Welcome to the CISSP Bootcamp

Your instructor:

Michael J Shannon

CISSP #42221 / #524169,
CCNP-Security, PCNSE7,
AWS Certified Security – Specialty,
GIAC GSEC, OpenFAIR, and
ITIL 4 Managing Professional

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

(ISC)² Code of Professional Ethics

All information security professionals who are certified by (ISC)² recognize that such certification is a privilege that must be both earned and maintained. In support of this principle, all (ISC)² members are required to commit to fully support this Code of Ethics (the "Code").

(ISC)² members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.

(ISC)² members are obligated to follow the ethics complaint procedure upon observing any action by an (ISC)² member that breach the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV.

"Code of Ethics: Complaint Procedures: Committee Members," Code of Ethics | Complaint Procedures | Committee Members ((ISC)², Inc, 1996), https://www.isc2.org/Ethics.

Code of Ethics Preamble

- The safety and welfare of society and the common good, duty to our principals, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior
- Therefore, strict adherence to this Code is a condition of certification

"Code of Ethics: Complaint Procedures: Committee Members," Code of Ethics | Complaint Procedures | Committee Members ((ISC)², Inc, 1996), https://www.isc2.org/Ethics.

Code of Ethics Canons

1. Protect society, the common good, necessary public trust and confidence, and the infrastructure

2. Act honorably, honestly, justly, responsibly, and legally

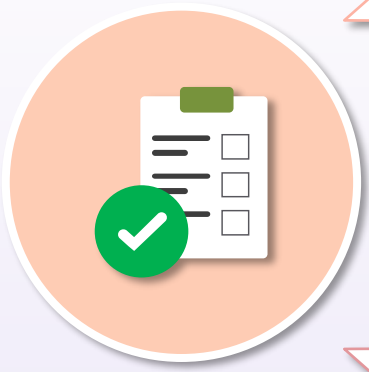
3. Provide diligent and competent service to principals

4. Advance and protect the profession

CISSP CAT Exam Information

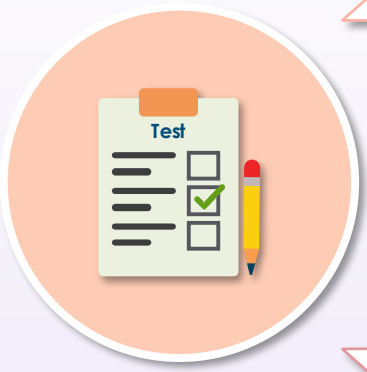
- Uses computerized adaptive testing (CAT) for all English exams
- Length of exam is 3 hours
- Multiple choice and advanced innovative item question types

CISSP CAT Exam Information



- Passing grade is 700 out of 1,000 points
- Exam language availability is English
- Authorized PPC (Pearson Professional Center) and PVTC (Pearson VUE Authorized Test Center) select Pearson VUE testing centers

CISSP Linear Exam Information



- Administered as linear, fixed-form exams
- Exam language availability is French, German, Brazilian Portuguese, Spanish-Modern, Japanese, Simplified Chinese, and Korean
- Multiple choice and advanced innovative item question types

CISSP Linear Exam Information

- Length of exam is 6 hours
- Passing grade is 700 out of 1,000 points
- Authorized PPC and PVTC select Pearson VUE testing centers

CISSP Examination Weights

Domains	Average weight
1. Security and risk management	15%
2. Asset security	10%
3. Security architecture and network security	13%
4. Communication and network security	14%
5. Identity and access management (IAM)	13%
6. Security assessment and testing	12%
7. Security operations	13%
8. Software development security	10%
Total	100%

Confidentiality

- Confidentiality measures the attacker's ability to get unauthorized data or access to information from an application or system
- Involves using techniques, often cryptography, to allow only approved users the ability to view sensitive information
- Confidential information can include passwords, cryptographic keys, personally identifiable information (PII), personal health information (PHI), intellectual property (IP), or other secret or top-secret information

High-level Confidentiality

- Uses hybrid encryption involving combinations of symmetric and asymmetric cryptosystems
- Employs advanced post-quantum and homomorphic cryptosystems
- Combines secure compartmentalization with the most recent modes of encryption available

Integrity

- Integrity measures an attacker's ability to manipulate, change, or remove data at rest and data in transit
- Involves implementing controls that make certain only authorized subjects can change sensitive information
- Might also include affirming the identity of a communication peer (origin authentication)
- Examples would be injection or hijacking attacks on data in transit, modifying files, changing access control lists, and DNS or ARP cache poisoning

High-level Integrity

The advanced goals of the Clark-Wilson model:

- Prevent unauthorized users from making modifications
- Ensure separation of duties prevents authorized users from making improper modifications
- Ensure well-formed transactions; maintain internal and external consistency

Availability

- Availability measures an attacker's ability to disrupt or prevent access to services or data
- Controls will protect systems and services from spoofing, flooding, denial-of-service (DDoS), poisoning, and other attacks that negatively affect the ability to deliver data, content, or services
- Vulnerabilities that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption

High-level Availability

Availability zones of cloud service providers

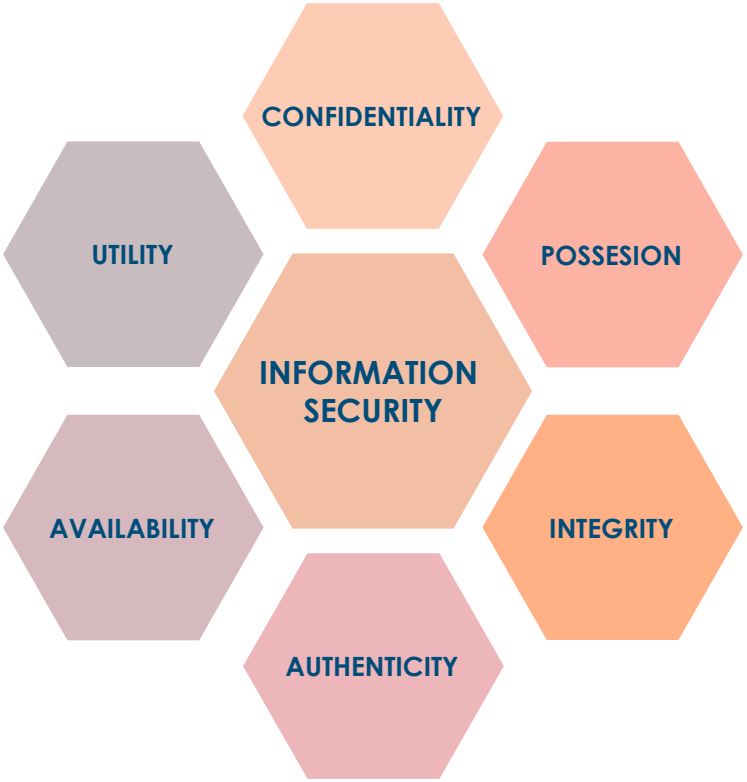
- Multiple datacenters in one
- Zones are tens of miles apart
- Connected with high-speed fiber (MANs)
- Placed in regions all over the world
- Can distribute through CDN services into metro areas

D.A.D

You can also describe the CIA goals of the security triad by looking at the opposite – D.A.D

- Disclosure is the unauthorized revealing of data and information
- Alteration is the unauthorized change or modification of data or systems
- Destruction involves rendering an entity inaccessible – can also add the element of lack of durability in some scenarios

The Parkerian Hexad



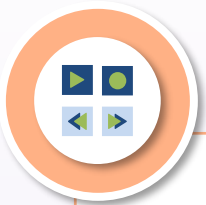
Parkerian Hexad Additions

Authenticity

Refers to the accuracy and identity of the origin of the entity or the information

Utility

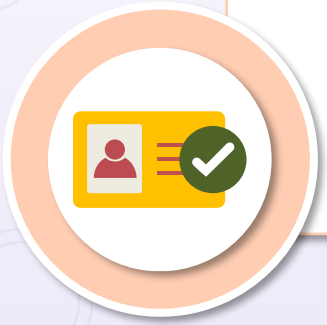
While an asset, such as data, would be confidential, controlled, integral, authentic, and available – it is not always useful or valuable in form



Possession

An attacker takes possession or control of a physical or logical asset – may still retain confidentiality

High-level Authenticity

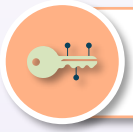


- Origin authentication is a basic form of authentication, as it only provides a degree of confidence that the correct password, passphrase, or private/secret key was used
- Additional levels of authentication rely on trusted third parties and certificates, digital signatures, and multi-factors, like biometrics
- A new trend is Knowledge-Based Authentication (KBA)

Non-Repudiation

The inability to refuse participation in a digital transaction, contract, or communication (S/MIME)

With cryptosystems a public/private key pair is used



The owner/creator of the private key must protect the key

The owner/creator of the private key must notify a trusted third party when the key is lost, stolen, or compromised

Is usually accomplished with digitally signed certificates

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	**Physical**	**Specifies connectors, data rates, and encoding bits**

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	**Link**	**Communication across a single link, including media access control**
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	**Network (or Internetwork)**	**Facilitate multihop communications across potentially different link networks**
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	**Transport**	**Connecting multiple programs on same system**
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	Presentation	Expressing and translating data formats
5	**Session**	**To accommodate multiple session connections**
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	To accomplish a networked user task
6	**Presentation**	**Expressing and translating data formats**
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	**Application**	**To accomplish a networked user task**
6	Presentation	Expressing and translating data formats
5	Session	To accommodate multiple session connections
4	Transport	Connecting multiple programs on same system
3	Network (or Internetwork)	Facilitate multihop communications across potentially different link networks
2	Link	Communication across a single link, including media access control
1	Physical	Specifies connectors, data rates, and encoding bits

The OSI Reference Model

Number	Name	Description
7	Application	HTTP, FTP, SMTP, DNS, TELNET
6	Presentation	ASCII, PNG, MPEG, AVI, MIDI
5	Session	SSL/TLS, SQL, RPC, NFS
4	Transport	TCP, UDP, SPX, AppleTalk
3	Network (or Internetwork)	IP, IPX, ICMP, ARP, BGP, OSPF
2	Link	PPP/SLIP, Ethernet, Frame Relay, ATM
1	Physical	Binary transmission, encoding, bit rates, voltages

The TCP/IP Reference Model

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

The TCP/IP Reference Model

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

The TCP/IP Reference Model

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

The TCP/IP Reference Model

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

The TCP/IP Reference Model

Number	OSI name	TCP/IP Model
7	Application	**Application**
6	Presentation	
5	Session	
4	Transport	**Transport** (host-to-host)
3	Network (or Internetwork)	**Internet** (internetwork)
2	Link	**Network Access**
1	Physical	

Least Privilege

- An aspect of AAA and IAM where the subject has just the proper level or amount of permissions and rights to perform the job role or responsibility and nothing more
- Should be built into all access control architectures
- Any deviation (escalation or elevation), if allowed, should go through an established change control IT service or service desk implementation
- Also referred to as "need to know" or staying within one's "pay grade" or classification level

NIST SP 800-53 Least Privilege

Authorize access to all security functions

Use non-privileged accounts or roles when accessing non-security functions

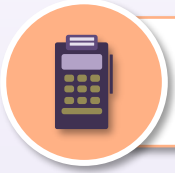
Prevent non-privileged users from executing privileged functions

Audit the execution of secure functions

ISO/IEC 27001 Least Privilege

Access to networks and network services

Management of privileged access rights



Use of privileged utility programs

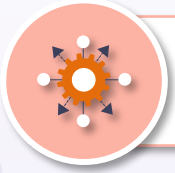
Access control to program source code

Defense in Depth (DiD)

- Also referred to as "Layered Defense"
- Using the least privilege and DiD principles is a function of "due care"
- Should be systematically planned and designed with outward-in or inward-out approach
- Can be applied to physical security or technical controls
- DiD is a common element of supply chain risk management (SCRM)

