Welcome Back to SECURITY+ DAY 05

Class will begin at 10:00 am
Central Standard Time

AUTOMATION, ORCHESTRATION, AND INCIDENT RESPONSE

Objectives

- Outline automation and scripting use cases, benefits, and considerations
- Describe the incident response process and life cycle
- Provide an overview of threat hunting
- Describe root cause analysis, digital forensics, and investigation of data sources

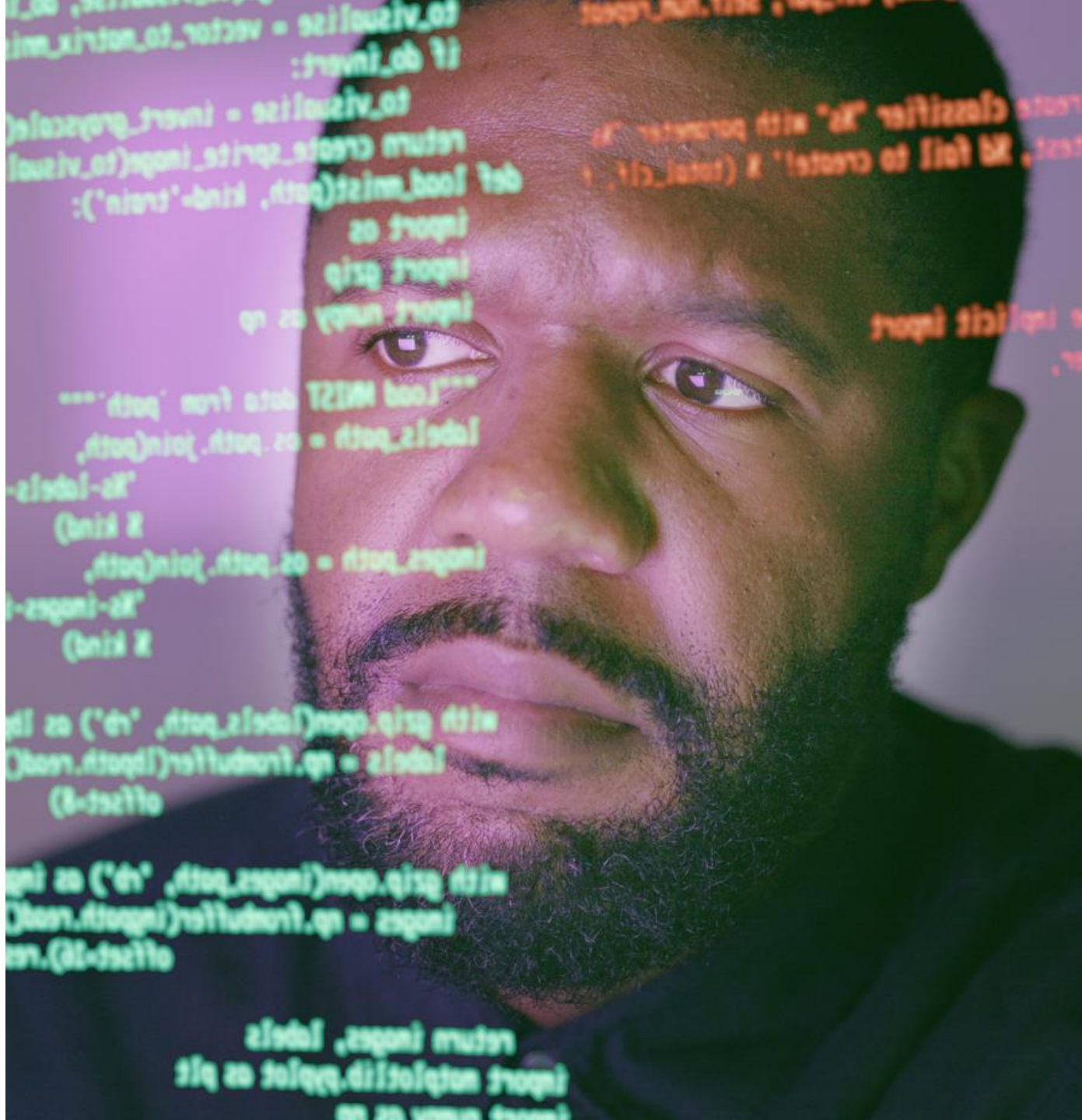
AUTOMATION VS. ORCHESTRATION

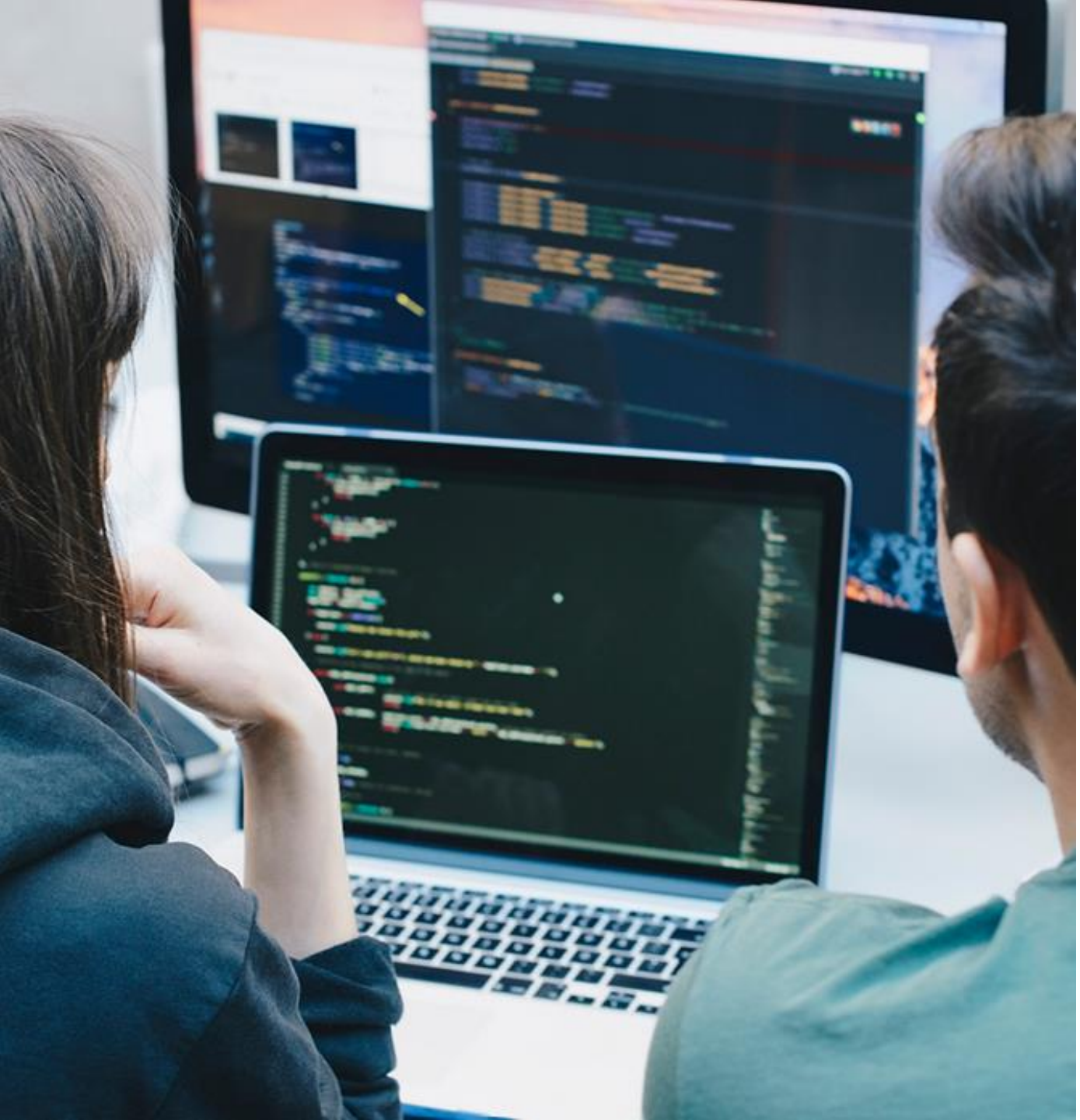
- IT automation involves generating a single task to run automatically without any human intervention
- Automation could involve sending alerts to a security information and event management (SIEM) system, dynamically triggering a serverless function at a cloud provider, or adding a record to a database when a batch job is run
- Enterprises often automate both cloud-based and on-premises tasks

- Orchestration involves managing several or many automated tasks or processes
- As opposed to focusing on one task, orchestration combines all the individual tasks
- Orchestration occurs with various technologies, applications, containers, datasets, middleware, systems, and more

AUTOMATION AND SCRIPTING USE CASES

- **User and resource provisioning** – Most modern enterprises have tightly integrated Joiner and Mover onboarding and provisioning processes that involve automation between human resources, legal, directory services, identity management (IdM), and inventory engines
- **Guardrails** – Cloud providers use JSON policies and Infrastructure as Code (IaC) to enforce least privilege policies and separation of duties to remove certain application programming interface (API) calls from privileged groups and users



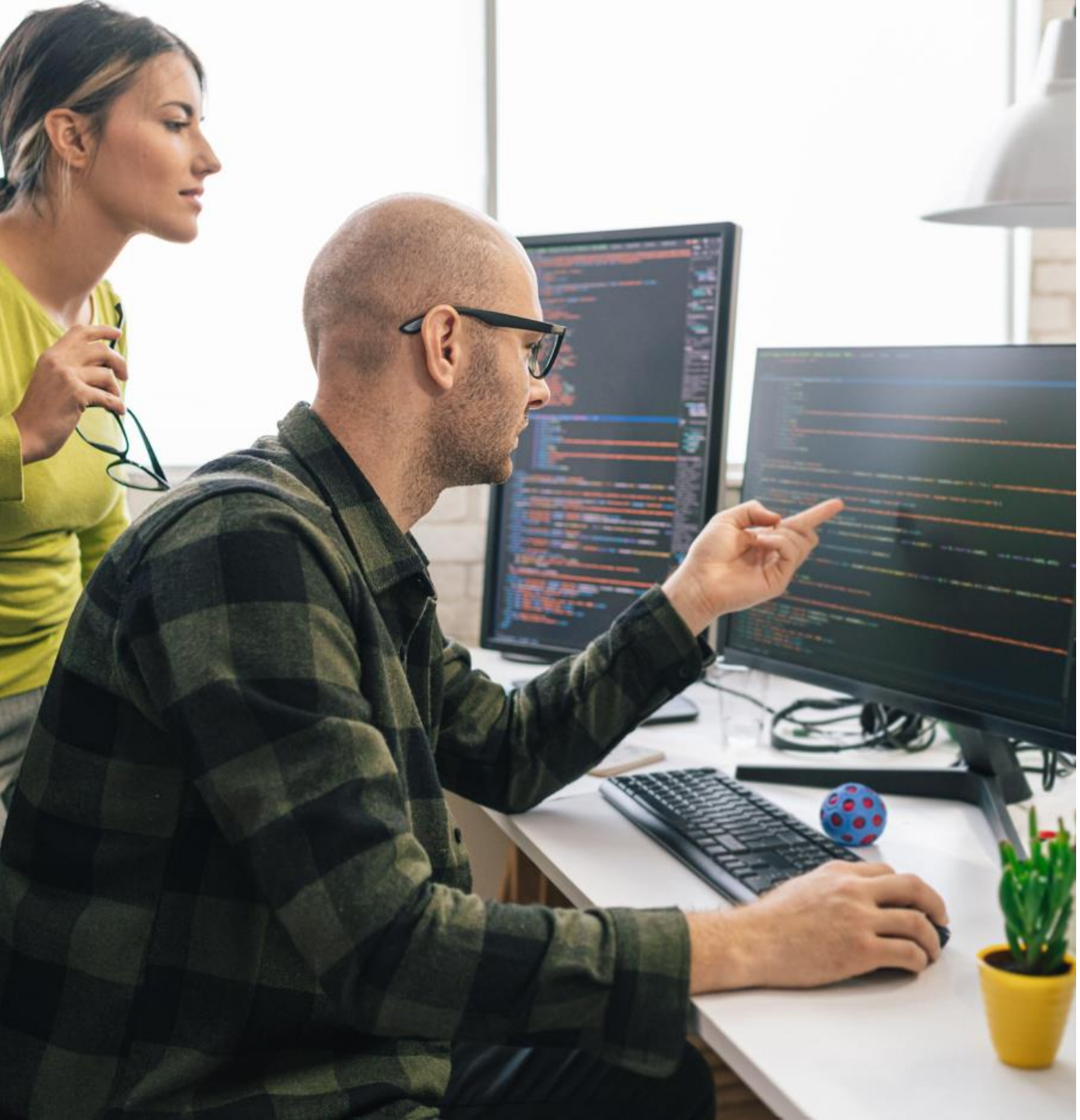


AUTOMATION AND SCRIPTING USE CASES

- **Security group firewalls** are layer 3/5 stateful packet filters applied to either subnets or virtual instances in hypervisors or cloud
- **Ticket creation and escalation** as part of a service desk deployment will run scripts and automated workflow:
  - Software-defined networks (SD-LAN, SD-WAN, SD-MAN)
- In modern LANs and data centers, **enabling/disabling services and access** controls is a common functions of scripts, automation, and IaC (JSON, YAML)

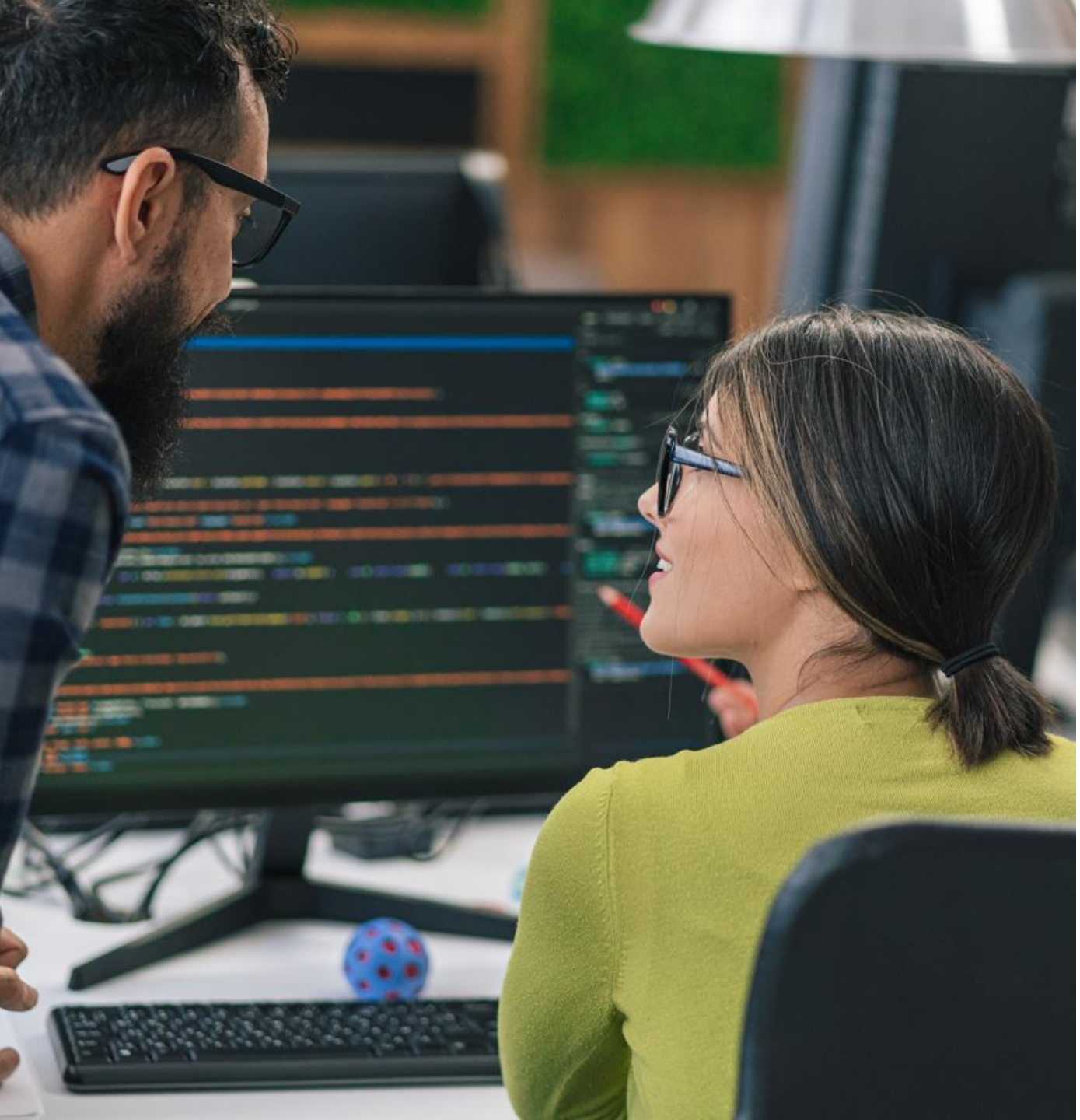
AUTOMATION AND SCRIPTING USE CASES

- As part of the DevOps life cycle [Agile, continuous integration/ continuous deployment (CI/CD)] automation is leveraged for **continuous integration and testing**
- Any **API** call or request can be automated (Python, Postman, etc.) to
  - Run tests to help quality assurance (QA) continuously check a product's quality
  - Generate light orchestrations that involve several API calls to perform a particular task on a microservice backend
  - Use preformed snippets to run Functions as a Service in the cloud



BENEFITS OF AUTOMATION

- Efficiency and productivity
- Time savings
- Enforcing baselines
- Standard infrastructure configurations



BENEFITS OF AUTOMATION

- Secure scalability
- Employee retention
- Reaction time
- Force multiplier

AUTOMATION CONSIDERATIONS

- Developers can reduce the **complexity** of automation by using established toolsets and integrated solutions
- Automation and scripting can reduce **costs** for provisioning/onboarding users and devices, reducing human interaction and potential configuration errors and troubleshooting

AUTOMATION CONSIDERATIONS

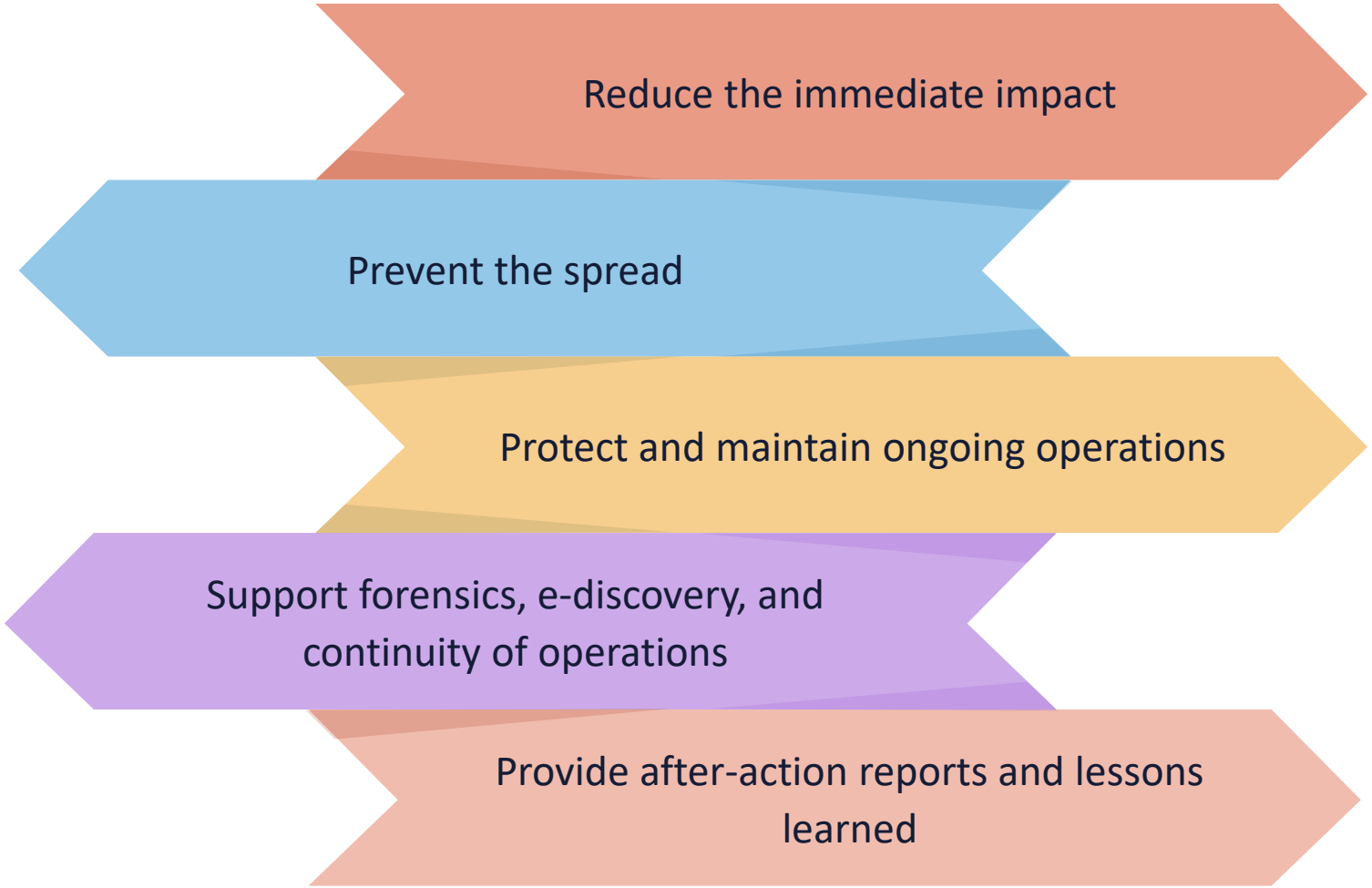
- In this context, a **single point of failure (SPOF)** is a flaw in the design, configuration, or implementation of the automation solution:
  - If the automation solution is not redundant and reliable, one loses the overall benefits
- Automation systems can also be a **technical debt** if implemented in a rush and/or without proper testing
- Ongoing **supportability** of automation and orchestration is another key factor

INCIDENT RESPONSE PROCESS

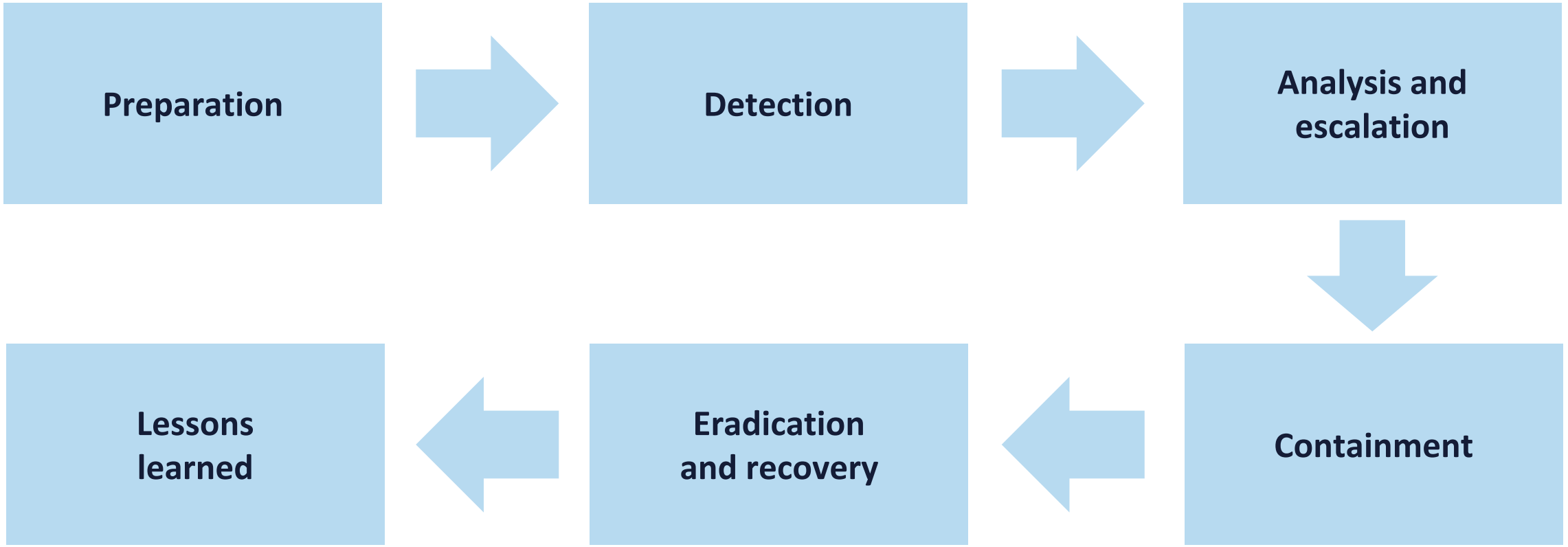
The classification of the negative event will determine action:

- Is it an event or an incident?
- What is the immediate impact on operations?
- What is the scope of impact?
- How prioritized or critical is the target?
- Can root cause analysis be performed quickly and easily?
- Does the incident trigger disaster recovery escalation?

