RISK MANAGEMENT CONCEPTS

Objectives

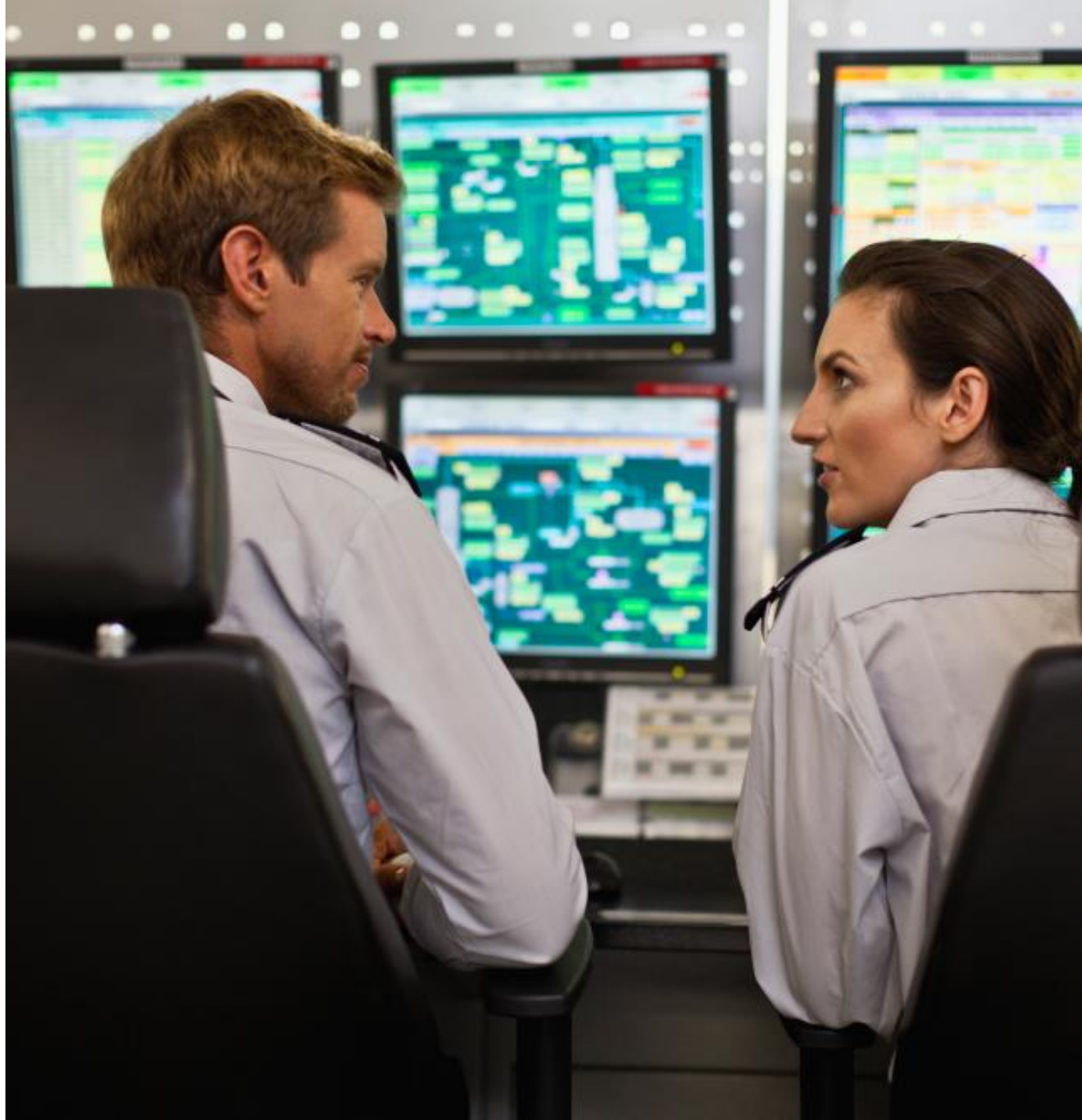
- Examine threat and vulnerability identification
- Explore risk analysis, assessment, scope, and response and treatment
- Compare control categories and types
- Learn about control assessments and continuous monitoring and measurement
- Know risk management reporting methods and continuous improvement
- Compare popular risk frameworks