Layered Security

End-to-end layered security with several components



Can be a single appliance with multiple integrated engines

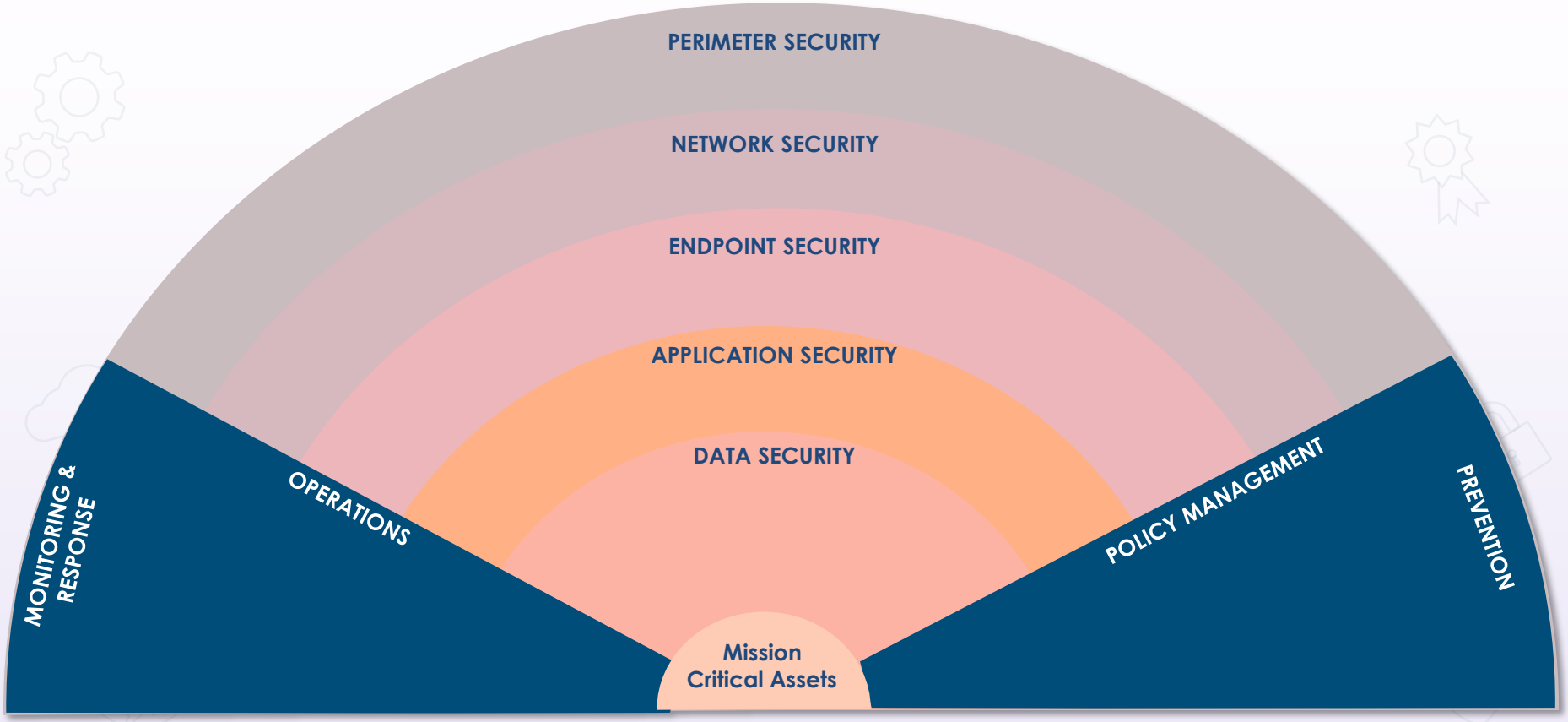
Can be physical or logical (virtual)

Applies to networks, applications, and physical

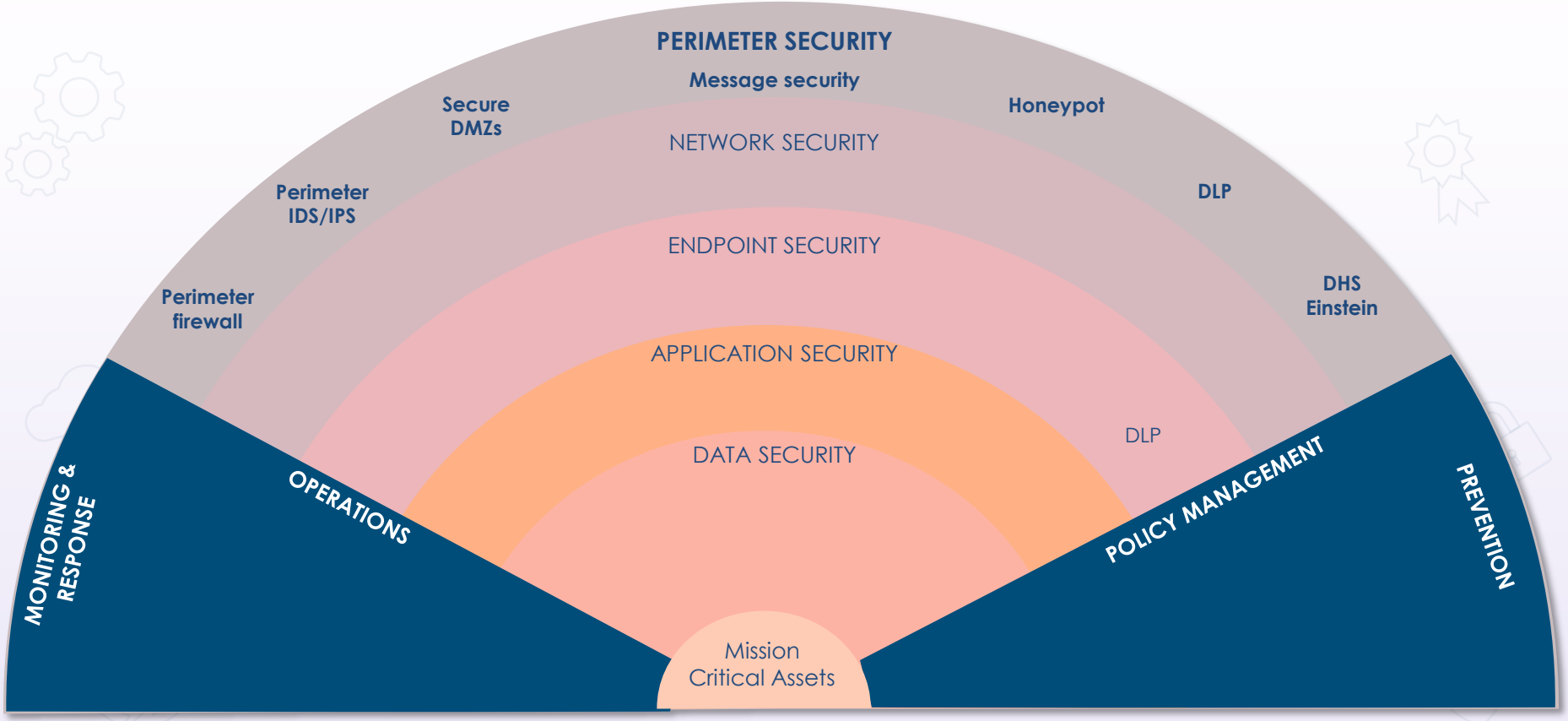
Defense in Depth Example

- The trend of de-perimeterization has increased the need for organizations protecting data and systems with DiD by implementing a combination of cryptographic schemes, more secure protocols, hardened systems, and NextGen access-control and endpoint protection services
- No longer totally depends on its DMZ/PAZ network boundary to the Internet and the various ISPs and ITSPs – basically removing the perimeter, or outer security boundary