GOALS OF INCIDENT RESPONSE



INCIDENT RESPONSE LIFE CYCLE

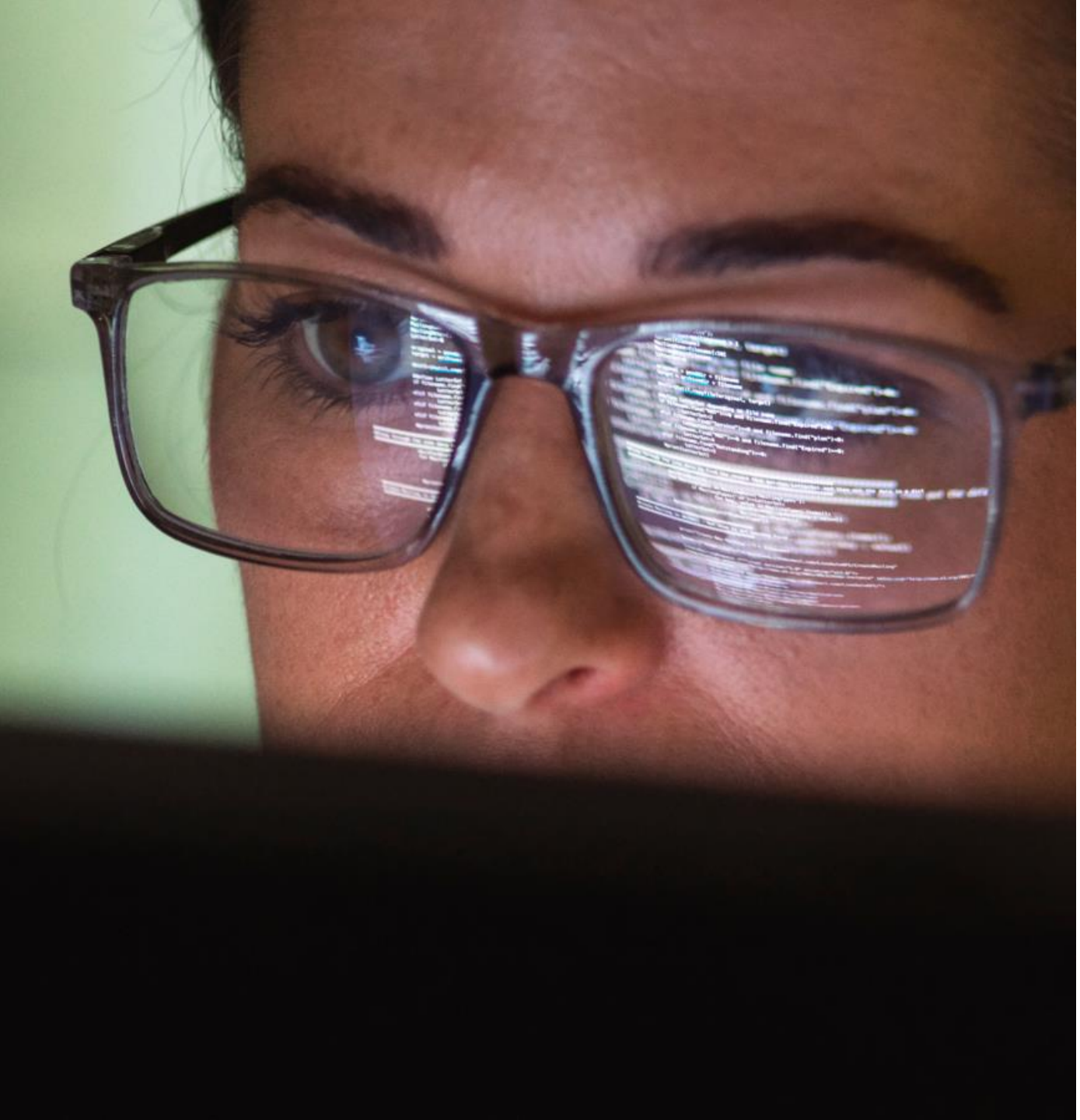


DETECTION

- Detection is also referred to as "identification"
- First responders or SIEM/security orchestration, automation, and response (SOAR) system must separate an event from an incident (or breach) immediately, using predefined metrics and experience
- Responders will implement techniques for categorizing and prioritizing the incident based on an established risk register or runbook

HOW WERE YOU ALERTED?

- Logs, alerts, and feeds
- Phone calls
- Text messages
- Logical and physical alarms
- Interactive monitoring in the security operations center (SOC)



ANALYSIS AND ESCALATION

- The analysis of incidents is a combination of an art and a science
- There are important questions to answer:
  - What is the scope of the incident?
  - Does it qualify for escalation or disaster recovery?
  - Are there obvious artifacts and indicators of compromise?
  - Can you discover the actions in the kill chain?
    - *To be explored in an upcoming lesson*
  - Can you quickly identify the root cause?

ESCALATION (ELEVATION)

- A workflow for escalating the incident to a higher service desk tier must be established
- Does the incident need to be passed from the first responders to an incident response team (IRT)?
- Many organizations have a SOC and a service desk along with an emergency Change Advisory Board (CAB)

CONTAINMENT

- Implement short-term processes, such as disconnecting devices from the network
- Quarantine malware with antivirus programs and security suites
- Leverage quarantine compartments, sandbox locations, detonation chambers, private clouds, and threat modeling environments
- Maintain separation, containment, and segregation with managed security service providers (MSSPs)

ERADICATION

- Potentially unwanted programs (PUPs) can be eradicated by advanced antivirus and antimalware suites
- Some artifacts may need to be moved to detonation chambers for further analysis and machine learning
- All findings should be reported to cloud partners and added to vulnerability repositories and shared reputation databases
- Advanced wiping tools may be needed to completely remove all malware footprints and artifact remnants

INCIDENT RESPONSE RECOVERY AND LESSONS LEARNED

- Recovery involves getting back to an acceptable state to continue to deliver the value proposition
- Complete remediation may not be possible even for an extended period
- After-action reports will be generated after exercises and actual incidents
- There should be a Lessons Learned database
- The success of redress and recovery depends on the level of testing and exercises performed

INCIDENT RESPONSE (IR) TRAINING

- A prime example of IR training is the Cybersecurity Infrastructure Security Agency (CISA)
- CISA helps organizations across the nation protect their IT enterprises and enable their cybersecurity talent
- CISA offers IR training courses free to government employees and contractors across federal, state, local, tribal, and territorial government, educational and critical infrastructure partners, and the general public

TESTING INCIDENT RESPONSE

- **Plan review (read-through):**
  - Group discussion, plan auditing, and Delphi and brainstorming sessions with stakeholders
- **Tabletop:**
  - Documented plans, diagrams, and logical and virtual walk-throughs to eliminate gaps/errors
- **Walk-through (exercise):**
  - Planned rehearsals and drills
  - Performed in stages and by department/building only
  - Should find additional gaps to those found during plan review and tabletop exercises

TESTING INCIDENT RESPONSE

- **Simulation:**
  - Focus on specific scenarios and areas
  - Use real business continuity plan (BCP) and disaster recovery plan (DRP) resources (recovery sites) and teams (swarm simulations)
  - Test snapshot recovery and hot spares
  - May be the highest-level test that most organizations conduct
- **Parallel:**
  - Conduct a real-world drill while still operating business
  - Is more resource-intensive than simulations
- **Full interruption:**
  - Conduct real-world drill while ceasing business activities
  - Is cost-prohibitive for most organizations

ROOT CAUSE ANALYSIS (RCA)

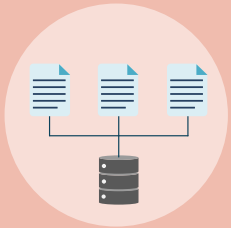
- RCA is a function of the Problem Management IT service practice
- A root cause is defined as a factor that introduced a non-conformance in an application, service, or system
- It is the core causative issue—the highest-level trigger—that sets in motion the entire cause-and-effect reaction that ultimately leads to the problem(s)
- RCA is defined as a collective term that describes a wide range of approaches, tools, and techniques used to uncover causes of problems

ROOT CAUSE ANALYSIS STEPS

Step 1

Define the problem

Step 2



Collect data

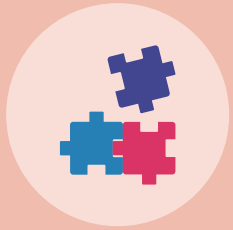
Step 3

Identify possible causal factors

Step 4

Identify the root cause(s)

Step 5



Recommend and implement solutions

THREAT HUNTERS

- Are also called “hunt teams"
- Involve groups of cyber investigators aggressively seeking out threats on a network or system
- Are often compliance or regulatory auditors
- Attempt to quickly recognize anomalies and discover historic patterns in data and Indicators of Compromise (IoC) to counter cybercriminals and mitigate threats
- Can also be red team vs. blue team exercises
- Will have a solid understanding of the cyber kill chain

CYBER KILL CHAIN

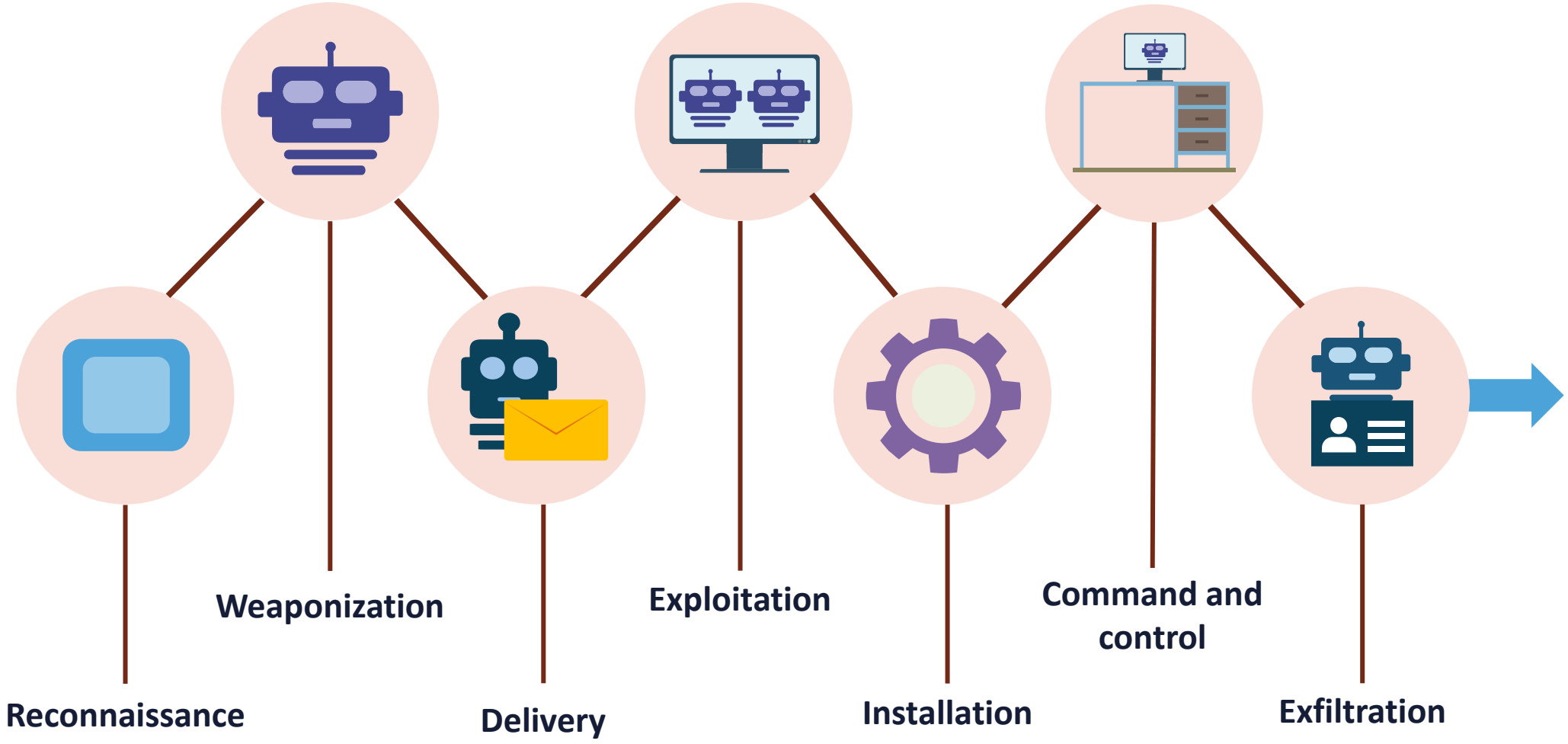
- A kill chain is the succession of steps and phases used during a structured external or internal cyberattack
- It is used by penetration testers and threat-hunting teams to better understand advanced persistent threats from exploits and malware attacks
- Kill chains were originally developed by Lockheed-Martin

A: Advanced
Targeted, coordinated, purposeful

P: Persistent
Targeted, coordinated, purposeful

T: Threat
Person(s) with intent, opportunity, and capability

SEVEN-STEP CYBER KILL CHAIN



WHY PERFORM DIGITAL FORENSICS?

- Laws have been violated
- Organizational policies have been violated
- Systems have been attacked
- Data and identity have been breached
- Intellectual property has been exfiltrated
- Privileged insiders are suspected of crimes
- It is the next incident response phase (root cause analysis/problem management)

E-DISCOVERY

- Cyber forensics is a main category of e-discovery
- E-discovery is innovative technology that has emerged over the last decade to lower the risks and costs associated with big data, especially in litigation and internal corporate and government investigations
- The e-discovery process includes four phases:
  - Identifying and collecting documents
  - Sorting through data by relevance
  - Creating production sets
  - Managing data

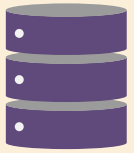
CYBER FORENSICS PROCESS

1. Identification of the crime
2. Collection of evidence
3. Examination of the evidence
4. Analysis of the evidence
5. Reporting on the findings of the analysis

COLLECTING AND HANDLING EVIDENCE

Employ forensic kits and laptops

Collect network traffic and various logs (SIEM)



Capture and hash system images and memory dumps using write-blockers

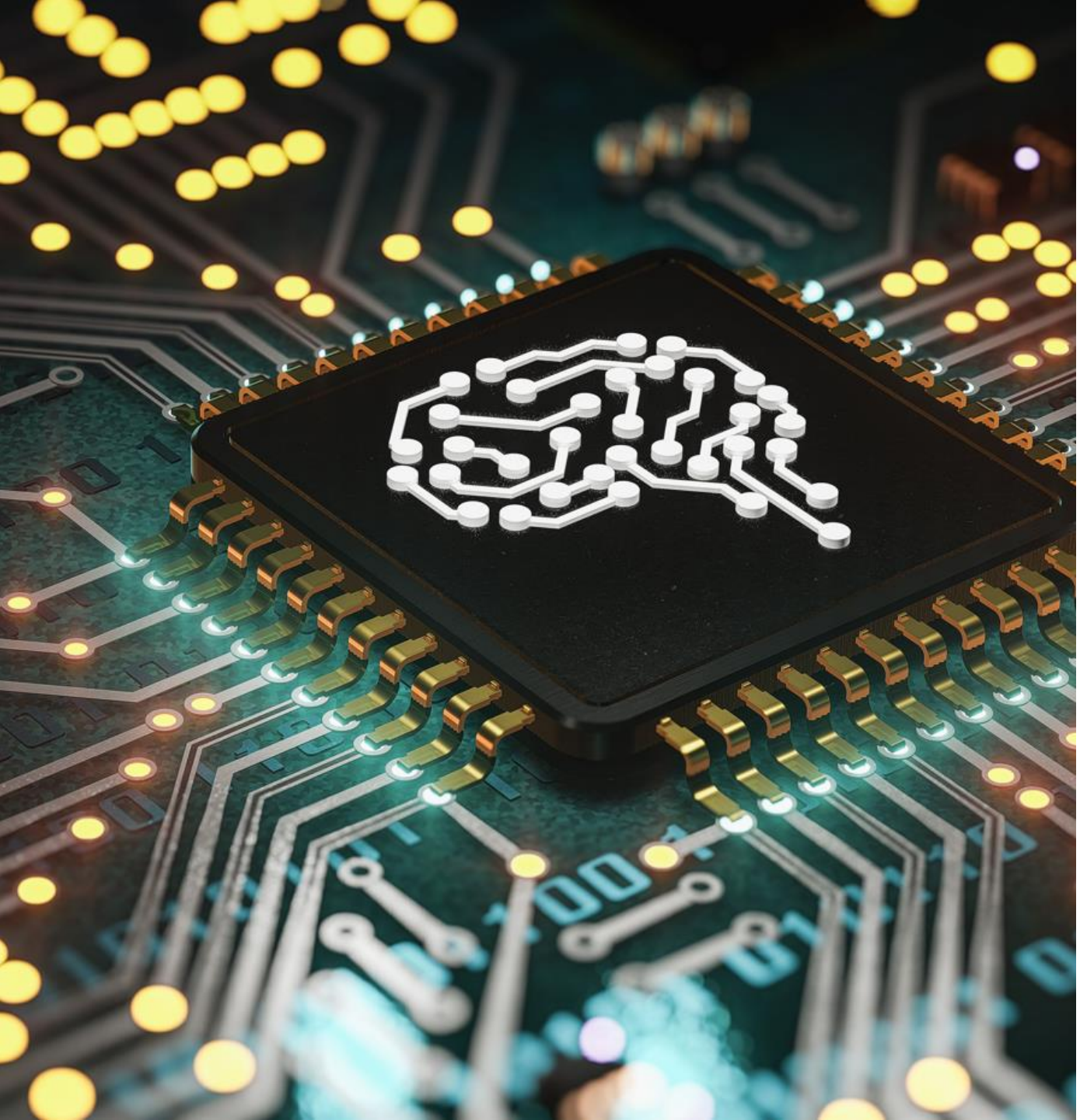
Document timeline of event sequence

Record time offsets

Create screenshots

Take pictures

Conduct interviews



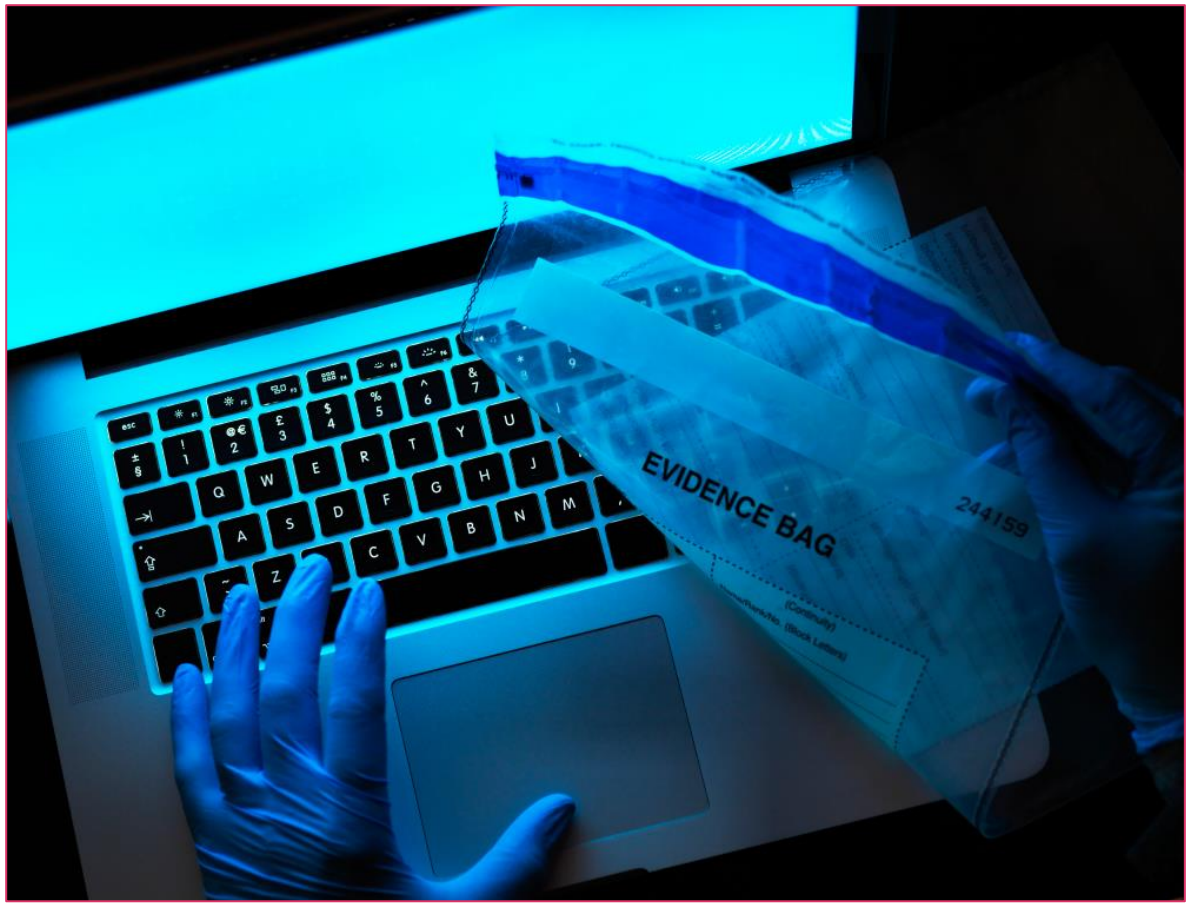
ORDER OF VOLATILITY

1. CPU and its cache
2. Kernel statistics, tables, and caches
3. Memory (RAM)
4. Temporary file systems and swap/slack space
5. Disk drives and volumes
6. Attached removable drives
7. Logged data to a remote location
8. Copies of data to archived media/cloud

