Welcome Back to CISSP Day 2

Michael J. Shannon

Class will begin at 10:00 am Central Standard Time

ASSET CLASSIFICATION, HANDLING, AND PROVISIONING

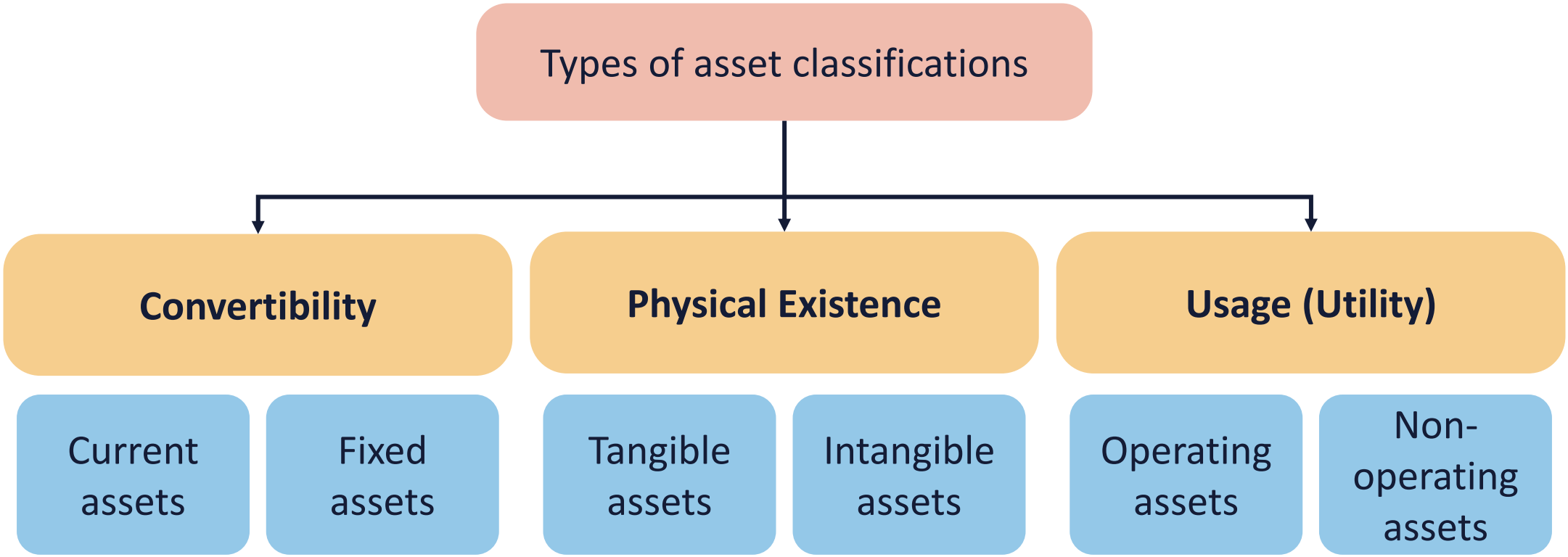
Objectives

- Examine asset classification
- Explore data classification
- Know about information and asset handling requirements
- Learn about secure provisioning of information and assets
- Examine information and asset ownership
- Explore asset inventory and management

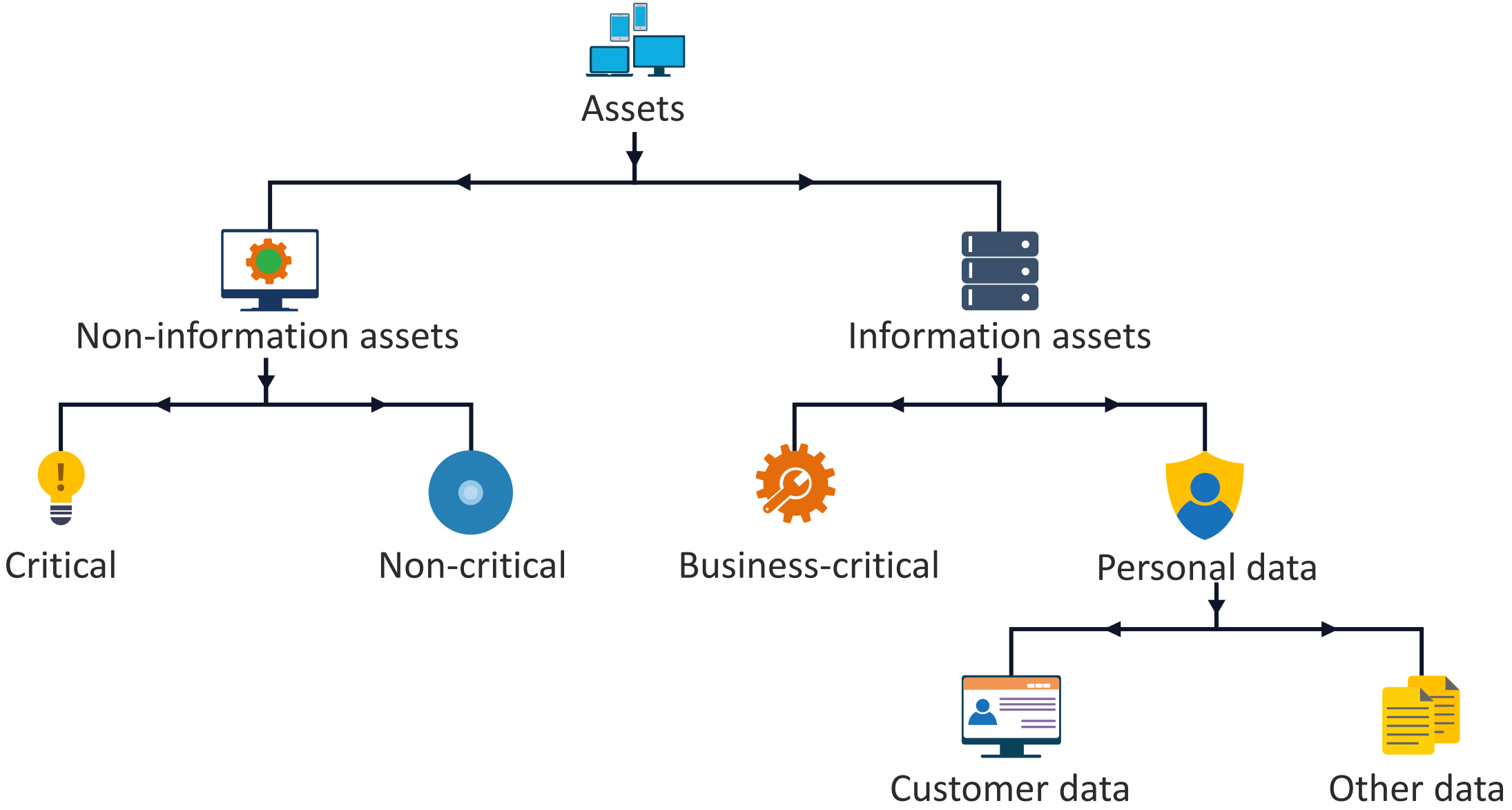
ASSET CLASSIFICATION

- The International Financial Reporting Standards (IFRS) framework defines an asset as: "A resource controlled by the enterprise as a result of past events and from which future economic benefits are expected to flow to the enterprise."
- Assets generally have three main attributes:
  - **Ownership**: Assets signify possessions that can be ultimately converted into cash and/or cash equivalents
  - **Economic value**: Assets have monetary worth and can be exchanged or sold
  - **Resource**: Assets are possessions that can be leveraged to produce future economic remunerations

TYPES OF ASSETS



TYPES OF ASSETS



EXAMPLES OF INTANGIBLE ASSETS

- Goodwill
- Brand
- Trademarks
- Licenses and permits
- Franchises
- Patents
- Copyrights
- Trade secrets
- Corporate intellectual property
- Domain names

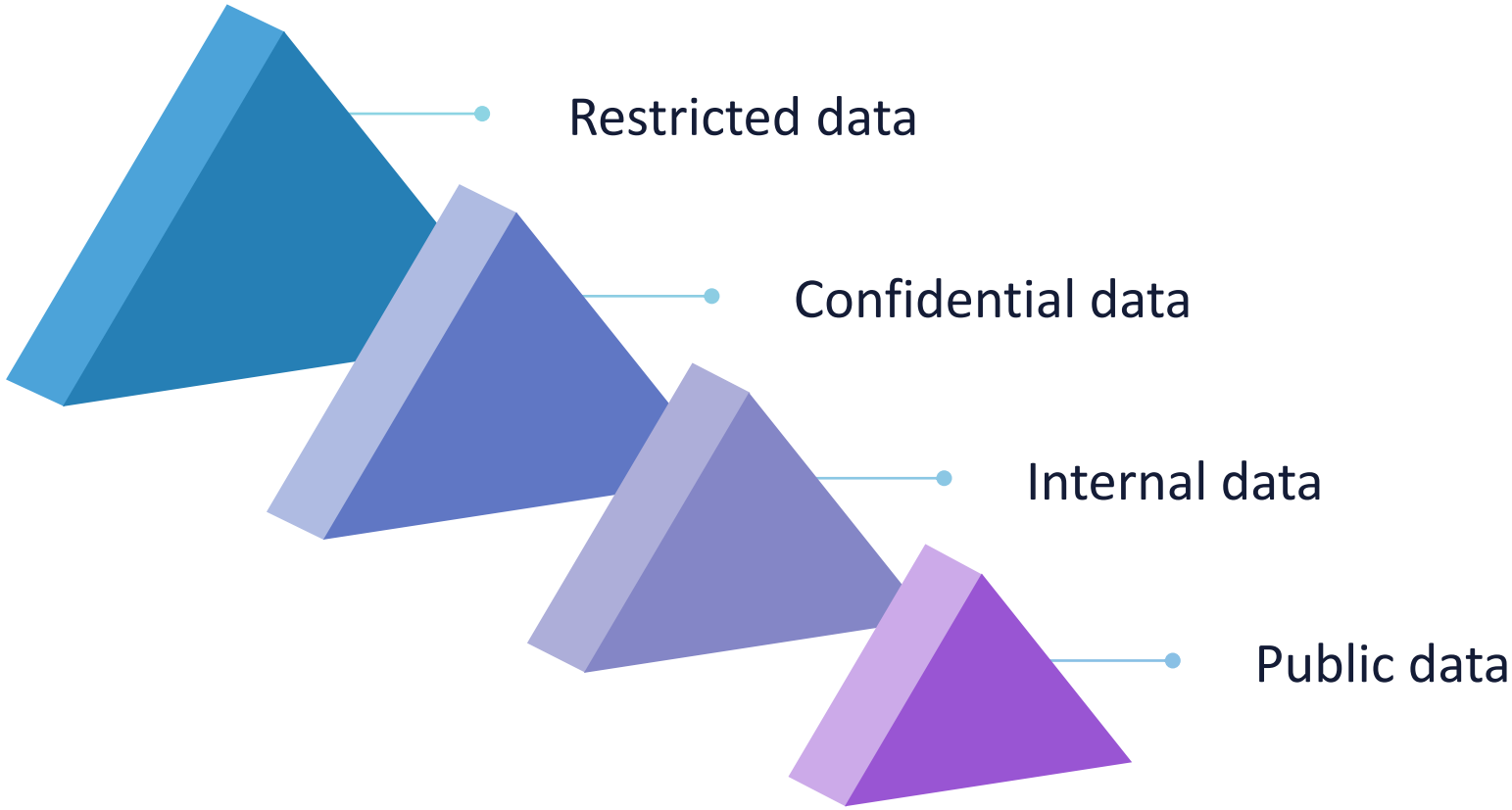
DATA CLASSIFICATION

- All organizations that desire to reach a higher level of maturity capability must employ a practical and accurate data classification initiative
- Data classification can be defined as a process of labeling and categorizing all data assets of the given organization
- It should be based on qualitative and/or quantitative values that consider data sensitivity and risk from a potential unauthorized disclosure

DATA CLASSIFICATION

- Classifying data will also endeavor to identify the probability (likelihood) and impact (magnitude) of a particular incident based on:
  - The type of data
  - The level of access to this data
- These two components, along with the possible business impact, will effectually define the most appropriate response and security controls based on risk treatment

COMMERCIAL DATA CLASSIFICATIONS



RESTRICTED DATA

- Restricted data and information is highly sensitive, and its use should be allowed only on a need-to-know basis
  - This will involve least privilege, separation of duties, and zero trust initiatives
- This category of data is initially protected with a non-disclosure agreement (NDA) as an administrative control to minimize legal risk
  - Restricted information includes trade secrets, personally identifiable information (PII), credit cards, or health information
- **Unauthorized disclosure would have a major financial or legal impact on the enterprise**

CONFIDENTIAL DATA

- Confidential information is team-wide, and its use should be contained within the business
- This information can include purchase costs of products and services in development, marketing materials, contracts, and agreements
- If divulged, confidential information **could negatively affect** the business and, eventually, the brand or corporate goodwill

INTERNAL DATA

- Internal information is organization-wide and only needs to be protected with limited physical, technical, and managerial controls
- Internal information may include the employee handbook, various policies, company-wide memos, organizational charts, etc.
- **If disclosed, internal information has a minimal impact on the business**

PUBLIC DATA

- Public data for public consumption
- It is typically openly shared on the organization's website and discussed in the local, regional, and/or global community
- Public information and does not require any additional controls other than measures to prevent website defacing or denial-of-service (DoS)

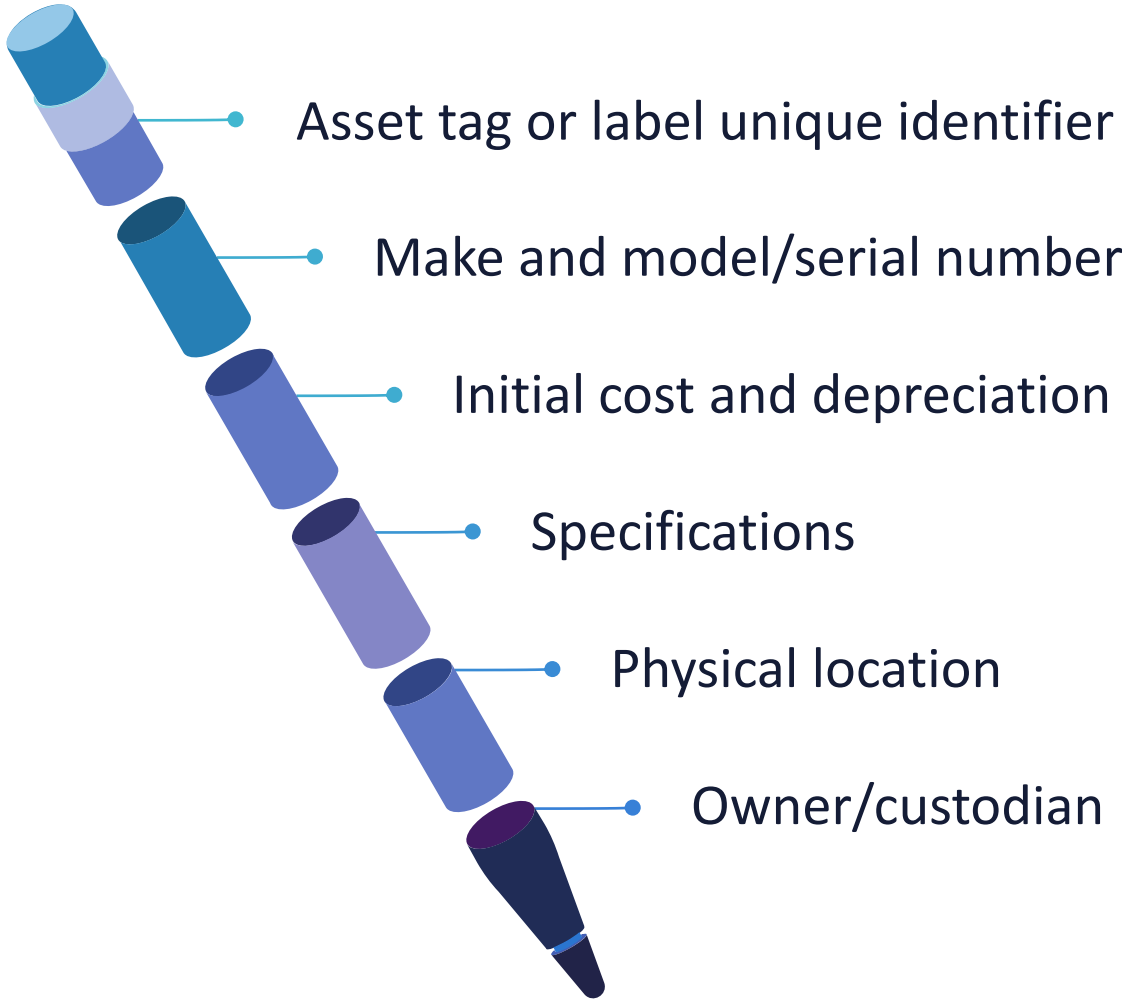
DEPARTMENT OF DEFENSE (DOD) SECURITY CLEARANCES

- **Top Secret**
  - Data or information that, if disclosed in an unauthorized manner, could realistically be likely to cause exceptionally severe damage to the national security
- **Secret**
  - Data or information that, if disclosed in an unauthorized manner, could realistically be likely to cause serious damage to the national security
- **Confidential**
  - Data or information that, if disclosed in an unauthorized manner, could realistically be likely to cause harm to the national security

INFORMATION AND ASSET HANDLING REQUIREMENTS

- The first requirement for handling information and assets is taking a complete inventory of all hardware components in use and stored as "hot spares"
- This includes servers, workstations, endpoints, infrastructure devices such as switches and routers, and any other physical appliances and modular components that are deployed or deployable
  - Remember wireless devices and multifunction appliances

Asset Database Requirements



TAGGING AND LABELING ASSETS

- Physical assets should have an asset tag affixed to the device whenever feasible
  - Unique database number or alphanumeric
  - Universal Product Code (UPC)
  - Quick Response codes (QR)
  - Radio Frequency Identification (RFID) or Near Filed Communication (NFC) tags
- Software applications should be labeled by usage, version number, license information, and the number of users
  - This data is typically stored in a configuration management database (CMDB)
- Cloud computing uses key/value pair tags