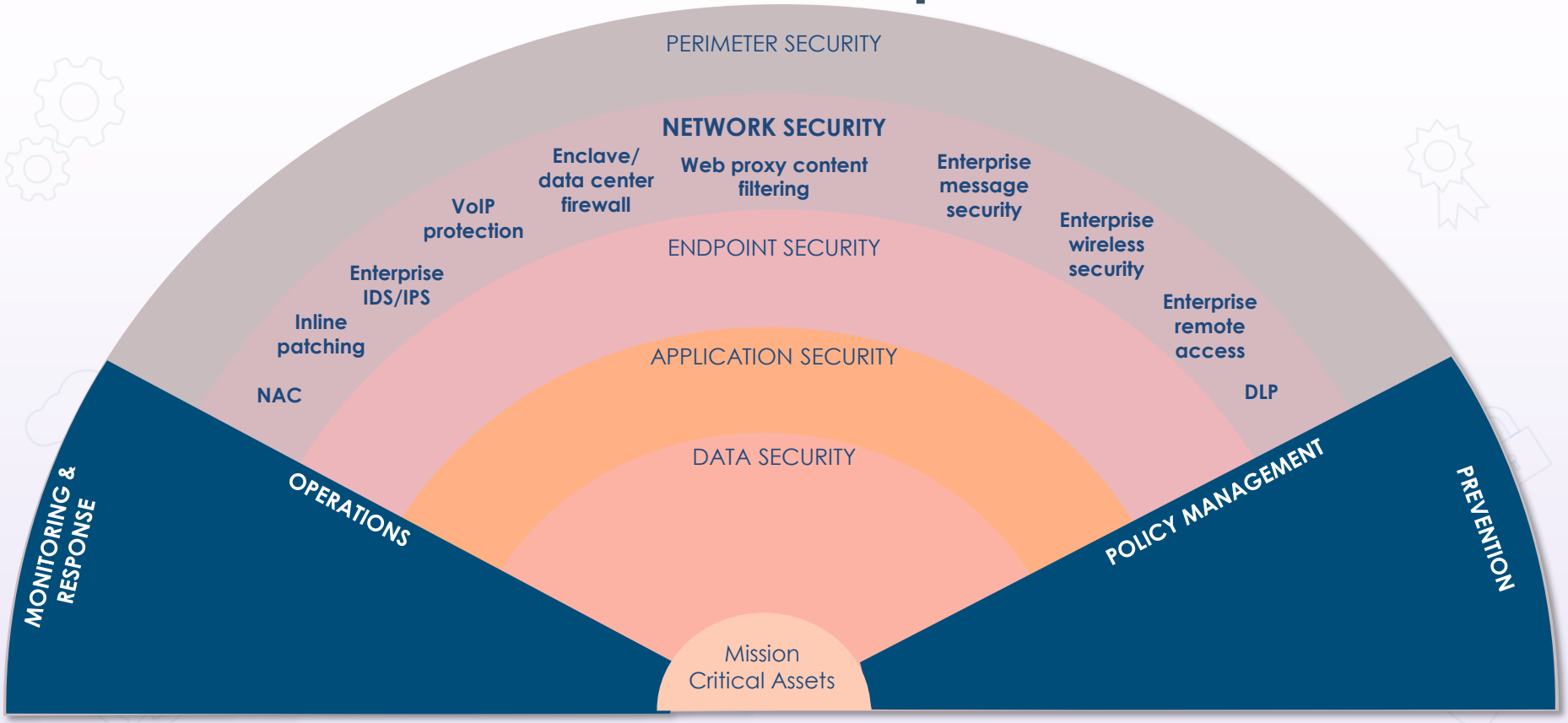
Defense in Depth



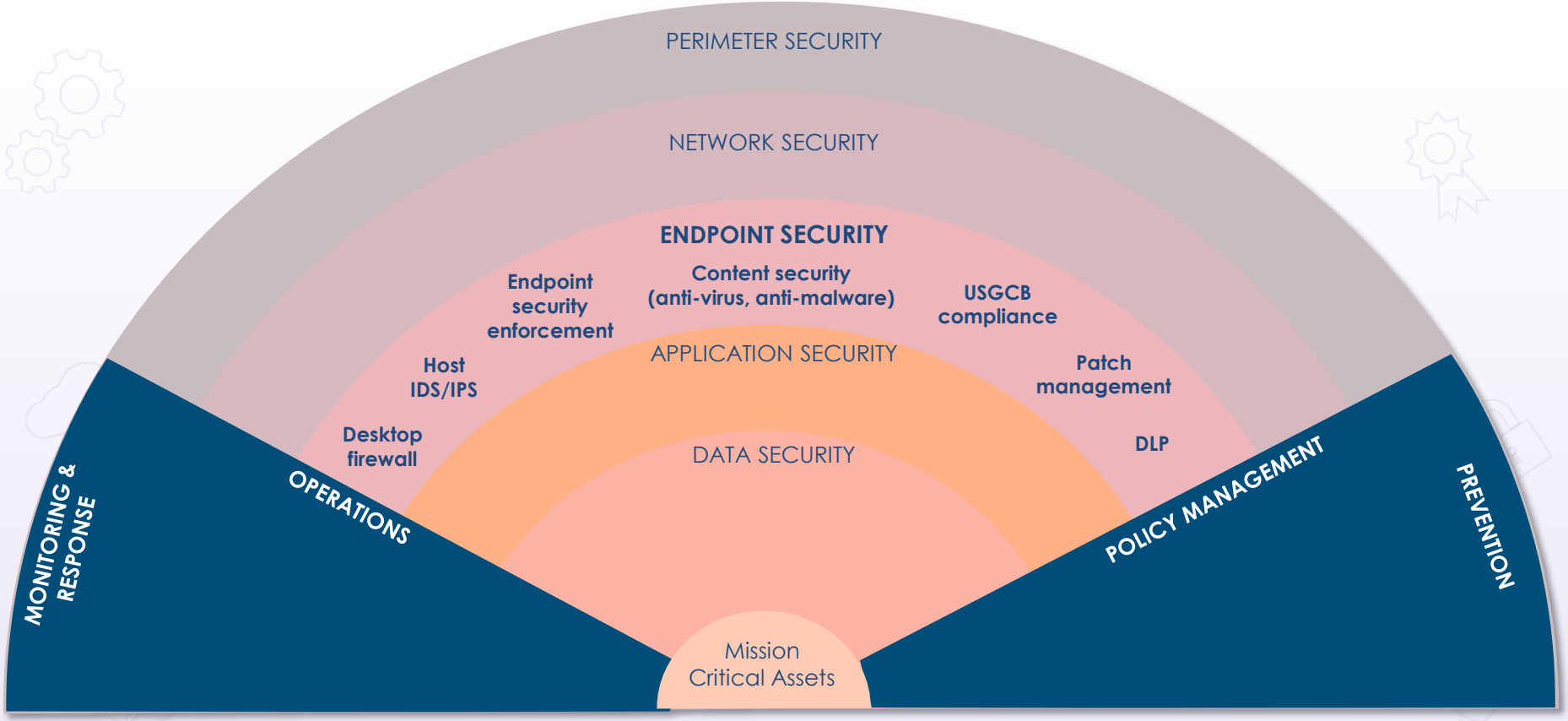
Defense in Depth



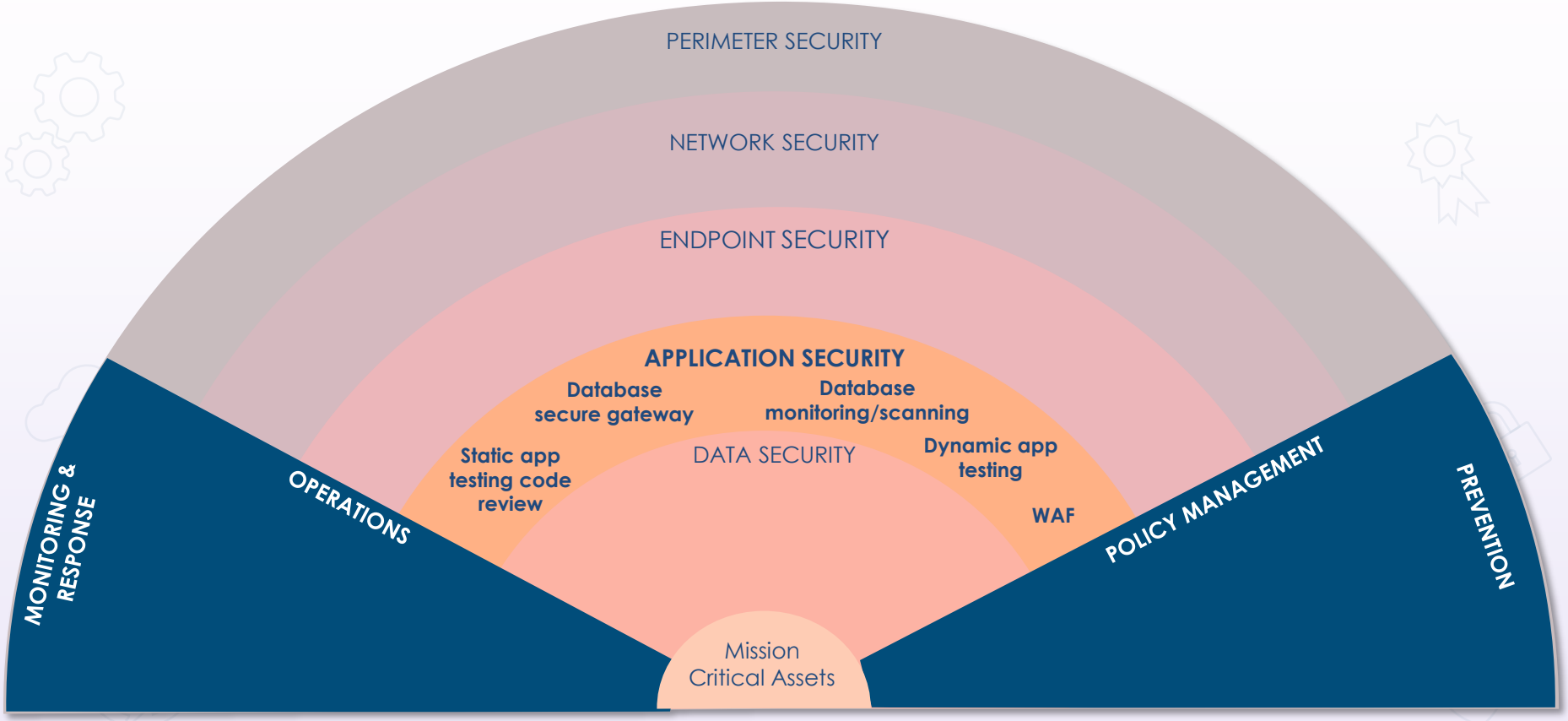
Defense in Depth



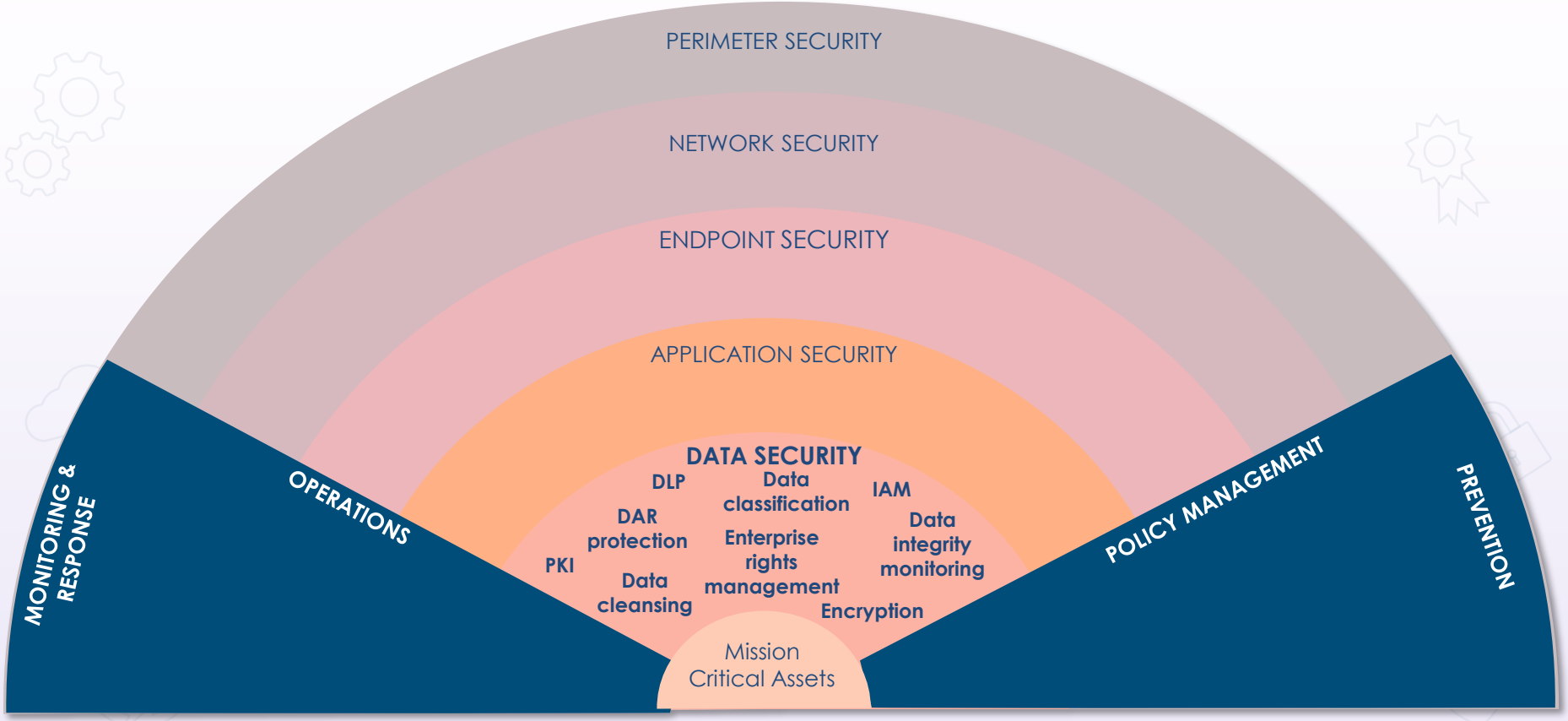
Defense in Depth



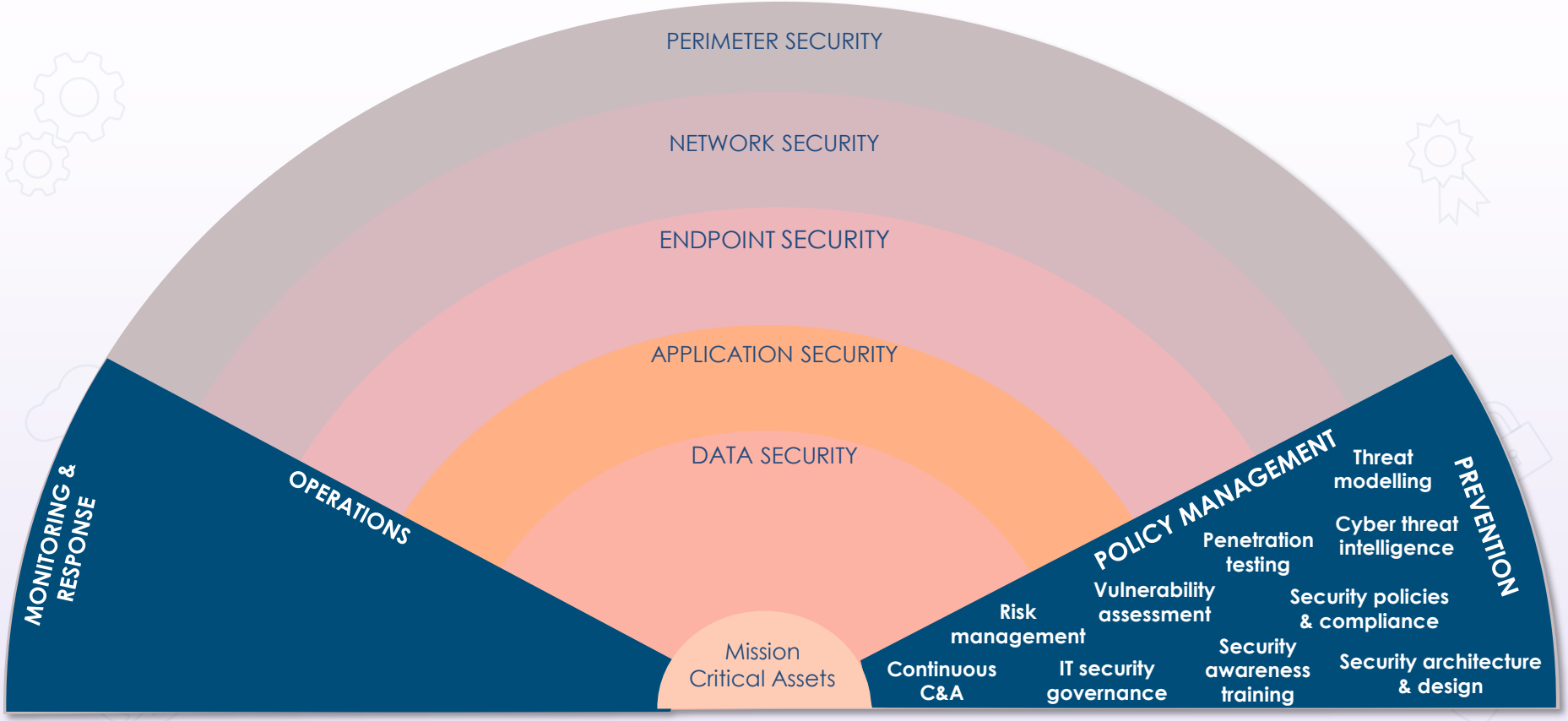
Defense in Depth



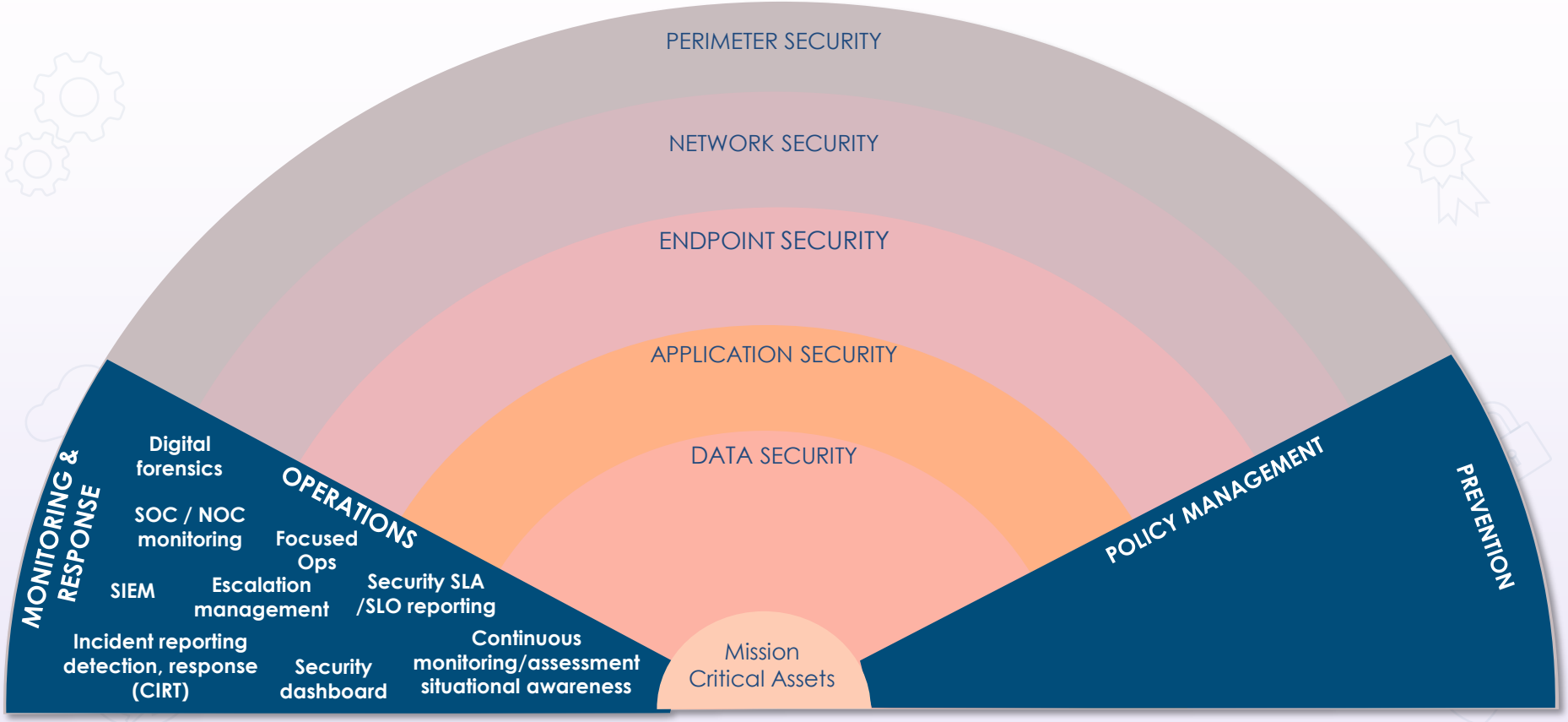
Defense in Depth



Defense in Depth



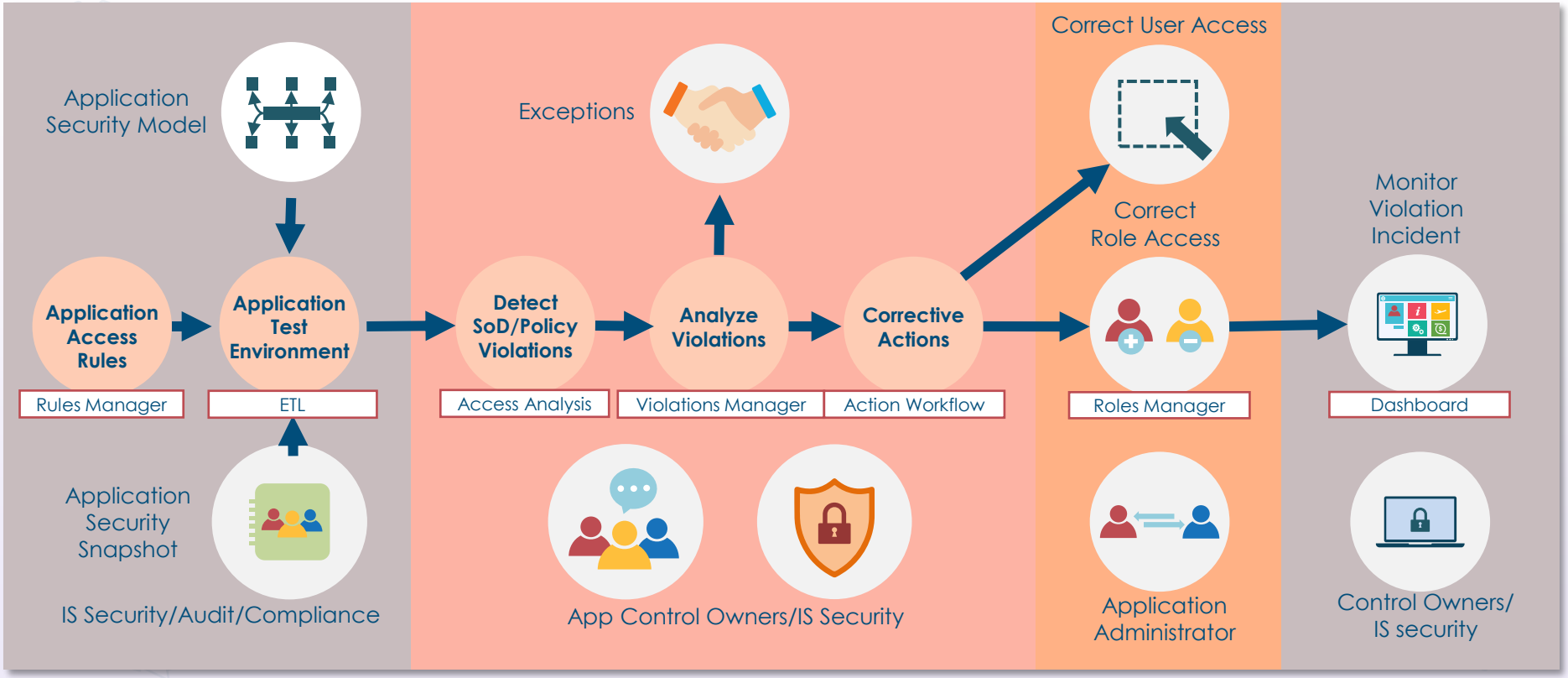
Defense in Depth



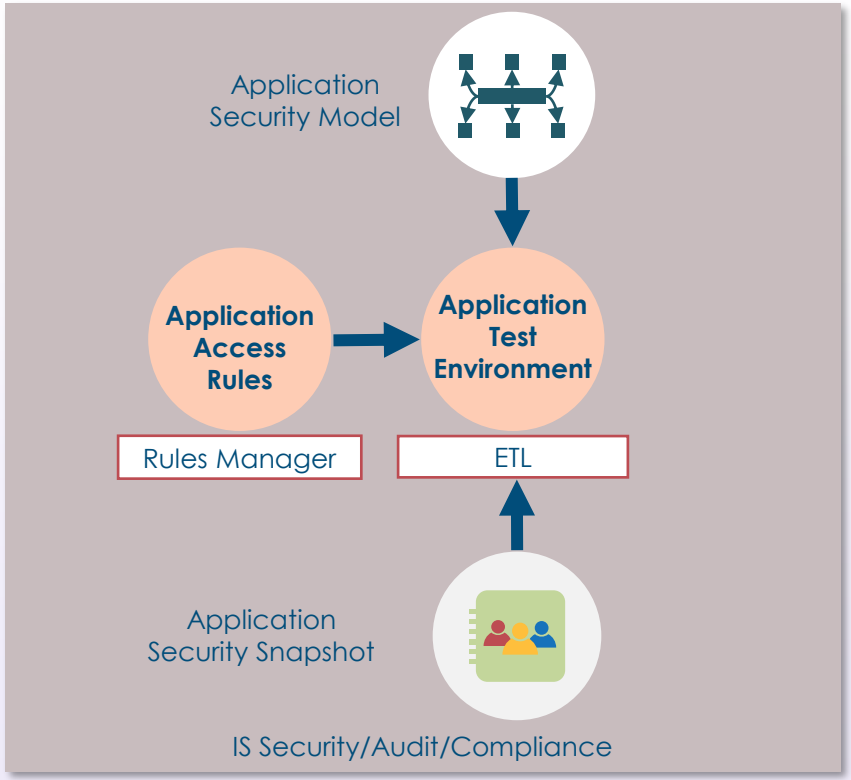
Separation of Duties (SoD)

- Also referred to as "segregation of duties"
- A principle where more than one entity is required to complete a particular task such as a separate Backup Operators group and a Data Restoration group
- SoD may also involve dual operator principles where two or more subjects are needed to modify or approve
    - Example: two signatures or cryptographic keys are required for certain actions
- Rotation of duties is also a related principle
    - Example: mandatory time-off or forced vacations