PROCESSING FORENSIC EVIDENCE

- Detect encrypted files and volumes
- Discover compressed files and folders
- Perform validation and pattern matching
- Leverage regular expressions and metacharacters in forensic kits
- Filter for suspected user data
- Filter security identifiers (SIDs) on shared systems for privacy reasons
- Perform discovery of hidden data in slack space
- Extract only meaningful data
- Conduct traces and calibrated estimates to determine suspect(s)

CHAIN OF CUSTODY



- Follows evidence through entire life cycle until possible court date
- Involves strict procedures for collecting, handling, and tagging evidence
- Provides a history and timeline of evidence handling
- Maintains evidence integrity
- Provides accountability
- Prohibits tampering
- Anticipates any admissibility issues, such as legal holds

LEGAL HOLD

- Refers to a process that an organization uses to retain all forms of pertinent data and information when it reasonably expects some type of litigation against it, or some need for future utility in a court of law
- Can be a restriction placed on a database or set of records because of existing or anticipated litigation, audit, government investigation, or other such activity that suspends the regular usage, processing, or disposition of data

CHAIN OF CUSTODY LABELING

Chain of custody				
Registered mail	Date/Time	Released by	Received by	Reason
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	
	Date	Name/agency/organization	Name/agency/organization	
	Time	Signature	Signature	

FORENSIC REPORTING

- Should have as much information as necessary but not a "data overload"
- May need to express in simpler terms or have different reports for different target audiences
- Provide electronic and physical documents of all findings
- Meet with proper authorities and possibly prepare to offer expert testimony
- Provide any needed clarification
- Identify overall impact on business and recommend any countermeasures
- Answer who, what, when, and how – important for court and other proceedings

INVESTIGATION OF DATA SOURCES: LOGS

- **Firewall** logs can provide traffic data in layer 2 frames up to deep packet application inspection using different outputs
- **Application** logs for email, web, SharePoint, file, directory, database servers, and more
- **Endpoint** logs such as Palo Alto Cortex XDR
- **OS-specific** security logs from Windows, UNIX, Linux, macOS, Solaris
- **Intrusion prevention system (IPS)/intrusion detection system (IDS)** logs, alerts, dumps, traps, informs
- **Network** logs from infrastructure device, security appliances, database activity monitors, and more

MONITORING SOURCE SYSTEMS AND EVENTS

- Simple Network Management Protocol (SNMPv3) traps and informs
- NetFlow collections (v5 and v9)
- Syslog trap messages
- SIEM system events
- SOAR analysis output
- Cloud-based machine learning (ML) and artificial intelligence (AI) visibility/analysis
- IPS sensor dumps and alerts
- Endpoint detection and response (EDR) logs (Palo Alto Traps)

SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)

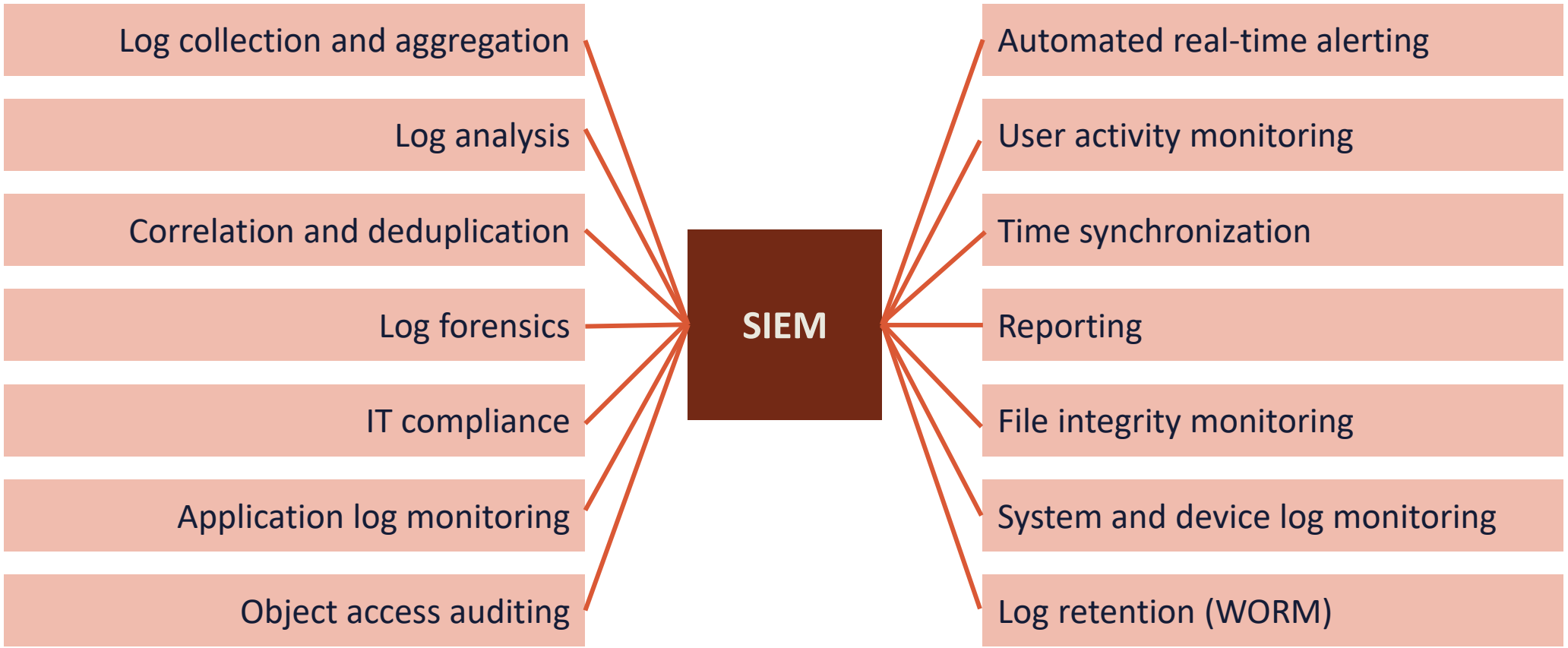
The term SIEM is a combination of security information management (SIM) and security event management (SEM)

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

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

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

SIEM


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

SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

- SOAR is an assortment of software services and tools:
  - Azure Sentinel
  - Splunk
  - Chronicle SOAR (part of the Google Cloud umbrella)
- It allows organizations to simplify and aggregate security operations in three core areas:
  - Threat and vulnerability management
  - Incident response
  - Security operations automation

SOAR

- Security automation involves performing security-related tasks without the need for human intervention
- It includes defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing

SOAR COMPONENTS

- SIEM use cases, categories, and rules are mapped to incident categories
- These categories are then mapped to three types of playbooks:
  - Manual (series of manual tasks)
  - Semi-automated (hybrid of automated and manual subtasks)
  - Fully-automated (completely automated)

SOAR COMPONENTS

- Four types of automation:
  - Defensive (anything that tries to prevent the threat or risk)
  - Forensic (anything that tries to retrieve additional evidence)
  - Offensive (anything proactive that tries to investigate an asset)
  - Deception (anything that retrieves or adjusts deception tools)

SOAR COMPONENTS

- Three different categories of action:
  - Enrichment (adding additional configuration management database (CMDB) or environment data)
  - Escalation (email, ticket escalation, Simple Notification Service (SNS), chat/messaging communication)
  - Mitigation (the modification of device configuration)

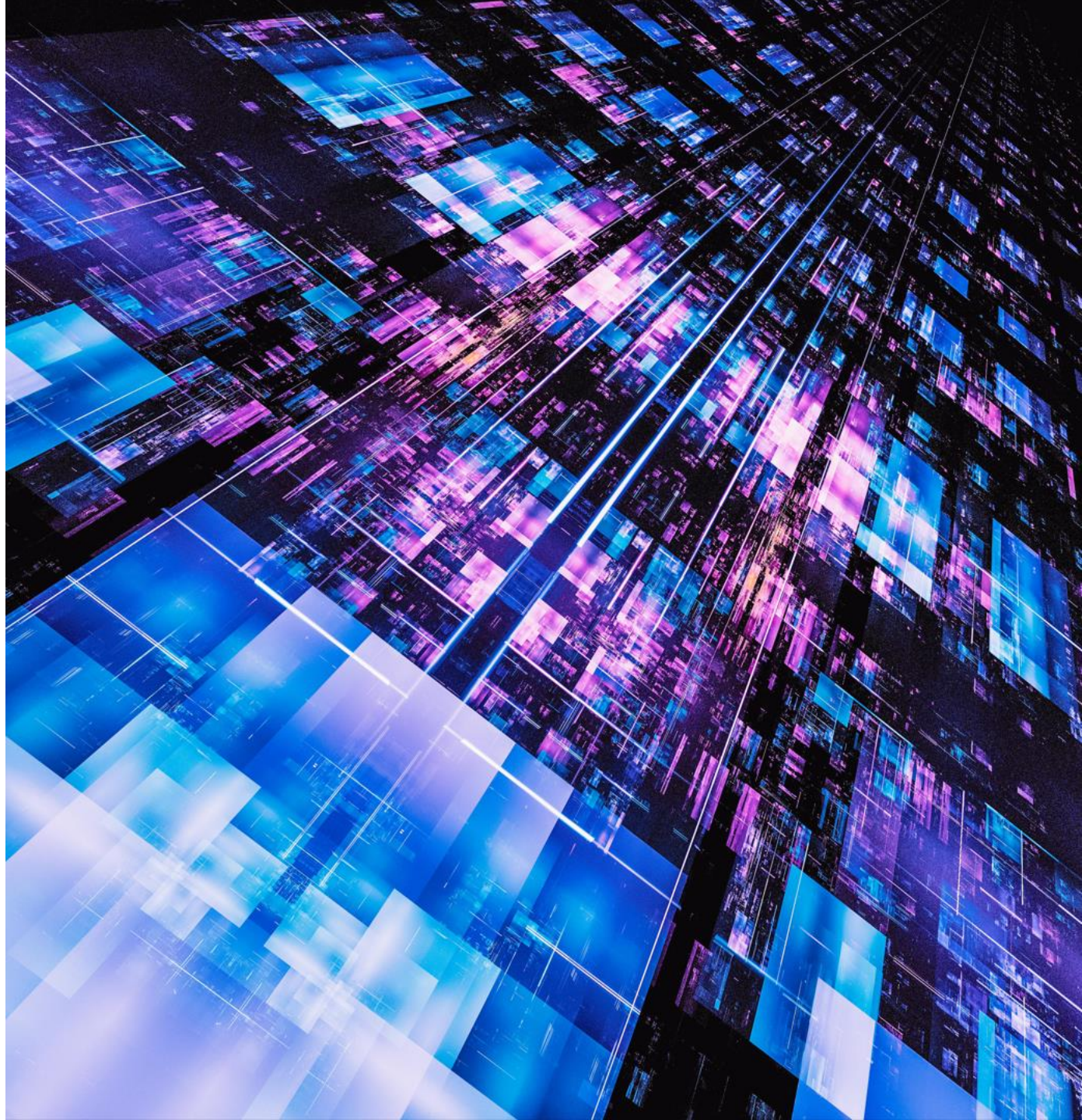
EFFECTIVE SECURITY GOVERNANCE

Objectives

- Define security governance and governance structures
- Examine roles and responsibilities
- Describe the considerations of external governance
- Outline security governance guidance, best practices, standards, policies, and procedures

SECURITY GOVERNANCE DEFINED

- 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

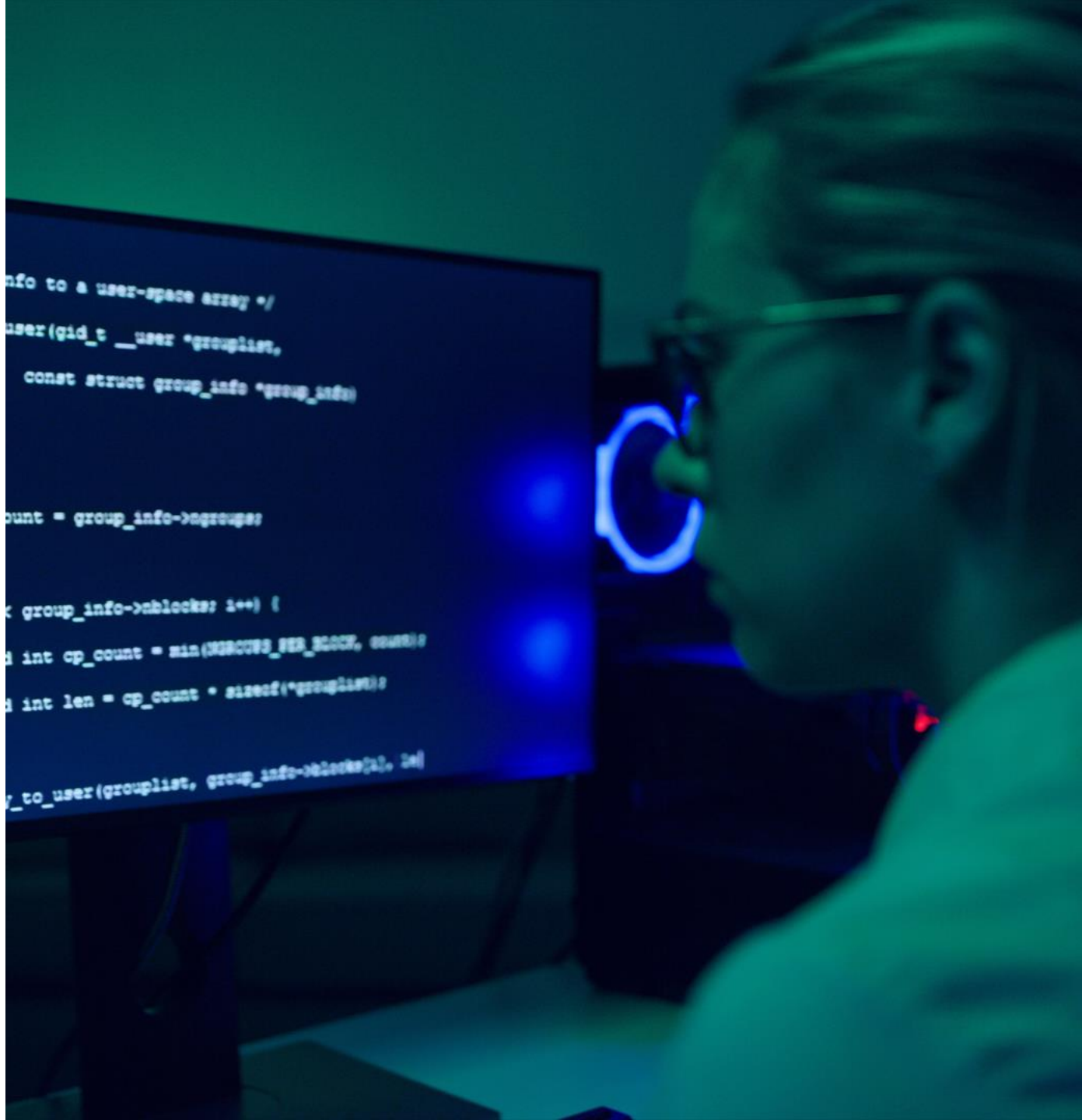


SECURITY GOVERNANCE DEFINED

- The need for governance exists any time a group of people comes together to accomplish an end
- Security governance typically focuses on three attributes or characteristics:
  - Authority
  - Decision-making
  - Accountability
- It 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 DEFINED

- 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
- It 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

- Creating a risk register (ledger)
- Aligning security strategy with organizational goals
- Publishing all compliance and regulatory requirements
- Performing a vital role in risk assessment and management:
  - Offering guidance into acquiring security controls to reduce risk
- Tracking and recording all compliance and remediation initiatives
- Documenting stakeholder interactions and reporting related workflows

CENTRALIZED VS. DECENTRALIZED GOVERNANCE STRUCTURES

- With centralized governance, the higher positions of management, such as executives and/or the C-suite, hold the decision-making authority:
  - It relies heavily on top-down decision-making
- With decentralized governance, management distributes the decision-making authority throughout the organization:
  - Decisions are made closer to the source of action and information
  - It is used in flatter, more projectized organizations

SECURITY GOVERNANCE BOARDS

- Board governance refers to a security framework or architecture that provides structure to a group of decision-making stakeholders (the board) and how it functions
- Board governance defines the roles and responsibilities of board members and executives in the form of a
  - Working board
  - Governing board
  - Advisory board

BOARD OF DIRECTORS (BOD)

- A board of directors is the governing body of an organization or company, whose members are elected by shareholders (in the case of public companies)
- The duties include setting strategy, overseeing executive management, and protecting the interests of shareholders, bondholders, and other stakeholders
- **Every public company must have a board of directors**

STEERING COMMITTEES

- A steering committee is a group of key organizational stakeholders that makes determinations regarding an organization's priorities or order of business, and manages its operations general counsel
- The goal of a steering committee is to oversee and support a project from the management level

STEERING COMMITTEES

- The Information Security Committee exists to offer recommendations to executive management and team leads concerning security efforts undertaken
- The committee may also coordinate and communicate the direction, current state, and continual oversight and improvement of information security initiatives:
  - For example, enterprise mobility management, cloud computing adoption, Wireless WPA3, and Zero Trust

SECURITY STEERING COMMITTEE RESPONSIBILITIES

1. Frame, review, and recommend information security policies
2. Evaluate the effectiveness of implemented policies
3. Offer clear guidance and management support for security initiatives
4. Ensure that security activities are executed in compliance with policy
5. Initiate security awareness and training programs
6. Identify and recommend non-compliance responses
7. Approve methodologies and processes for information security
8. Identify significant threat changes and vulnerabilities

GOVERNMENT AGENCIES

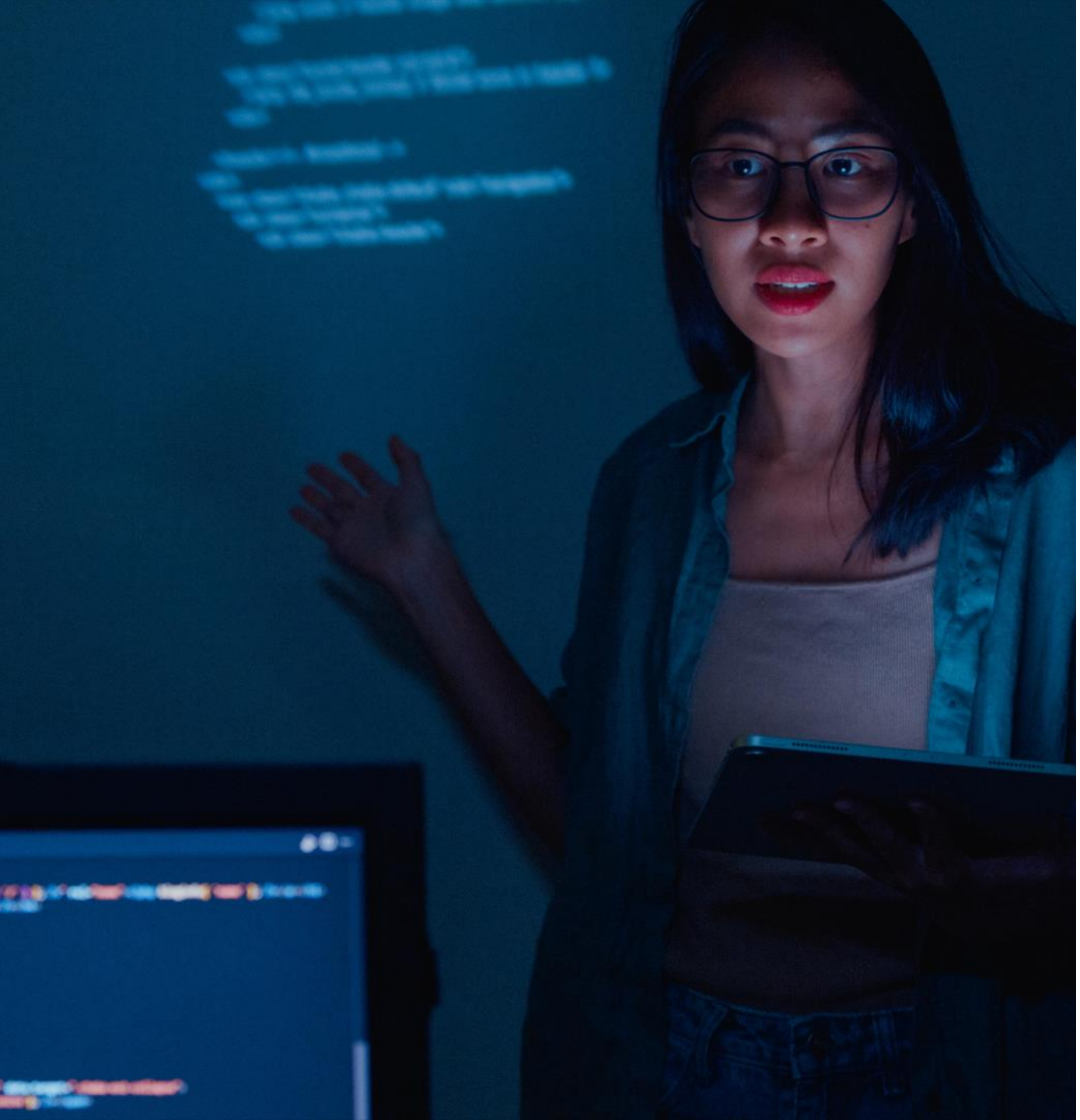
- **Cybersecurity and Infrastructure Security Agency (CISA)** – leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure
- **United States Customs and Border Protection (CBP)** – has the mission to keep terrorists and their weapons out of the U.S. along with securing trade and travel while enforcing regulations, including immigration and drug laws
- **Office of Homeland Security Situational Awareness (OSA)** – provides operations coordination, information sharing, situational awareness, common operating picture, and executes the DHS Secretary's responsibilities across the homeland security enterprise
- **Office of Intelligence and Analysis (I&A)** – assists the Homeland Security Enterprise with the timely intelligence and information it needs to keep the homeland safe, secure, and resilient

ROLES AND RESPONSIBILITIES

- 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

OWNERS

- 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
- Physical and logical asset owners may
  - Determine the classification level
  - Conduct labeling and tagging
  - Grant additional shares and rights



