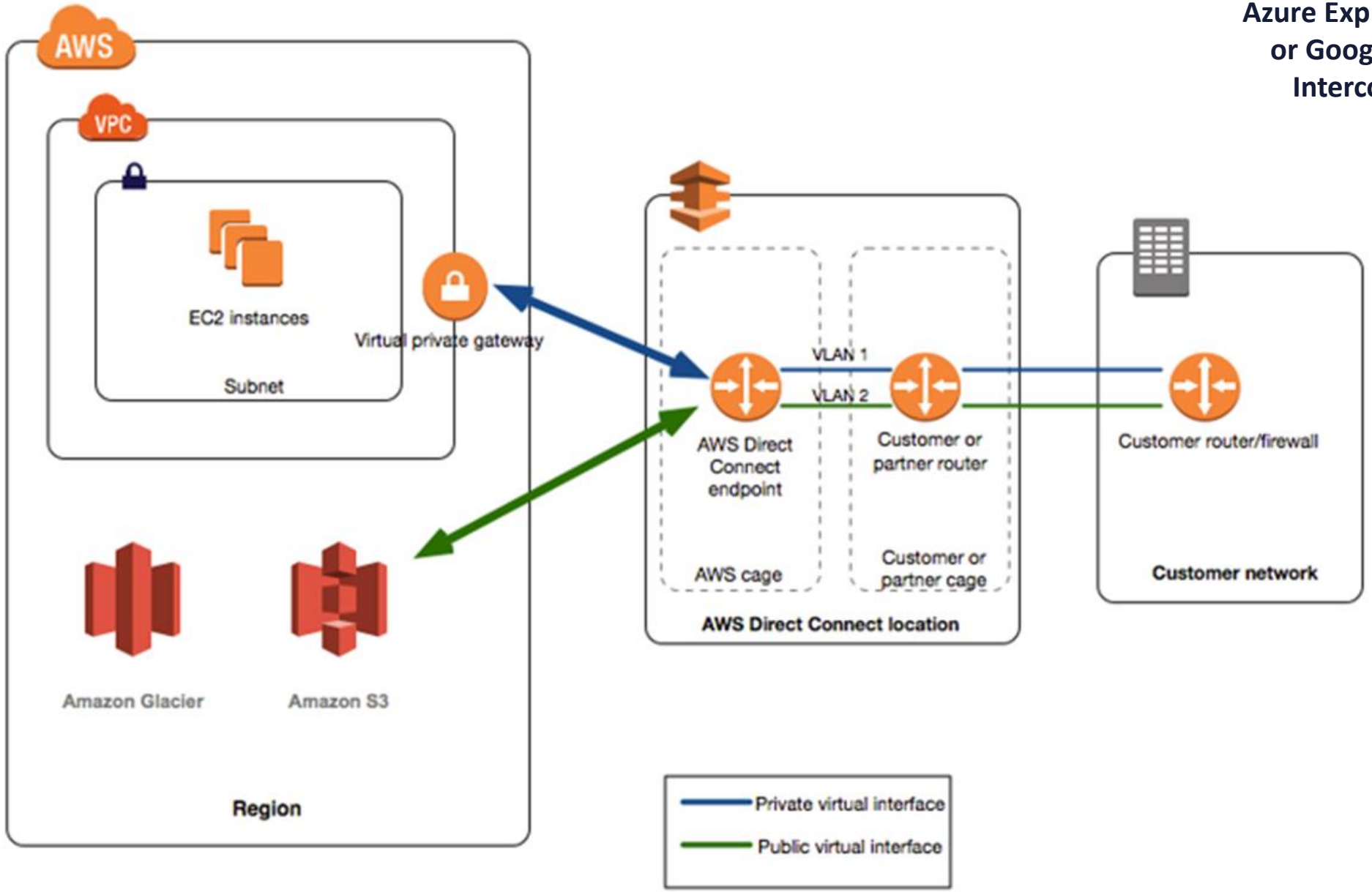
- Personal computers use bits (1s or 0s) whereas quantum computers use qubits
- These are typically subatomic particles like electrons or photons
- Quantum computing derives its power from the fact that qubits can represent numerous possible combinations of 1 and 0 at the same time
- This ability to simultaneously be in multiple states is called superposition

Edge Computing

- Edge computing is a distributed computing standard that brings compute services and data storage close to the site where it is needed to speed up response times and preserve bandwidth
- CDN solutions place cached versions of content (often in elastic Redis in-memory storage clusters) at metro area edge locations
- Security is a shared responsibility model between customers, ISPs, and CDN providers
- **Edge computing can also be characterized by using direct solutions like AWS Direct Connect, Azure ExpressRoute, and Google Interconnect**