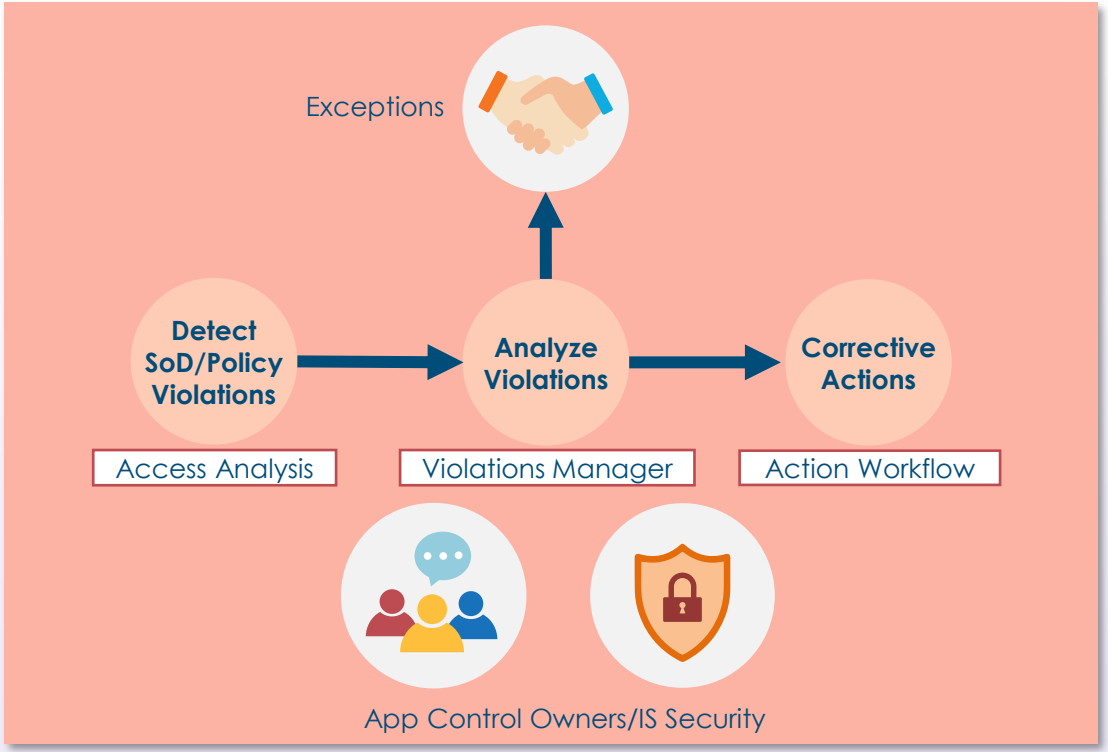
Separation of Duties Example



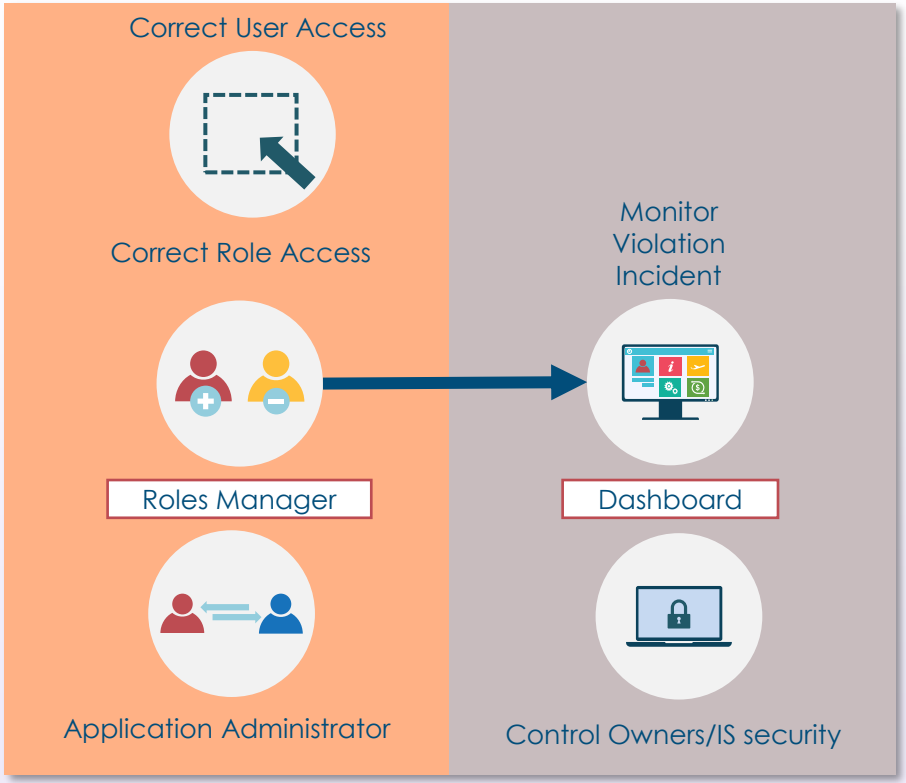
Separation of Duties Example



Separation of Duties Example



Separation of Duties Example



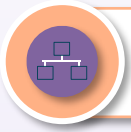
Keep it Simple

- Security practitioners must always find the delicate balance between securing and protecting data, applications, and systems while maintaining user productivity, business synergies, and delivery of the value proposition
- Over-complexity can often lead to configuration errors
- Example: too complex of a password policy will create vulnerability
    - **Bizarre-Spandex-Dolphin** would take a computer about 7 hundred sextillion years to brute force crack
    - **W$g8*bK2y5Dz7** would take about 2 million years to crack

Zero Trust

Is an evolving paradigm moving focus to users, assets, and resources

Uses zero trust principles to design industrial and enterprise infrastructure and workflows

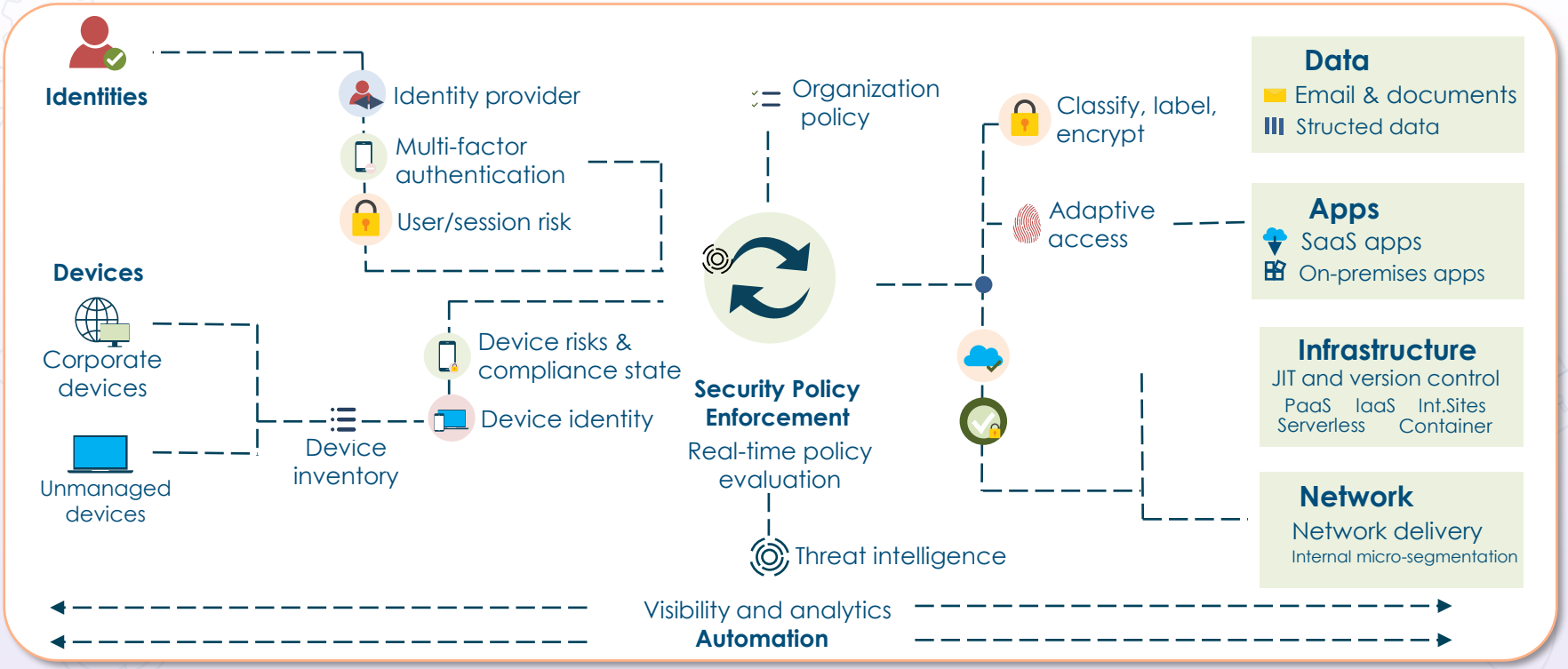


Assumes no implicit trust given to subjects based merely on their physical or network location

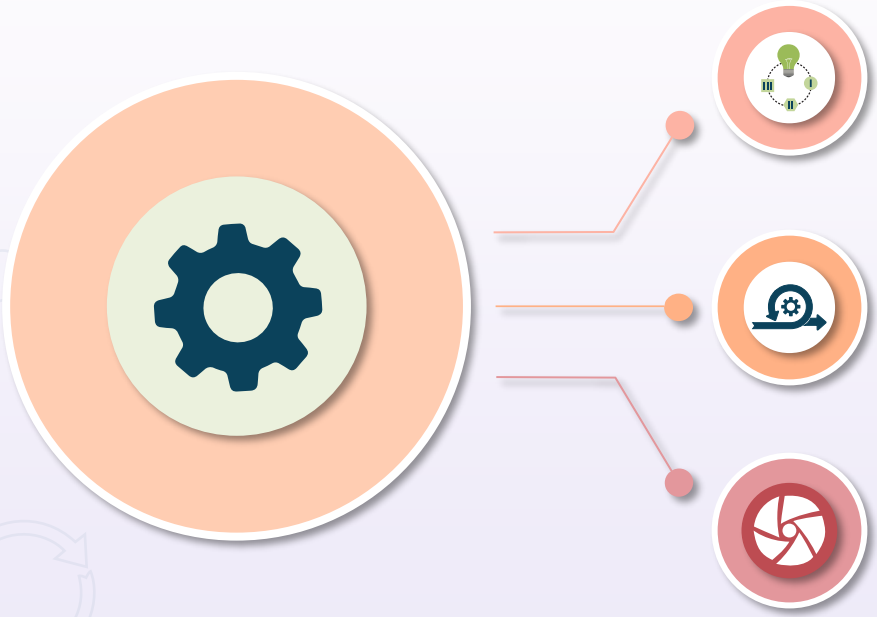
Performs authentication and authorization as distinct tasks before a session is established

Focuses on protecting resources and not network segments or location

Zero Trust Architecture



Secure Defaults



Secure by design

Program or application is developed with security integrated into the entire software development life cycle (SDLC)

Secure by deployment

Deployed into an environment where security is highly considered in the network and system design

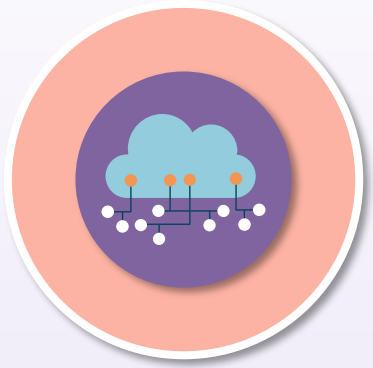
Secure by default

Design consideration assumes that the application is natively secure without any modifications or extra controls

Secure Defaults

- The existing default configuration settings are the most secure possible
- Often delivered using Infrastructure as Code
- Often not the most productive or user-friendly
- Can be native to the platform or policy-based
- Can involve other principles like compartmentalization and mediated access

Example: Microsoft Azure Security Defaults



- Require all users to register for Azure AD Multi-Factor Authentication
- Require administrators to perform multi-factor authentication (MFA)
- Block legacy authentication protocols
- Require users to perform multi-factor authentication when necessary
- Protect privileged activities such as access to the Azure portal

Fail Securely

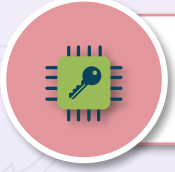
- Involves the implementation of a mode of system termination functions that prevents loss of the secure state when a failure occurs or is detected in the system or application
- The failure still might cause damage to some system resource or system entity