CUSTODIANS

- Custodians are also referred to as “controllers”
- They should maintain the assets from a technical and operational perspective
- Custodians often interact directly with owner stakeholders and answer to executive managers (C-suite)
- Often responsible for ensuring confidentiality, integrity, authenticity, availability and non-repudiation of assets

STEWARDS

- Will manage assets from a business perspective
- May interface with other departments such as legal, human resources, mobile application, and digital asset managers
- Are more likely to deal directly with internal and external customers and stakeholders
- Often ensure compliance (standards and controls) and data quality

OFFICERS

- The buck should stop here, although it is not uncommon that the custodians/controllers take the hit when goals are not accomplished
- C-suite or C-team includes CEO, CIO, CISO, CPO, CTO, and other new forms of chief officers
- These are totally responsible for due diligence and adherence to security governance
- They will often answer to steering committees and various boards such as the BOD

RACI CHARTS

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

	GRC* department	Legal department	Security team	IT operations
Establish the provider requirements	R/A	C	C	I
Build the governance scheme	R/A	C	C	I
Assess cloud vendor	A	I	R	R
Build the architecture	I	I	A/R	R
Conduct cloud migration	I	I	C	A/R

**GRC – Governance, Risk, and Compliance*

EXTERNAL GOVERNANCE CONSIDERATIONS

- Despite the size or the industry, every organization must adhere to specific laws and regulations
- **Regulatory compliance** describes the actions an organization takes to comply with those rules and policies as part of its operations
- When it comes to data, there are rules for handling sensitive information
- To be in regulatory compliance, organizations set up internal processes to keep data safe and secure - otherwise, they may be fined, sued or face criminal prosecution

EXTERNAL GOVERNANCE CONSIDERATIONS

- Some laws and regulations may be driven by the applicable business sector or industry, for example Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH) Act, Sarbanes-Oxley, or Payment Card Industry Data Security Standard (PCI DSS)
- The scope can be global, international (treaties), national, state/province/parish, county, or local
- Guidance, such as the International Electrotechnical Commission/International Organization for Standardization (ISO/IEC) or National Institute of Standards and Technology (NIST), cannot supersede or overwrite governmental laws and regulations at any level even local

DEMO: GUIDANCE AND BEST PRACTICES

In this demo…

We will explore several popular guidance's and best practices for security

BEST PRACTICES AND GUIDELINES

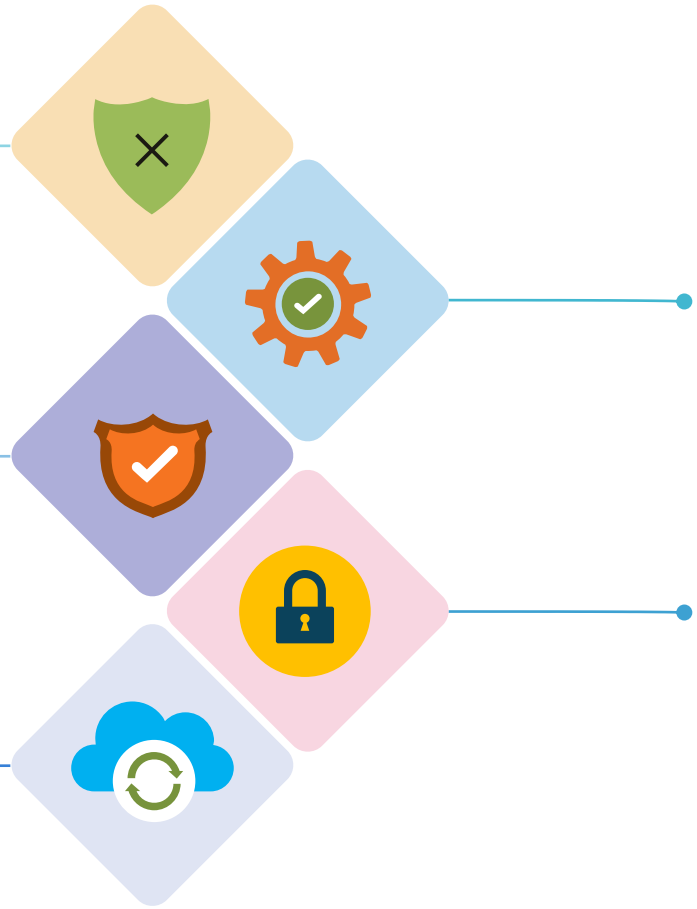
- Guidelines provide a list of suggestions on how one can do things more effectively
- Guidelines and practices are like standards, but are more flexible and not usually mandatory
- They are used to define how standards should be developed or to guarantee adherence to general security policies

SECURITY GUIDELINES

NIST Computer Security Resource Center

Center for Internet Security (CIS) Top 18

Cloud Security Alliance (CSA) – Cloud Controls Matrix (CCM)



National Security Agency (NSA) Security Configuration Guides

CISA Cybersecurity Best Practices

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 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

POLICIES

- 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

POLICIES

- 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

DEVELOPING AN INFORMATION SECURITY POLICY

- **Sanctioned:**
  - The policy has the support of executive management
  - It requires visible participation and action, ongoing communication and championing, investment, and prioritization
- **Applicable:**
  - The policy is applicable to the organization
  - Strategically, the information security policy must support the guiding principles and goals of the organization
  - Tactically, it must be relevant to those who must comply

DEVELOPING AN INFORMATION SECURITY POLICY

- **Realistic:**
  - The policy can be effectively executed
  - Policies must represent the actual environment in which they will be deployed
  - Information security policies and procedures should only express what is achievable
  - If the policy is to advance the organization's guiding principles, one can also assume that a positive outcome is anticipated
  - **A policy should never set up constituents for failure but instead should offer a clear track for success**

DEVELOPING AN INFORMATION SECURITY POLICY

- **Flexible:**
  - The policy can accommodate change and be adapted if necessary
  - An adaptable information security policy recognizes that information security is not a static, point-in-time endeavor, but rather an ongoing process designed to support the organizational mission
- **Comprehensive:**
  - The policy scope includes all relevant parties - it is inclusive
  - An information security policy must consider
    - Organization objectives
    - International law
    - Cultural norms of its employees
    - Business partners, suppliers, and customers
    - Environmental impacts
    - Global cyber threats

DEVELOPING AN INFORMATION SECURITY POLICY

- **Enforceable:**
  - The policy is statutory and is enforced
  - Enforceable means that administrative, physical, or technical controls can be put in place to support the policy
  - Compliance can be measured and, if necessary, appropriate sanctions applied
  - Enforcement stages should be well-documented:
    - Verbal reprimand
    - Written warning
    - Punitive actions
    - Temporary suspension
    - Permanent termination
    - Legal actions

STANDARDS AND POLICIES EXAMPLES

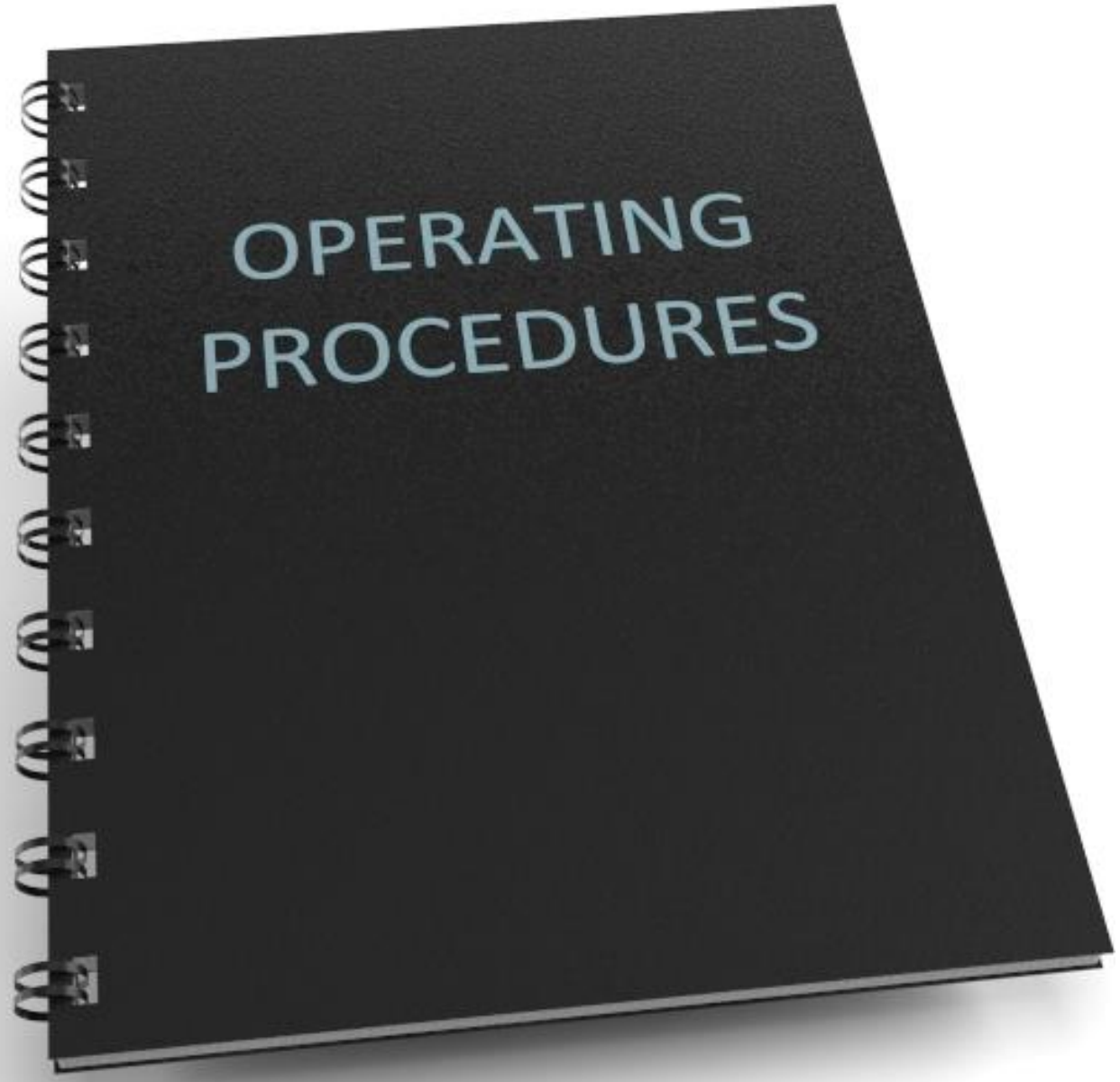
- Password
- Access control
- Physical security
- Encryption
- Information security
- Business continuity
- Disaster recovery
- Incident response
- Software development life cycle (SDLC)
- Change management
- Acceptable Use Policy (AUP)

ACCEPTABLE USE POLICY (AUP)

- Is 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 and acceptable language
  - Avoid illegal activities
  - Avoid disturbing or disrupting other systems
  - Do not reveal personal information
  - Do not reveal confidential information

SAMPLE AUP CATEGORIES

- Mobile device policy
- Virtual private network (VPN)/software-defined perimeter (SDP) usage
- Operating systems and software
- Social media
- Removable media
- Augmented reality
- Personal cloud storage
- Clean desk



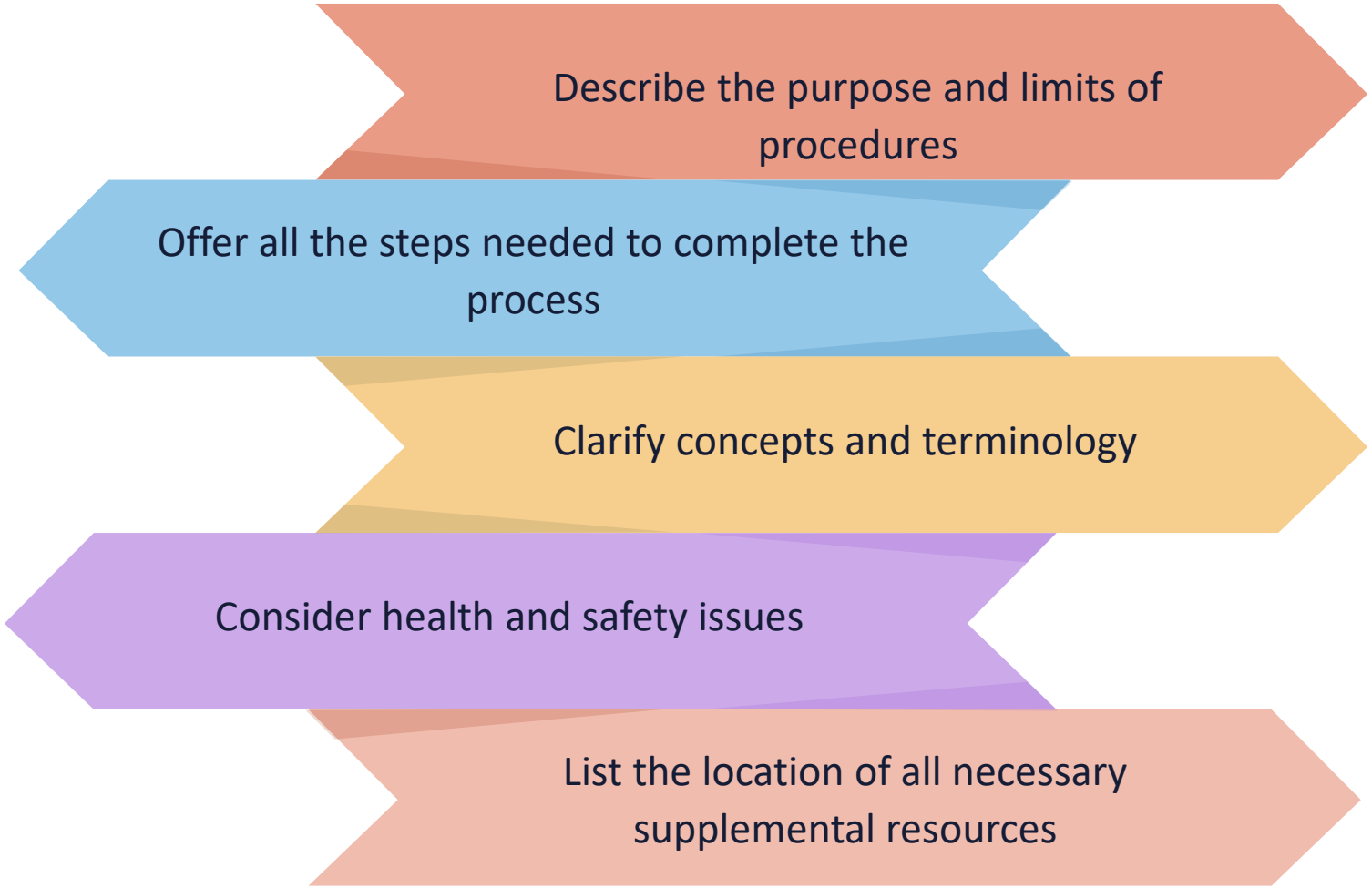
PROCEDURES

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

STANDARD OPERATING PROCEDURE (SOP)

- Are step-by-step instructions that define how workers carry out routine tasks
- Can greatly improve
  - Efficiency
  - Quality
  - Performance
  - Communication
  - Compliance with regulations

SOP CONSIDERATIONS



CHANGE MANAGEMENT PRACTICE

- The change management practice is also called the change control practice
- The change control process reduces risk in security policy by delivering a systematic approach to assess and manage proposed and subsequent changes:
  - Normal changes
  - Standard changes
  - Emergency changes
- It assures that changes are carefully assessed for possible impacts on project scope, schedule, and resources, allowing for informed decisions

ONBOARDING (PROVISIONING)

- Provides assets, guidance, knowledge, skills, and behavior needed for associated job roles:
  - Videos, printed material, computer-based training (CBT), lectures, formal and informal meetings, and mentors
- Offers introductions and an explanation of standards and practices, including SOPs:
  - Clearly defined roles and responsibilities
- Provisions all devices and equipment
- Delivers security awareness and AUP expectations
- Includes additional Human Resources activities:
  - Removal of any ambiguity and uncertainty
- Offboarding or deprovisioning is the reverse process

AUTOMATING ONBOARDING AND OTHER PROCESSES

- Enterprises often deploy systems that involve self-service onboarding of personal devices
- These processes can be fully and semi-automated with runbooks and playbooks:
  - SIEM and SOAR systems are emerging solutions
- The Joiner or Mover 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

MONITORING AND REVISIONS

- The proper usage of various visibility tools will result in comprehensive monitoring and proper revisions and improvements:
  - SIEM systems
  - Intrusion detection system (IDS)/intrusion prevention system (IPS) sensor logs
  - Application logs (system, security, application logs)
  - Firewall logs
  - Simple Network Management Protocol (SNMP) traps and informs
  - NetFlow records
  - Database activity monitor (DAM) reports
  - Software as a Service (SaaS) solutions

RISK MANAGEMENT

Objectives

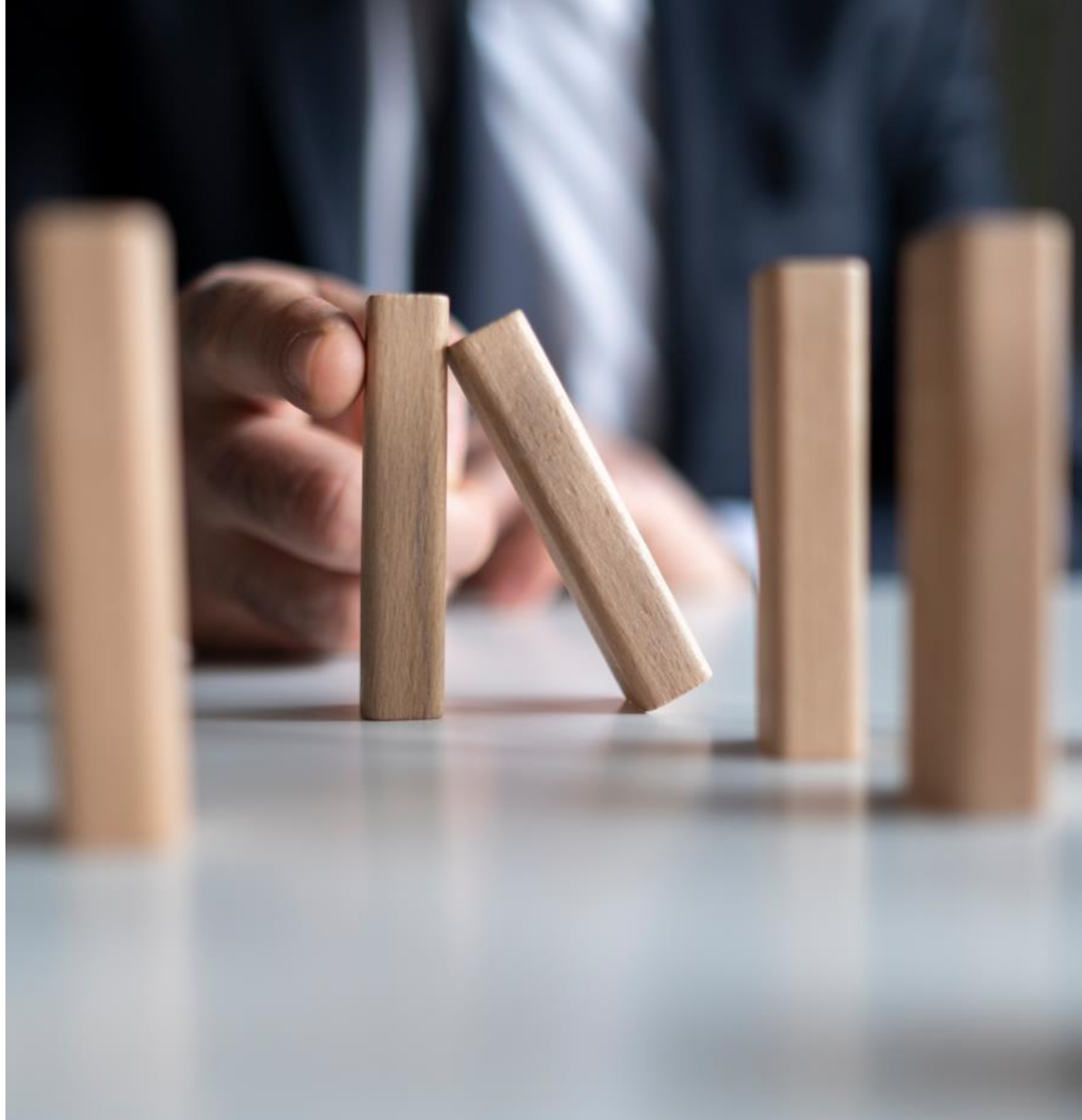
- Define risk management, identification, assessment, and analysis
- Compare risk treatment and handling approaches
- Explore risk registers and ledgers
- Describe risk reporting
- Learn about business impact analysis

DEFINE RISK MANAGEMENT

- Risk management is the continuous process of handling risks to organizational operations, including mission-critical services and functions, physical and logical assets, and people
- The results of this management might be
  - Establishing the context for risk-related activities
  - Conducting an asset and risk assessment
  - Implementing a risk mitigation strategy based on established risk treatment
  - Employing techniques and procedures for the continuous monitoring of the security state of information systems

DEFINE RISK MANAGEMENT

- Inherent (total) risk:
  - The vulnerabilities and risks that the organization faces before safeguards are implemented
  - The present baseline or system/application state before a formal assessment begins
- Residual risk:
  - The vulnerability or risk that remains after the mitigating controls are introduced
- **Residual = inherent risk – safeguards (controls)**