Edge Computing

AWS Direct Connect, Azure ExpressRoute, or Google Cloud Interconnect



Confidential Computing

- Confidential Computing is a Private Cloud built within a Public Cloud Infrastructure
- Applications, data, and workloads within a Confidential Cloud deployment are protected by a blend of hardware-grade encryption, memory isolation, and other services that assure workload, data, and platform integrity
- Confidential Clouds are typically created on-demand at runtime and the workloads and data function completely masked from insiders, bad actors, and malicious processes
- All aspects of a workload are secure even in the event of a physical host breach

Internet of Things

- The explosion of Internet of Things (IoT) and Internet of Everything (IoE) presents a challenge for embedding computing vulnerability discovery
- Systems are often powered by specialized chips or system-on-a-chip (Arduino, Raspberry Pi) as well as some older unpatched version of Linux or Microsoft Windows
  - Sensors and smart devices
  - Smart vehicles and drones
  - Robotics
  - Facility automation and controllers
  - Commercial appliances and medical devices
  - HVAC, security, and environmental systems

OWASP IoT Top Ten Vulnerabilities

1. Weak, guessable, or hardcoded passwords
2. Insecure network services
3. Insecure ecosystem interfaces
4. Lack of secure update mechanisms
5. Use of insecure or outdated components
6. Insufficient privacy protection
7. Insecure data transfer and storage
8. Lack of device management
9. Insecure default settings
10. Lack of physical hardening

Enterprise Mobility Management

Initiatives must consider cloud access

- Organizations must securely configure mobile hardware, firmware, O/S, management agents, and the apps used for business
- Solutions should reduce risk, so employees are able to access the necessary data from nearly any location, **including cloud access**, using a wide variety of mobile devices
- EMM may be a combination of mobile device management (MDM) and mobile application management (MAM)
- **CSPs now offer 5G Gateways as PaaS**

Related Technology Considerations

- **Ephemeral Computing**
  - Ephemeral computing is the process of creating a virtual computing environment on an ad-hoc temporary basis and then disposing of the environment when necessary or the resources are no longer in demand
  - The consumer only pays for what is used
  - Examples would be functions-as-a-service with AWS Lambda and Azure Functions

- **Serverless Technology**
  - Functions are a form of serverless technology
  - These are technologies for running code, managing data, and integrating applications, all without managing Windows, Linux, and MacOS servers
  - Serverless technologies feature automatic scaling, built-in high availability, and a pay-for-use billing model to increase agility and optimize costs

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

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, eDiscovery, & cloud forensics (SEF)
- Supply chain management, transparency, and accountability (STA)
- Threat & vulnerability management

Download the CCM Bundle

- For this open book CCSK exam be sure to download the CCM bundle which includes the matrix and questionnaire Excel spreadsheets
- Have them open while taking the exam
- Practice quickly searching based on keywords
- Go to:

https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

The European Union Agency for Cybersecurity

ENISA

- ENISA, is the EU's agency committed to attaining a high collective level of cybersecurity across Europe
- It was created in 2004 and strengthened by the EU Cybersecurity Act
- The goals of ENISA are as follows:
  - Contribute to EU cyber policy
  - Improve the trustworthiness of information and communications technology (ICT) products, services and processes with cybersecurity certification schemes
  - Cooperate with Member States and EU bodies
  - Assist Europe to prepare for future and emerging cyber challenges

ENISA Offerings

- Empowering communities
- Cybersecurity policy
- Operational cooperation
- Capacity building
- Trusted solutions
- Foresight and Knowledge

https://www.enisa.europa.eu/media/news-items/cloud-computing-speech

https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment

ENISA Vulnerabilities with Loss of Governance

- Unclear roles and responsibilities (weak enforcement of role definition)
- Problems synching contractual obligations or responsibilities that are external to the cloud deployment
- Conflicts between SLA clause promises are responsibilities with different stakeholders
- Audits or certifications that are not available or accessible to customers
- Hidden dependencies when creating cross-cloud or multi-cloud deployments
- Lack of standard technologies and solutions

ENISA Vulnerabilities with Loss of Governance

- Storing data in multiple regions and jurisdictions with a lack of transparency and visibility
- Lack of protection from provider going out of business by not having source escrow agreements (vendor-lock-out)
- No control over the vulnerability assessment or penetration testing processes
- The certification schemes are not aligned or adapted to cloud computing infrastructure
- Lack of information on other jurisdictions
- Lack of completeness and transparency in terms of use
- Vague asset ownership