Fail Securely

Implement secure defaults to deny access

Deploy failure undo changes or rollback to secure state

Check return values and conditional code/filters for failure defaults



Ensure that even with loss of availability, confidentiality and integrity remain

Fail Open vs. Fail Closed Firewalls

Fail open

If there is a component failure or system crash of a firewall or IPS sensor, the traffic is still allowed to flow from the ingress interface to the egress interface in order to prevent inconvenience to users or productivity of data flows

Fail closed

If there is a component failure or system crash of a firewall or IPS sensor, the traffic is NOT allowed to flow from the ingress interface to the egress interface in order to prevent an attacker from launching an exploit by forcing a failure

Privacy by Design

- Individuals do not always understand the possible consequences for their privacy when they interact with applications, systems, products, and services
- Failure to design for privacy can have direct negative effects at both the individual and societal levels affecting
    - an organizations' brands
    - the financial bottom line, and
    - future prospects for growth

NIST Privacy Framework

NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management, Version 1.0

A voluntary toolkit developed in partnership with various industry stakeholders

Envisioned to assist organizations in identifying and managing privacy risk

Goal is to protect individual privacy

Helps to build innovative products and services

Privacy by Design

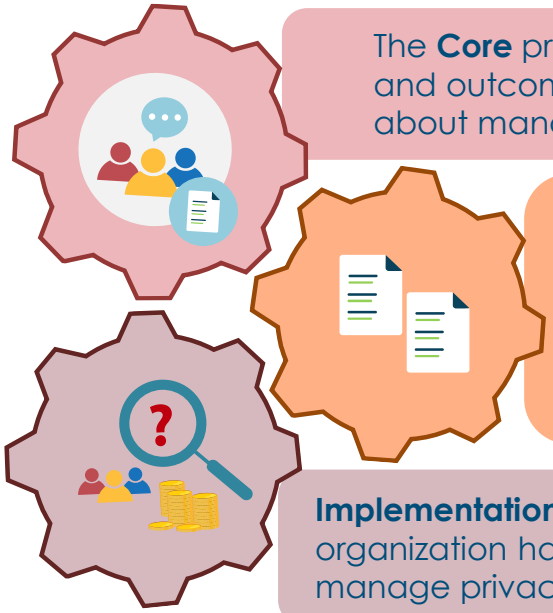
Taking privacy into account as you design and deploy systems, products, and services that affect individuals

Realizing that privacy issues can be different when dealing with other countries and jurisdictions (General Data Protection Regulation, or GDPR)

Communicating about your organizational privacy practices with all stakeholders

Encouraging cross-organizational workforce collaboration by developing profiles, selection of tiers, and achievement of outcomes

NIST Privacy Framework



The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles are a selection of specific functions, categories, and subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its target profile

Trust but Verify

- This is not a "zero trust" approach to security but does introduce stronger identification mechanisms
- To fulfill an MFA "something you have" prerequisite, we continue to deploy physical tokens that generate different one-time passwords (OTPs) every 60 seconds or with mobile phones using OTPs being sent as text messages
- Mobile malware can intercept these messages and forward them to fraudsters.
- This rising threat has driven NIST to recommend moving away from SMS-based OTPs

Trust but Verify

- The advanced verification comes in the form of more stringent multi-factors such as biometric authentication
- Vendors offer identity and access management solutions with identity analysis for attribute-based access control (ABAC)
- May eventually lead to expanded usage of user behavioral analytics (UBA) and artificial intelligence (AI) to enhance and improve the "trust but verify" model in certain environments

Aligning Security with Business

- A security practitioner must align all security functions to a business's strategy, value proposition, charters, goals, mission, and objectives
- This alignment must permeate through all organizational processes including governance, steering committee charters, and corporate initiatives to name a few
- Security strategists must account for any major changes to organizational operations or activity

Security Must React to Changes

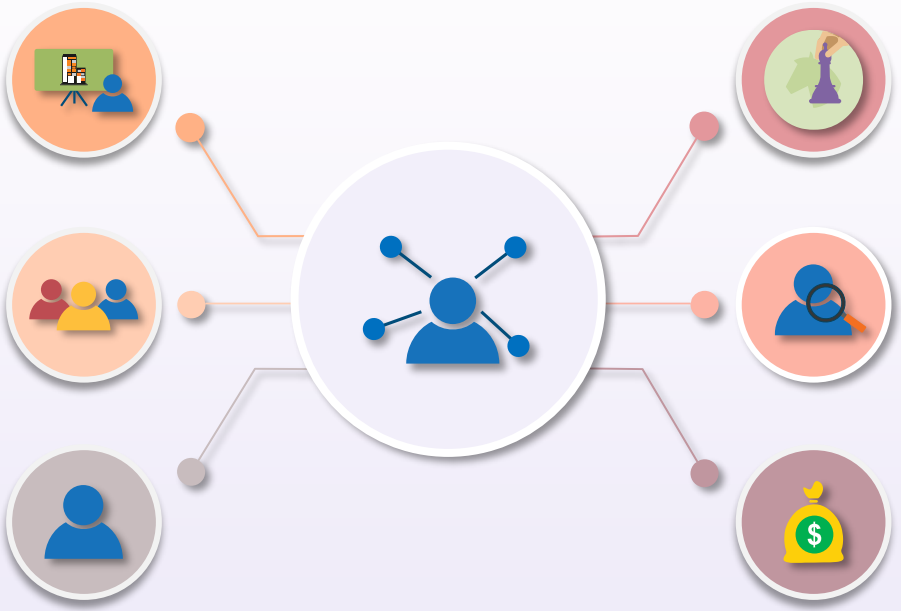
Mergers are a deal to join two existing companies into one new ongoing enterprise

Divestitures and de-mergers involve cleaning up access rights, identity information, and data loss prevention

Legal ramifications such as dark periods may have to be enforced

Privacy issues, data sharing, and interconnection agreements may be involved with a change to business operations

Internal Influences to Consider



External Influences to Consider

Organizational Roles, Responsibilities, and Processes

- Security initiatives require a broad awareness of organizational roles and responsibilities
- Companies are organized in different ways, such as top-down, flat, or outsourced
- Directory services are often closely aligned and mapped to organizational duties and job titles
- Roles and responsibilities will often directly affect access control methodologies and sensitivity levels for mandatory access architectures

Responsibilities Can Drive RBAC Methods

- With role-based access control (RBAC), access decisions typically rely on organizational charts, roles, responsibilities, or locations in a user base
- The role is often set based on evaluating the essential objectives and architecture of the enterprise aligned with the subject's job title and responsibilities
- The security practitioner must be aware of these details

Data and Asset Ownership

- Are often the creators in a Discretionary Access Control (DAC) model
- Determine the classification level
- Decide on handling and tagging (labels)

Data and Asset Ownership

- Manage assets from a business perspective
- Often deal directly with customers (internal and external)
- Ensure compliance (standards and controls) and data quality

Data and Asset Ownership

Maintain the assets from a technical perspective

Often deal directly with stakeholders and management

Ensure confidentiality, integrity, authenticity, and availability of data and assets

Data and Asset Ownership

- Chief Information Officer (CIO)
- Chief Privacy Officer (CPO)
- Chief Information Security Officers (CISO)

Due Diligence

- Due diligence relates to the act of performing thorough research before committing to a particular plan of action
- It involves proper information gathering, planning, testing, and strategizing before development, production, and deployment
    - Comprehensive background check practices for hiring
    - Investigating a cloud service provider (CSP) thoroughly before signing a memorandum of understanding (MOU)
    - Testing and evaluating nonrepudiation techniques (digital signatures) before signing contracts or using code

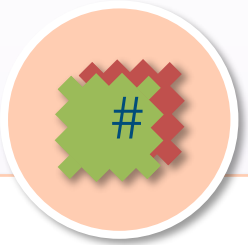
Due Diligence

- Often involves understanding which framework is required by law or is applicable under vendor due diligence
- For example, how federal agencies adhere to security mandates when Controlled Unclassified Information (CUI) must reside in a nonfederal system and organization
- Relates to supply chain security as well

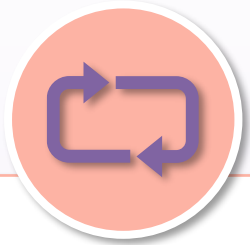
Due Care

- Refers to the degree of attention that a reasonable person takes for a particular entity
- Is the level of judgment, attention, and activity that a person would engage in under similar circumstances
- Refers to ongoing activities

Due Care Activities



Performing the necessary maintenance and patch management to keep a system or application available and secure



Taking all the necessary precautions to ensure that an IP packet arrives with CIA properly applied using various controls

Using security principles like least privilege, defense in depth, SoD, zero trust, and more for continual improvement and maturity

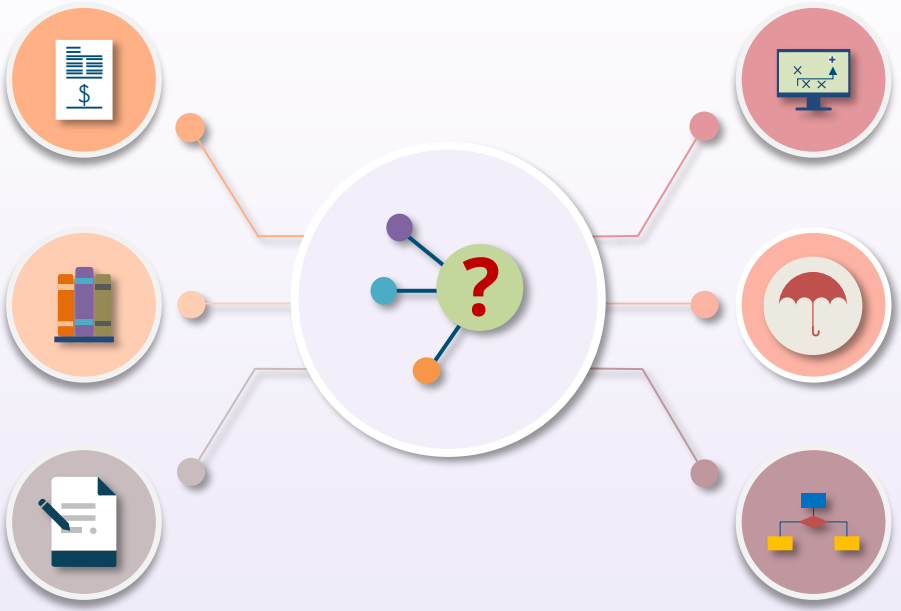
Governance

- The need for governance exists anytime a group of people comes together to accomplish an end
- Typically focuses on three attributes or characteristics:
  - authority
  - decision-making, and
  - accountability
- Is focused on the structure and processes for sound decision-making, accountability, management, and conduct at the top of an organization
- It directs how an organization's objectives are determined and achieved, how risk is controlled and addressed, and how the delivery of value is improved

Security Governance

- Is broadly defined as the rules that protect the assets and continuity of an organization
- It includes mission statements, charters, declarations of value propositions, policies, standards, and procedures
- Guides the course and control of organizational security operations, initiatives, and activities
- The security practitioner's strategy will be derived from effective security governance

Security Governance Activities



Compliance and Other Requirements

- Compliance is defined as observing a rule, such as a policy, standard, specification, or law
- Regulatory compliance outlines the goals organizations want to accomplish to certify that they understand and take actions to comply with policies, relevant laws, and regulations
- For example, companies that provide products and services to the U.S. federal government must meet certain security directives set by NIST
- Specifically, NIST SP 800-53 and SP 800-171 are two common mandates with which companies working within the federal supply chain may need to comply