RISK IDENTIFICATION AND ASSESSMENT

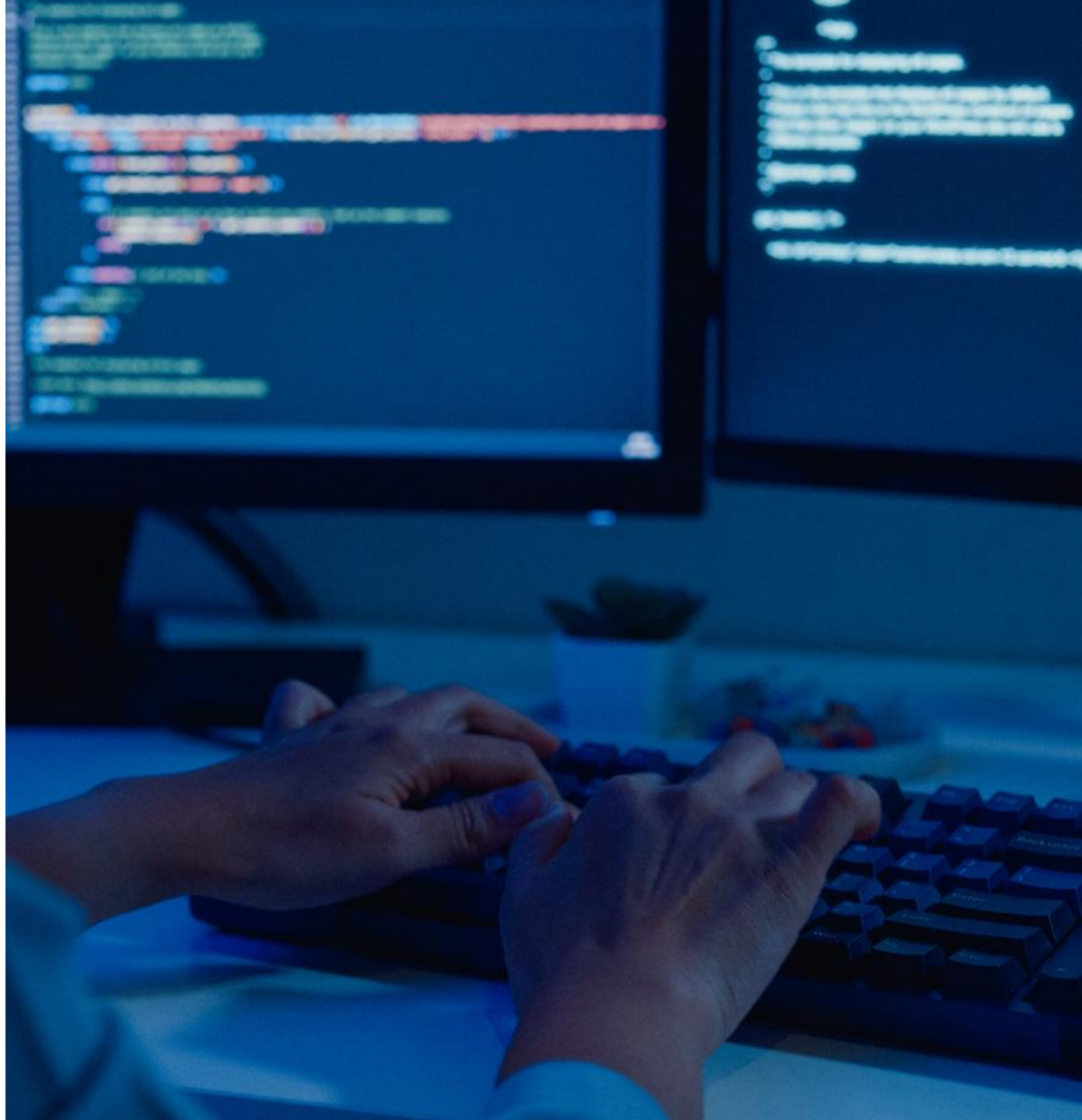
- According to the Center for Internet Security (CIS) Top 18 Controls, two initiatives must be conducted before the most critical assets (data and people) can be protected:
  1. Inventory and Control of Enterprise Assets
  2. Inventory and Control of Software Assets
- These initiatives will contribute greatly to risk identification and assessment activities

INVENTORY AND CONTROL OF ENTERPRISE ASSETS

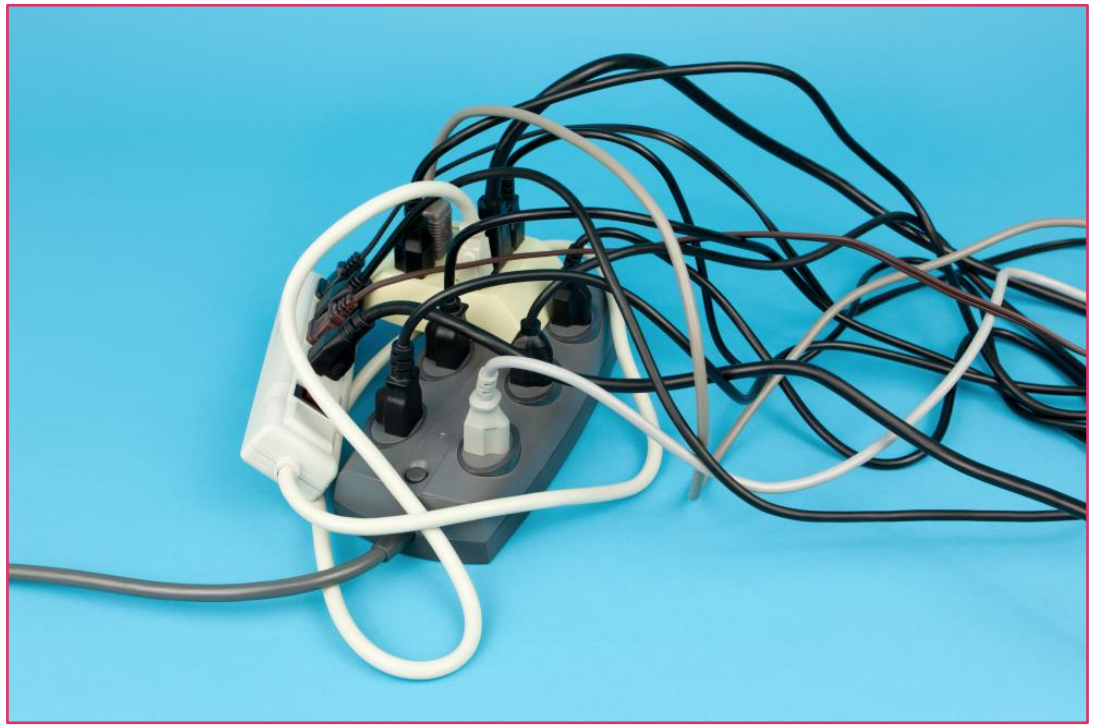
- Before the security practitioner can identify and assess risk, they must "know what they have"
- This involves actively tracking, labeling, and inventory of all enterprise assets:
  - End-user devices (stationary, portable, and mobile)
  - Network infrastructure devices
  - Security devices and appliances
  - Servers and hypervisors
  - Non-computing/Internet of Things (IoT) devices
  - Any physical component connected virtually, remotely, and to cloud environments
- The security practitioner should accurately know the entirety of assets that need to be monitored and protected within the enterprise

INVENTORY AND CONTROL OF SOFTWARE ASSETS

- The security practitioner must vigorously manage (inventory, track, and repair) all operating system software and applications on all networks (production, management, storage area, hypervisor) so that only authorized software is installed and run
- This includes virtual assets at cloud providers in infrastructure, platform, and Software as a Service deployments
- Any unauthorized and unmanaged software must be located and prevented from installation or execution (ghost or shadow IT) in accordance with policies and procedures

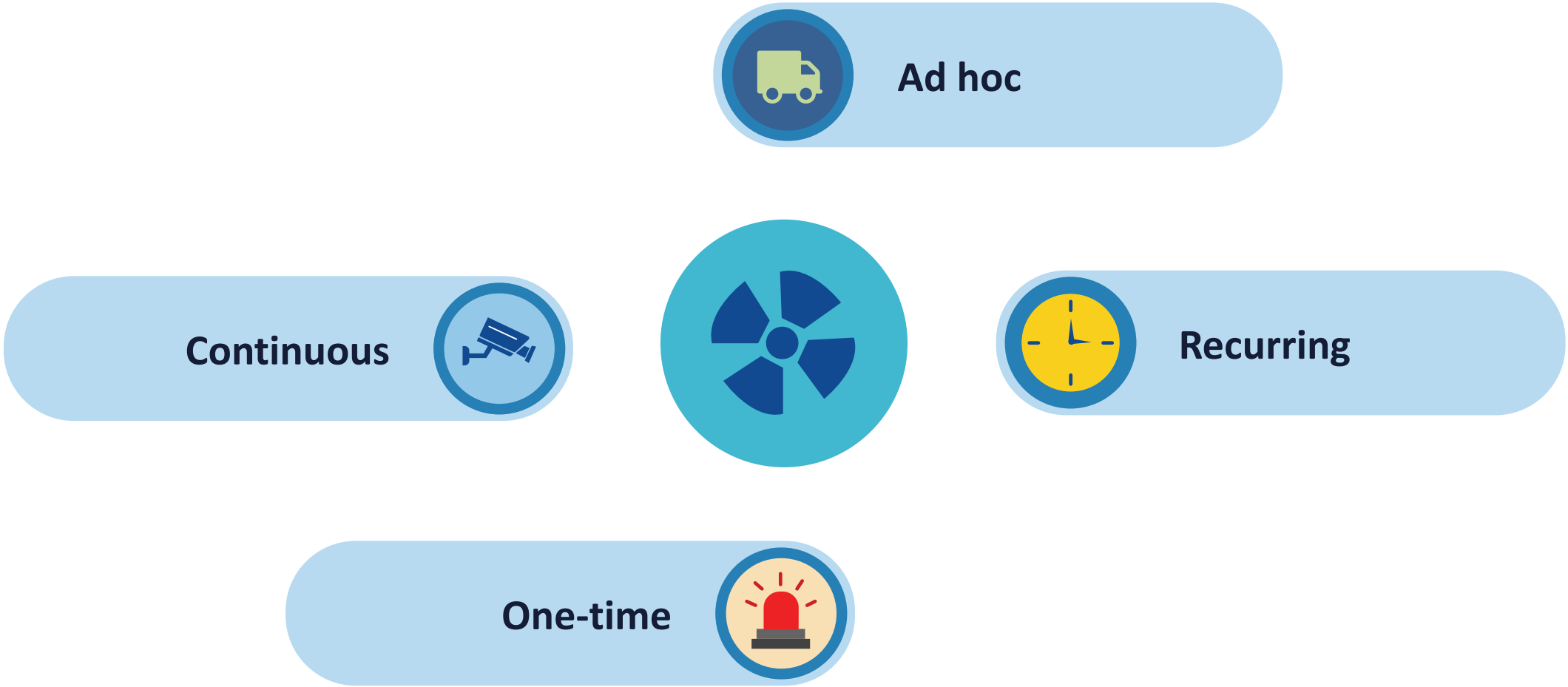


RISK IDENTIFICATION AND ASSESSMENT



- Risk identification involves the qualitative and/or quantitative evaluation of the most probable risks and threats to organizational assets
- The practitioner should determine the potential impact (magnitude) and likelihood (probability) against the mission-critical assets first

RISK IDENTIFICATION AND ASSESSMENT



RISK IDENTIFICATION AND ASSESSMENT

Hazard identification

Hazards

- Fire
- Explosion
- Natural hazards
- Hazardous materials spill or release
- Terrorism
- Workplace violence
- Pandemic disease
- Utility outage
- Mechanical breakdown
- Supplier failure
- Cyber attack

Property & magnitude

Vulnerability assessment

Assets at risk

- People
- Property, including buildings and critical infrastructure
- Supply chain
- System/equipment
- Information technology
- Business operations
- Reputation of or confidence in entity
- Regulatory and contractual obligations
- Environment

Vulnerability

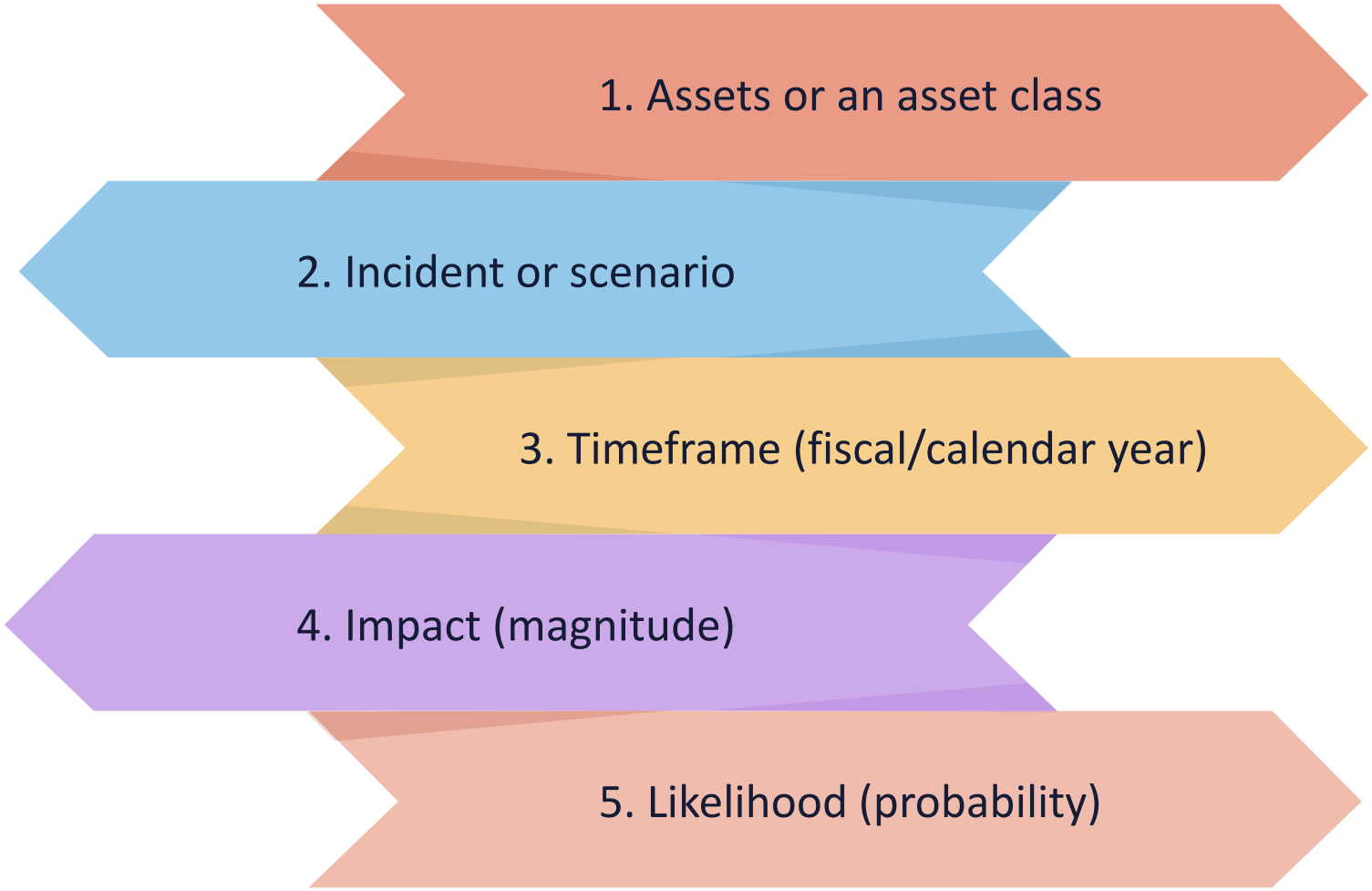
Impact analysis

Primary and secondary loss

- Casualties
- Property damage
- Business interruption
- Loss of customers
- Financial loss
- Environmental contamination
- Loss of confidence in the organization
- Fines and penalties
- Lawsuits

https://www.ready.gov/risk-assessment

FIVE KEY ELEMENTS OF RISK ANALYSIS



QUALITATIVE RISK ANALYSIS

- The most common method used in risk and security
- Descriptive approach using subjective opinions, history, and scenarios to determine risk levels:
  - Expert judgement
  - Best practices
  - Experience
  - Intuition
- Often involves interviews, questionnaires, surveys (Delphi), and conducting brainstorming sessions and workshops addressing assets, known risks, known vulnerabilities, common threats, and historical impacts

QUALITATIVE RISK ANALYSIS HEAT MAPS

			Impact				
			Negligible	**Minor**	**Moderate**	**Critical**	**Disastrous**
			1	2	3	4	5
Likelihood	**Frequent**	5	Medium	Medium	High	High	High
	Likely	4	Medium	Medium	Medium	High	High
	Occasional	3	Low	Medium	Medium	Medium	High
	Seldom	2	Low	Low	Medium	Medium	Medium
	Improbable	1	Low	Low	Low	Medium	Medium

QUANTITATIVE RISK ANALYSIS

- Quantitative risk analysis is a scientific/mathematical approach to getting monetary and numeric results based on
  - Asset values (cost and depreciated)
  - Impact (magnitude) or severity of the incident
  - Probability (likelihood) of occurrence
  - Threat frequency
  - Costs and effectiveness of safeguards
- The resulting probabilities are based on percentages, mathematical formulas, and calibrated estimation
- Even a semi-quantitative approach will be preferable to a purely qualitative analysis

CLASSIC QUANTITATIVE ANALYSIS (WHITMAN)

- **AV (asset value):**
  - Value of the asset according to the organization
- **EF (exposure factor):**
  - Percentage of asset loss caused by identified threat
- **SLE (single loss expectancy):**
  - Potential loss if attack occurs
  - (Asset value * exposure factor)
- **ARO (annualized rate of occurrence):**
  - Estimated frequency the threat will occur within a single year
- **ALE (annualized loss expectancy) = (SLE * ARO)**

QUANTITATIVE RISK ANALYSIS

Whitman risk analysis						
Asset	**Threat**	**Asset value**	**Exposure factor**	**Single loss expectancy**	**Annualized rate of occurrence**	**Annualized loss expectancy**
SRV_1	Fire	$15,000	100%	$15,000	0.1	$1,500
SRV_2	Fire	$20,000	100%	$20,000	0.1	$2,000
SRV_1	Flood	$15,000	100%	$15,000	0.0001	$1.5
SRV_2	Flood	$20,000	100%	$20,000	0.0001	$2.0
SRV_1	Virus (no AV software)	$15,000	10%	$1,500	365	$547,500
SRV_1	Virus (with AV software)	$15,000	10%	$1,500	1	$1,500

RISK TREATMENT

- Treatment and handling may also be referred to as "risk appetite"
- Any combination of treatments can be used with risk management
- Analysts must also consider any exemptions or exceptions for certain privileged users, air gapped systems, or special use case applications

RISK TREATMENT (HANDLING): ACCEPT

- **Risk acceptance:**
  - Do not implement any additional safeguards
  - Justification in writing is often required
  - This can also be the process of "ignoring" the risk
- Examples:
  - Only having one supplier or vendor for hardware or services relying on their uptime reputation
  - Leasing a facility in a 100-year flood zone
  - Deciding not to add a cyber security rider to your existing business insurance policy
  - Continuing with a Wi-Fi Protected Access (WPA2)-secured wireless local-area network (WLAN)

RISK TREATMENT (HANDLING): TRANSFER

- **Risk transference** is also referred to as risk sharing:
  - Passing off risk to a third party or shared party
- Examples:
  - Purchasing an insurance policy or additional cyber insurance
  - Leveraging a shared responsibility model (SRM) with a cloud service provider (IaaS)
  - Leasing a warm/cold disaster recovery facility with another similar business that is several miles away using a reciprocal agreement

RISK TREATMENT (HANDLING): AVOID

- **Risk avoidance** involves deciding not to undertake actions or engage in activities that introduce or increase risk
- Being too risk-averse can lead to missing out on opportunity or advantages
- Examples:
  - Not processing and storing credit card information of customers on-premises
  - Not using a cloud service provider for DevOps or managed data services
  - Avoiding the use of any clear-text protocols, such as HTTP, Lightweight Directory Access Protocol (LDAP), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), or telnet
  - Not storing sensitive data in a personal cloud service, such as Dropbox or Google Drive

RISK TREATMENT (HANDLING): MITIGATE

- **Mitigation** involves the strategic and tactical use of an array of technical, administrative, and physical controls to reduce risk to an acceptable level
- Enterprises will implement safeguards that will reduce risk exposure – the risk may still exist, but the impact is reduced
- Examples:
  - Implementing endpoint protection, such as Palo Alto Cortex XDR
  - Upgrading the edge firewall appliance
  - Using a cloud-based security information and event management (SIEM)/security orchestration, automation, and response (SOAR) solution like Azure Sentinel or a managed security service provider (MSSP) solution from Fortinet
  - Hiring armed security guards

RISK HANDLING APPROACHES

Expansionary

Enterprise intends to increase the number of resources to allocate to treat risk as needed on an ongoing basis

Conservative

Enterprise is frugal and extremely careful to spend more money, acquire controls, add personnel

They would rather find compensating controls

Neutral

Enterprise will take a balanced approach to risk treatment

The appetite is neither expansionary or conservative unless necessary

RISK ASSESSMENT DOCUMENTS

- These assessments will record the processes used to identify probable threats and propose subsequent action plans if the hazard occurs
- The document will declare assets at risk (people, buildings, information technology, utility systems, machinery, raw materials, and finished goods)
- There are many templates and prototypes available online
- These documents will be used to construct risk registers and ledgers

CREATING A RISK REGISTER (LEDGER)

- Is a compilation of information related to vulnerabilities, risks, and countermeasures:
  - Repository of identified risks, impact, scenarios, and potential responses
- Populated from after-action reporting, lessons learned, case studies, and assessments
- Often represented as a table/scatter plot from a spreadsheet or database view
- May be an important tool to fulfill regulatory compliance

Identified risks	Root causes	Probability and impact	Ranking	Categories	Priorities	Time and cost objectives	Potential responses	Risk owners	Assumptions

RISK LEDGER MATRIX

		Event type								
		Accidental leak	**Espionage**	**Financial fraud**	**Misuse**	**Opportunistic data theft**	**Physical theft**	**Product alteration**	**Sabotage**	**Violence**
Intent	**Nonhostile**									
	Reckless insider	X			X			X		
	Untrained/distracted insider	X			X			X		
	Outward sympathizer	X			X					
	Unknown (nonhostile or hostile)									
	Supplier	X	X	X	X	X		X		
	Partner	X	X	X	X	X		X		
	Hostile									
	Irrational individual	X			X		X		X	X
	Thief		X	X		X	X			
	Compromised insider	X	X	X	X	X	X	X	X	X
	Activist		X		X	X	X	X	X	
	Terrorist						X		X	X
	Organized crime		X	X		X	X	X		
	Competitor		X			X		X	X	
	Nation state		X			X		X	X	

OTHER RISK DOCUMENT CONCEPTS

- **Risk owners** are persons or entities responsible for managing threats and vulnerabilities that might be exploited such as a chief information security officer (CISO), data custodian, virtual asset manager, or other technical risk stakeholder
- **Key risk indicators (KRIs)** are meaningful metrics for measuring the likelihood and impact of an incident and if the results exceed established risk appetite
- A **risk threshold** is a quantifiable level of uncertainty and impact from risk, below which an organization will accept a risk and above which an organization will not accept a risk