THREAT AND VULNERABILITY IDENTIFICATION

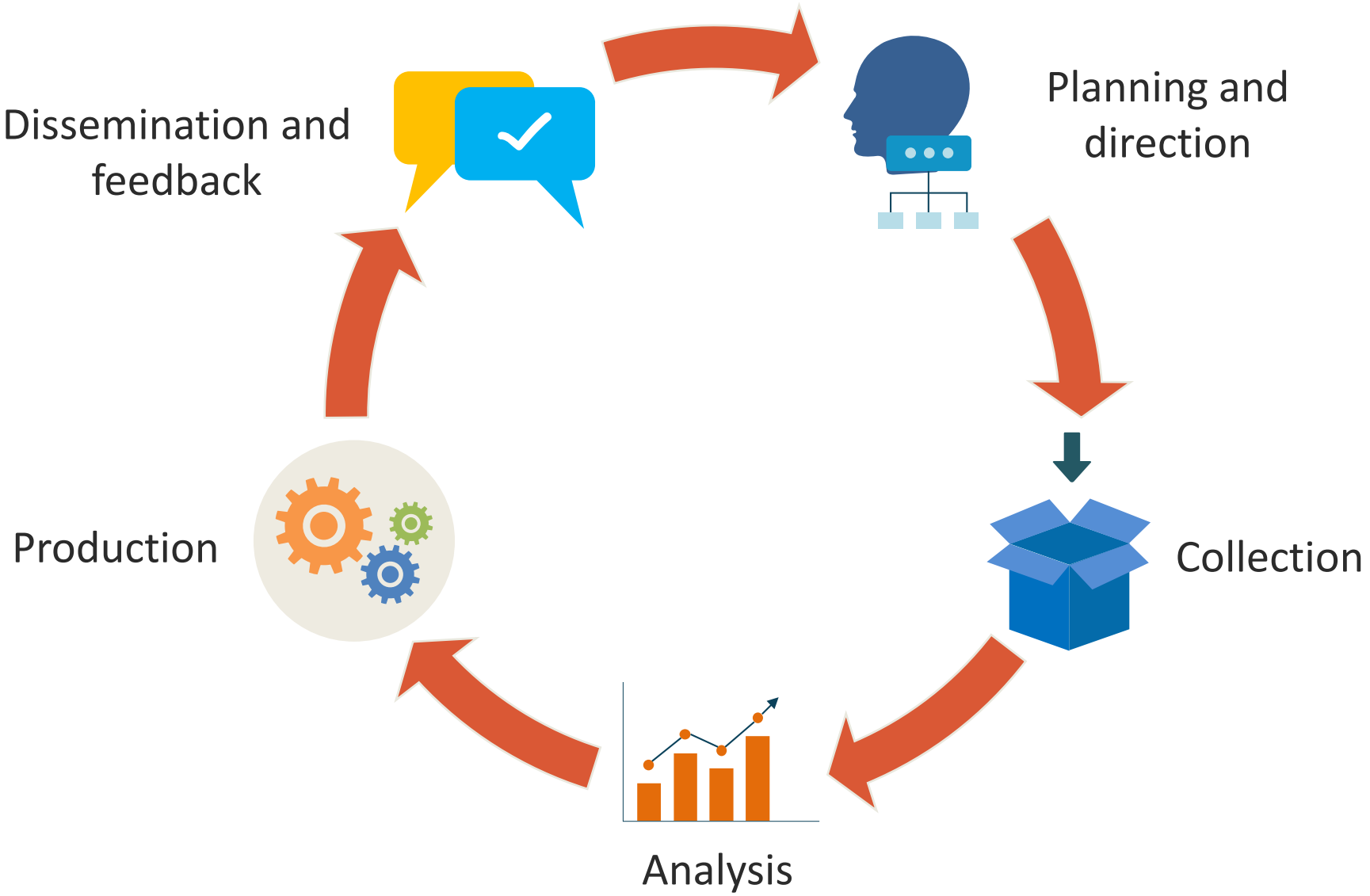
- NIST broadly defines a threat as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
- Also, the potential for a threat-source to successfully exploit a particular information system vulnerability."