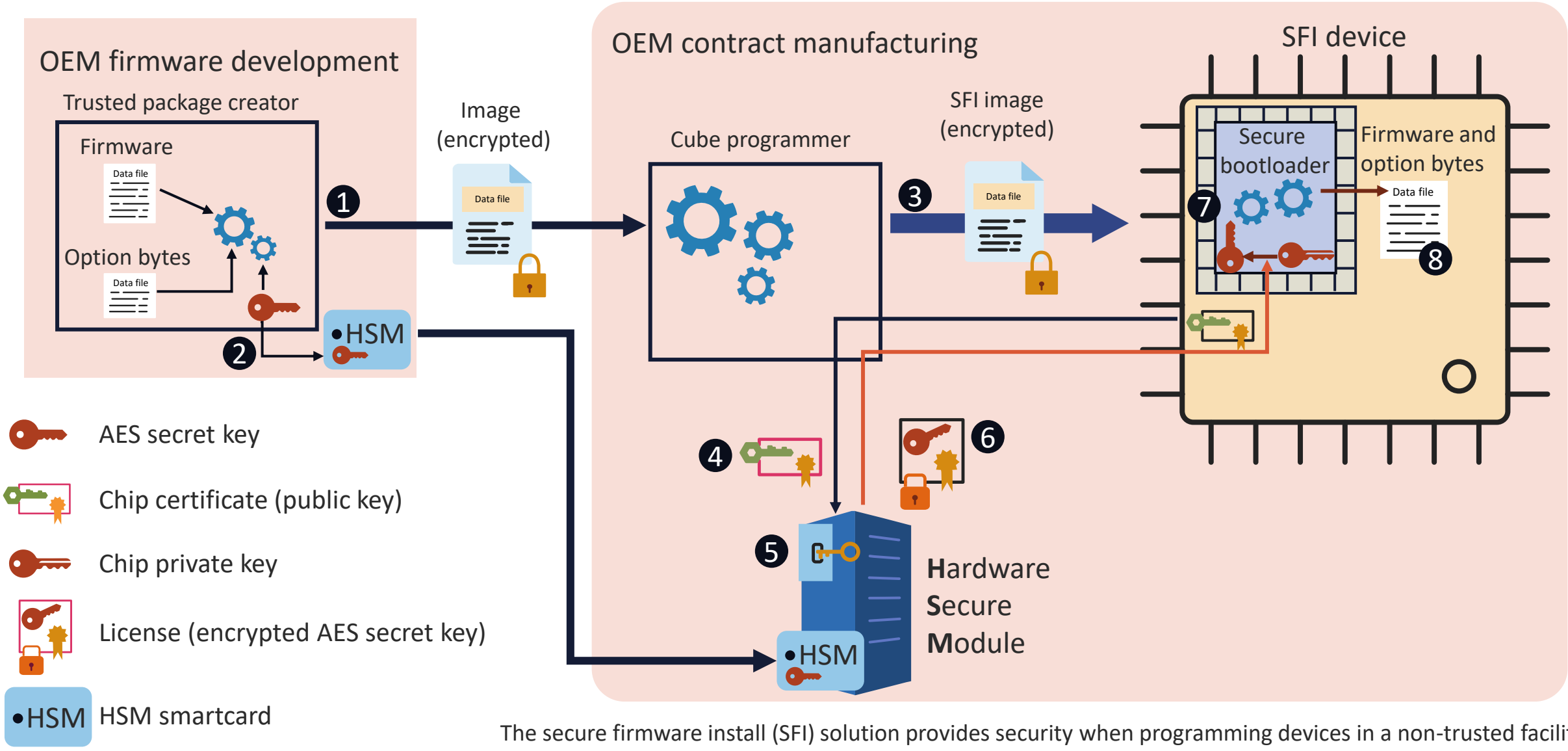
SECURE PROVISIONING OF INFORMATION AND ASSETS

- Secure asset provisioning involves a collection of dedicated toolkits and processes that support critical and valuable data such as licenses, passwords, keys, device IDs, certificates, configuration settings, and more
- These assets must be securely automated and programmed into devices during manufacturing and distribution

SECURE PROVISIONING OF INFORMATION AND ASSETS

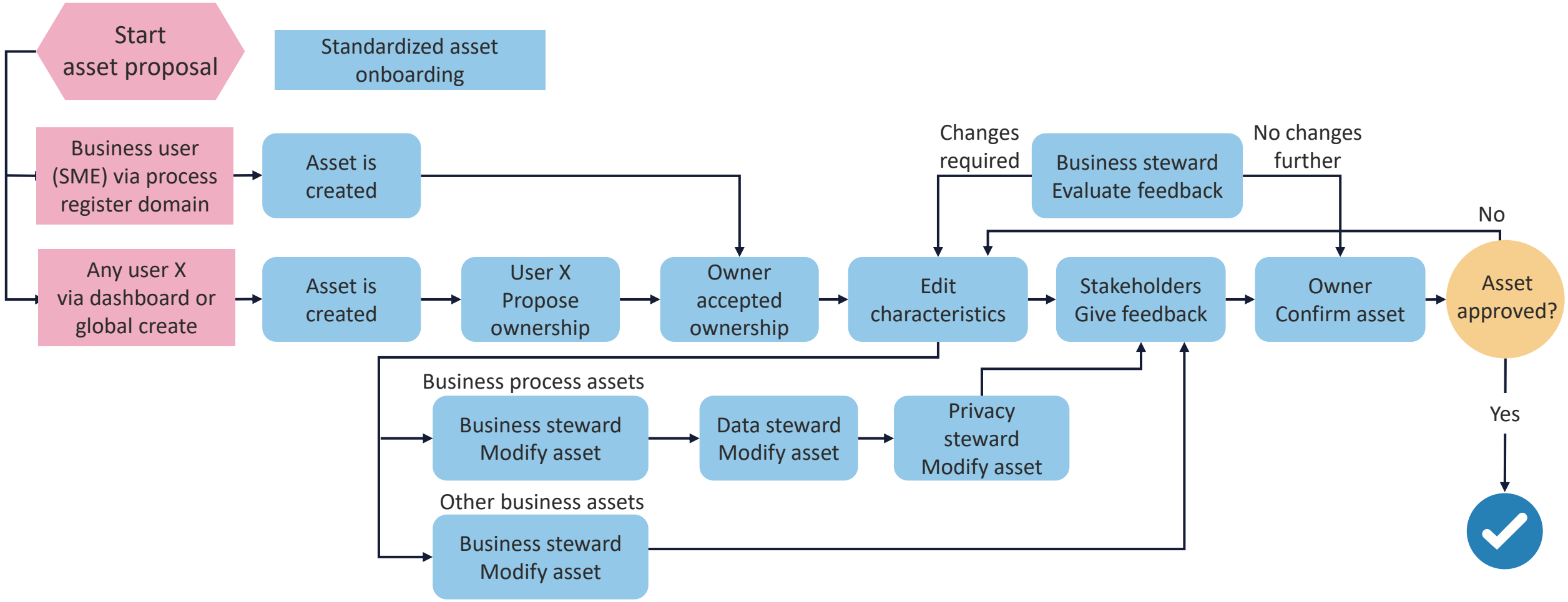
- Secure device manufacturing also involves employing digital trust assets during production for confidentiality and authentication during the operational phases
- Keys, certificates, and database secrets must be protected as soon as they are generated until integrated into each device

SECURE HARDWARE PROVISIONING



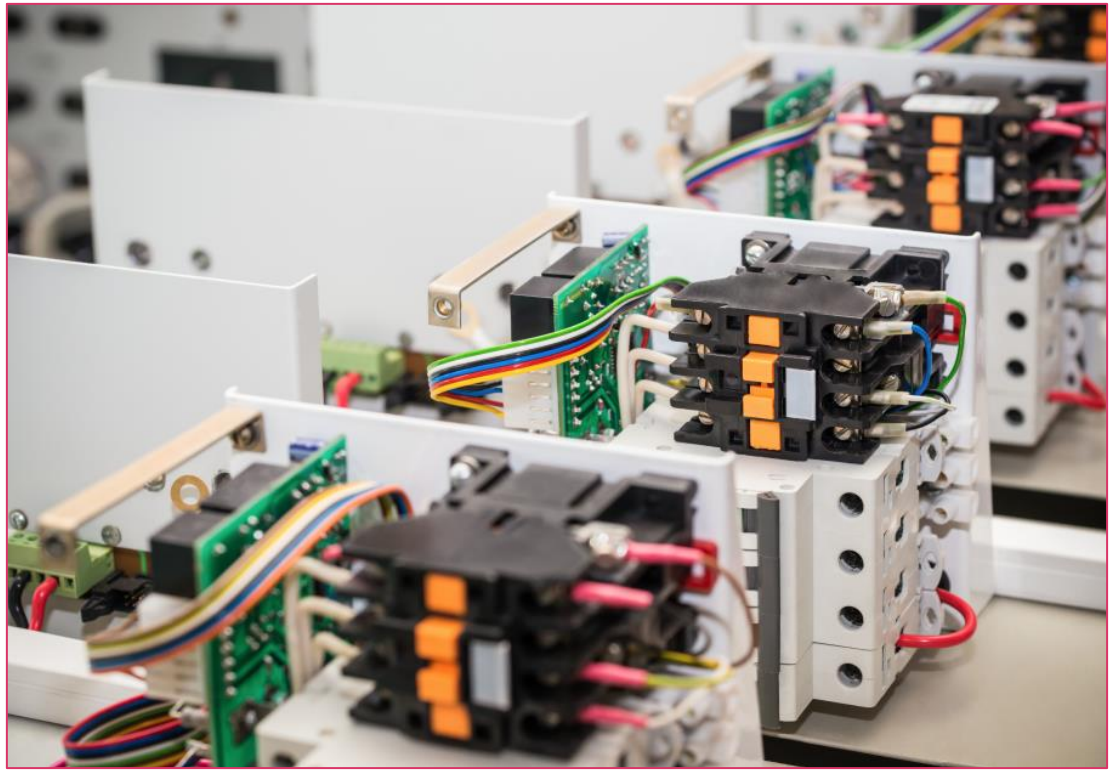
The secure firmware install (SFI) solution provides security when programming devices in a non-trusted facility

ASSET PROVISIONING LIFECYCLE



PHYSICAL ASSET OWNERSHIP

- In some business and organizational environments, employees and even contractors can be the "owners" of physical assets
- The use cases can include:
  - Enterprise mobility management (EMM) environments that use "bring your own device" (BYOD)
  - Some employees who experience a mass layoff may be allowed to keep certain assets from while they were previously stewards or custodians
  - Long-term employees who are retiring may be rewarded or gifted by retaining ownership of devices or even company vehicles as a package



ASSETS THAT MAY BE EMPLOYEE OWNED

- Cell phones
- Laptop computers
- Vehicles
- Recording equipment
- Pads and specialty assistants
- Workstations
- Printers and multifunction devices
- Headphones and monitors

TANGIBLE ASSET INVENTORY

- Tangible assets inventory is the measurement of the economic resources that have physical substance and are used in the production of goods
- Tangible assets can be either short-term or long-term, depending on how quickly they are consumed or depreciated
- Examples of tangible assets inventory include raw materials, goods in process, and finished products

Google BeyondCorp Asset Inventory

Information	Description
Serial number	Serial number of the device
Import date	Date the device was imported into your admin console
Type	Device type (e.g., Android)
Asset tag	Asset tag or ID that’s assigned to the device
Status	Whether the device is assigned to a user; possible values: assigned, unassigned A device is assigned when a user adds their corporate account to the device. To see who a device is assigned to, click the device. For company-owned Chrome devices to be assigned, the device must be enrolled in Chrome Enterprise. Devices that are only under fundamental management always appear as unassigned, even if a user signs in to the device. To see who is using the device, open the list of laptop and desktop devices and search for devices that are under fundamental management.

INTANGIBLE ASSET INVENTORY

- The Merriam-Webster dictionary defines intangible as something that is "not capable of being touched or not having physical substance"
- Intangible assets are simply possessions that have value but no physical substance
- For example, one of most organization’s most cherished intangibles are things like name recognition, reputation, and corporate goodwill

PLACING VALUE ON INTANGIBLES

1. **Price approach** – estimating the amount of money that would be needed to replace the intangible asset

2. **Marketplace approach** – comparing the intangible assets owned to those owned and recently sold by comparable entities

3. **Revenue approach** – converting any expected monetary remunerations that will be gained from the asset to a set amount that can be logged on a balance sheet

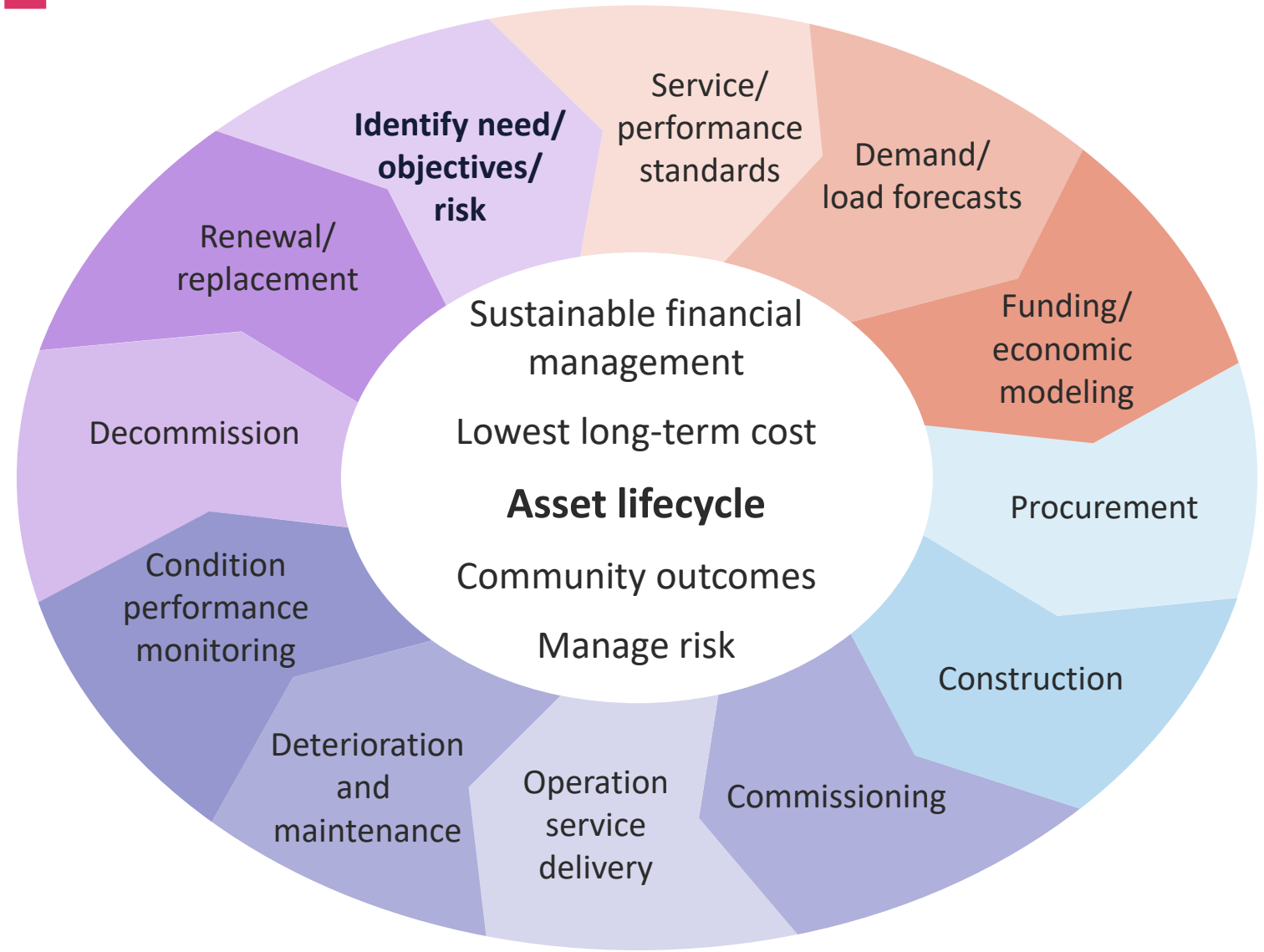
ASSET MANAGEMENT

- According to the International Organization for Standardization (ISO), asset management is the "systematic and coordinated activities and practices through which an organization optimally and sustainably controls its assets and asset systems"
- "It includes their associated performance and risks and expenditures over their life cycles for the purpose of achieving a defined strategic plan"

ASSET MANAGEMENT

- "It is the overall long-term plan for the organization that is derived from, and embodies, its vision, mission, values, business policies, stakeholder requirements, objectives, and the management of its risks"
- "Effective implementation of asset management requires a disciplined approach which enables an organization to maximize value and deliver its strategic objectives through managing its assets over their whole life cycles"

EXAMPLE: SERVICENOW ASSET MANAGEMENT LIFECYCLE



DATA LIFECYCLE, CONTROLS, AND COMPLIANCE

Objectives

- Examine data roles and states
- Explore the data lifecycle
- Compare data scoping and tailoring
- Learn about data standards selection
- Examine data protection methods

DATA STATES

Data at rest

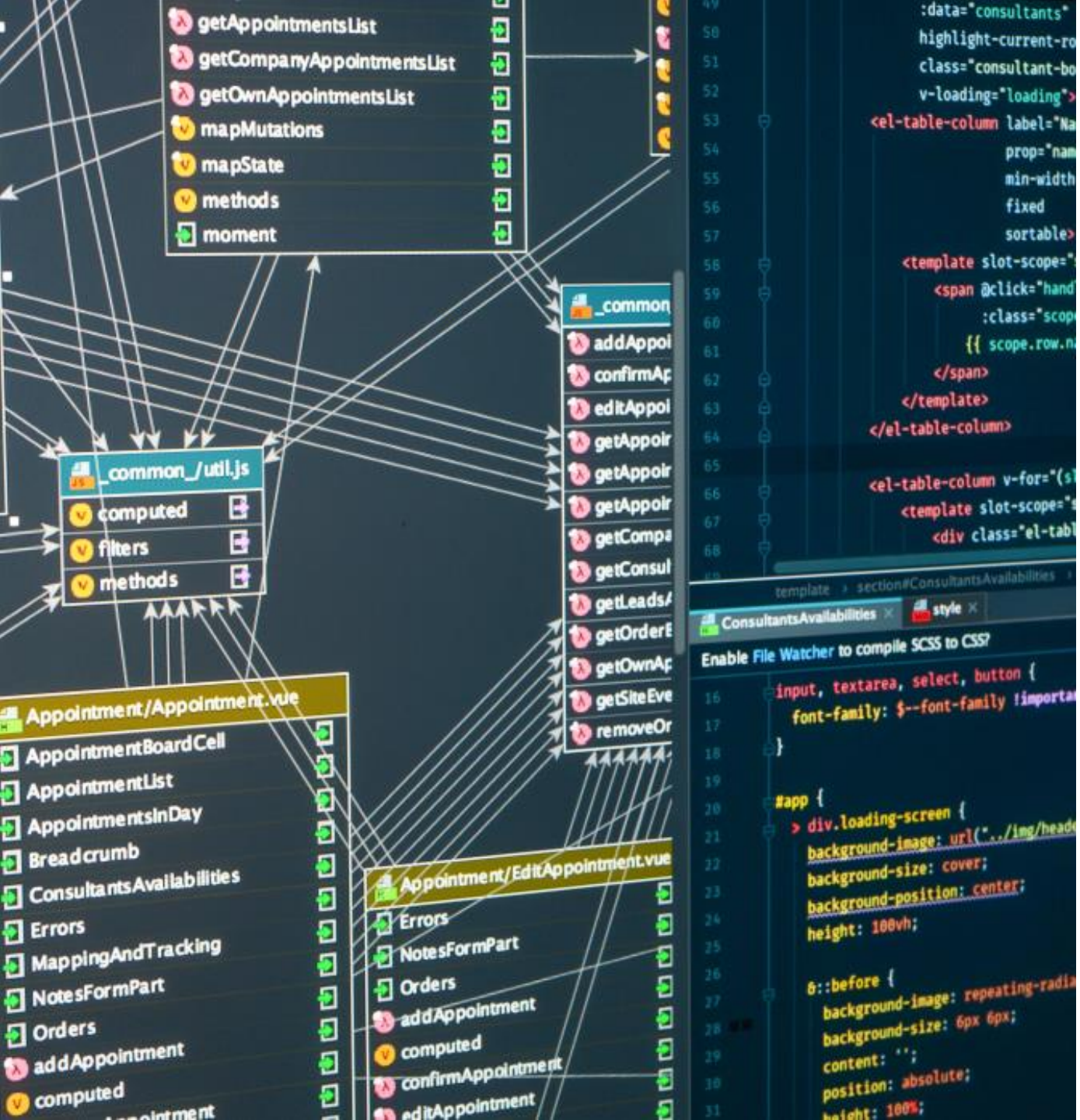
File, object, volume (block) data on drives, arrays, databases, and memory cards

Data in transit

Data moving across wired, wireless, PAN, cellular, and satellite networks

Data in use

Data that is volatile in CPU registers, RAM memory, swap files, caches, Redis Clusters, etc.