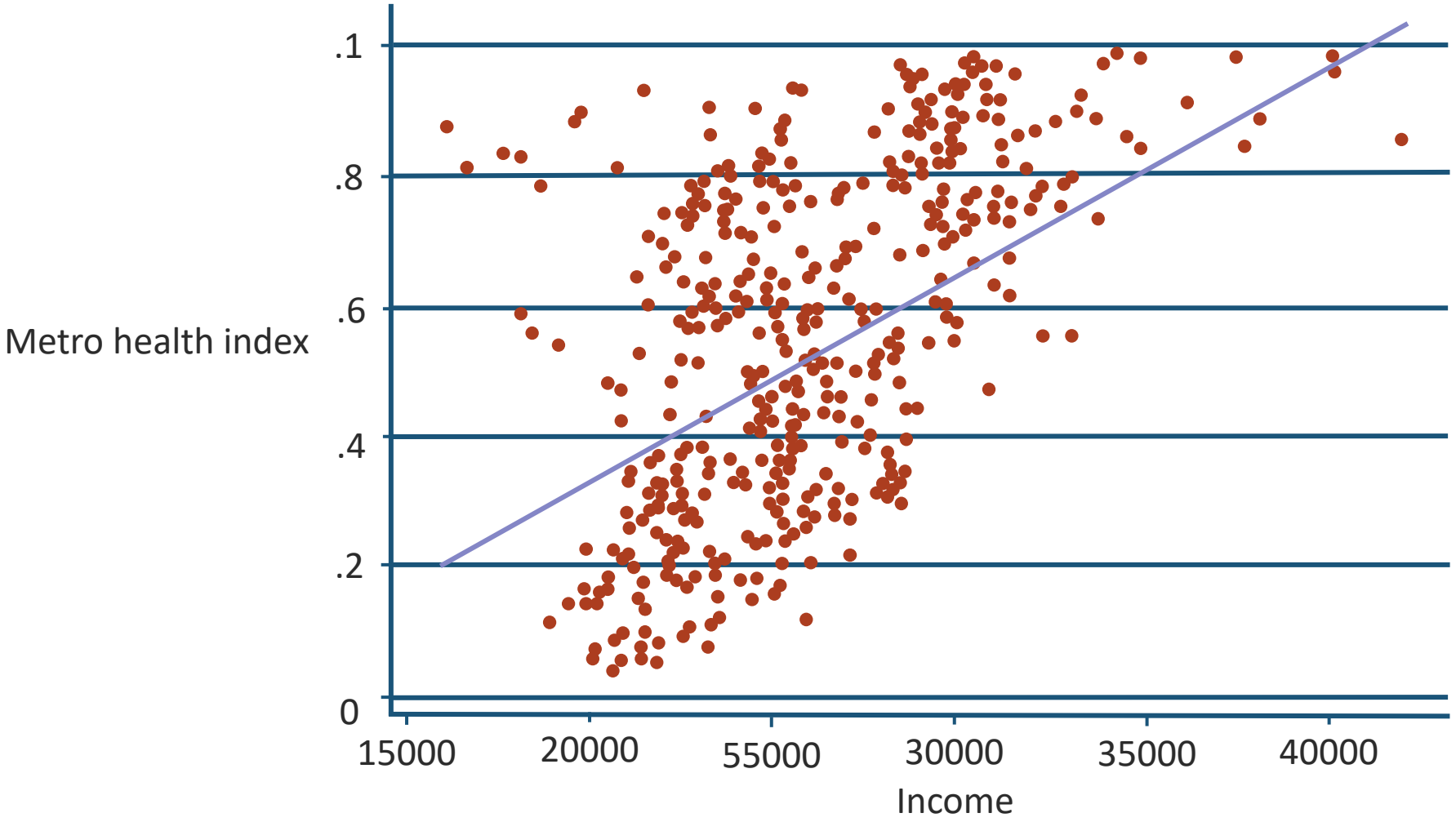
RISK REPORTING

- Risk reports should have just as much information as necessary but not a "data overload"
- Reports should be concise and yet comprehensive:
  - Written reports and summaries
  - White papers, special publications
  - Published to an intranet
  - Live presentations (in-person or conferencing sessions)
- Analysts may need to express in simpler terms or have different reports for **different target audiences:**
  - Possibly include a glossary of terms
- Dashboards are very effective (Python and R programming)

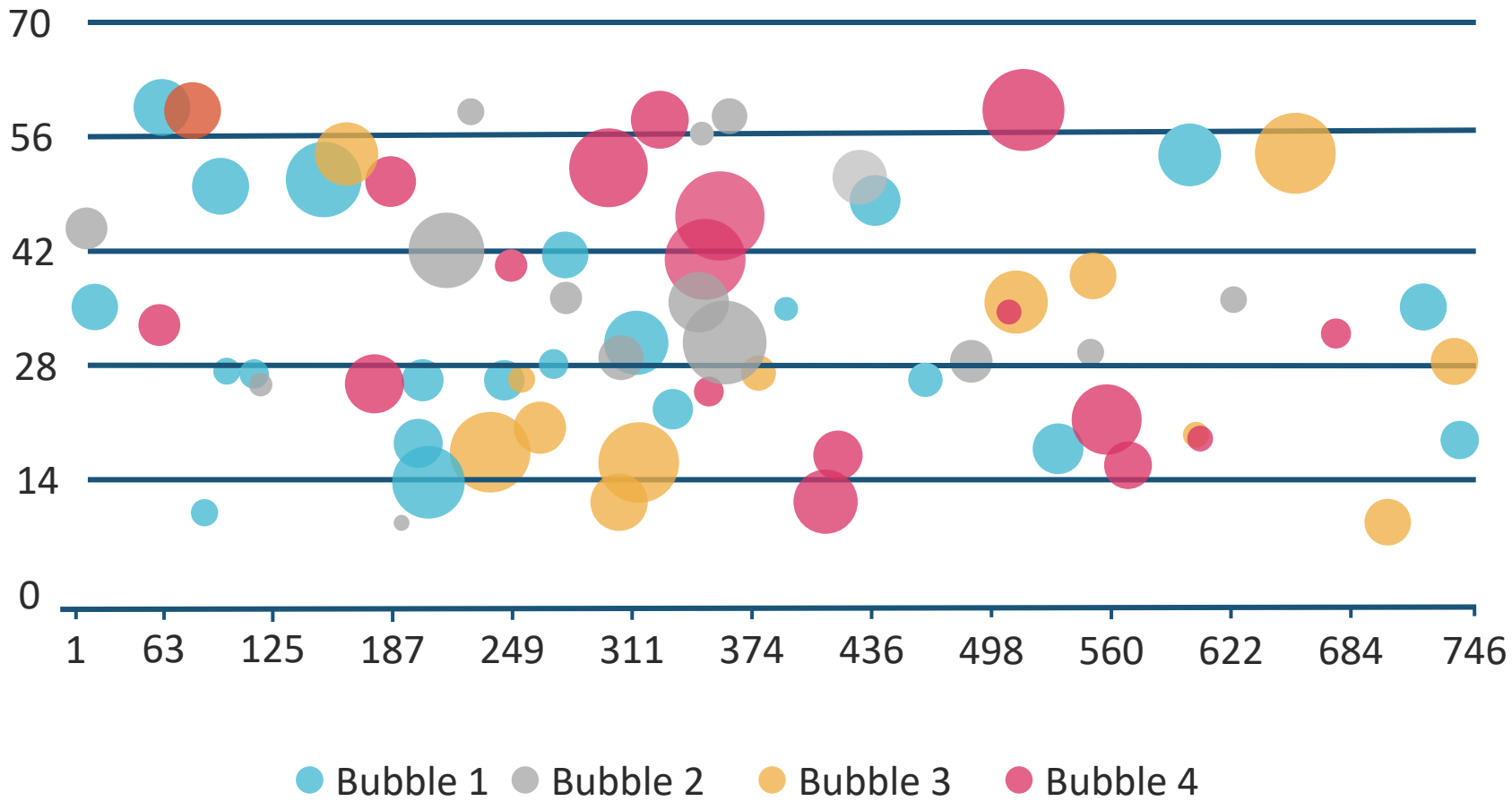
RISK REPORTING

- Understand the optimal aspects of visual communications:
  - Avoid three-dimensional representation
  - Use a palette of sequential colors
  - Consider possible "color blindness" and sight-impaired audiences
  - Avoid pie charts or simple histograms and consider using:
    - Scatterplots
    - Bars and bubble charts
    - Density plots
    - Boxplots

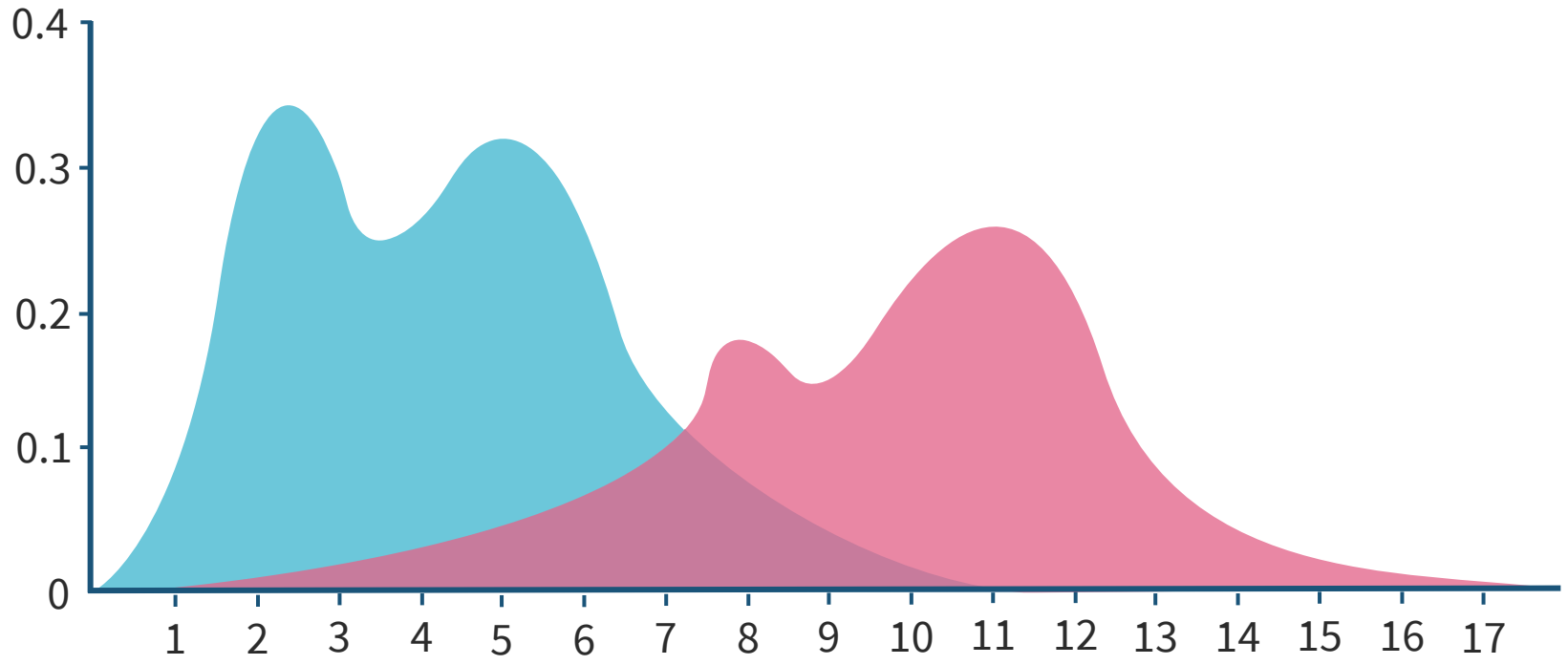
SCATTERPLOTS



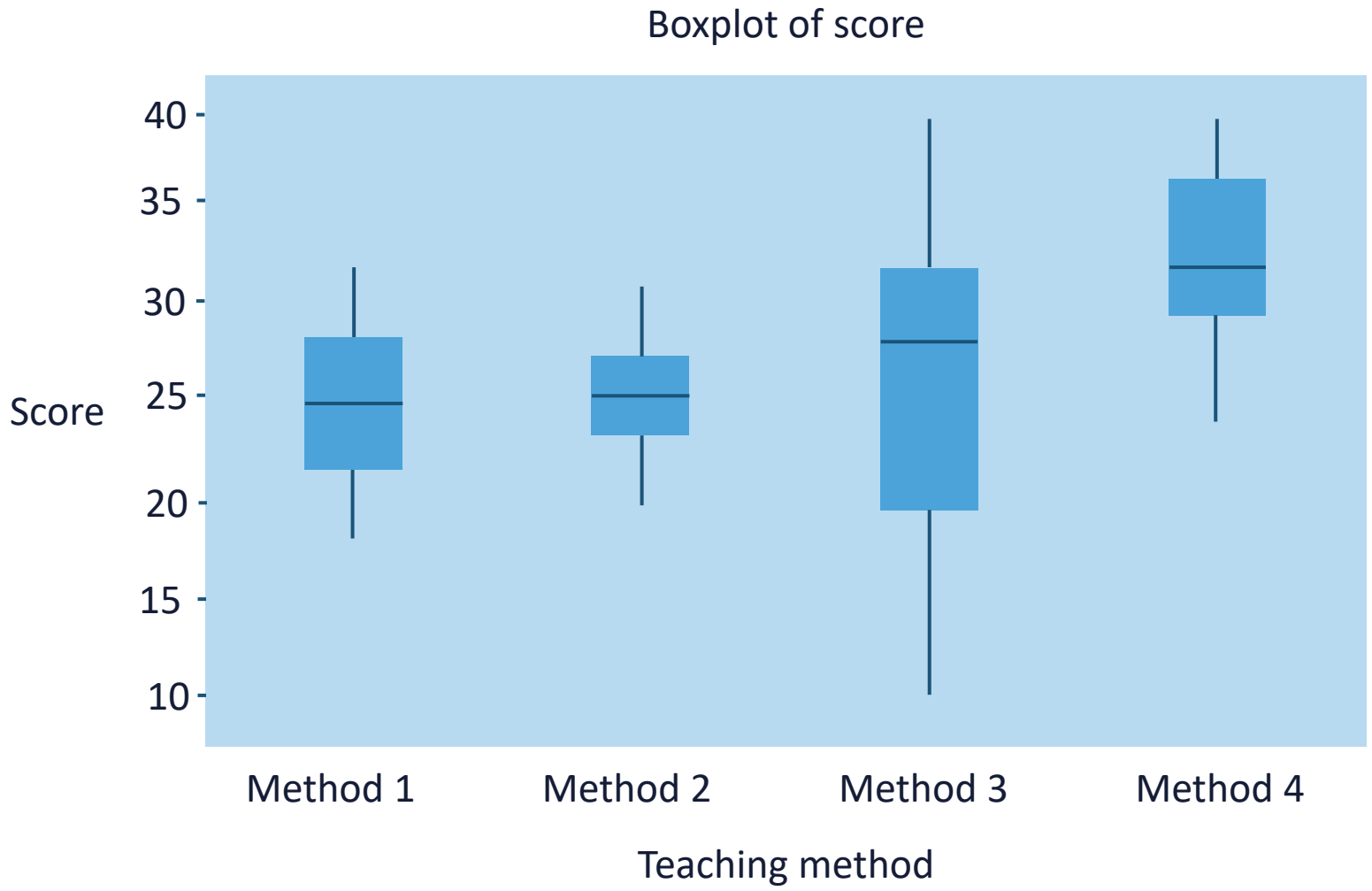
BUBBLE CHARTS



DENSITY PLOTS



BOXPLOTS

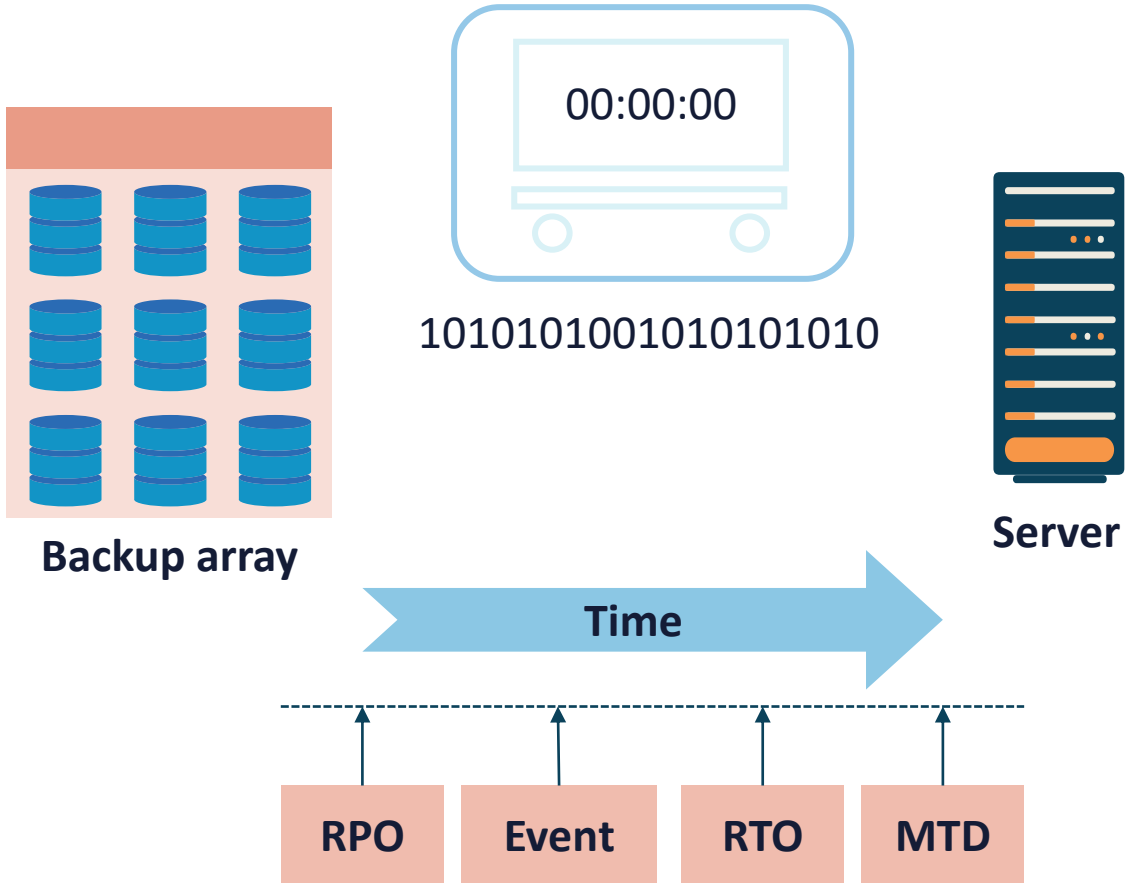

Boxplot of score
Score
40
35
30
25
20
15
10
Method 1
Method 2
Method 3
Method 4
Teaching method

BUSINESS IMPACT ANALYSIS (BIA)

- A BIA predicts the consequences of a disruption to a business and collects information needed to develop recovery strategies
- Potential loss scenarios should be identified from risk assessment
- Activities may include developing questionnaires, conducting workshops, distributing stakeholder surveys, and performing follow-ups and gap analysis

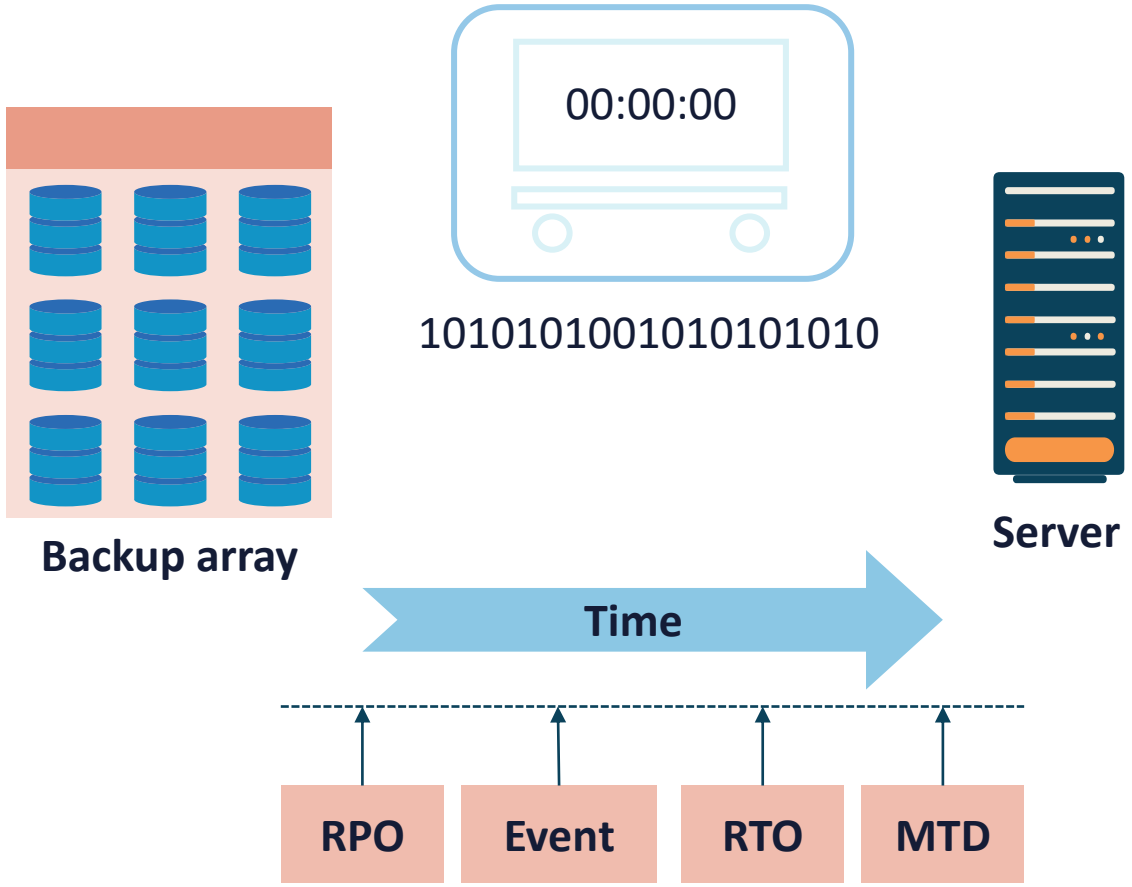
BIA METRICS: RTO

- The **Recovery Time Objective (RTO)** is the amount of time needed to recover a resource, service, application, or function
- It must be less than or equal to the maximum tolerable downtime (MTD)
- Any solutions must be completed within this time frame, or it is considered an unacceptable loss
- Ways to reduce RTO include
  - Adding physical security
  - Adding redundancy
  - Purchasing insurance
  - Investing in better generators
  - Investing in faster recovery solutions