THREAT AND VULNERABILITY IDENTIFICATION

- Threats and vulnerabilities are best defined quantitatively by the security managers to deliver accurate assessments and to acquire control resources
- It should be approached by simply compiling a vague list of "scary things"
- Begin with the most critical assets and those with the highest likelihood that a threat agent's actions will result in a loss (frequency and magnitude)
- It can be a derived value from the threat capability of actors combined with the resistance of existing security controls



THREAT INTELLIGENCE (IDENTIFICATION) LIFECYCLE



THREAT IDENTIFICATION MUST BE COMPREHENSIVE

- Site and facility security
- Client endpoints
- Infrastructure devices (L2/3)
- Servers and load balancers
- Security appliances
- Wireless and telephony LAN components
- Client and server applications
- Specialty controllers and embedded systems
- Custom devices and equipment

RISK ANALYSIS, ASSESSMENT, AND SCOPE

- The **scope** of the risk analysis and assessment must be established first:
  - Physical facility, site, or campus security
  - Wireless guest VLAN
  - Corporate LAN
  - Intranet servers
  - DMZ/public access zone
  - Server farms
  - Data center
  - Storage area network (SAN)
  - Hypervisor clusters
  - Cloud deployment (including hybrid)
  - Supply chain

POPULAR VULNERABILITY DATABASES

National Vulnerability Database (NVD)

DISA IAVA Database and STIGS

Common Vulnerabilities and Exposures (CVE)

Open Vulnerability and Assessment Language (OVAL)

VulnDB – Vulnerability Intelligence

IBM X-Force

QUALITATIVE RISK ANALYSIS

- According to NIST, qualitative analysis uses "a set of methods, principles, or rules for assessing risk based on **nonnumerical** categories or levels."
- Qualitative analysis involves gathering and evaluating nonnumerical data (i.e., text documents, diagrams, video, or audio) to comprehend concepts, opinions, or experiences
- It can also be used to get in-depth insights into a security challenge or to generate new ideas for initiatives

QUALITATIVE RISK ANALYSIS

- Qualitative analysis is arguably a more subjective tactic that uses evaluation and estimation
- It can be valuable when the manager has access to:
  - Real-world scenarios
  - Expert judgment (subject matter expertise)
  - Applicable case studies
  - Best practices and guidance
  - Third-party support (e.g., insurers, auditors, pen testers)
  - Intuition (an art and a science)
- It often involves interviews and surveys (e.g., Delphi Methods), brainstorming sessions, workshops, tabletop testing, and consulting with experts

QUALITATIVE HEAT MAPS

		Negligible	Minor	Moderate	Critical	Disastrous
		1	2	3	4	5
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

SEMI-QUANTITATIVE ANALYSIS

An approach that delivers approximate and relative measurements instead of absolute quantification

Impact

- Negligible = 1 (no impact)
- Minor = 2 (< $1 million)
- Moderate = 3 (≥ $1 million)
- Critical = 4 (≥ $100 million)
- Disastrous = 5 (complete)

Likelihood

- Improbable = 1 (almost never)
- Seldom = 2 (not in 5 years)
- Occasional = 3 (once in last 5 years but not in last year)
- Likely = 4 (once in last year)
- Frequent = 5 (several times a year)