DATA OWNER ACTIVITIES

- Compiling and approving data glossaries, schema, and definition sets
- Managing functions that are relevant to data quality and accuracy
- Certifying information used inside and outside of the organization
- Appraising and approving a master data management (MDM) strategy, tactics, and activities
- Working with other data owners to resolve issues and misconfigurations throughout business functions

DATA CUSTODIANS

- In some areas, the data custodian is referred to as a "controller"
- A data custodian is often responsible for developing and maintaining technical and security controls for certain data collections
  - They ensure confidentiality, integrity, authenticity, and availability of data and assets
- The goal is to support and fulfill the data governance framework standards established by the data owner and officers

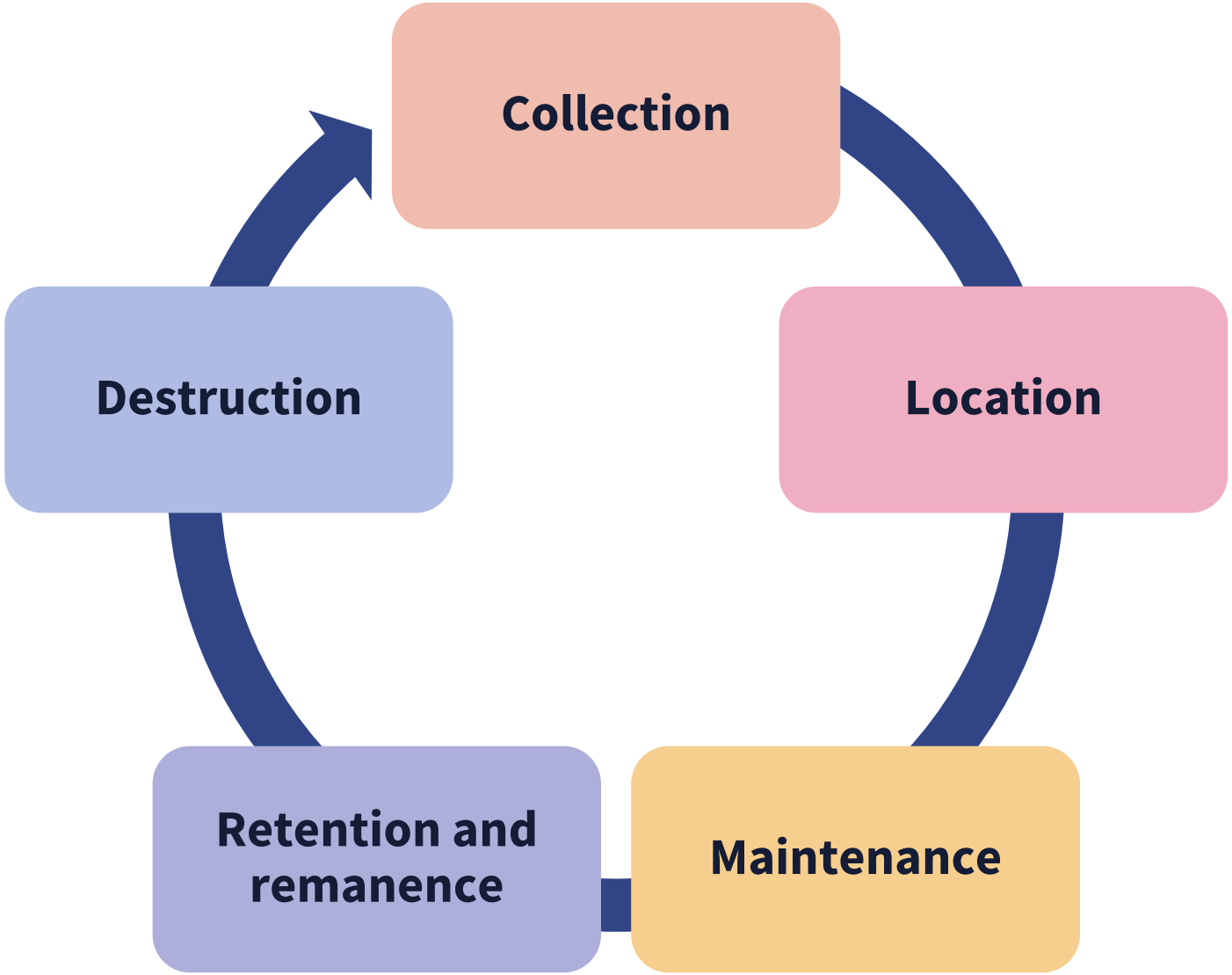
DATA STEWARDS

- The primary difference between a data owner and a data steward is that the data steward manages the quality of the defined datasets daily and is more customer-focused (internal and/or external)
- Data stewards are subject matter experts (SMEs) who understand and can describe the importance of the information and its regular use
- A data steward regularly teams up with other stewards within an organization for various projects and programs in a "data steward council"

DATA USERS AND PROCESSORS

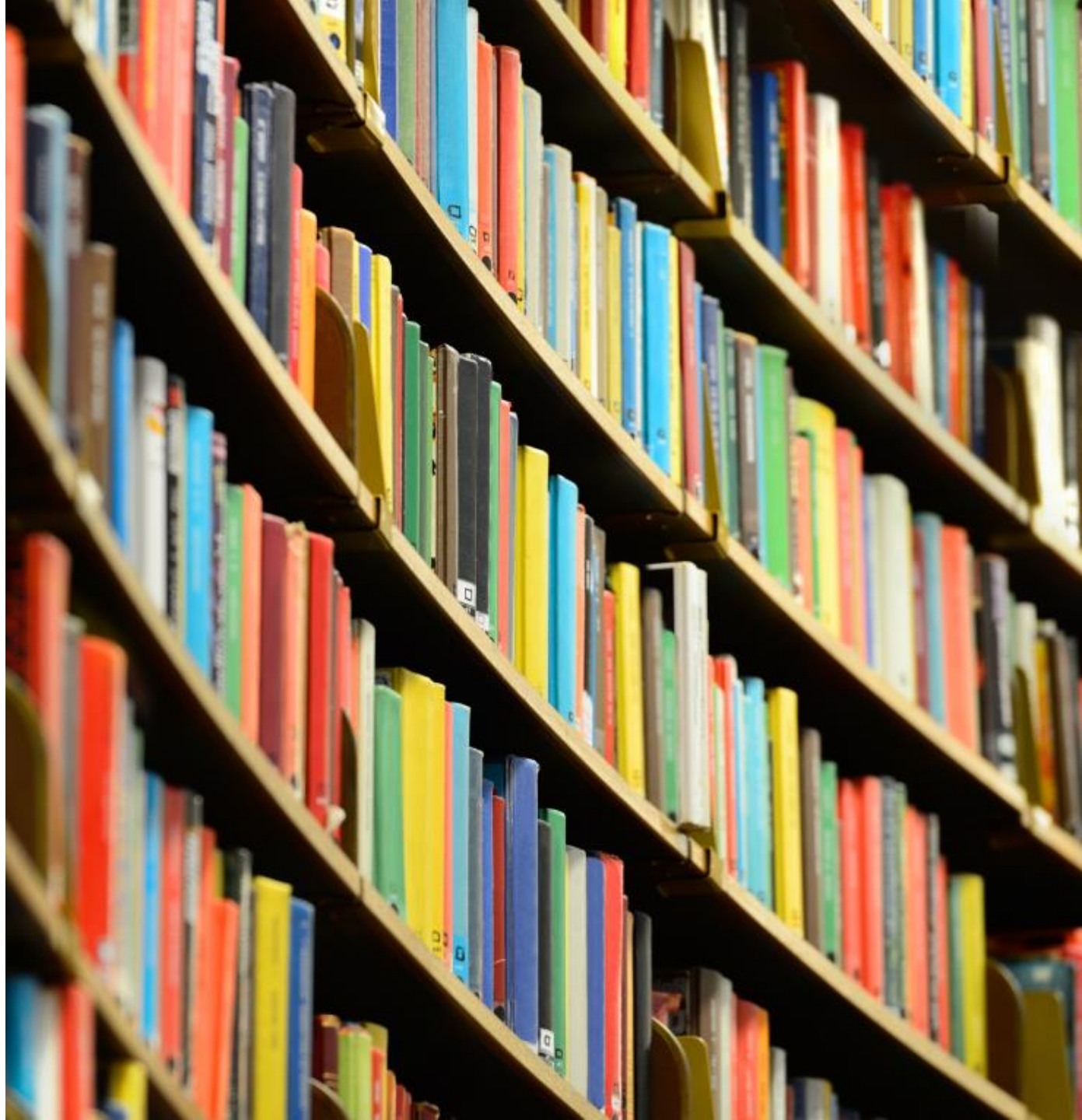
- Data users and processors are the individuals who utilize the data and information for daily organizational or business activities
- They may also perform raw data input and batch jobs as part of their job roles and responsibilities
- Example might include:
  - Salespersons and sales managers using acquired sales leads
  - Managers leveraging approved glossaries for reporting
  - Human resources communicating unauthorized language or verbiage as part of a diversity, equity, and inclusion (DEI) strategy

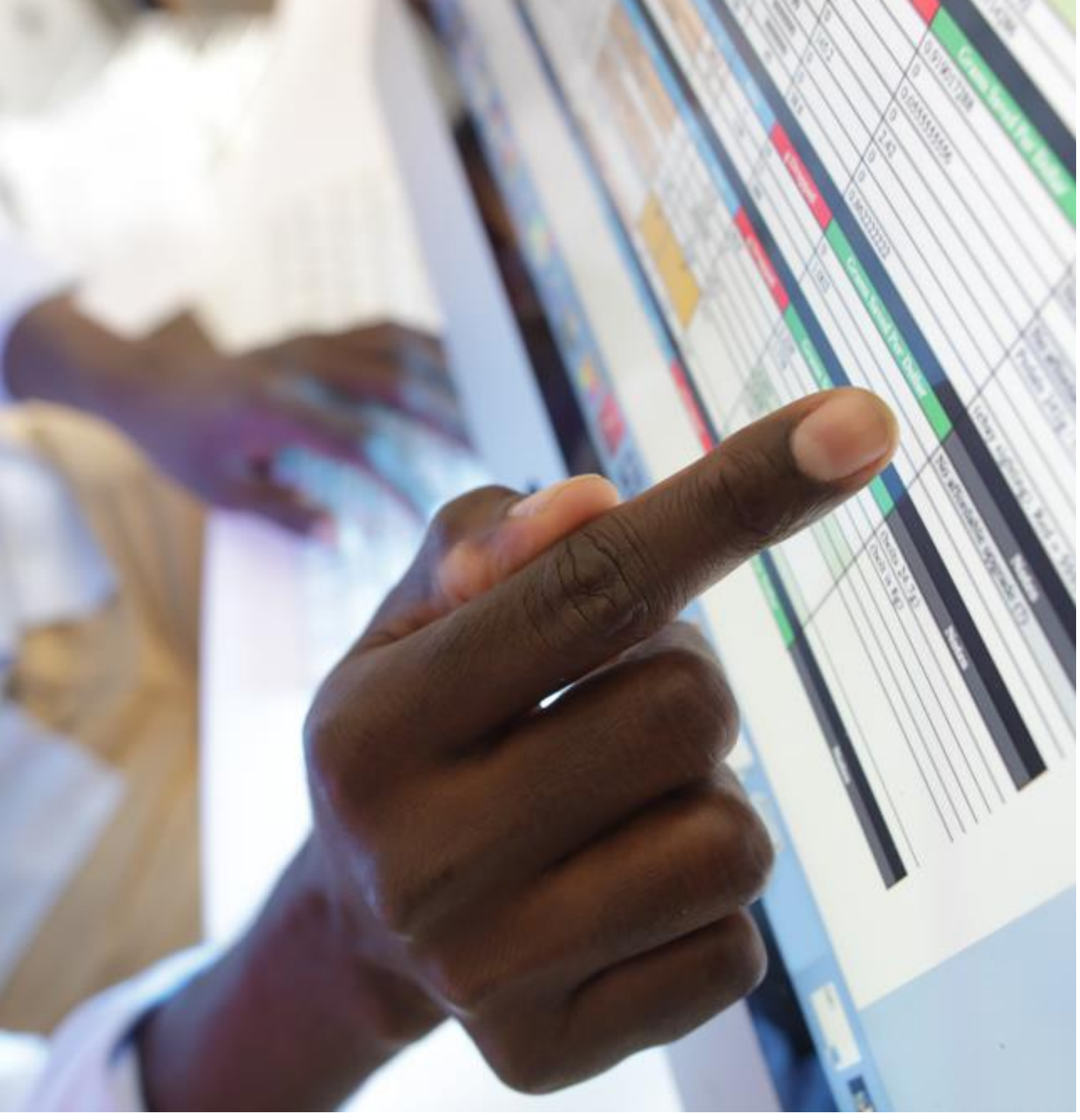
CISSP DATA LIFECYCLE



DATA LIFECYCLE: COLLECTION

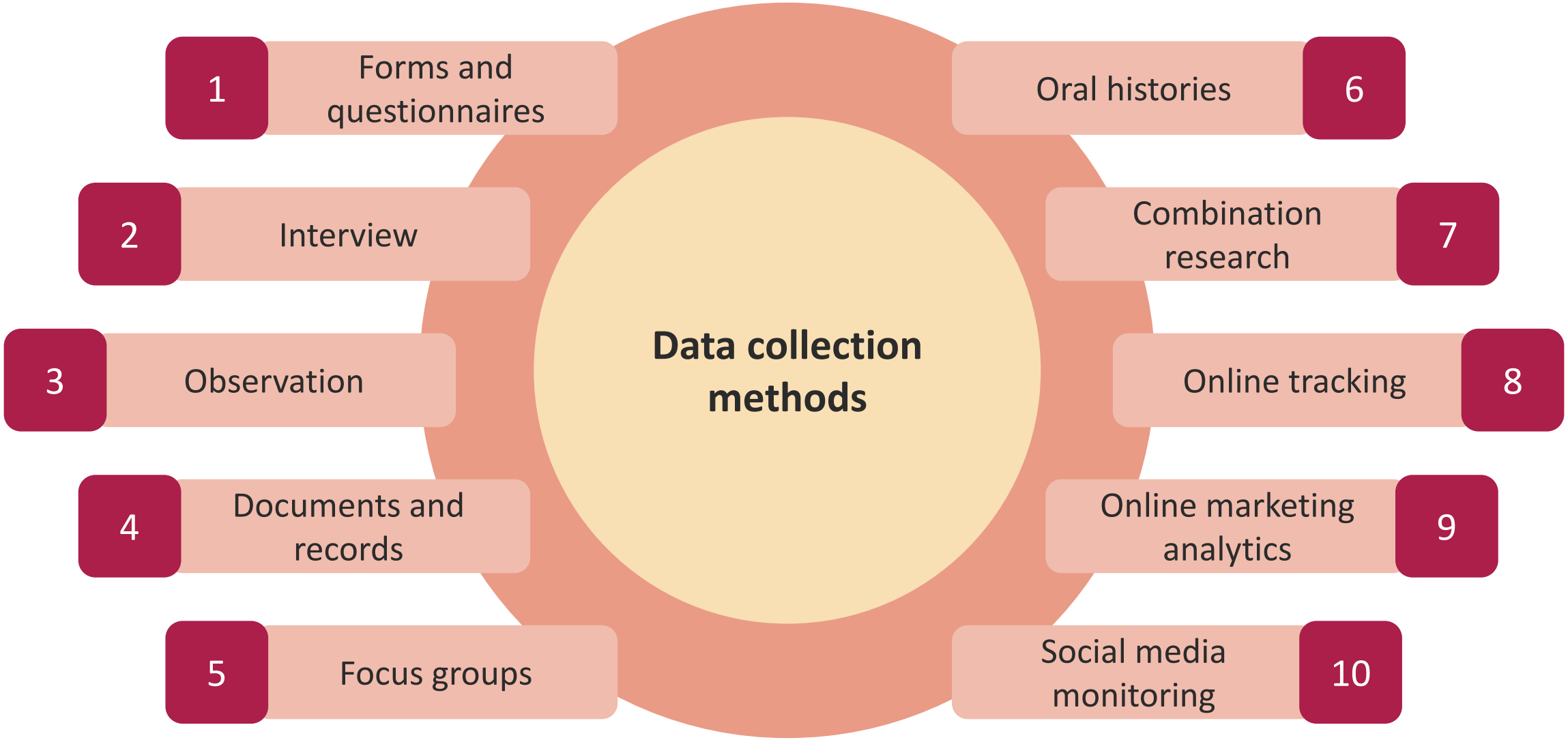
- The first stage **is mandatory** and involves collecting, generating, creating, and acquiring data from various internal and external sources
- This stage is also referred to as data creation, data acquisition, or data entry
- Collected data can be structured, semi-structured, and unstructured
- Other activities include labeling/tagging, categorizing, handling, ownership/custodianship, and even transformation