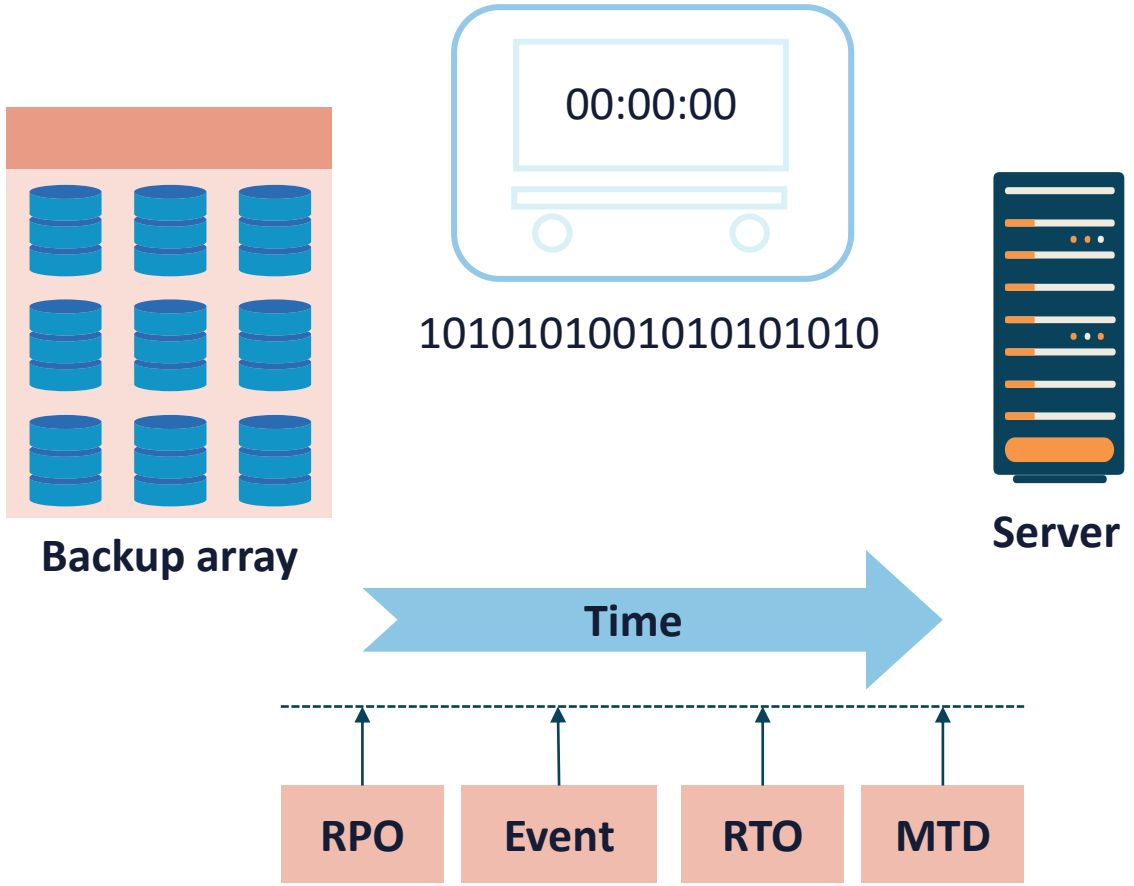
BIA METRICS: MTD

- The maximum tolerable downtime (MTD) is also called maximum allowable downtime (MAD)
- This BIA metric represents the absolute maximum amount of time that a resource, service, or function can be unavailable before the entity starts to experience a catastrophic loss
- When the MTD is exceeded, the disaster recovery plans (DRPs) are often triggered



BIA METRICS: RPO

- The Recovery Point Objective (RPO) is often represented as the target amount of time within which a process must be restored after disruption
- It is commonly a point when some manual or automated task occurred
- The activity point, relative to a disaster, is where the recovery process begins:
  - Last Known Good Configurations
  - Database transaction logs
  - Snapshots
  - Recovery volumes
  - State machine instances



MEAN TIME BETWEEN FAILURES (MTBF)

- MTBF is the measurement of the reliability of a hardware system (Cisco/Juniper router), component, or hot spare
- This data often comes from Original Equipment Manufacturers (OEMs), retailers/distributors, or third-party consumer reporting
- The MTBF of solid-state drives (SSDs) is usually rated in the millions of hours, so an MTBF of 1 million hours means that the average lifespan of a device is over 114 years
    - Industrial SSDs typically have ratings between 2 million hours (about 228 years) or 5 million hours or 570 years

MEAN TIME TO REPAIR OR REPLACE (MTTR)

- This meaningful metric determines how long it will take in minutes, hours, or days to repair or replace a failed system, component, application, or service
- The MTTR is often calculated for replacements and hot spares
- This BIA measurement is heavily affected by supply chain disruptions, backorders, and vendor (manufacturers, wholesalers, distributors) dislocation
- It is typically a mathematical average value based on experience and documentation:
  - MTTR = (total down time)/(number of breakdowns)

SECURITY COMPLIANCE AND THIRD-PARTY RISK

Objectives

- Explore compliance monitoring and reporting
- Describe the consequences of non-compliance
- Consider privacy issues
- Examine vendor assessment and selection
- Compare agreement types

COMPLIANCE

- 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 MONITORING

- Compliance monitoring is a continuous process to ensure that all organizational subjects are adhering to all policies and procedures in the published policies and procedures
- Goals of compliance monitoring include:
  - Exposing compliance risk issues in an organization's operations or functions
  - Helping organizations achieve consistent regulatory compliance and avoid areas of non-compliance
- Compliance monitoring is often considered an important part of security governance and overall cybersecurity posture
- Failure to conform with compliance requirements can result in severe fines and business disruptions

COMPLIANCE MONITORING ACTIVITIES

- Monitoring for continuous certification and accreditation
- Publishing all compliance and regulatory requirements
- Tracking and recording all compliance and remediation initiatives
- Supporting a compliance manager enforcing a Separation of Duty (SOD) or larger Zero Trust initiative
- May be an activity for one with the role of a data steward in some organizations

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 CARE

- 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
- It involves all ongoing operational controls
- Many organizations with rely on an ITIL4 continual improvement framework to optimize due care to elevate them to a higher Capability Maturity Model (CMM) level

ATTESTATION

- Compliance attestation is a formal validation document that is used to certify an organization's status to interested external parties
- According to ISO/IEC, attestation is the issue of a "statement" based on a decision that specific requirements have been met
- SOC 2 is an attestation report that offers in depth information and assurance about an entity's availability, processing integrity, confidentiality, and privacy controls

ACKNOWLEDGEMENT

- Compliance acknowledgment typically involves a statement affirming that an authorized enterprise understands and will adhere to their confidentiality obligations and a security and privacy mandate such as:
  - Sarbanes-Oxley (SOX)
  - Health Insurance Portability and Accountability Act (HIPAA)/Health Information Technology for Economic and Clinical Health (HITECH)
  - SOC1/2
  - Payment Card Industry Data Security Standard (PCI DSS)
  - General Data Protection Regulation (GDPR)
  - CSA Cloud Controls Matrix (CCM)
  - Other regulations and governance

COMPLIANCE MONITORING AUTOMATION

- Compliance processes are time-consuming, and when there is no automation involved, it quickly uses productive hours
- A manual workflow can take around 150 hours, while an automated compliance tool may only need about 10-12 hours to complete
- Compliance automation tools ensure the protection of data and are governed according to the applicable regulations such as GDPR
- Tasks can include self-assessment, planning and monitoring controls, testing, and reporting
- Compliance automation tools can assist enterprises to reduce non-compliance risk, improve efficiency, and attain better visibility

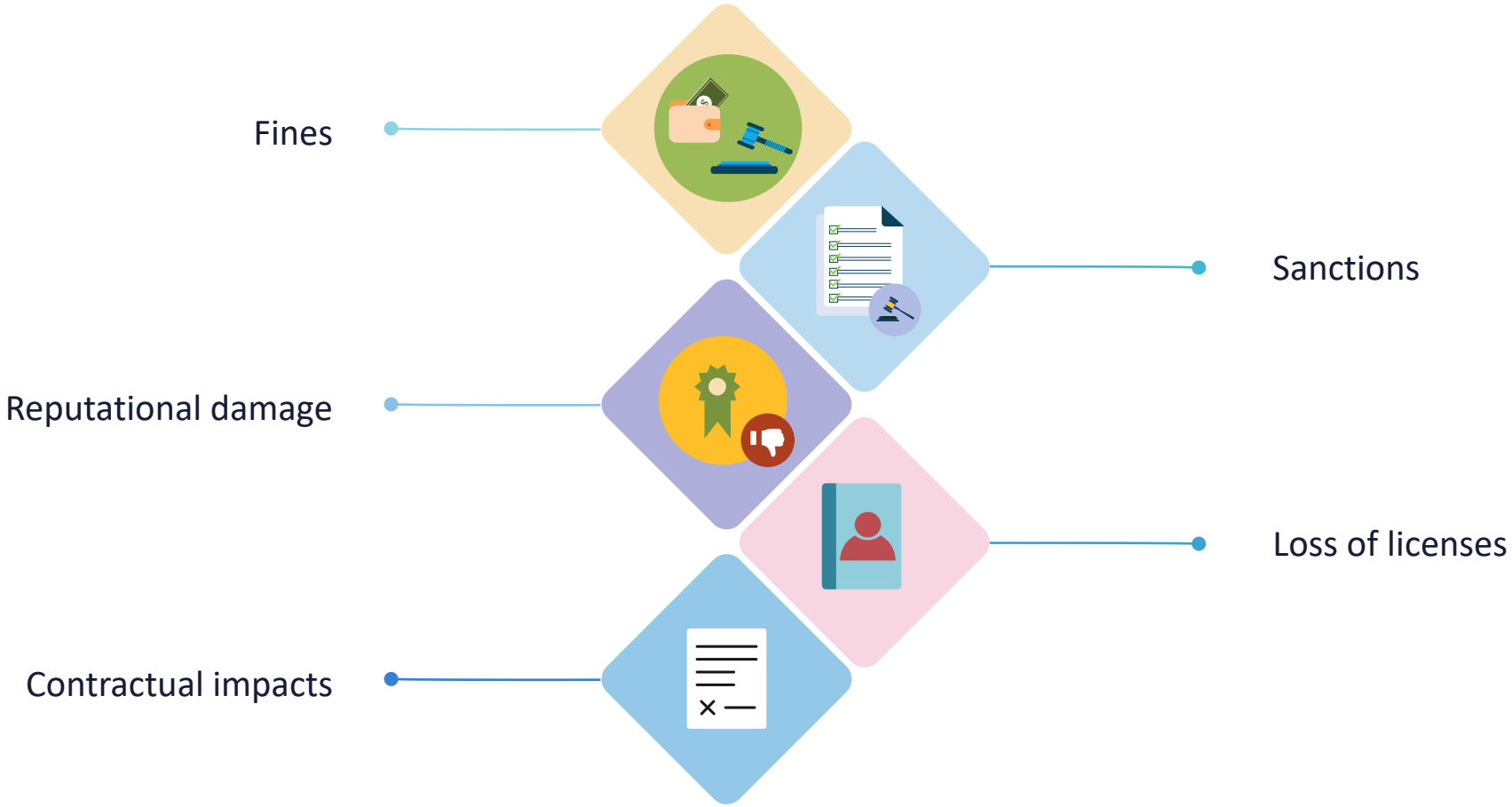
INTERNAL COMPLIANCE REPORTING

- Internal compliance reporting allows organizations to institute internal controls, monitor employee behavior, and detect potential fraud, misconduct, or non-compliant activities to:
  - Adhere to regulatory requirements
  - Maintain stakeholder trust
  - Mitigate risk
  - Support ethical considerations and corporate social responsibility (CSR)
  - Establish internal governance and performance monitoring

EXTERNAL COMPLIANCE REPORTING

- External compliance refers to following the rules, laws, and standards set by a Government entity
  - The primary goal is to avoid any negative impact on the organization such as fines, penalties, and loss of corporate goodwill
  - The state or province in which the firm is incorporated is concerned with defining these compliances
  - External compliance reports and audits are reviewed by regulatory bodies for determining compliance status, certification, and/or accreditation
  - These can vary per industry, applicable regulations, and geographical locations

CONSEQUENCES OF NONCOMPLIANCE



Privacy Considerations

- Legal implications
- Local/regional, national/global distinctives
- Data subjects (controller vs. processor)
- Ownership
- Data inventory and retention
- Right to be forgotten

Right to Be Forgotten

- According to the EU GDPR: "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay if one of a number of conditions applies"
- "Undue delay" is typically about a month
- Organizations must also take reasonable measures to validate the person requesting erasure is truly the data subject

https://gdpr.eu/right-to-be-forgotten/

Right to Be Forgotten

- The right to be forgotten merges with people's right to access their personal information
- The right to control one's data is meaningless if people cannot act when they no longer consent to processing, when there are significant errors within the data, or if they believe information is being stored unnecessarily
- In these cases, an individual can request that the data be erased
- This is not an absolute right as the GDPR walks a fine line on data erasure

https://gdpr.eu/right-to-be-forgotten/

Vendor Assessment and Selection

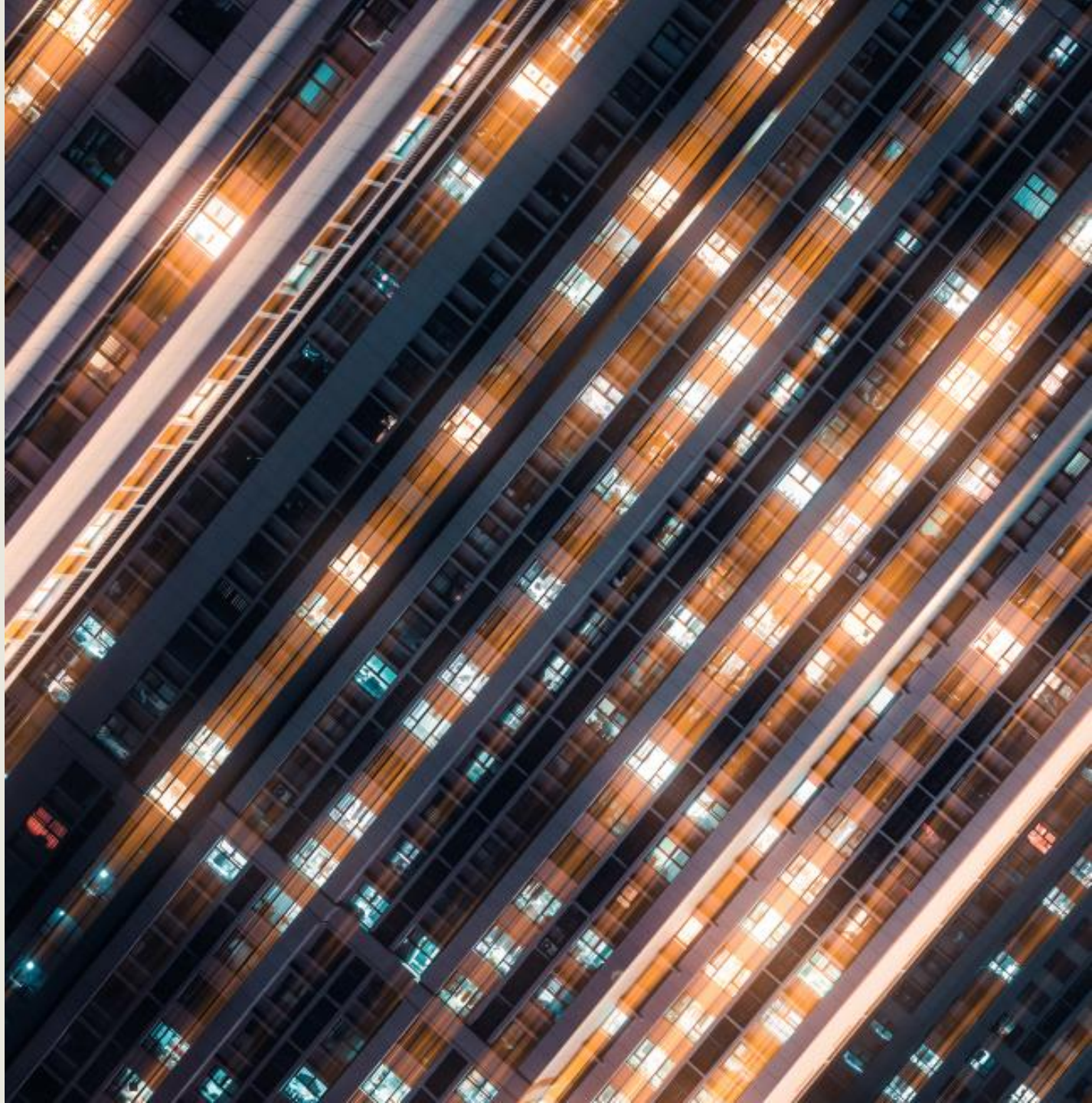
- Penetration testing
- Right-to-audit clause
- Evidence of internal audits
- Independent assessments
- Supply chain analysis

Vendor Assessment and Selection

- Vendor selection
- Due diligence
- Conflicts of interest
- Questionnaires
- Rules of engagement

Case Study: The CSA Cloud Controls Matrix

- The Cloud Controls Matrix is a cybersecurity control framework for cloud computing that aligns to the Cloud Security Alliance (CSA) best practices
- It is considered the de-facto standard for cloud security and privacy
- There is an accompanying questionnaire, CAIQ, that populates the "STAR" registry and offers a set of "yes or no" questions based on the security controls in the CCM



Cloud Controls Matrix v4

	A	B	C
1	CCM™	CLOUD CONTROLS MATRIX v4.0.6	
2	**Introduction**		
6	The CCM V4 spreadsheet includes five tabs:		
7	• Introduction.		
8	• CCM Controls.		
9	• CCM Implementation Guidelines.		
10	• CCM Auditing Guidelines.		
11	• CCM Scope Applicability (Mappings).		
12	• Consensus Assessments Initiative Questionnaire (CAIQ).		
13	• Acknowledgments.		
14			
15	**II. Components Description**		

Nondisclosure agreements (NDA)

- This is also called a "confidentiality agreement"
- NDAs are legally enforceable contracts that generate a confidential/private relationship between an entity that has sensitive information and an entity who will gain access to that information
- A confidential relationship means one or both parties has a duty not to share that information
- These can be signed:
  - At the outset of a pre-engagement meeting
  - Early in the interview process
  - As part of the hiring and post-termination process
  - In anticipation of a Memorandum of Agreement (MOA) or Memorandum of Understanding (MOU)

Memorandum of Agreement

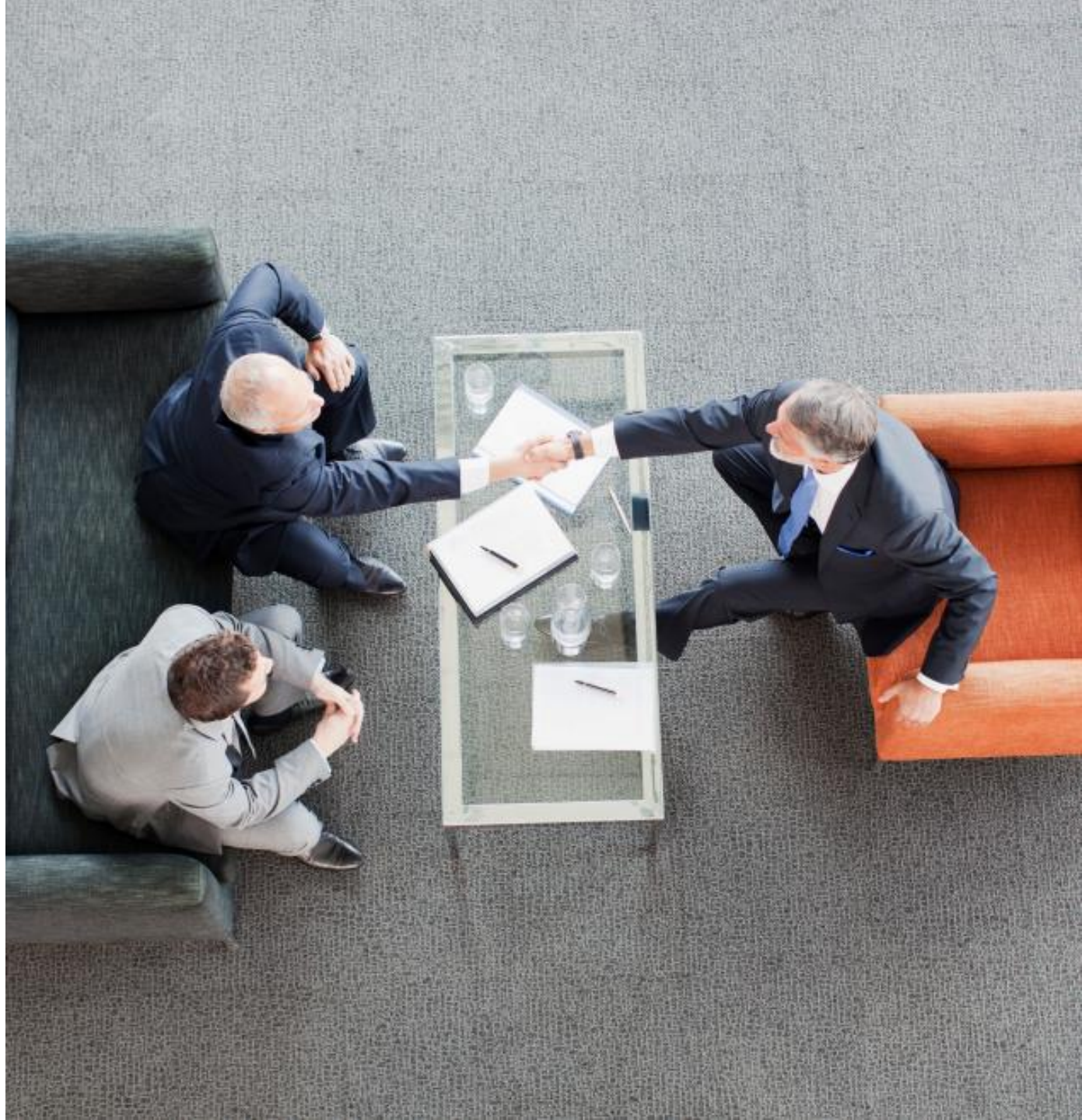
- A Memorandum of agreement is a written document describing a cooperation between two entities that want to work together on a project or an agreed-upon objective
- It serves as a legal document that describes the details of a partnership agreement and is more formal than a verbal agreement but less formal than a contract
- Organizations can use this to establish and outline shared agreements
- An MOA may be used regardless of whether currency will be exchanged as part of the agreement

Memorandum of Understanding

- A memorandum of understanding is a nonbinding agreement that declares each party's objectives in performing a business transaction or initiating a new partnership
  - This form of agreement may also be referred to as a letter of intent (LOI) or MOA
- If a business is in the beginning phases of a transaction with another party, an MOU is often the first step toward a formal agreement via a binding contract
- It openly defines how the parties will work together and what are the mutual expectations and responsibilities
- The goal is to attain a mutual understanding of the partnership so that both parties can move forward into an enforceable contract

Service-level Agreement (SLA)

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



Master Service Agreement (MSA)

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

Work Order (WO)

- A work order is a document that delivers all the information about an ongoing maintenance task and outlines a process for completing that activity
- Work orders can include details regarding:
  - Who authorized the job
  - The scope
  - Who the job/task is assigned to
  - What are all expectations (delivery time or date)

Statement of Work (SOW)

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

Business Partnership Agreement (BPA)

- A BPA establishes rules for two or more parties going into business together
- It is a legally binding document that outlines every detail of the business operations, ownership stakes, financials, accountabilities, and decision-making approach and strategies
  - General partnerships
  - Limited partnerships
  - Limited liability partnerships
  - Limited liability limited partnerships

Audits, Assessments, and Awareness

Objectives

- Describe internal and external audit and attestation
- Explore penetration testing
- Define user guidance and training
- Examine mock phishing campaigns
- Explain security training monitoring and reporting

Internal Audit and Attestation

- An internal security audit operates by attesting that all organizational information systems are adhering to a set of internal or external criteria regulating data security, network security, and infrastructure security
- Internal criteria include the company's IT policies, procedures, and security controls
- Internal audit should objectively assess the organization's overall strategy for handling emerging threats from a governance, architectural, operational, and technology standpoint