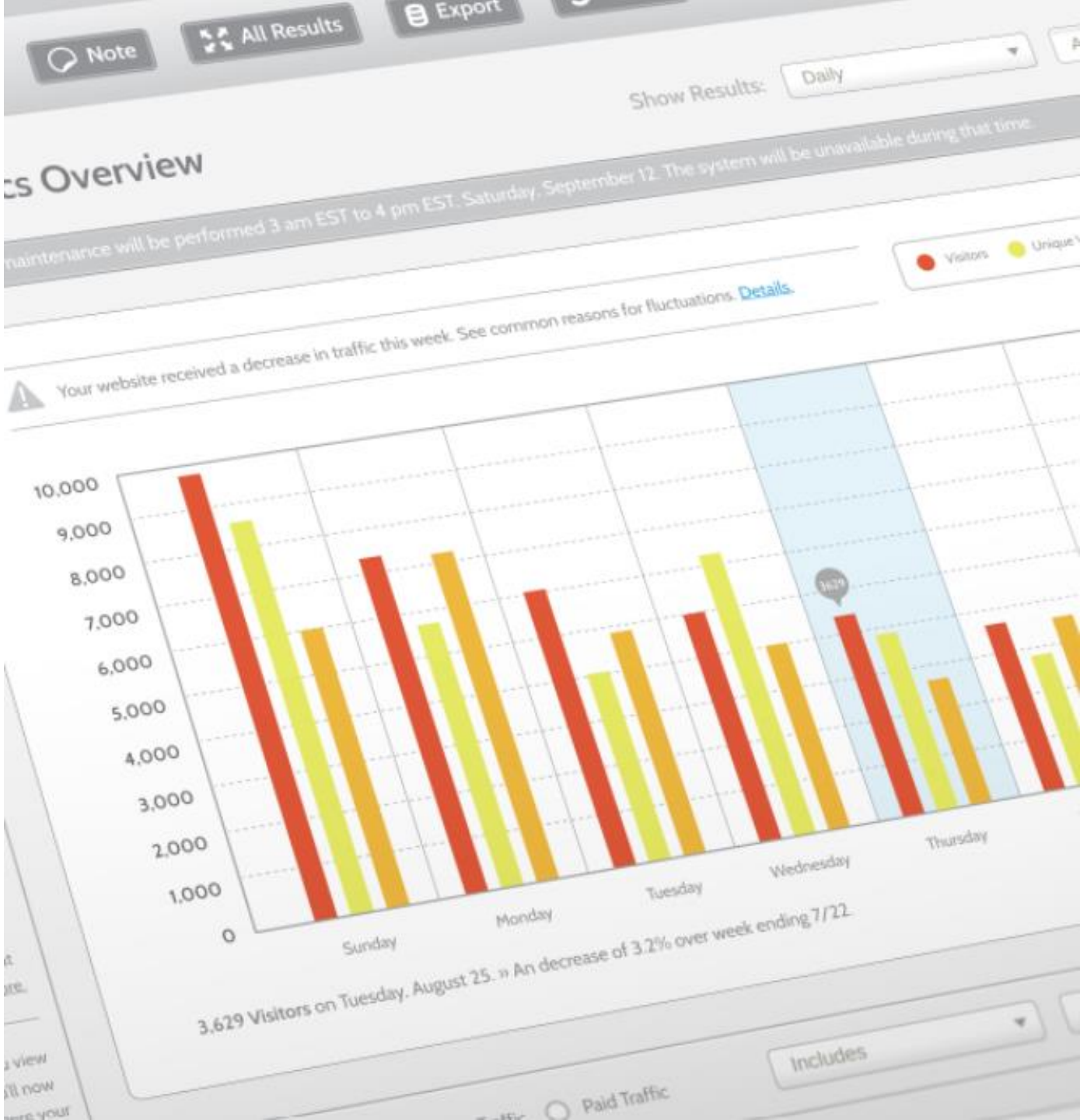
Risk of event = 4 (material impact) x 3 (moderate likelihood) = 12

QUANTITATIVE RISK ANALYSIS

- Quantitative risk analysis is a mathematical methodology for obtaining monetary and numeric outputs based on the following:
  - Asset values
  - Impact and magnitude (severity)
  - Probability and likelihood of occurrence
  - Threat frequency
  - Threat actor attributes
  - Costs and effectiveness of safeguards