DATA LIFECYCLE: COLLECTION

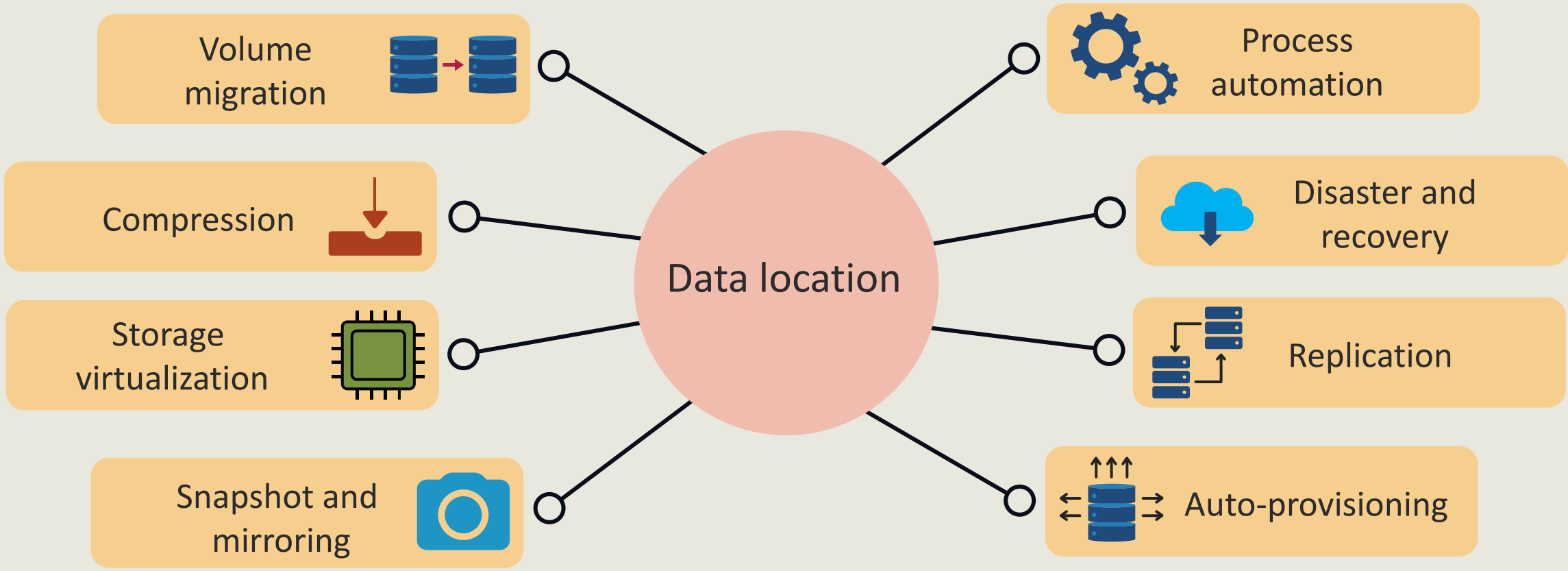
- Generally, there are three types of consumer data:
  - First-party data: Collected directly from users by the organization
  - Second-party data: Data shared by another organization about its customers (or its first-party data)
  - Third-party data: Data that has been aggregated and sold by organizations that do not have a link to your enterprise or end users


Data collection methods
1
Forms and questionnaires
2
Interview
3
Observation
4
Documents and records
5
Focus groups
6
Oral histories
7
Combination research
8
Online tracking
9
Online marketing analytics
10
Social media monitoring

DATA LIFECYCLE: LOCATION

- **This optional phase** involves the storage of data in block/volume, file, and/or object storage
- It is critical to have maximum visibility into all possible locations of the same data
- Effective data lifecycle management assists in generating a single source of truth by storing the original data in a central repository on-site or the cloud
- The type of data that is from the first phase will determine where and how it should be stored (located)

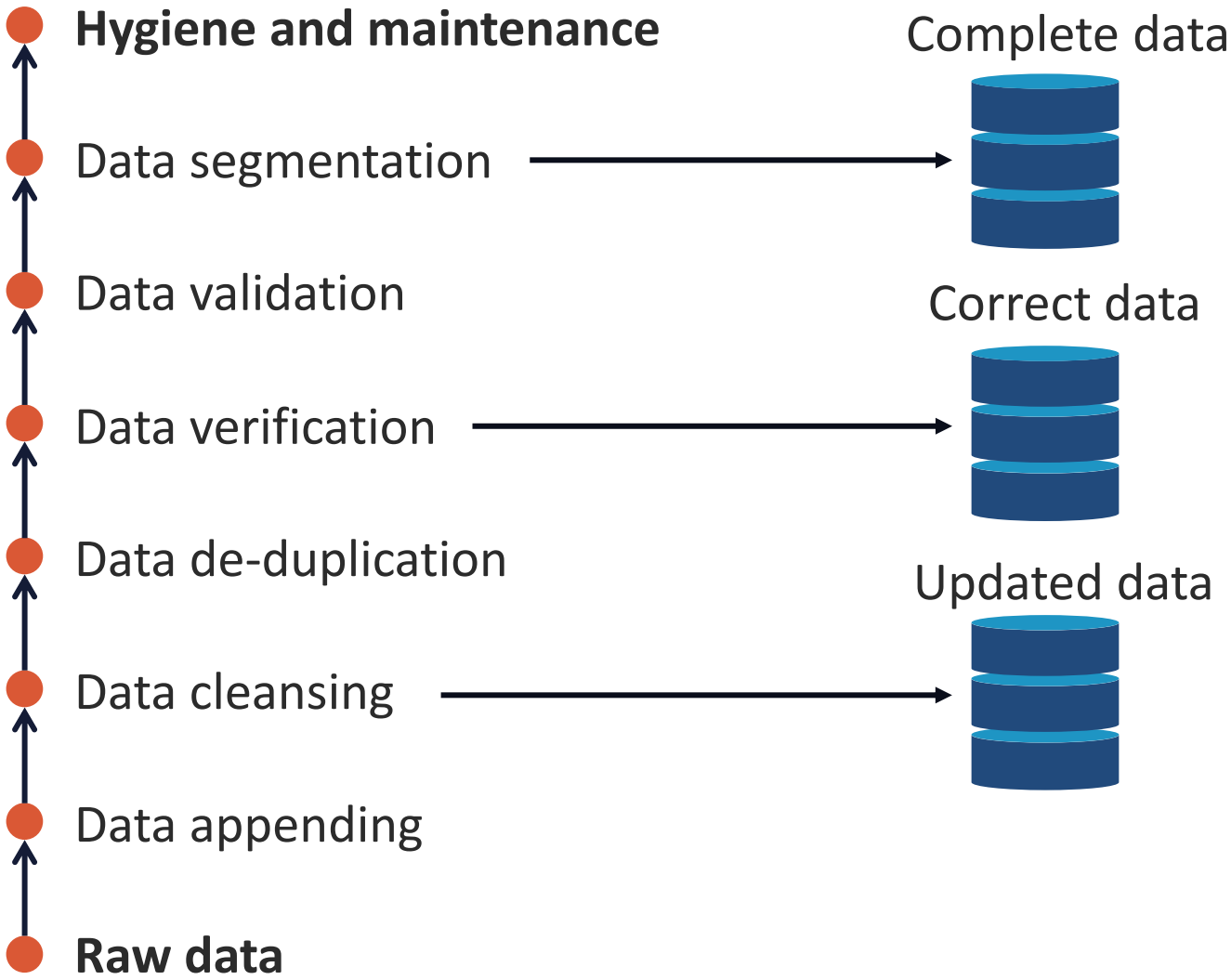
DATA STORAGE (LOCATION) USE CASES



DATA LIFECYCLE: MAINTENANCE

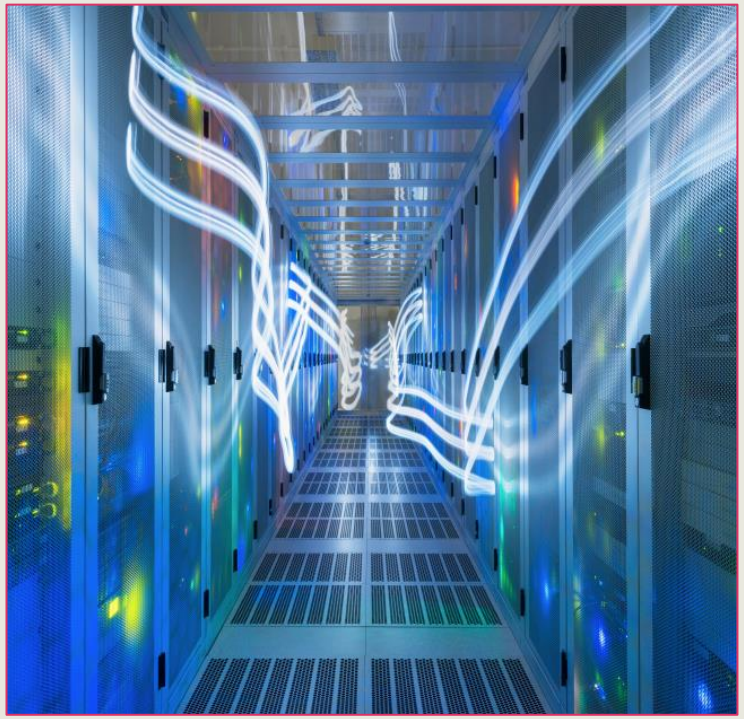
- Data maintenance is supported by the GDPR concept of data minimization
- The only data that should be maintained is data that has utility, value, and is meaningful
- Raw data > information > knowledge > wisdom
- **Data maintenance is also called processing** involving:
  - **Encryption:** Scrambling human-readable data into a format that can only be decoded by authorized personnel
  - **Wrangling:** Cleaning and transforming data from its raw state into a more accessible and functional format
  - **Compression:** Reducing the size of a piece of data and making it easier to store by restructuring or re-encoding it
  - **Processing and analysis:** Such as tokenization or data lakes

DATA MAINTENANCE AND MANAGEMENT ACTIVITIES

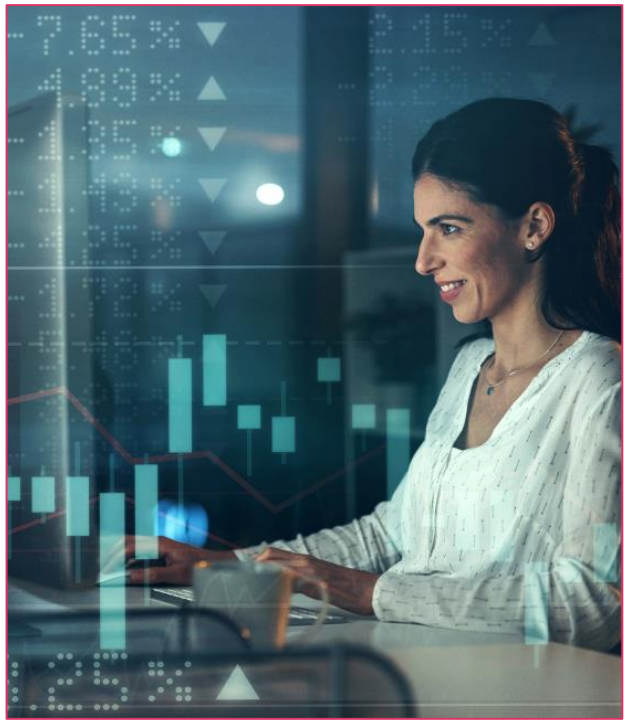


DATA LIFECYCLE: DATA RETENTION AND REMANENCE

- Data should be retained according to best practices, policy, security governance, laws, mandates, and/or regulations
- Retention generally refers to long-term archiving as opposed to location and storage
- **Data remanence is the situation when remnants, fragments, or artifacts of data can be recovered, even after proper wiping or erasure**
  - Data remanence makes sensitive information vulnerable to unethical hacking and data theft when the organization supposedly disposed of, transferred, resold, or stored data on various media formats

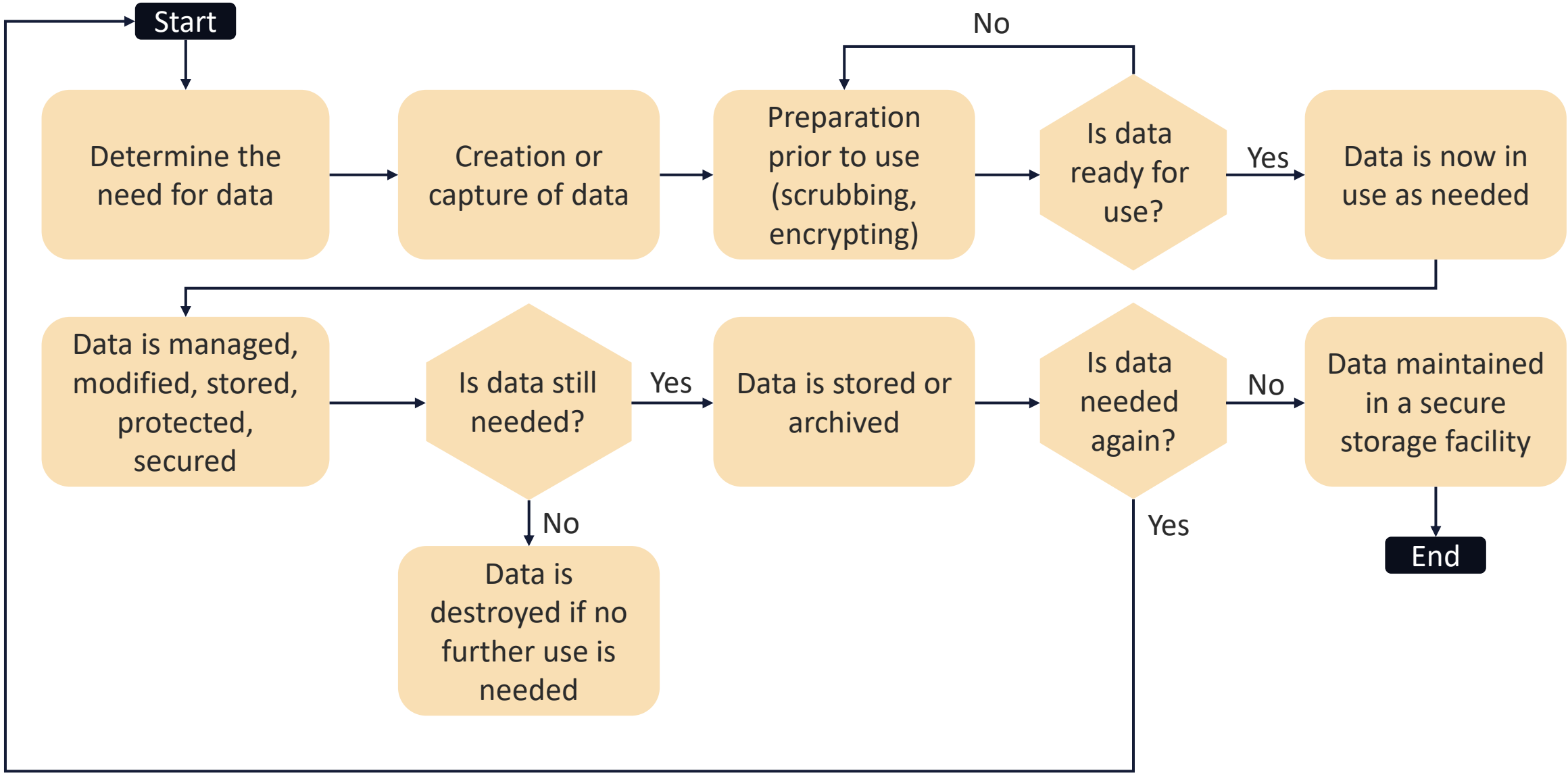


DATA LIFECYCLE: DATA RETENTION AND REMANENCE



- **End of life (EOL)**
  - In the context of data, as opposed to products or equipment, "end of life" relates to when the utility expires and is discarded or destroyed in the next phase
- **End of support (EOS)**
  - Also known as "end of service"– this is when the organization no longer provides data maintenance or updates, and the current iteration is the final version

DETERMINING DATA EOL AND EOS



DATA LIFECYCLE: DESTRUCTION

- According to NIST, "Media sanitization is one key element in assuring confidentiality"
- Confidentiality is defined as "preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information"
- Additionally, "a loss of confidentiality is the unauthorized disclosure of information"

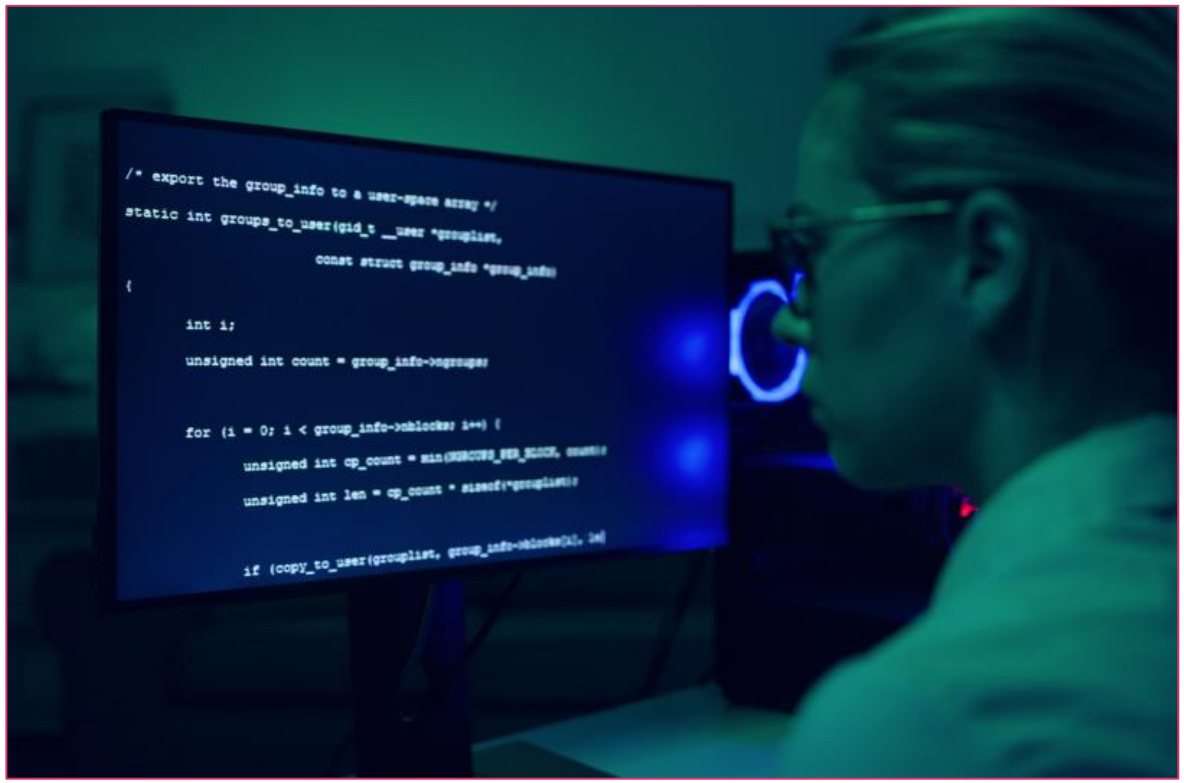
DATA LIFECYCLE: DESTRUCTION

- Organizations basically have three options for destroying data and media:
  - **Overwriting** (crypto-shredding): Covering up old data with information or ciphertext
  - **Degaussing and wiping** (DoD): Erasing the magnetic field of the storage media or wiping tools
  - **Physical destruction**: Employs techniques such as shredding, crushing, or furnaces