Compliance Policy Requirements

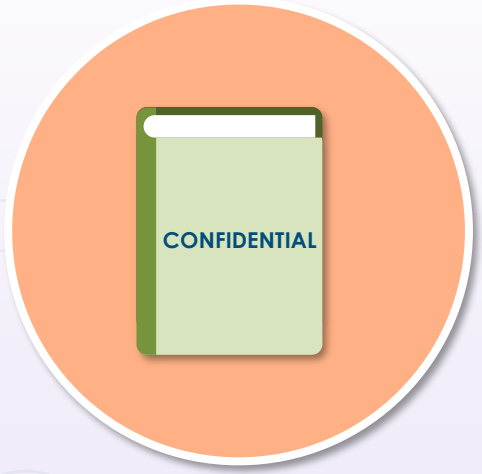
Security governance is often responsible for publishing all compliance and regulatory requirements for the organization

- All personnel compliance and remediation initiatives should be tracked and recorded in a compliance database
- There should be guidelines for using special compliance scanners for finding user vulnerabilities
- The risk register (or ledger) can also be used to help fulfill compliance policy requirements

Privacy Policy Requirements

- Describe controls to protect intellectual property (IP), personally identifiable information (PII), personal health information (PHI), and other sensitive data from data leakage, loss, and breaches
- Often needed to assure adherence to regulations such as the Computer Fraud and Abuse Act, Electronic Communications Privacy Act, and the Identity Theft and Assumption Deterrence Act
- For example, for the avoidance of penalties from GDPR:
  - The first is up to €10 million or 2% of the company's global annual turnover of the previous financial year, whichever is higher
  - The second is up to €20 million or 4% of the company's global annual turnover of the previous financial year, whichever is higher

Data Privacy



Privacy protection is often mandated in regulations or industry compliance standards such as HIPAA or PCI-DSS

- Identify all data owners and processors
- Discover incidents of data remanence (physical attributes or artifacts of data that can remain on a storage device)
- Implement collection limitation
- Policy that allows collected PII and PHI to be scrubbed before sharing with a research institute or healthcare community cloud
- Introduce data loss prevention (DLP) engines

Intellectual Property (IP)

- The global shift towards service-oriented enterprises has enlarged the role of intangible assets and intellectual property
- The need for protection and control of data loss and leakage has increased drastically

Intellectual Property (IP)

- Copyrights and trademarks
- Patents and formulas
- Trade secrets and marketing campaigns
- Digital rights and licenses
- Cryptographic keys and passwords

Privacy and Data Breach Consequences

Primary and secondary loss

- Productivity
- Response
- Replacement
- Fines and judgments
- Competitive advantage
- Reputation

Digital Rights Management (DRM)

- 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

Example: Digital Rights Management for PDFs

Manage document usage	Deny unauthorized sharing	Stop screen captures or printing to files	Enforce expiration	Revoke access based on least privilege
Restrict to specific IP CIDR ranges	Watermark PDF files	Track document usage	Integrate with command-line interface for usage	Integrate with e-commerce solutions

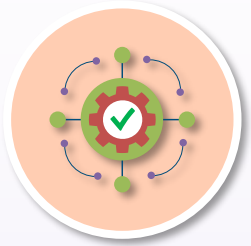
Data Minimization for Privacy

- A directive that states that collected and processed data should not be used or kept unless it is critical to operations
- The details should be determined early in the lifecycle to support data privacy standards such as GDPR

Tokenization for Privacy Enhancement

- Data tokenization is a technique used to remove directly identifying elements
- The process replaces the raw data with randomly generated tokens (or pseudonyms)
- It is most often deployed with structured data like card numbers and national identifying numbers (SSN)
- In order to comply, the original data does not leave the enterprise – even to a cloud service provider
- Tokenization can be combined with encryption to achieve further defense in depth

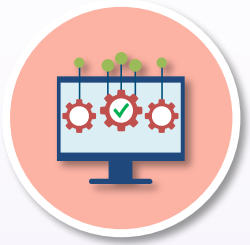
Security Control Frameworks



ISO/IEC 27000

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

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



NIST Special Publication 800-53 Revision 4

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

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

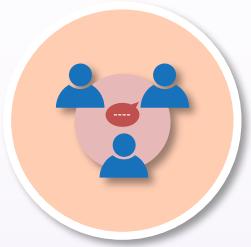
Is very good for large businesses, as well as those with a US connection

COBIT 5

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

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

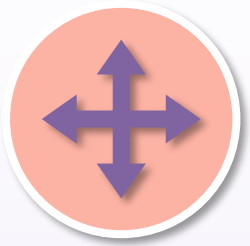
Security Control Frameworks



AGATE

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

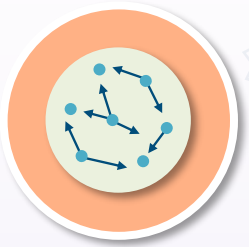
A framework for modeling computer or communication systems architecture



IDABC

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

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



OBASHI

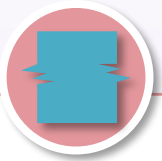
OBASHI provides a method for capturing, illustrating, and modeling the relationships, dependencies, and data flows between business and information technology assets and resources in a business context

Cybercrime Issues

Organizations will face cyber threats in three main areas

Disruption

Cybercriminals will use new ransomware to seize the Internet of Things (IoT)



Distortion

Spread of misinformation by bots and automated sources will cause a compromise of trust

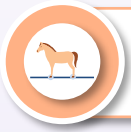
Deterioration

Advances in smart technology will negatively impact an enterprise's ability to control information

Cybercrime Issues

AI-enhanced adaptive malicious software

AI fuzzing to start, automate, and accelerate zero-day attacks



Machine learning poisoning Trojans and backdoors

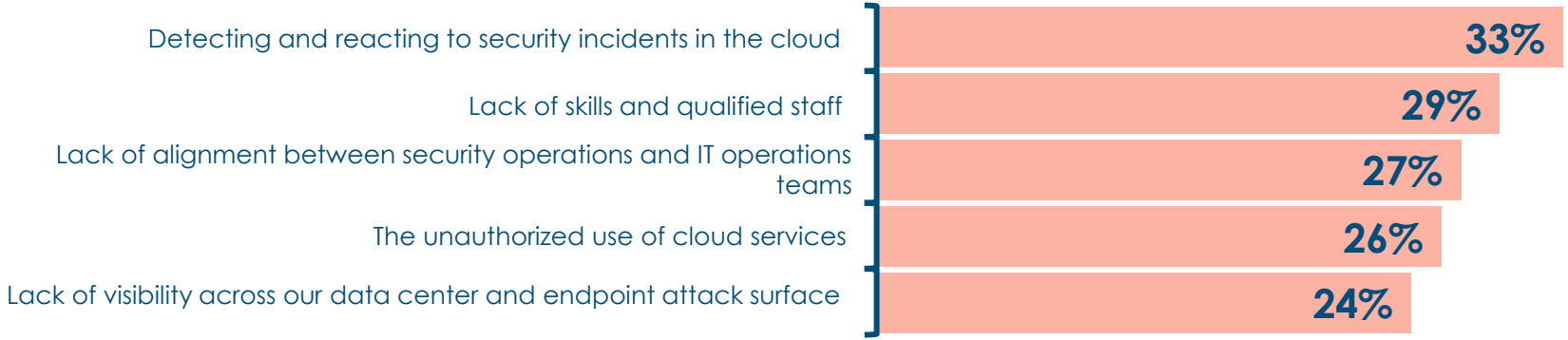
Hacking smart contracts based on buggy deployment

Vulnerabilities of cloud computing

Cybercrime Issues

What are the biggest cybersecurity challenges currently experienced by your organization today?

(Percent of respondents, N=456, three responses accepted, five most frequently reported challenges shown)



"Oracle and KPMG Cloud Threat Report 2019." Accessed April 6, 2021. https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf.

Cloud Security Challenges

Which of the following represents the biggest cloud security challenges for your organization?

(Percent of respondents, N=456, five responses accepted, seven most frequently reported challenges shown)

"Oracle and KPMG Cloud Threat Report 2019." Accessed April 6, 2021. https://www.oracle.com/a/ocom/docs/dc/final-oracle-and-kpmg-cloud-threat-report-2019.pdf.

Data Breaches

- The most common cyber attacks used to externally perform data breaches are ransomware, malware variants, phishing, and Denial of Service (DoS/DDoS) botnets
- The most common internal threat is the personally compromised privileged insider

Data Breaches

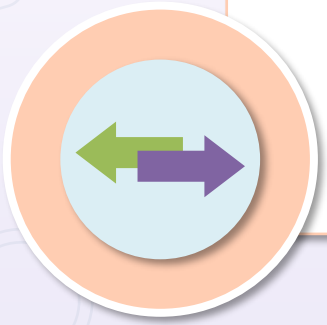
- Data breaches have become more widespread primarily due to cloud computing and the increased use of digital storage
  - Social media breaches accounted for 56% of data breaches in the first half of 2018 (IT Web)
  - Over the past 10 years, there have been 300 data breaches involving the theft of 100,000 or more records (Forbes)
  - The U.S. had 1,244 breaches in 2018 and 446.5 million exposed records (Statista)
  - Data breaches exposed 4.1 billion records in the first six months of 2019 (Forbes)
  - As of 2019, cyber-attacks are considered among the top five risks to global stability (World Economic Forum)

Licensing Issues

Security professionals must be familiar with the issues involving software licensing and agreements

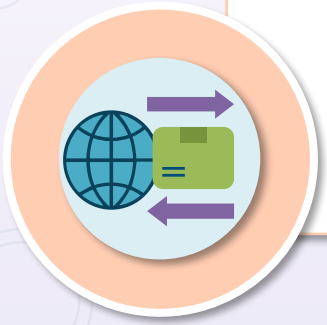
- Contractual license agreements
  - Written contracts and digitally-signed
- Shrink-wrap license agreements
  - Written on packaging
- Click-through license agreements
  - During install
- Cloud service provider license agreements
  - Depends on managed service

Import and Export Issues



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

Import and Export Issues



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

Trans-border Data and Information Flow

- Considerations should always include the flow of data, information, and goods across international borders and all legal and regulatory implications
  - These issues can change rapidly based on various geo-political factors
- Security initiatives must also consider variances in cultural norms
  - Customs, sensitivities, and behaviors (for example, European vs. Asian customs)
- Policies, controls, and procedures can differ based on region
  - Countries are typically under different regulations and mandates
  - AGATE, IDABC, OBASHI, ITIL, ISO, or TOGAF
- The Department of Commerce's Bureau of Industry and Security (BIS) controls nonmilitary cryptographic exports
- Cloud computing is transcending traditional boundaries and jurisdictional barriers and introducing new challenges

Policy Development and Implementation

- Policies, specifically security policies, establish a general framework within which to work and a guiding direction to take in the future
- The function of a policy is to classify guiding principles, direct behavior, and offer stakeholder guidance and a security control implementation roadmap.
- An information security policy is a directive that outlines how an enterprise plans on protecting its data, applications, and systems
- It helps ensure compliance with legal and regulatory requirements and preserve an environment that sustains security principles
- Policy documents are high-level overview publications that guide the way in which various controls and initiatives are implemented

Developing an Information Security Policy

Policies That Change Based on New Technologies

- IoT hardware authentication policies
- User Behavioral Analytics (UBA) policies
- AI and machine/deep learning policies
- Cloud provider interaction policies
- Enterprise mobility management policies

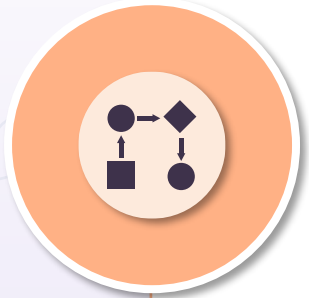
Standards

- Standards allow an information technology staff to be consistent and systematic
- Standards specify the use of specific technologies in a uniform way, because no one individual practitioner can know everything
- They also help to provide consistency in the enterprise, because it is unreasonable to support multiple versions of hardware and software unless necessary
- Standards are usually mandatory, and the most successful IT organizations have standards to improve efficiency and keep things as simple as possible