CLASSIC WHITMAN ANALYSIS

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



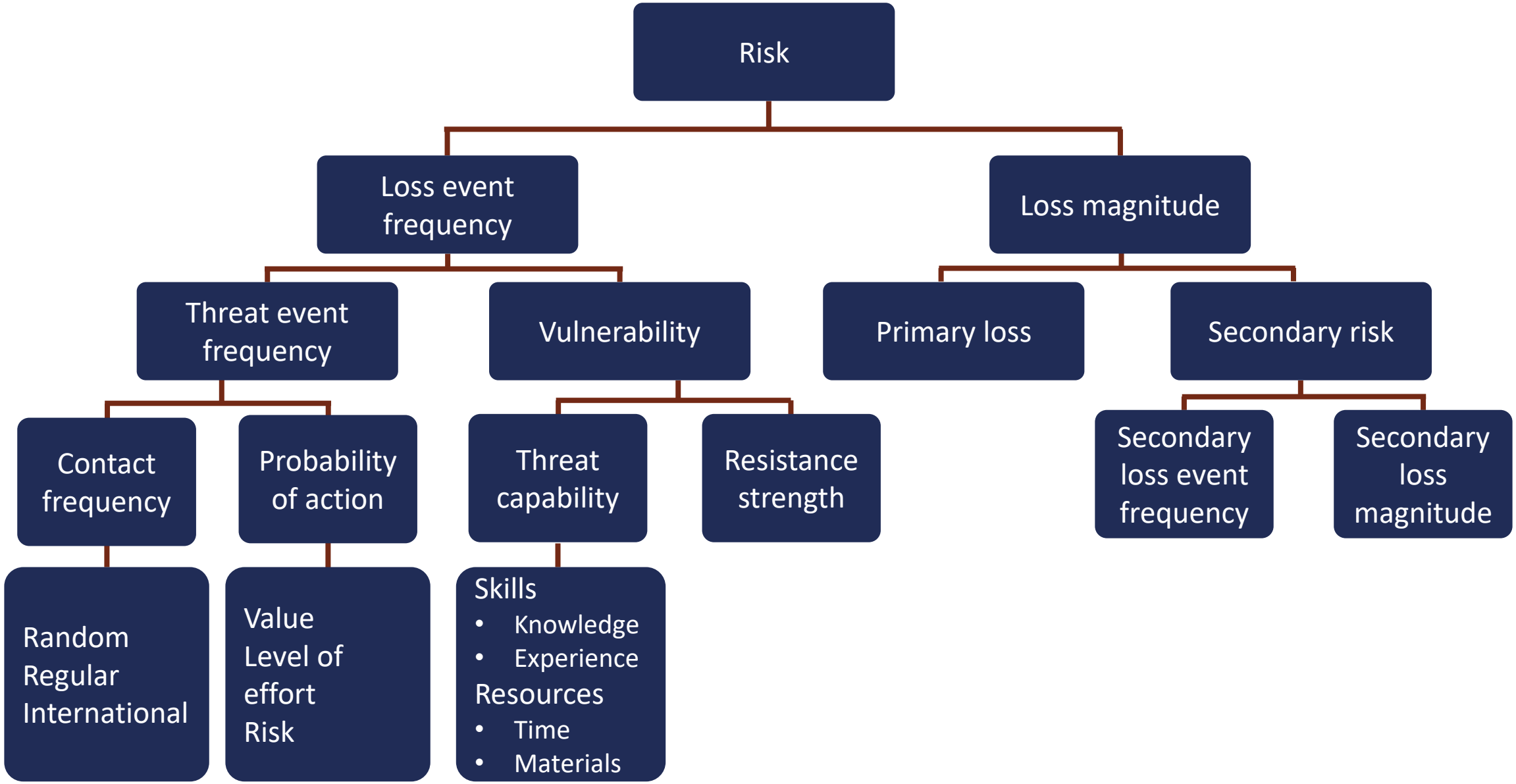
CLASSIC WHITMAN ANALYSIS

Risk analysis						
Asset	Threat	Asset value	Exposure factor	Single loss expectancy	Annualized rate of occurrence	Annualized loss expectancy
SRV_1	Fire	$15000	100%	$15000	0.1	$1500
SRV_2	Fire	$20000	100%	$20000	0.1	$2000
SRV_1	Flood	$15000	100%	$15000	0.0001	$1.5
SRV_2	Flood	$20000	100%	$20000	0.0001	$2.0
SRV_1	Virus (no AV software	$15000	10%	$1500	365	$547,500
SRV_1	Virus (with AV software	$15000	10%	$1500	1	$1500