DATA SCOPING

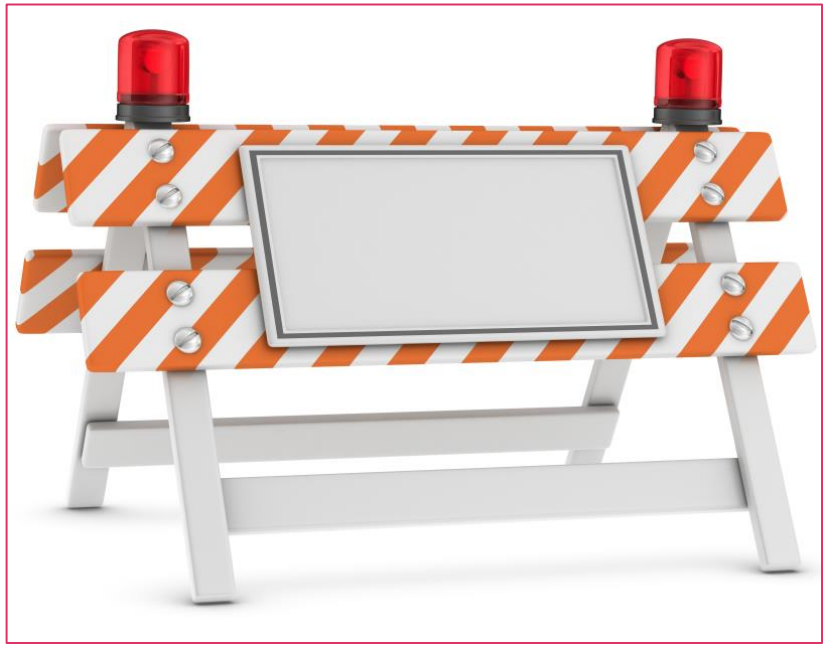
- Data scoping consists of deciding the boundaries within which certain data or controls apply
- Scoping often involves eliminating baseline security controls that are not relevant, such as removing privacy controls when private data does not exist
- Scoping can include focusing on controls applicable to the specific data being processed, such as deploying a database activity monitor (DAM) system and removing the IPs

DATA TAILORING



- Tailoring refers to customizing a set of security controls to match the organizational charter or mission regarding data or system requirements
  - An example would be modifying the database client application timeout requirement from 10 minutes of inactivity to 5

SCOPING VS. TAILORING



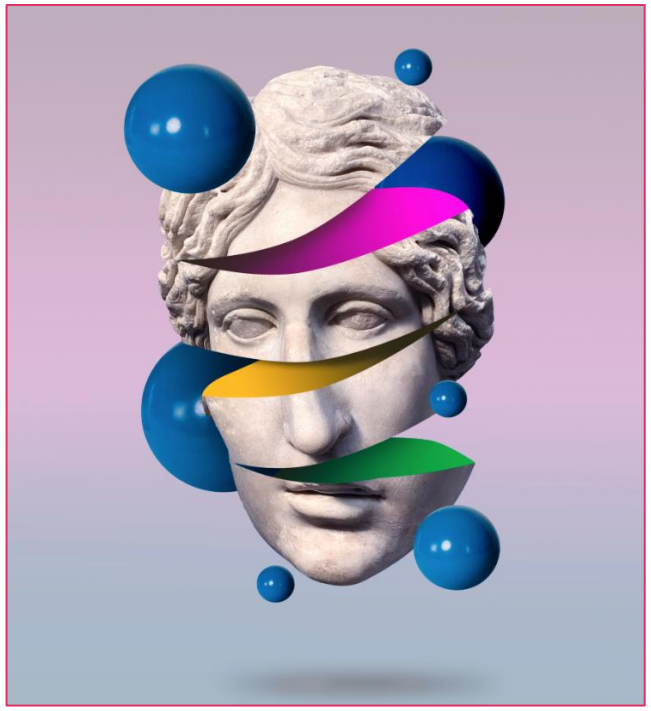
Data scoping describes the contextual boundaries

Tailoring fine-tunes controls to address the specific operational environment

DIGITAL RIGHTS MANAGEMENT (DRM) / INFORMATION RIGHTS MANAGEMENT (IRM)

- DRM is access-control technology that protects licensed digital intellectual property (IP)
- DRM is used by publishers, manufacturers, and IP owners for digital content and device monitoring
- Digital media licensees attempt to balance the rights of IP owners and Internet users by protecting rights and profits for digital product manufacturers and retailers
- **DRM protects copyrighted digital music files, apps, software programs, films, TV shows, games, and other media**

DIGITAL RIGHTS MANAGEMENT (DRM) / INFORMATION RIGHTS MANAGEMENT (IRM)



- Security managers may have to contend with DRM and IRM from one of two perspectives:
  - They work for an organization that produces various forms of content that must be protected from piracy, copyright infringement, and ransomware
  - They must have visibility into end users violating acceptable use policies and unauthorized usage of unauthorized digital information
- Consumer advocacy groups state that DRM initiatives deny fair digital media access
  - However, DRM continues to be a practical way to manage digital privacy, avoid piracy, and ensure fair compensation to IP owners

DRM SOFTWARE SOLUTIONS

Compatibility with necessary content sharing protocols

Trackability and analytics to monitor access

Integration with existing content infrastructure

Installation environment or SaaS model

Alerts and notifications

DATA LOSS PREVENTION (DLP)

- Data loss prevention (DLP) is a collection of hardware and software tools and programs that help safeguard that sensitive data (IP, PHI, PII) is not leaked, lost, tainted, stolen, or read by unauthorized users
- DLP is generally considered a program (initiative) and not simply a product
- It offers 3 forms of protection:
  - **Network DLP**
  - **Endpoint DLP**
  - **Cloud-based DLP**

DATA LOSS PREVENTION (DLP)

Data

- Trade secrets
- Account numbers
- Social Security numbers
- Intellectual property
- Personal health records

Can leak

- Stored on network or shared drives
- Copied on external removable media devices
- Transmitted electronically – email, instant message (IM), online, etc.

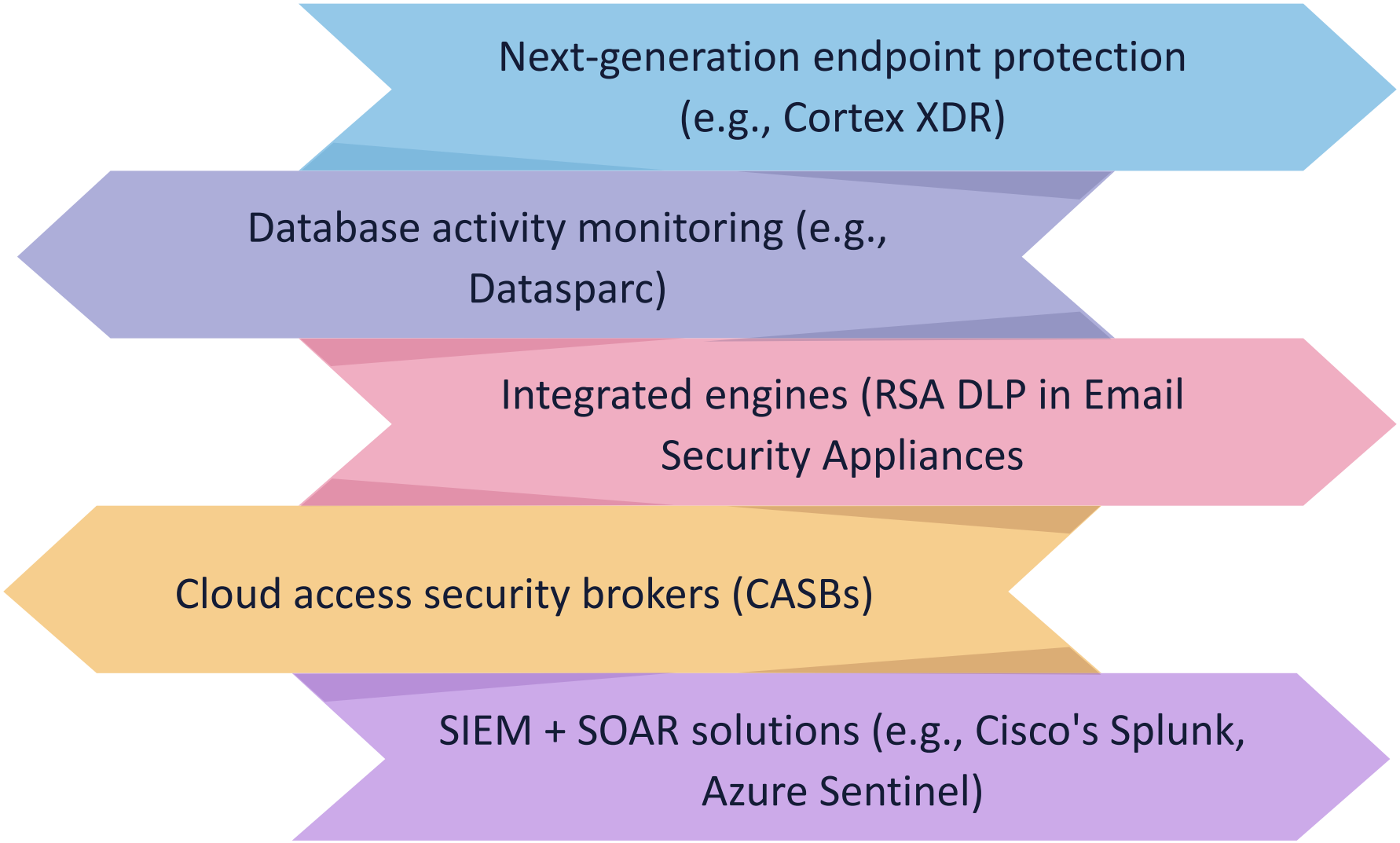
To an outsider

- Competitors
- Regulators
- Unauthorized internal users
- Press or media

Resulting in a breach

- Company defamation
- Monetary expense for each record lost
- Legal liabilities
- Loss of assets
- Breach of customer trust
- Closure of the business

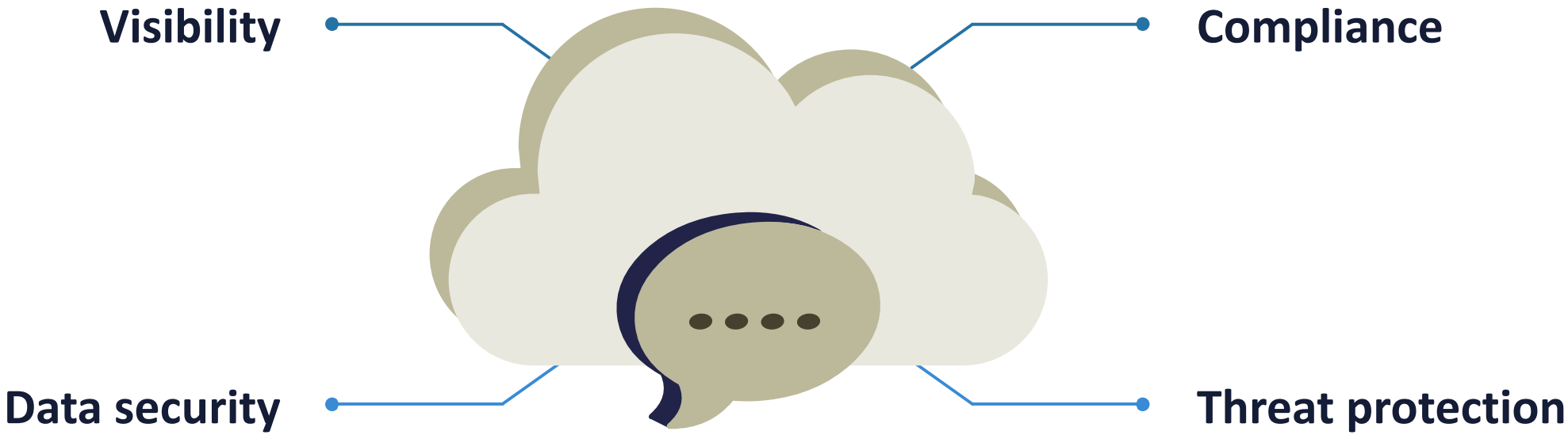
COMMON DLP SOLUTIONS



CLOUD ACCESS SECURITY BROKERS (CASB)

- A cloud access security broker (CASB) is also called a cloud service broker or cloud access gateway
- One of the first to offer a product marketed as a "CASB" was Skyhigh Networks, acquired by McAfee in January 2018
- They are **API-based** (i.e., AWS PrivateLink partners) **or Proxy-based** (i.e., Palo Alto's Aperture)
- A CASB will typically offer SaaS solutions for federated access (i.e., single sign-on [SSO]), data loss and leak protection, and compliance support

THE FOUR PILLARS OF CASB



SECURE DESIGN PRINCIPLES AND MODELS

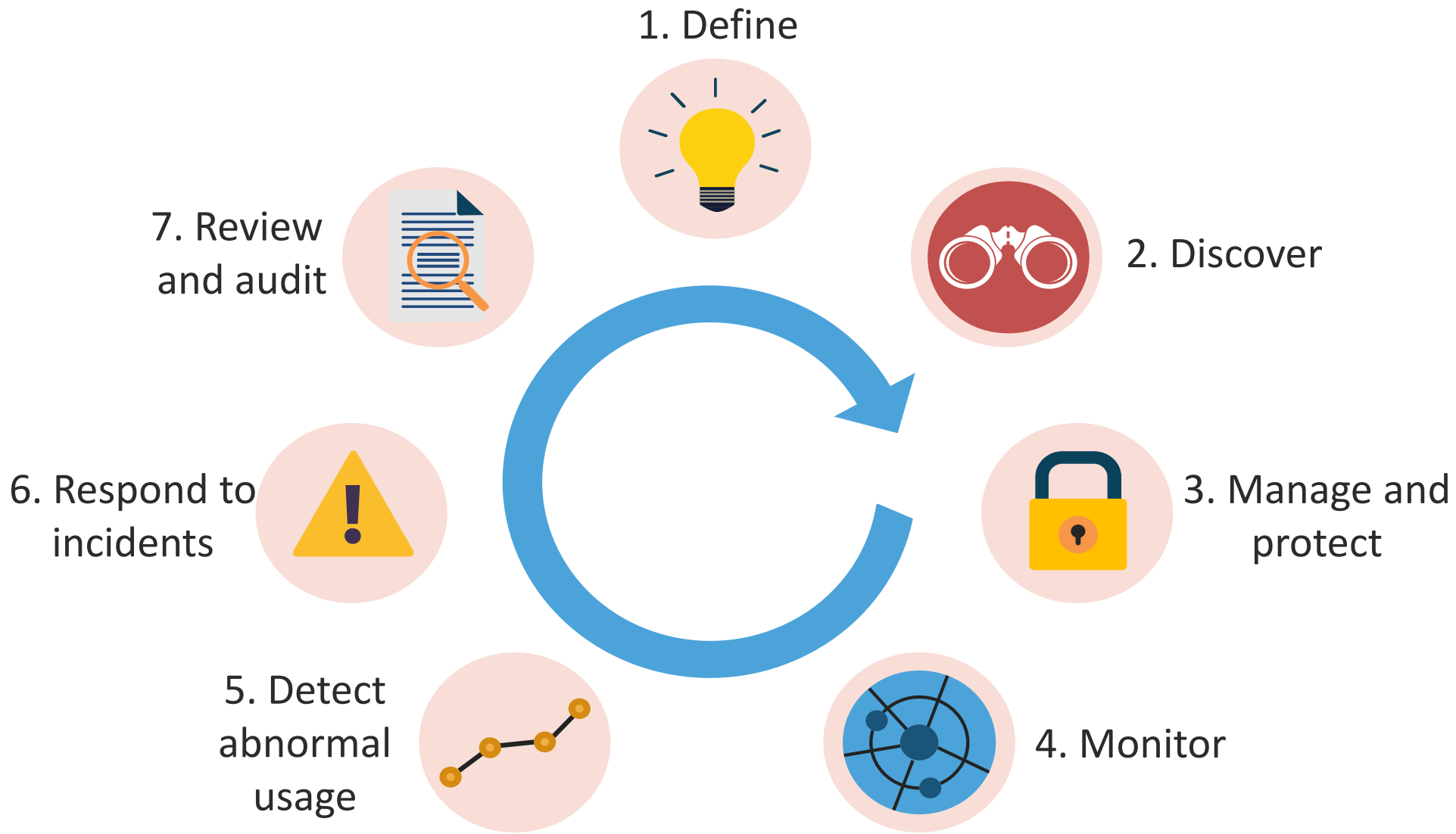
Objectives

- Examine principles like least privilege, Defense in Depth, secure defaults, fail securely, segregation of duties, and keep it simple
- Explore Privacy by Design and Default and shared responsibility models
- Know about threat modeling
- Compare Zero trust to Trust but Verify
- Learn about Secure Access Service Edge (SASE)
- Survey fundamental concepts of security models

LEAST PRIVILEGE

- According to NIST, least privilege is the principle that "a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function"
- It is also referred to as "need to know" or "staying within one’s pay grade"
- It is a critical component of modern Zero Trust initiatives and must be strictly enforced regardless of the access control model (DAC, MAC, RBAC, ABAC, etc.)