Guidelines

- Guidelines provide a list of suggestions on how one can do things more effectively
- They are similar to standards but are more flexible and not usually mandatory, as they are used to define how standards should be developed or to guarantee adherence to general security policies
- Some of the best guidelines available are in repositories known as "best practices"
  - NIST Computer Security Resource Center
  - NSA Security Configuration Guides
  - Center for Internet Security (CIS) Top 20

Procedures (Processes and Practices)



- Procedures are usually required although they are the lowest level of the policy chain
- Procedure documents are longer and more detailed than standards and guidelines documents
- Procedure documents include implementation details, usually with step-by-step instructions and graphics
- Procedure documents are extremely important for helping large organizations achieve the consistency of deployment necessary for a secure environment
- Procedures are also known as practices

Standard Operating Procedures (SOPs)

- Step-by-step instructions that define how workers carry out routine tasks
- Can greatly improve
  - efficiency
  - quality
  - performance
  - communication, and
  - compliance with regulations

SOP Considerations

Describe purpose and limits of procedures

Offer all the steps needed to complete the process

Clarify concepts and terminology

Consider health and safety issues

List the location of all necessary supplemental resources

Acceptable Use Policy (AUP)

- Considered one of the most important sections of a written security policy
- Identifies how employees are expected to use resources in the organization
- Defines rules of behavior/code of conduct
  - Use proper land acceptable language
  - Avoid illegal activities
  - Avoid disturbing or disrupting other systems
  - Do not reveal personal information
  - Do not reveal confidential information

AUP Categories

AUP Administrative Controls

- Change management processes
- Least privilege policy
- Mandatory vacations
- Separation of duties
- Rotation of duties
- Clean desk policy
- Social media usage

AUP Enforcement

- Initial verbal reprimand/warning
- Official written warning
- Temporary suspension with or without pay
- Termination
- Criminal or civil legal action (incarceration, reimbursement, and/or restitution)

Employment Candidate Screening and Hiring

- HR and Legal departments must work closely with security policy steering committees to determine best practices
- At the start of an interview, it is not uncommon to sign a non-disclosure or confidentiality agreement
- Many organizations have employees sign an additional employment contract
- New employees should sign off on all security policies as well as the Acceptable-Use Policy

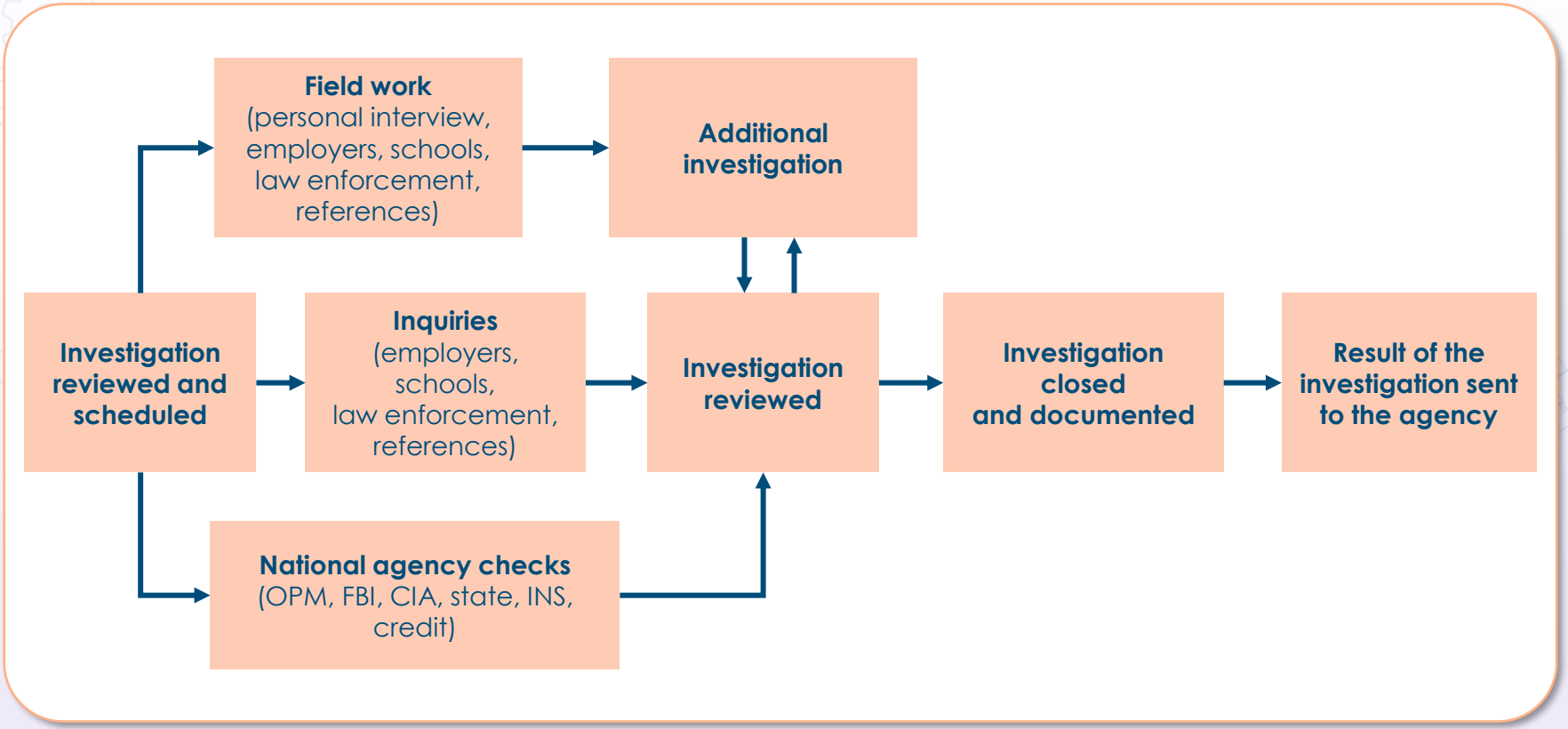
Employment Candidate Activities

- Working with "headhunter" organizations and online hiring sites, like indeed.com
- Confirming all references
- Approving education, certifications, and experience
- Additional fact-checking of résumés
- Performing background and credit checks
- Adhering to compliance and privacy requirements
- Conducting technical or phone interviews before on-site meetings

Conducting Investigations

- Employment candidate screening and hiring
- Promotions to higher sensitivity levels
- Periodic review of employment policies
- Compliance and privacy policy requirements
- Incident response and forensic investigations

National Background Investigation Bureau (NBIB)



Onboarding

New hire procedures

- Provide assets, guidance, knowledge, skills, and behavior needed for role on team
  - Videos, printed material, CBT, lectures, formal and informal meetings, and mentors
- Introductions and explanation of standards and practices (standard operating procedures – SOP)
  - Clearly define roles and responsibilities
- Provisioning all devices and equipment
- Deliver security awareness and AUP expectations
- Additional Human Resources activities
  - Remove any ambiguity and uncertainty

Non-disclosure Agreements (NDAs)

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

Automating Onboarding

- Enterprises often deploy systems that involve self-service onboarding of personal devices
- Employee registers a new device, and the native supplicant is automatically provisioned for that user and device and installed using a supplicant profile that is preconfigured to connect the device to the corporate network
- Can use a Software as a Service provider
- Offboarding is the reverse process

Employment Termination and Transfer Best Practices

- Termination depends on the circumstances
  - Document all procedures for revoking outgoing employee access before termination
  - Monitor and audit the employee closely in last hours or days of service
  - If possible, terminate face-to-face and with a witness

Employment Termination and Transfer Best Practices

- Meet all regulatory (WARN and SOX) requirements
- Delete/disable accounts and revoke certificates and digital signatures
- Return property (physical and IP)
- Modify/update corporate controlled social media
- Add former employees to list of potential threat agents
- Do follow-up interviews if possible

Employee Release and Exit Interviews

- Identify factors that led to employee leaving
  - How can the organization improve to keep employees, if applicable?
  - Discover any potential unknown security vulnerabilities
- Remind exiting employee of their agreements and responsibilities
  - Review the NDA that they signed when they started
  - Remind them of what they are forbidden to discuss with others
- Adhere to well-defined offboarding security policies and procedures
  - Collect all corporate assets and property

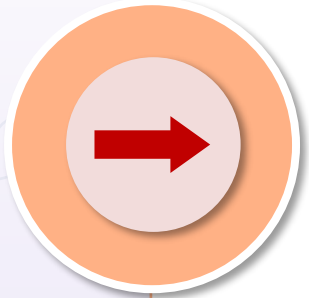
Service Level Agreements (SLAs)

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

Organizational Level Agreements (OLAs)

- An OLA documents the pertinent information for regulating the relationship between internal service recipients and an internal IT area (service provider)
- The difference between an SLA and an OLA is what the service provider is promising the customer (SLA) vs. what the functional IT groups promise each other (OLA)
- An OLA often corresponds to the structure of an SLA with a few specific differences based on the enterprise

Memorandum of Understanding (MOU)



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

Reciprocal Agreements

- A reciprocal agreement is between two organizations with similar infrastructure and technology
- These agreements are difficult to legally enforce
- The most common goal is that one can be a recovery site for the other in case of a disaster or lengthy outage
- A quid pro quo arrangement in which two or more parties agree to share their resources in an emergency or to achieve a common objective
  - Data backup: whereby two departments or organizations agree to store one each other's backup data on their computers
  - Disaster planning: whereby each party agrees to allow another to use its site, facilities, resources, etc., after a disaster

Interoperability Agreement (IA)

- Agreement between two or more entities for collaboration and data exchange
- Often used by sister companies under a holding group
- Binding agreements for sharing information systems, telecommunications, software, and data
- Not the same as a reciprocal agreement (RA)
- Another example would be the Interconnection Security Agreement (ISA) that a customer signs for AWS Direct Connect or Azure ExpressRoute

Third-party Risk Factors

- Vendors and supplier reliability
- Supply chain quality and security
- Business partner privacy vulnerability
- End-of-life (EOL) products and services
- End-of-service (EOS) posture

Security Awareness Education and Training

Awareness	Training and education

• Commonly under-utilized
• Can often be overdone
• Increase awareness through
  • self-paced CBT modules, videos, and classroom training
  • posters, newsletter articles, email, and bulletins
  • combining the carrot and stick, or
  • reminding users with system banners, drink cups, mousepads, notepads, and other media
	• Awareness training for users in sensitive areas or with elevated roles
	• Security training for new hires
	• Technical security training for IT staff members
	• Advanced ongoing information security training for security practitioners and engineers
	• Specialized instructions for the "C-suite" and other key stakeholders

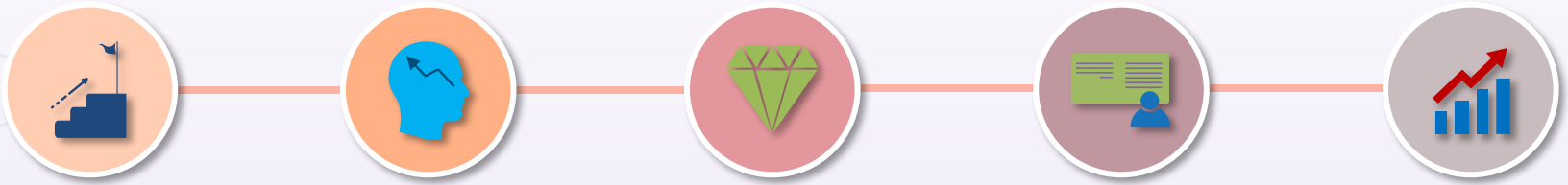
Security Awareness Education and Training

- Organization's mission, charter, and vision
- All applicable policies and procedures
- Example security topics:
  - Password and badge policy (MFA)
  - Tailgating/piggybacking
  - Clean desk
  - Anti-phishing
  - Social engineering and hoaxing awareness
  - Data loss prevention
  - Governance and regulations

Role-based Security Training

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

Example Awareness Program Development



Identify program scope, goals, and target audiences

Motivate and get buy-in from management and employees

Identify the optimal and affordable training modalities

Administer and maintain the security awareness and training

Evaluate and improve continuously