Security Audit Committees

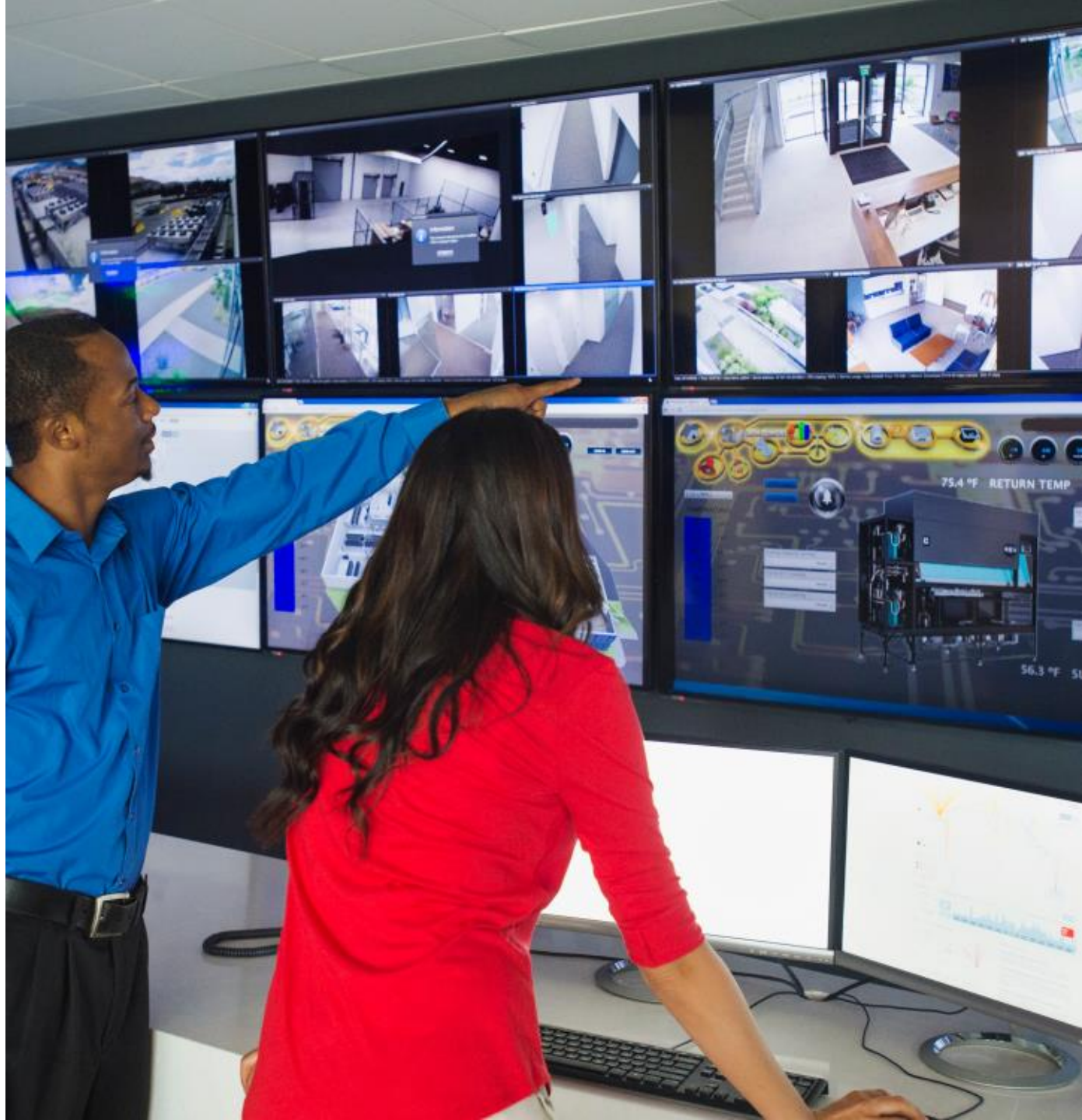
- The audit committee is responsible for assisting independent auditors to examine the organization's security reporting system in a process independent of management by:
  - Offering critical oversight of the corporation's reporting processes, internal controls, and independent auditing
  - Providing checks and balances
  - Allowing a forum for discussing security concerns candidly and objectively
- An audit committee is typically appointed by the board and is composed of directors who are not part of management

Duties of Internal Audit Committees

- Risk oversight
- Ethics and compliance
- Oversight of independent auditors
- Oversight of internal audit
- Manage controls and reporting

Self-assessment Audits

- The **self-assessment with independent validation (SAIV)** approach is a more cost-effective assessment solution
- The organization's internal audit activities leverage a capable, independent validator who is well-versed in security assessment methodology
- The goal is to deliver an independent validation of the internal audit activity's self-assessment
- In addition to reviewing the self-assessment, the validator also confirms work completed by the self-assessment team and interviews senior management



External Audit and Attestation

- In an external audit, an organization compares itself to an established standard
  - ISO 27001 is an example of a compliance audit with a certification as the result
  - CSA certifies auditors for cloud security, and they use the Cloud Controls Matrix (CCM)
- The level for audits can be further segmented based on the agreed-upon procedures that are involved in the scope

Audits vs. Assessments

- There is technically a difference between an assessment and an audit
- An assessment could be seen as an "audit plus"
- Assessments compare with both standards and industry practices, the auditor's knowledge and experience, etc.
- For example, Payment Card Industry Data Security Standard (PCI DSS) is an audit, but organizations are required to go through a penetration test as well, which is an assessment
  - Therefore, PCI DSS can also be called an assessment

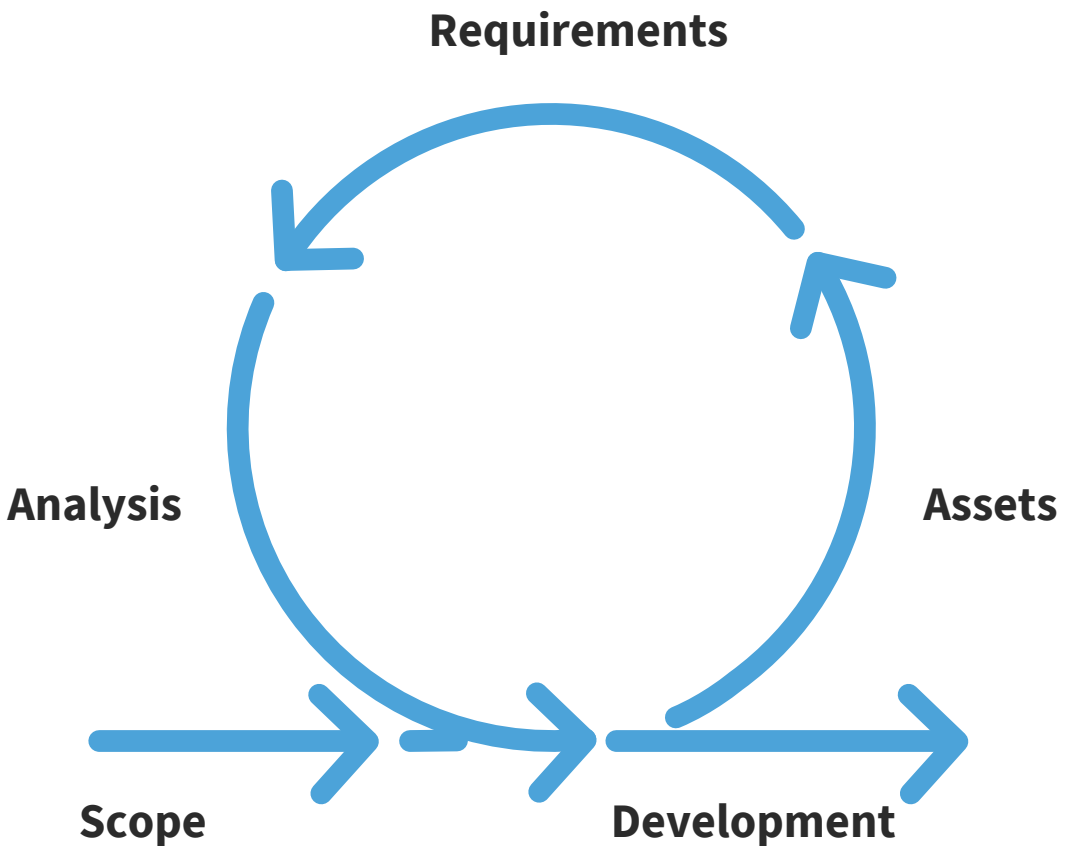
Security Examinations

- Security examinations are used to certify security professionals at various experience levels to participate in auditing and assessments
- Common examples of security examinations are:
  - CompTIA Security+
  - CompTIA Advanced Security Practitioner (CASP+)
  - Certified Information Systems Security Professional (CISSP) from ISC^2
  - Certified Information Security Manager (CISM) from ISACA

Independent Third-parties

- The audit of information security is a comprehensive assessment that evaluates, often with gap analysis, the current state of security controls in the organization
- It enables the planning of timely actions to raise the level of difficulty or resistance to threat agents
- When applied to DevSecOps, a third-party security audit is an exhaustive assessment of all code, documentation, and processes related to a software system by an independent security firm
- The goal of an audit is to uncover potential security risks which can then be patched by the software's developer

Independent Third-party Audit Process



Penetration Testing

- Penetration testing is a process used to collect information and actively expose vulnerabilities in a system or application by conducting actual exploits and red team attacks
- Penetration testing is conducted as a **known** environment, **partially known** environment, or **unknown environment**, where the tester assumes the attacker role to discover vulnerabilities and weaknesses
- Pentesting can be launched against physical, technical, and/or logical controls

Penetration Testing

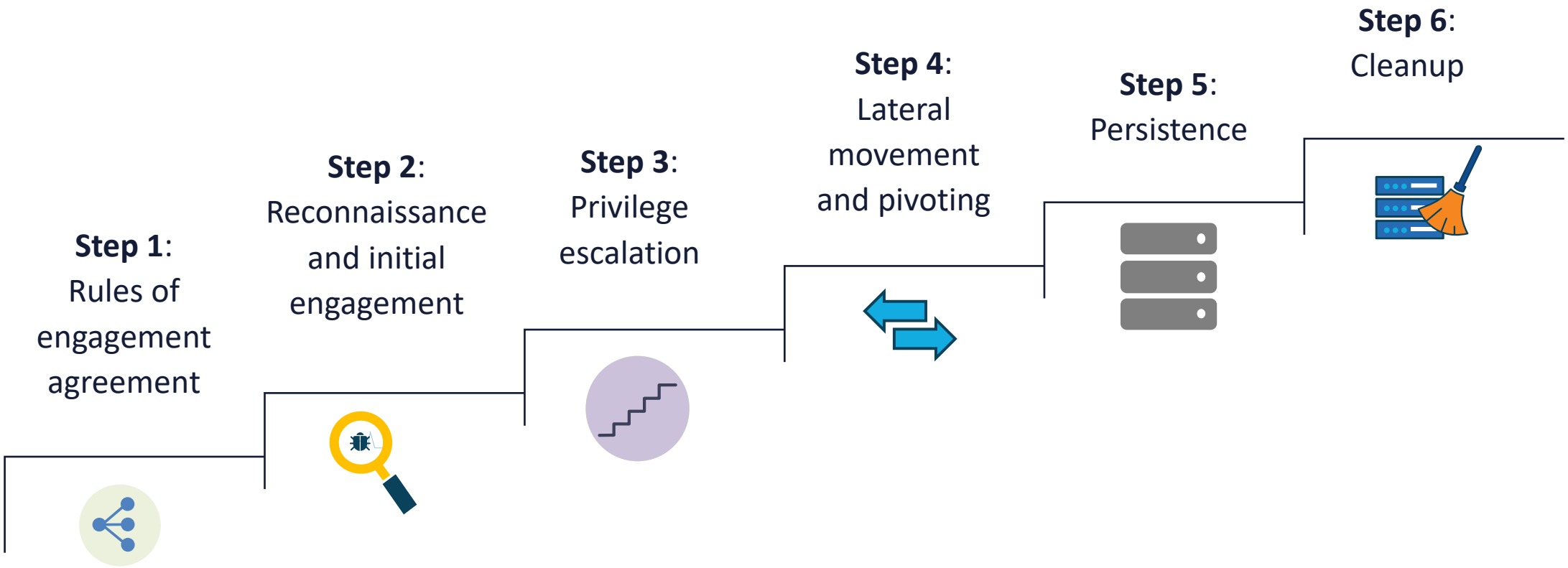
Penetration testing can also be useful for determining:

- How well the system tolerates real world-style attack patterns
- The likely level of sophistication an attacker needs to successfully compromise the system
- Additional countermeasures that could mitigate threats against the system
- The defenders' ability to detect attacks and respond appropriately

Penetration Testing Attributes

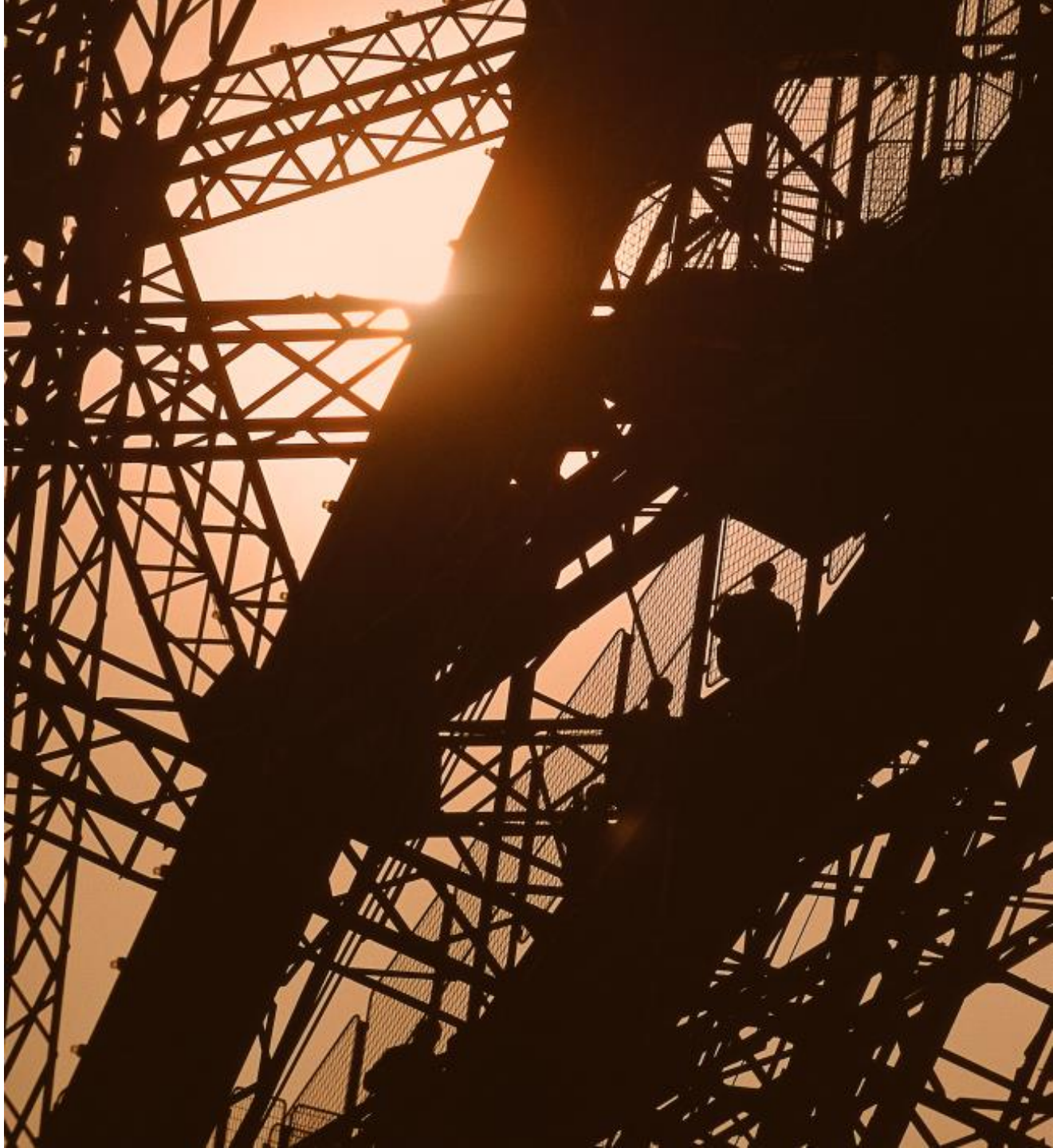
- Known, partially known, vs. unknown environment
- Credentialed vs. non-credentialed
  - Guest user credential
  - Privileged user credential
- Offensive (red team, threat hunting) vs. defensive (blue team)
- Integrated with vulnerability assessments, incident response testing, and other decision-making initiatives
- Intrusive vs. non-intrusive
- Passive vs. active

Penetration Test Life Cycle



Penetration Testing Frameworks

- **SSAF** – framework provided by Open Information Systems Security Group (OISSG); a not-for-profit organization based in London
- **OSSTMM** – open-source security testing created by Institute for Security and Open Methodologies (ISECOM)
- **OWASP** – popular methodology used widely by security professionals, created by a non-profit organization focused on advancing software security
- **PTES** – Penetration Testing Execution Standard methodology was developed to cover the key parts of a penetration test
- **NIST** – National Institute of Standards and Technology provides a manual that is best suited to improve the overall cybersecurity of an organization



User Guidance and Training Topics

Policy documents and handbooks

Password policies and management

Situational awareness

Insider threats and use of honey tokens

User Guidance and Training Topics

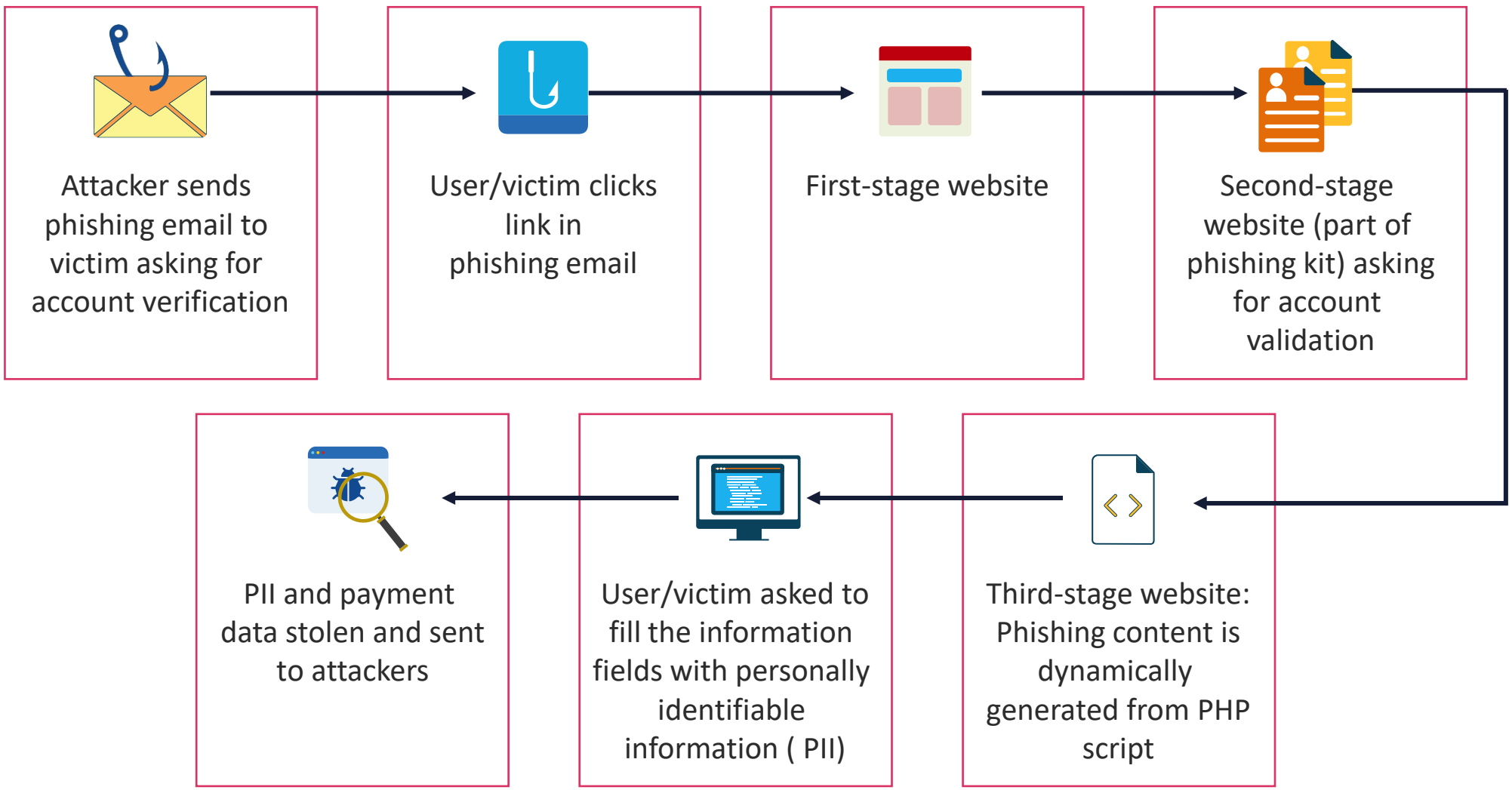
Anomalous behavior and social engineering

Hybrid/remote work environments

Removable media and cables

Operational security

Phishing Attack



Phishing Campaigns

- A phishing campaign is an email hoax designed to replicate a real attack against employees as part of security awareness training
- This is a critical exercise since cybercriminals use phishing, the fraudulent attempt to obtain sensitive information such as intellectual property, credentials, and credit card details by spoofing a trustworthy organization or reputable partner in an email communication
- These initiatives are used to support security training for new hires and ongoing anti-phishing awareness for all stakeholders
- The goal is not to entrap and punish employees but rather raise awareness and instruct

Security Training Monitoring and Reporting

Security training monitoring and reporting must be scoped to the specific audience to deliver different types of security training:

- Basic security awareness training
- Technical security training
- Security management training
- Compliance training

Security Training Monitoring

- Regardless of the training modality, participants should be able to answer surveys and evaluations about all aspects of the experience
- Participants should also be provided with an avenue for giving open-ended subjective feedback

Security Training Monitoring

- The Net Promoter Score (NPS) is considered the gold standard customer experience metric
- In this context, the NPS score measures participant loyalty by looking at their probability of recommending a given security training experience
- NPS scores are measured with a single-question survey and reported with a number ranging from -100 to +100, where a higher score is desirable

Security Training Reporting

- The NPS score evaluation would only be a part of the reporting process
- Often peer and supervisory evaluations should be performed to offer valuable critique and reinforcing feedback to the one delivering the training
- This evaluation should also include the origin content, graphical representations, test questions, and various modalities of the training
- All reporting best practices mentioned in this Security+ training should be considered

Thank You for attending SECURITY+

Class will begin at 10:00 am
Central Standard Time