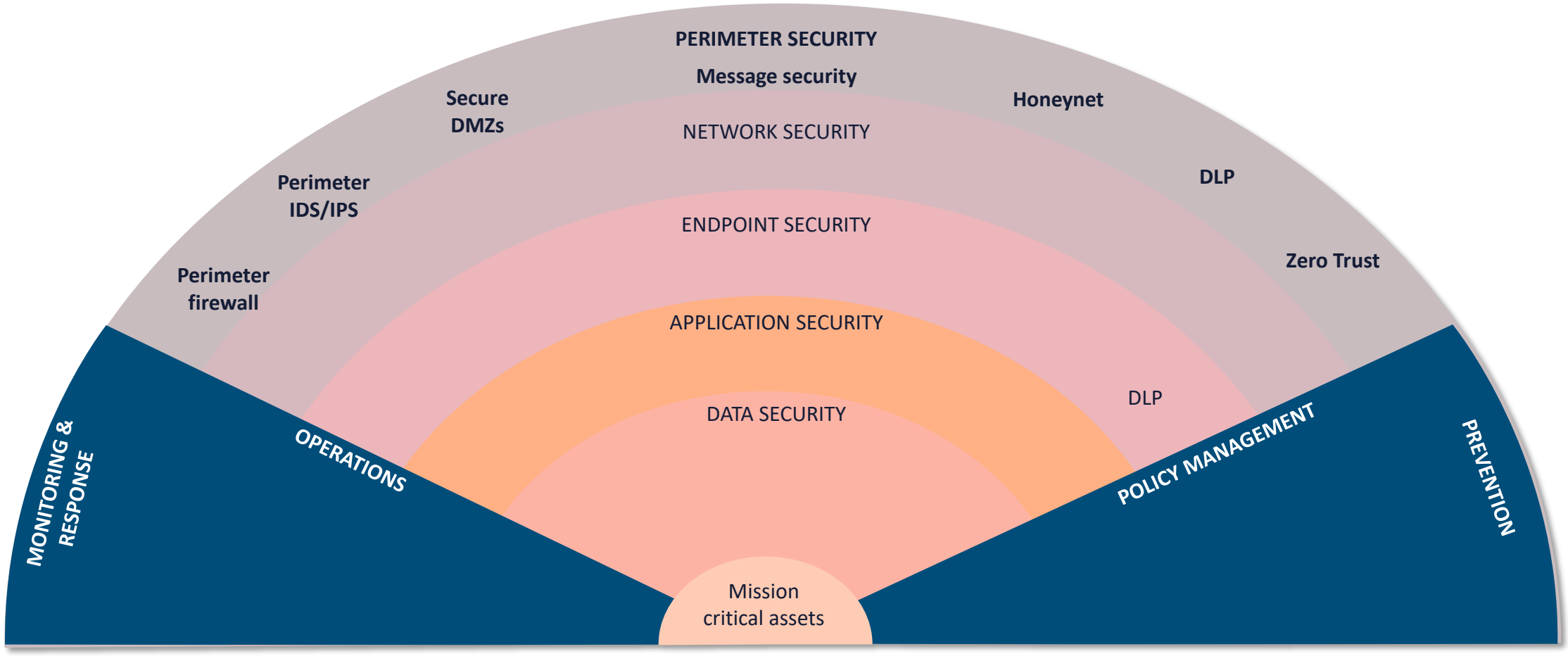
ENFORCING LEAST PRIVILEGE



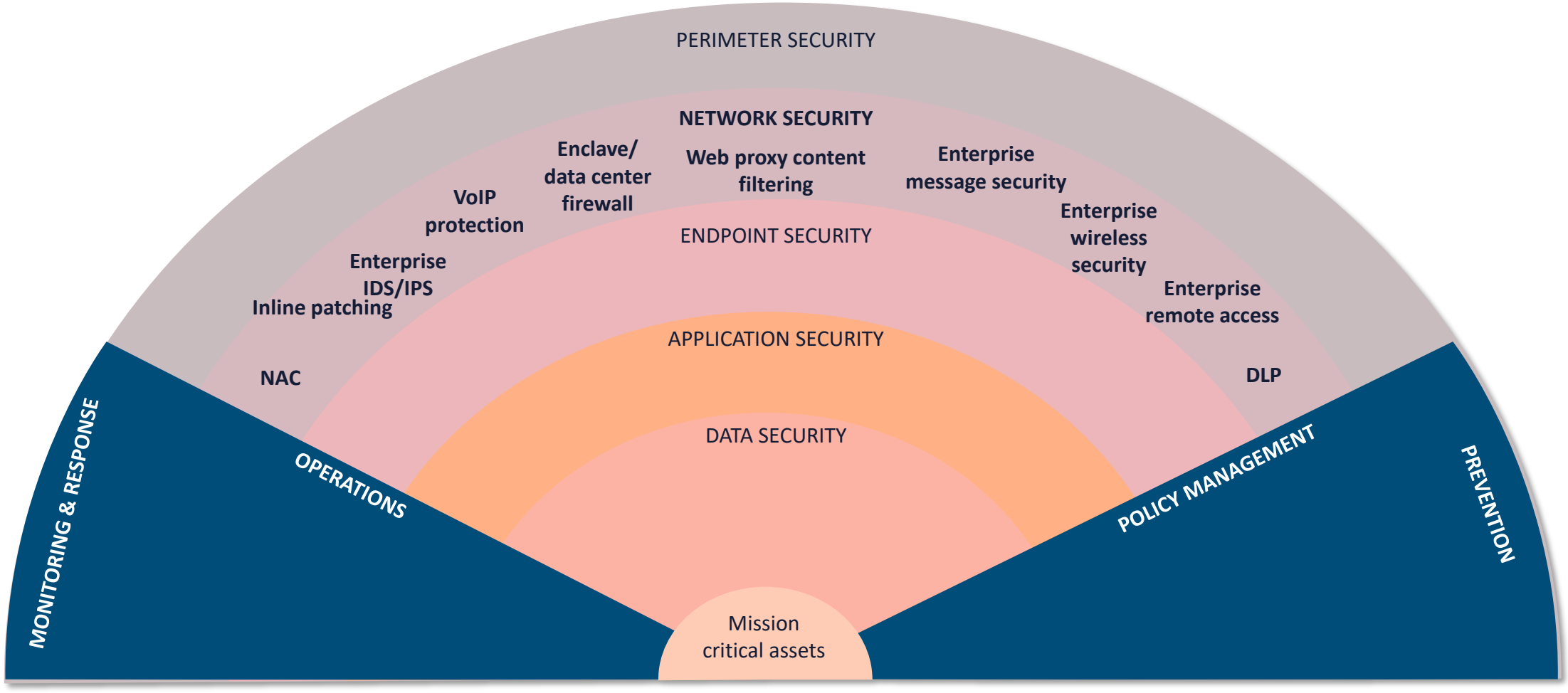
DEFENSE IN DEPTH (DiD)

- DiD is also referred to as a "layered defense" approach
- Using the least privilege and DiD principles is a function of "due care"
- It can be applied to physical security or technical controls
  - With physical, it should be systematically planned and designed with an outward-in or inward-out approach
  - It can be a single appliance with multiple integrated engines
- **DiD is a common element of supply chain risk management (SCRM)**

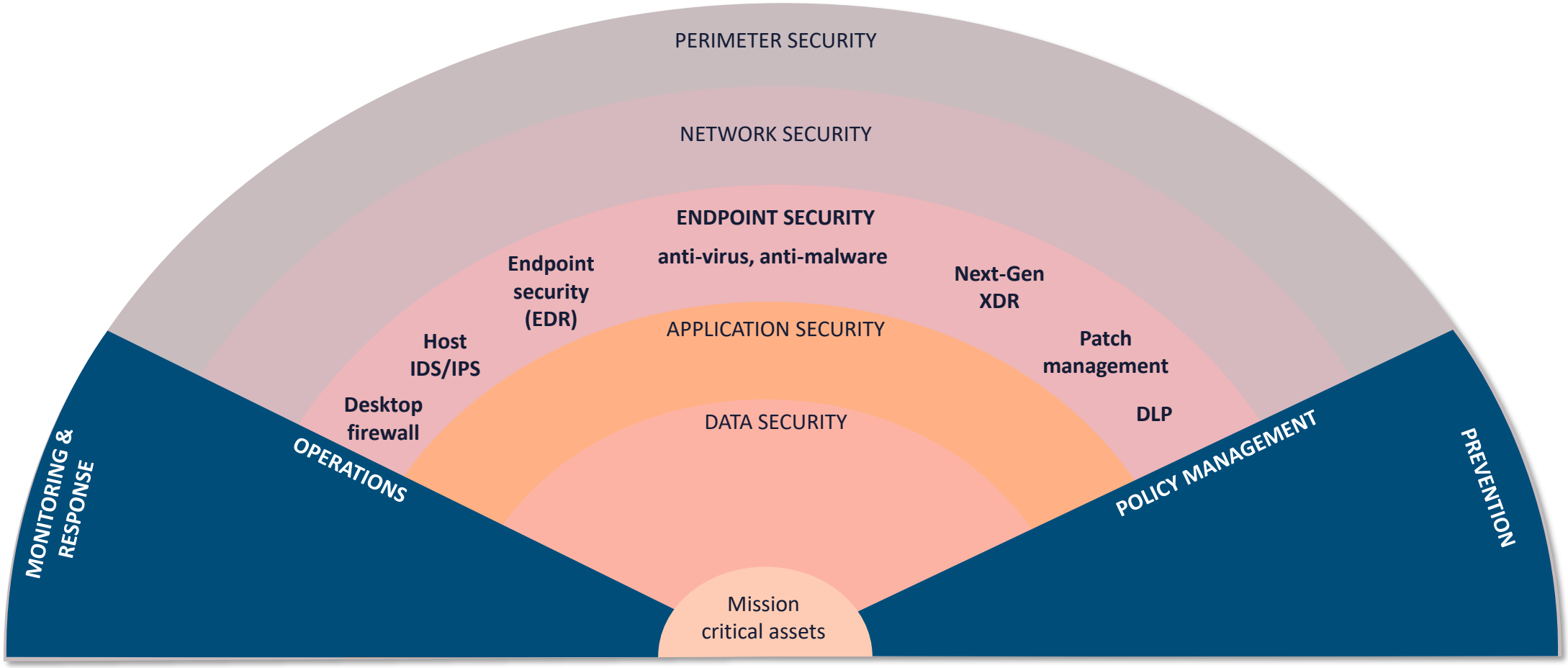
TECHNICAL & ADMINISTRATIVE DEFENSE IN DEPTH



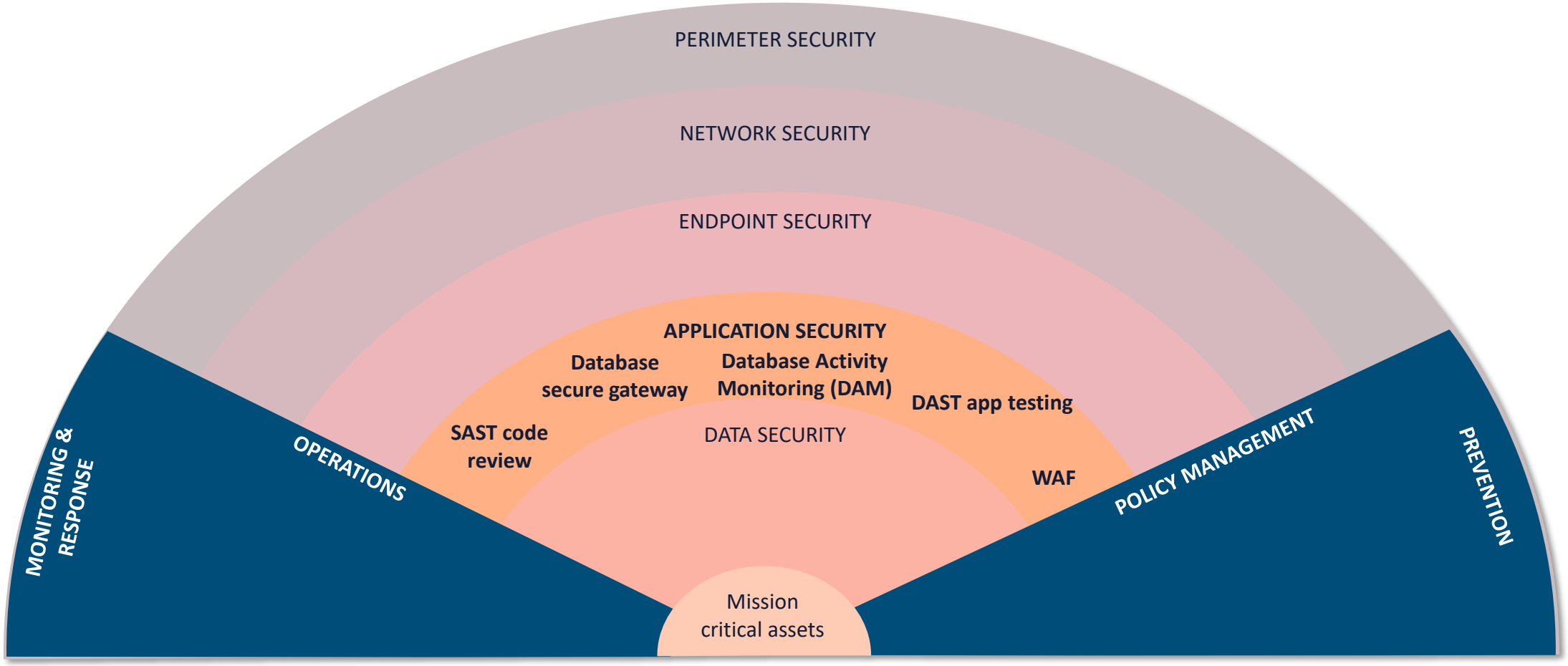
DEFENSE IN DEPTH (DID)



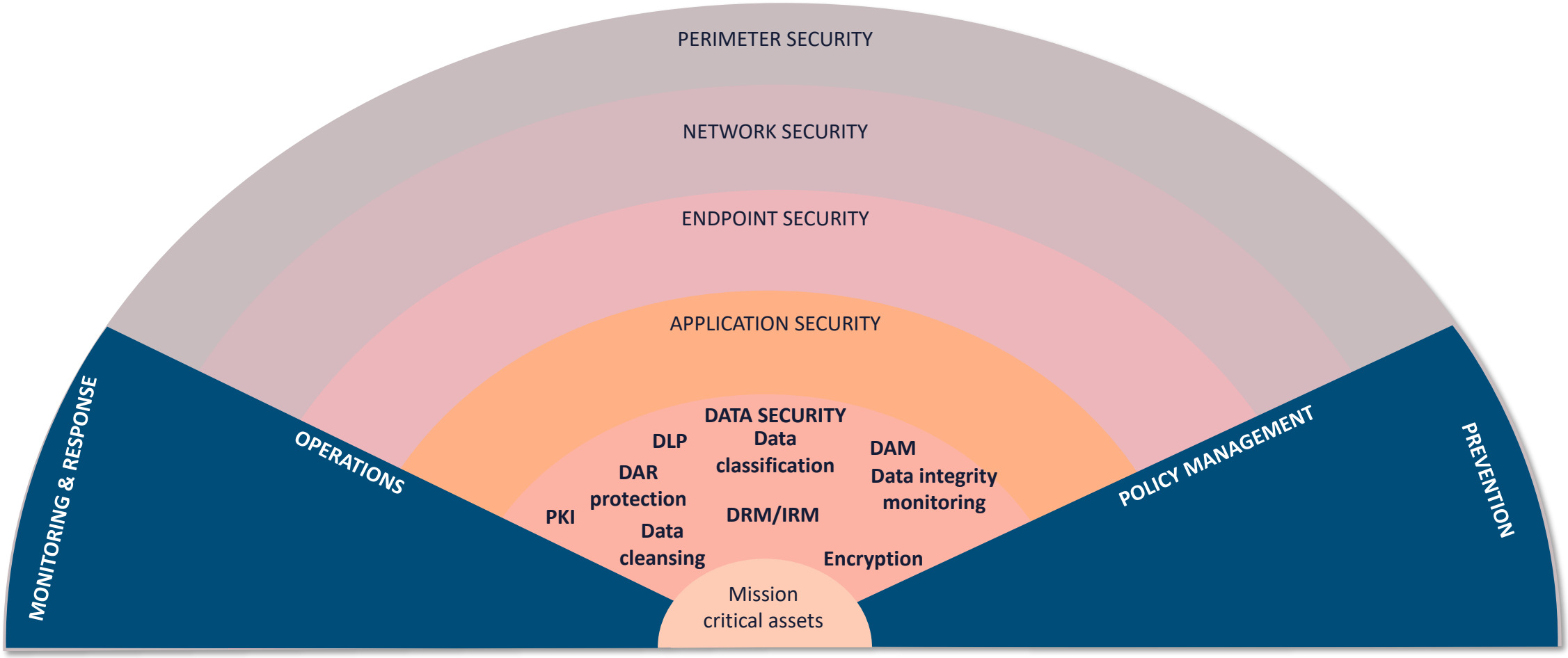
DEFENSE IN DEPTH (DID)



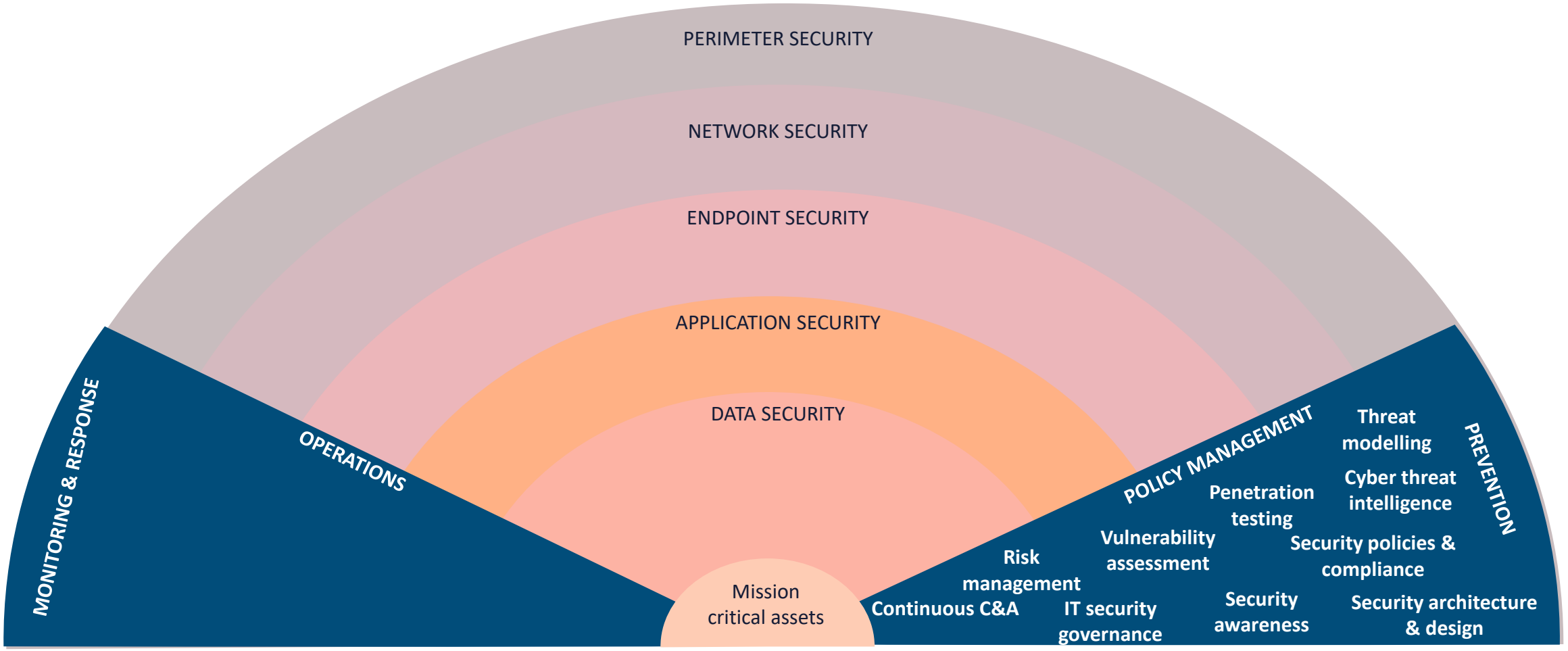
DEFENSE IN DEPTH (DID)



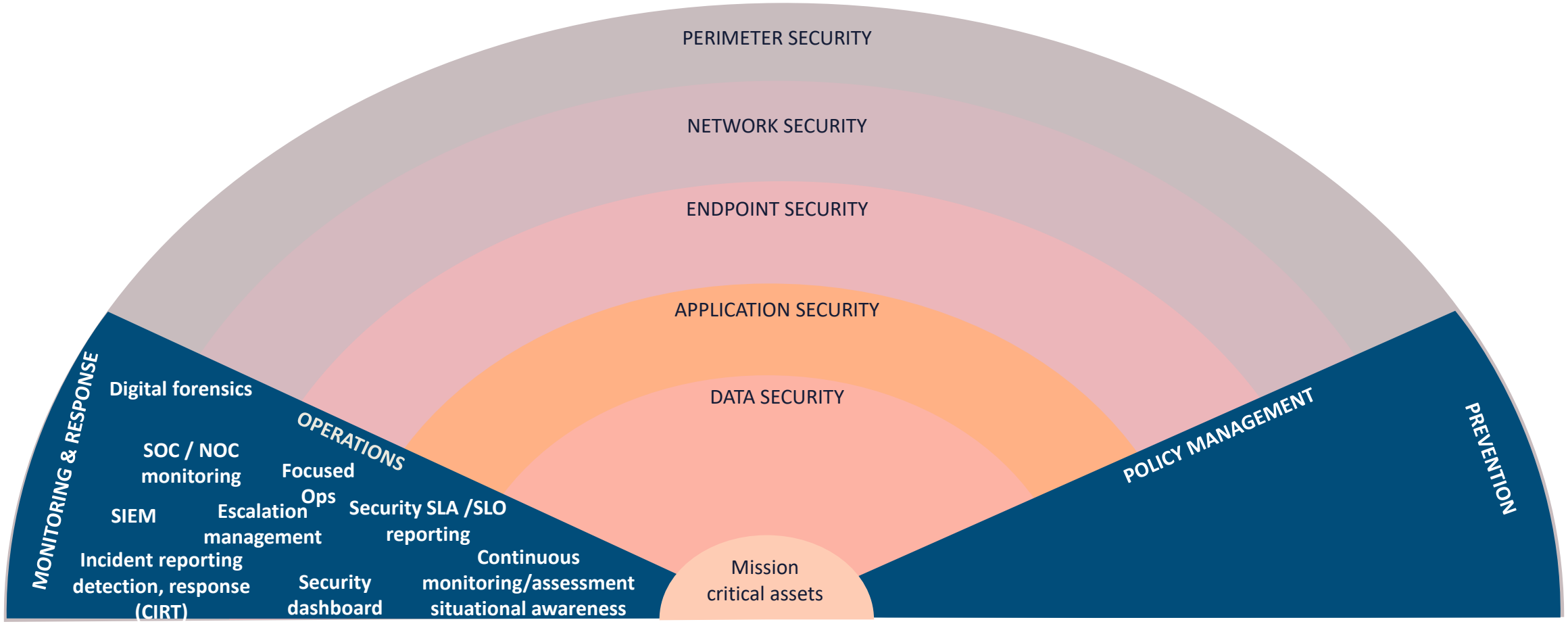
DEFENSE IN DEPTH (DID)



DEFENSE IN DEPTH (DID)



DEFENSE IN DEPTH (DID)



SECURE DEFAULTS

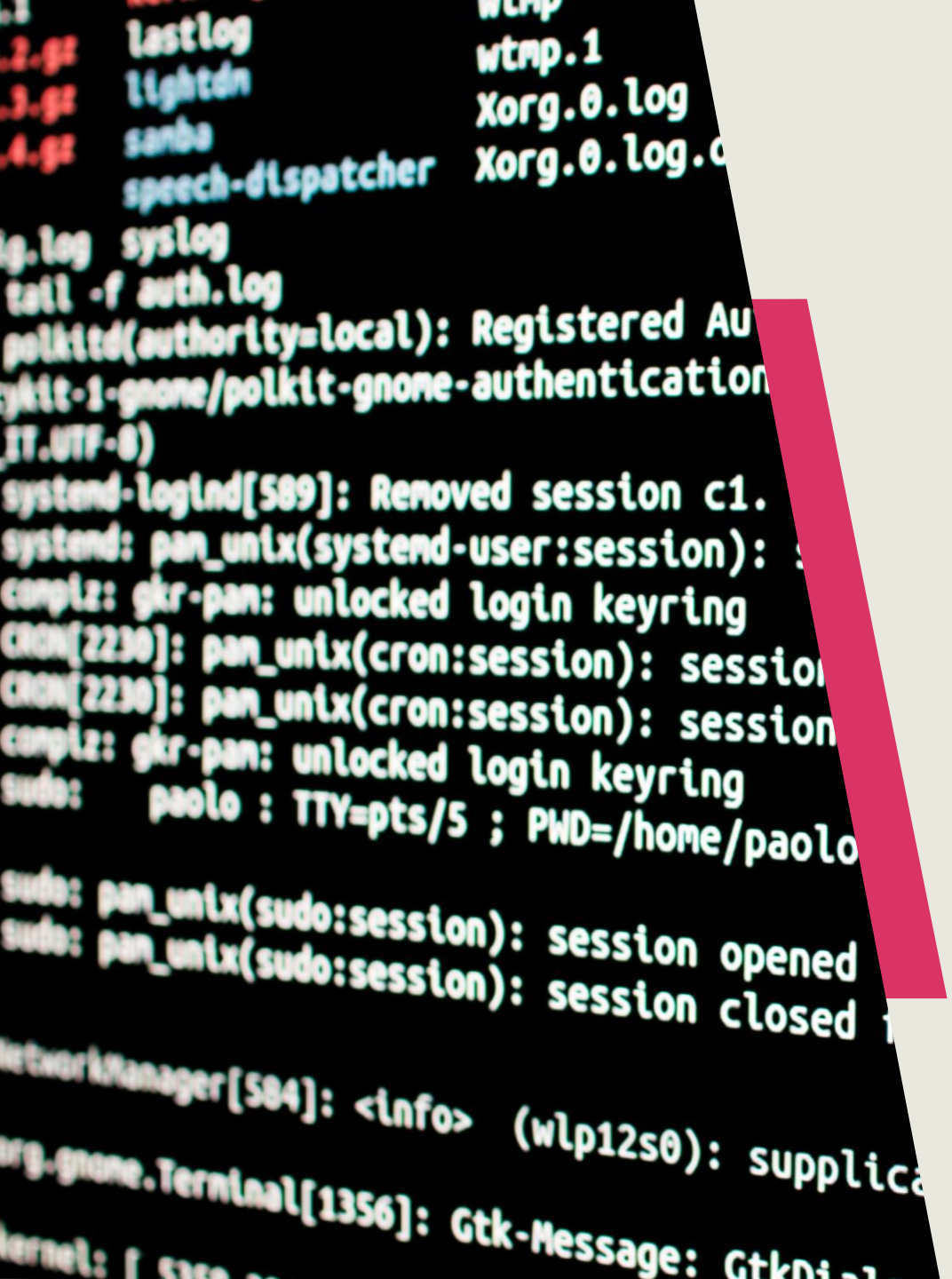
- The secure defaults principle states that the default configuration of a system (including its integral subsystems, components, and instruments) is a restrictive and conservative enforcement of the written security policy
- This principle applies to the initial (or default) configuration of a system, including the security engineering and design of access controls
- It uses a "deny unless explicitly authorized" strategy

SECURE DEFAULTS

- The primary configuration facet of this principle also demands that any "as shipped" configuration of a system, subsystem, or component does not contribute to security policy violations
- This initiative should avert a situation where systems operating in the default state require configuration by the operational user
- Automation and infrastructure as Code is a critical enabler for secure defaults

FAIL SECURELY

- The "fail securely" principle contends that when a system or server fails, it should have the minimum impact possible on the system’s security or functionality
- A fail-secure system reacts in such a way that access or data-in-transit is denied in case of a failure
- For instance, a fail-secure door lock will stay locked in an access control system if power is lost, or an internal battery dies



FAIL SECURELY

- Handling errors securely is a critical requirement of secure coding
- According to OWASP, security mechanisms should be designed so that a failure will allow the same execution path as disallowing the operation
- For instance, security methods such as *isAuthorized()*, *isAuthenticated()*, and *validate()* **should all return false** if there is an exception when processing
- If security controls can trigger exceptions, they must be exact about what that condition really means

SEGREGATION OF DUTIES (SoD)

- Also referred to as "separation of duties" – it is a principle where more than one subject is required to complete a particular task
  - For example, a separate Backup Operators group from a Data Restoration group
- SoD may also involve dual operator principles where two or more subjects are needed to modify or approve
  - For example, two signatures or cryptographic keys are required for certain actions
- Rotation of duties is also a related principle
  - For example, mandatory time off or forced vacations

MORE SoD EXAMPLES

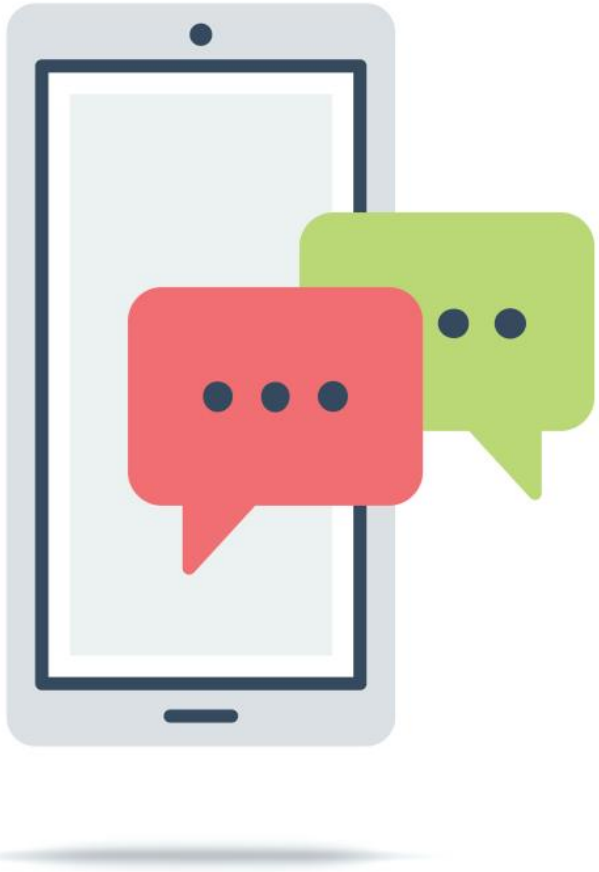
- One user requests access to an application, another person accepts the request, and a third person audits the access
- One subject chooses a vendor, another one negotiates the SLA, and a third manager monitors the vendor's performance
- One individual identifies a risk, another person analyzes it, and a third person mitigates the risk with controls
- One administrator requisitions the acquisition of a next-gen endpoint detection and response (EDR) system, a second manager approves the purchase, and a third records the purchase in the accounting system and configuration management database (CMDB)

KEEP IT SIMPLE AND SMALL

- Amazon Web Services (AWS) has some excellent suggestions for keeping it simple and small in their Well-Architected initiative, including:
  - Democratize advanced technologies by simplifying implementation by delegating complex tasks to a cloud vendor (i.e., Software as a Service [SaaS])
  - Perform operations as code using scripts to automate processes in response to events, reducing human error and improving simplicity and consistency

KEEP IT SIMPLE AND SMALL

- Additional best practices from AWS include:
  - Make recurrent, small, revocable modifications by designing workloads and functions that are scalable and loosely coupled to reduce the blast radius and enable faster rollback when failures happen
  - Decrease operational overhead by using managed serverless services where possible



PRIVACY BY DESIGN AND DEFAULT

- It is said that Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Canada, may have coined this term well before the GDPR made it popular
- According to Cavoukian, "Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization’s default mode of operation."

PRIVACY BY DESIGN AND DEFAULT

- Privacy by Design means that privacy is already integrated into technology, IT systems, services, and products to ensure data protection
- Basically, the entire engineering process is conducted with privacy in mind, while safeguarding personal data becomes as important as any other functionality
- The foundation of Privacy by Design rests on seven core principles, providing a guiding framework for integrating privacy into your business’s daily operations

PRIVACY BY DESIGN PRINCIPLES

1. Proactive and not reactive
2. Preventative and not counteractive
3. Privacy as the default setting

PRIVACY AS THE DEFAULT SETTING

Purpose specifications

Define a purpose for collection, retention, disclosure, and use of personal data

Use, disclosure, and retention limitation

Limit the use, retention, and disclosure of personal information to the relevant purposes

Data minimization

Minimize the collection of data and the identifiability and linkability of personal data

PRIVACY BY DESIGN PRINCIPLES

4 Embedded into all software design lifecycles

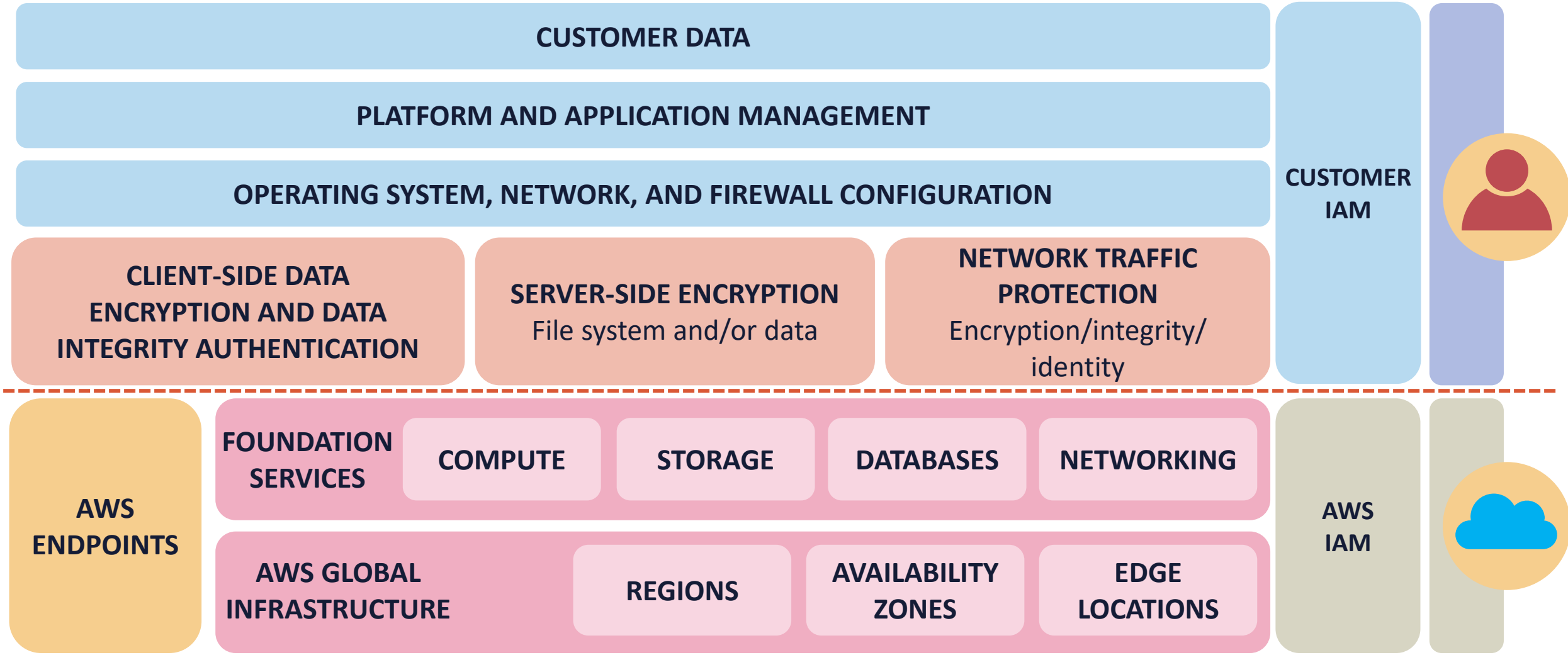
5 End-to-end security with full data lifetime protection

6 Comprehensive visibility and transparency

SHARED RESPONSIBILITY MODEL (SRM)

- The shared responsibility model is a security and compliance framework that determines the accountabilities of cloud service providers (CSPs) and consumers
- **Providers**, such as AWS, Azure, or GCP, monitor and react to security threats **of the cloud** itself and its underlying infrastructure
- Customers, including individuals and organizations, to protect data and other assets (functions and code) they store **in or on any cloud** environment

INFRASTRUCTURE AS A SERVICE SRM EXAMPLE



MICROSOFT AZURE SRM

Responsibility	SaaS	PaaS	Iaas	On-prem	
Information and data	●	●	●	●	**Customer responsibility**
Devices	●	●	●	●	
Accounts and identities	●	●	●	●	
Identities and directory infrastructure	◔	◔	●	●	**Responsibility varies by service type**
Applications	○	◔	●	●	
Network controls	○	◔	●	●	
Operating systems	○	○	●	●	
Physical hosts	○	○	○	●	**Responsibility moves to cloud provider**
Physical network	○	○	○	●	
Physical datacenter	○	○	○	●	
Microsoft ○ Customer ●					

DATA-CENTRIC THREAT MODELING

- There are several types of threat modeling (e.g., system threat modeling is threat modeling performed for operational systems to improve their overall security)
  - Application threat modeling was covered in earlier in *Threat Modeling, SCRM, and Security Awareness*
- Data-centric system threat modeling is focused on defending specific types of data within systems (i.e., file, object, block)
  - Simply following generic "best practices" for security is inadequate for protecting critical, high-value data

SP 800-154, GUIDE TO DATA-CENTRIC SYSTEM THREAT MODELING

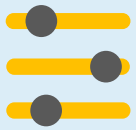
- According to NIST, "The publication provides information on the basics of data-centric system threat modeling so that organizations can successfully use it as part of their risk management processes"
- "The general methodology provided by the publication is not intended to replace existing methodologies, but rather to define fundamental principles that should be part of any sound data-centric system threat modeling methodology"

DATA-CENTRIC THREAT MODELING

Identify
What kinds of data do you have?

Understand
Sources of regulated and sensitive data, how they're used, and how they're shared

Control
Establishing policies, controls, and a governance model with audits



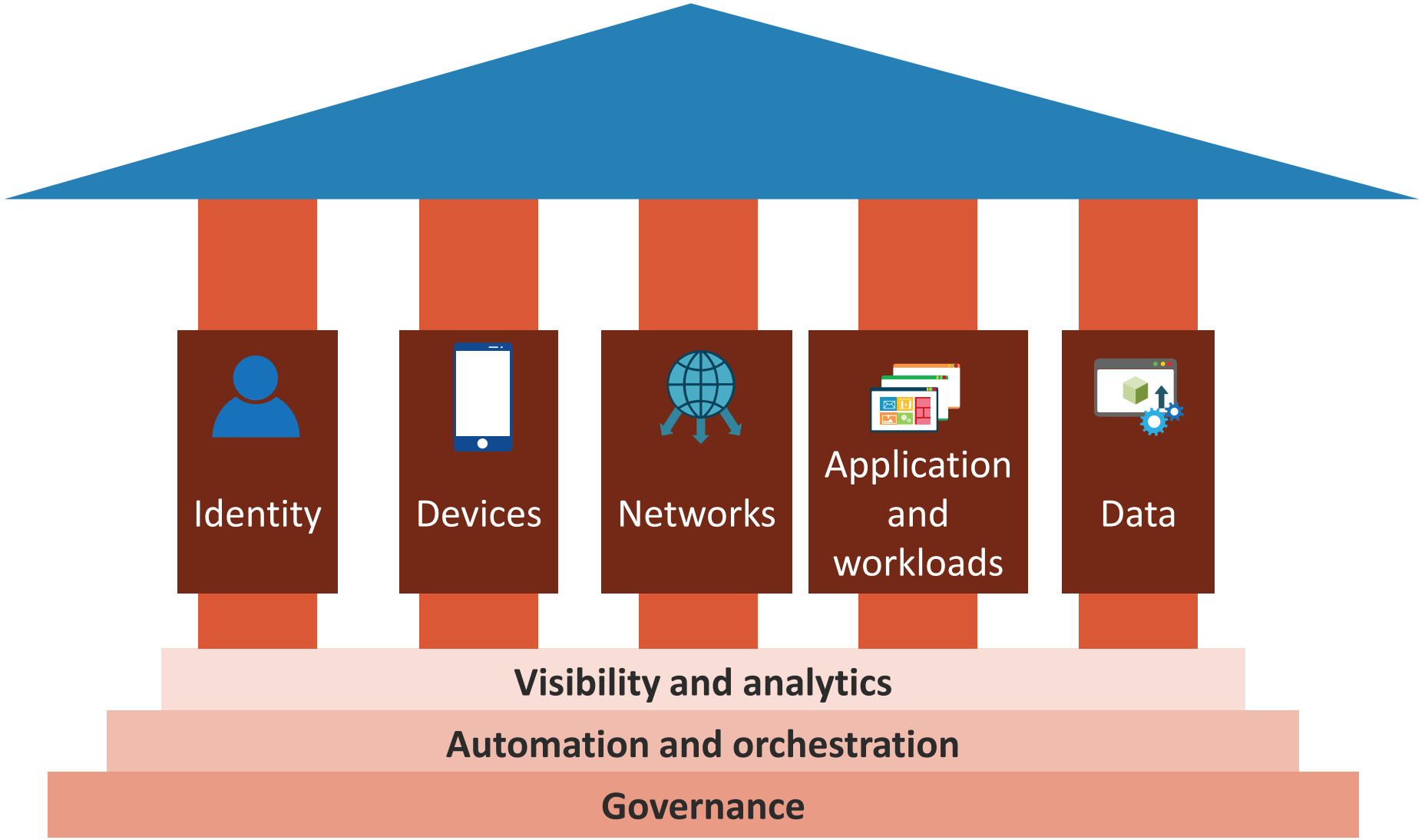
Protect
Implementing the correct level of data protection

Audit
Reporting and auditing to prove how data is used, who used it, and for what purpose

ZERO TRUST (ZT)

- The NIST SP 800-207 offers the following Zero Trust and Zero Trust Architecture (ZTA) operative definitions:
  - "Zero Trust provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised"
  - "ZTA is an enterprise’s cybersecurity plan that uses Zero Trust concepts and encompasses component relationships, workflow planning, and access policies"
  - "Therefore, a Zero Trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan"

PILLARS OF ZERO TRUST SECURITY



SEVEN TENETS OF ZERO TRUST (NIST SP 800-207)

1. All data sources and computing services are considered resources
2. All communication is secured regardless of network location
3. Access to individual enterprise resources is granted on a per-session basis
4. Access to resources is determined by a dynamic policy
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture

SECURE ACCESS SERVICE EDGE (SASE)

- The rapid increase of teleworkers, outsourcing, cloud computing, and the increasing complexity of cyber threats have driven many organizations to reassess their approach to security
- The secure access service edge (SASE) is an excellent approach that provides a unified network and security framework by integrating SD-WAN (or MAN) and cloud-native security features, such as secure web gateways (web application firewalls), cloud access security brokers, firewall-as-a-service and Zero Trust initiatives
- These solutions help modern organizations implement scalable, agile and secure network access solutions

ACCESS CONTROL MODELS

- Security models are used to determine which subjects can access resource objects
- They are typically implemented by enforcing integrity, confidentiality, origin authentication, and nonrepudiation controls
- The model designer determines how the models will be used and integrated into specific designs
- It may be done by an individual or committee
- Security is best enforced with a multilevel or hierarchical security system

COMMON ACCESS CONTROL MODELS

Access control model	Description	Example	Flexibility	Granularity	Scalability	Complexity
Discretionary access control (DAC)	User control access, simple permissions setup	File/folder permissions on a computer	Limited, controlled by users	Low, relies on user discretion	Limited, especially in larger organizations	Relatively simple
Mandatory access control (MAC)	Central access controls on labels	Government security clearance levels	Low, strictly controlled by authority	Medium, based on security labels	Moderate, suitable for specific needs	Moderate, requires careful panning
Role-based access control (RBAC)	Access assigned based on user roles	Employee roles determining access	Medium, based on predefined roles	Medium to high, role-specific permissions	Highly scalable, ideal for large orgs	Moderate, especially in role setup
Attribute-based access control (ABAC)	Access based on multiple attributes	Healthcare data access based on role, location, time	High, decisions based on various attributes	High, tailored to specific attributes	Highly scalable, accommodates dynamic needs	High, due to policy complexity

FUNDAMENTAL CONCEPTS OF MANDATORY ACCESS CONTROL (MAC) MODELS

- MAC is strictly nondiscretionary and secures data by assigning sensitivity labels, then compares labels to the level of user sensitivity
- It is appropriate for extremely secure systems, such as multilevel secure military applications
- Its main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized

FUNDAMENTAL CONCEPTS OF MANDATORY ACCESS CONTROL (MAC) MODELS

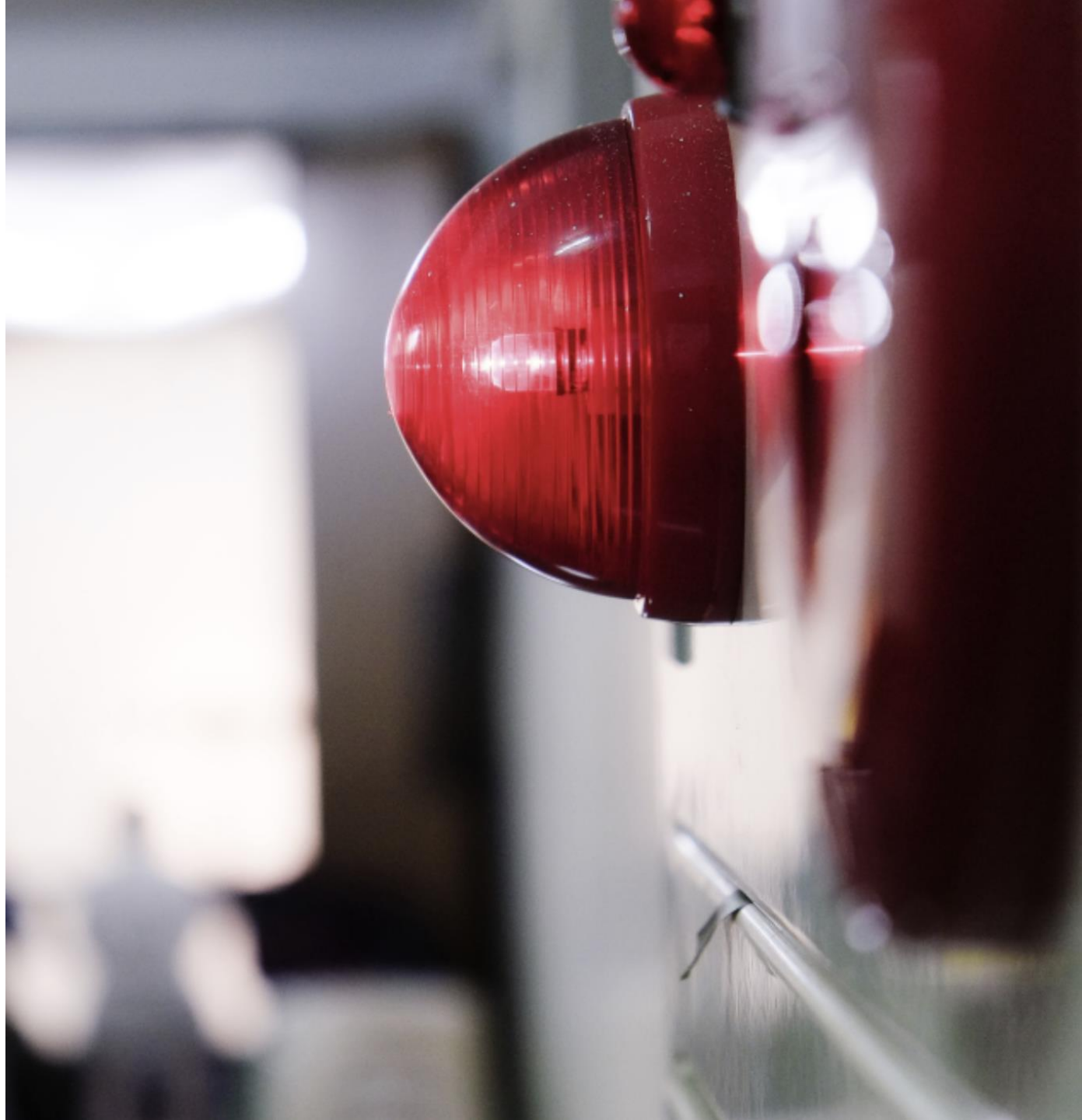
- All MAC systems evolved from the Bell-LaPadula model for confidentiality
  - This was the first mathematical model with a multilevel security policy used to define the concept of a secure state machine and models of outlined rules of access

BELL-LAPADULA MODEL

- It is a **confidentiality model** that focuses on ensuring that subjects with different clearances are properly authenticated by having the necessary security clearance, need to know, and formal access approval before accessing an object under different classification levels

BELL-LAPADULA MODEL

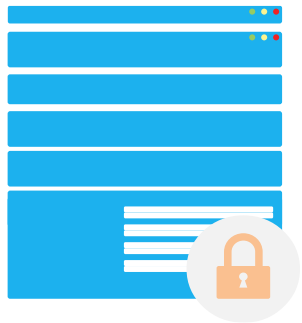
- The state of a machine is collected to verify the security of a system as it defines the behavior of a set number of states, the transitions between those states, and the subsequent actions that can take place
- A particular state typically consists of all current permissions and instances of subjects accessing objects
- If a subject can access objects only in adherence with the security policy, then the system is considered secure



BELL-LAPADULA MODEL

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

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



Strong star property rule: A subject who has read and write capabilities can only perform those functions at the same security level (nothing higher and nothing lower)

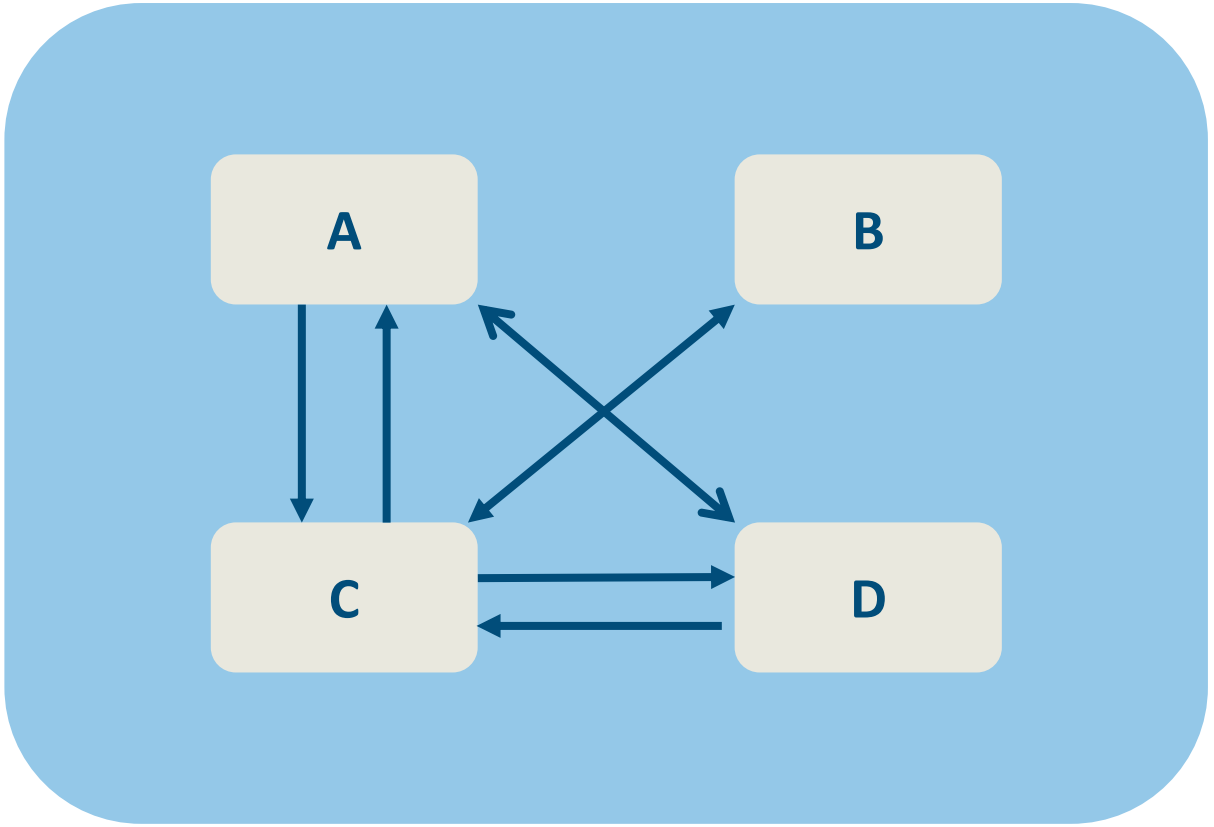
Tranquility principle: Subjects and objects cannot change their security levels once they have been instantiated/created

BIBA INTEGRITY MODEL

- Developed after Bell-LaPadula, it uses a lattice of integrity levels (unlike Bell-LaPadula)
  - **Simple integrity rule (no read-down)**: States that a subject cannot read data from a lower integrity level
  - **Star integrity rule (no write-up)**: States that a subject cannot write data to an object at a higher integrity level
  - **Invocation property**: States that a subject cannot invoke/call upon a subject at a higher integrity level
- Is also an information flow model (like Bell-LaPadula) because they are most concerned about data flowing from one level to another

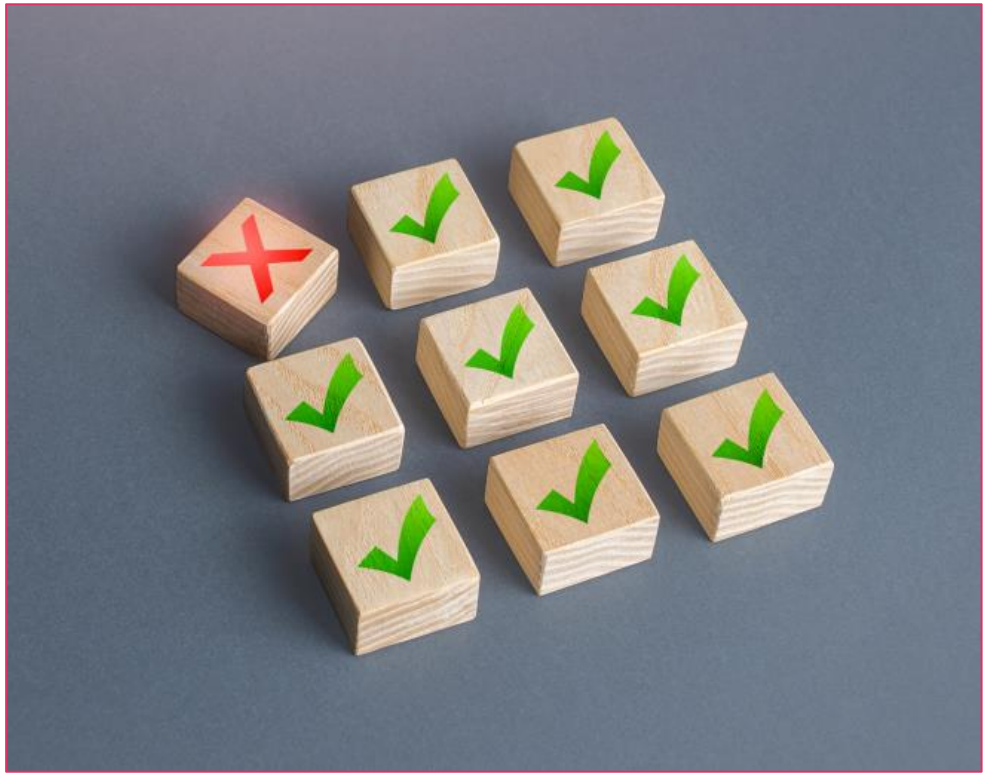
INFORMATION FLOW MODELS

Object	A	B	C	D
A	N/A		X	X
B		N/A	X	
C	X	X	N/A	X
D	X		D	N/A



CLARK-WILSON (CW) INTEGRITY MODEL

- CW was developed after the Biba model and is highly focused on information and data integrity
- Objects can be modified by subjects using read/write operations
- Integrity verification procedures (IVPs) are programs that run periodically to check the consistency of clinical documentation integrity (CDIs) – integrity rules that are usually defined by vendors



CLARK-WILSON GOALS

- To prevent unauthorized users from making any modifications
- To ensure that a segregation of duties initiative prevents authorized users from making improper modifications
- To confirm well-formed transactions
- To maintain internal and external consistency