FACTOR ANALYSIS OF INFORMATION RISK (FAIR) TM

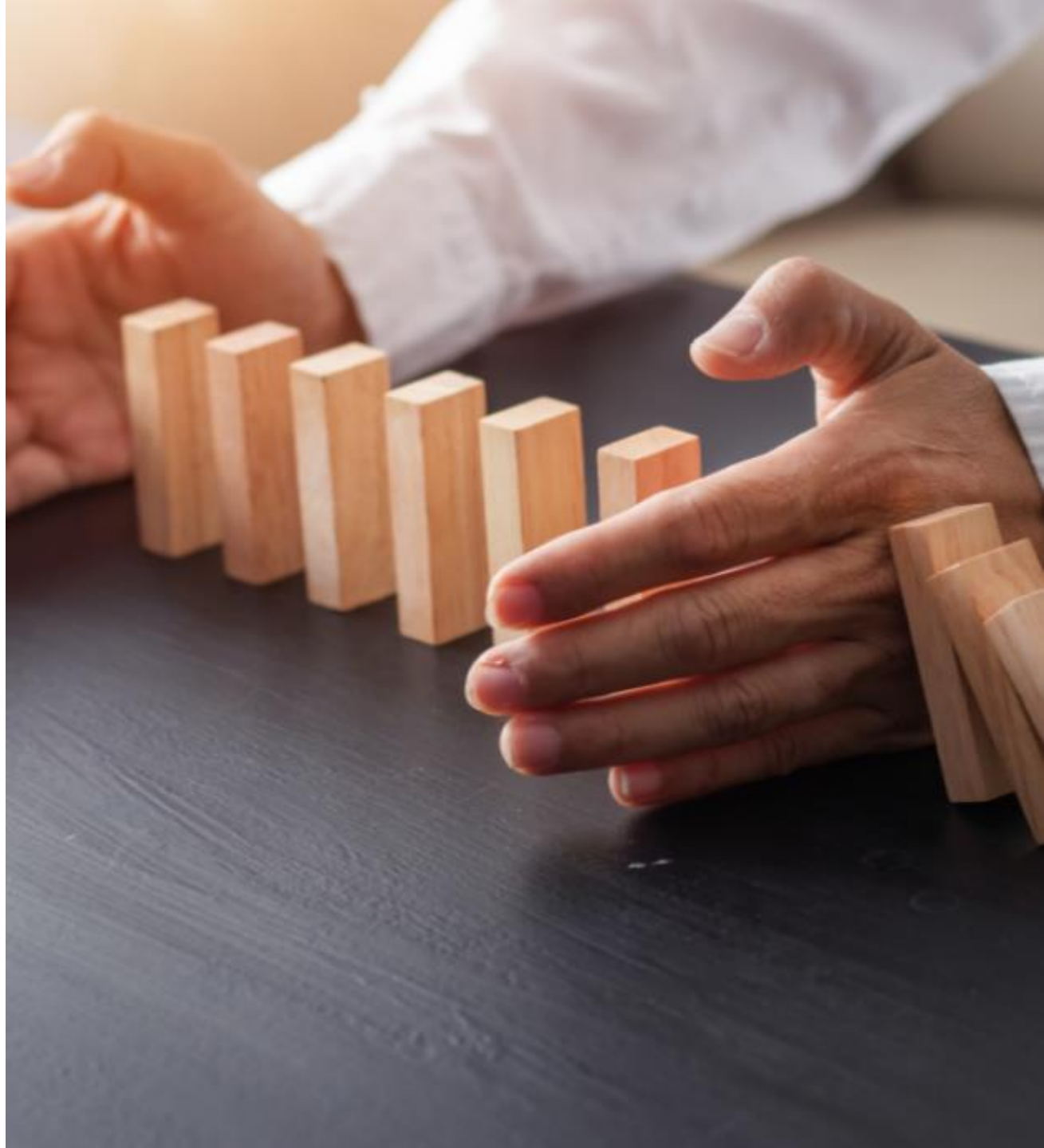
- Factor Analysis of Information Risk (FAIR™) is an internationally recognized quantitative model for information security and operational risk
- FAIR offers a methodology and taxonomy for identifying, analyzing, and quantifying cyber and operational risk in mathematical and financial terms
  - It does not focus output on qualitative color charts or numerical weighted scales
- FAIR establishes a foundation for creating a robust method for managing information risk

FAIR TAXONOMY



RISK TREATMENT: ACCEPTANCE

- Risk acceptance involves:
  - Not introducing any additional safeguards or controls to lower residual risk
  - Determining that the cost of additional countermeasures far exceeds the value or revenue generation of the asset or asset class
  - The process of simply "ignoring" the risk
- Acceptance will often demand that the security manager(s) justify the decision in writing or before decision makers



RISK TREATMENT: AVOIDANCE

- Risk avoidance commonly entails:
  - Deciding not to undertake actions or engage in initiatives that introduce or increase risk or vulnerability
- Examples include:
  - Not processing and storing credit card information of customers on-site
  - An acceptable use policy (AUP) that forbids the use of personal cloud storage like Dropbox
  - Avoiding the use of generative AI based on lack of expertise in machine learning
- Being too risk-averse can lead to missing out on opportunities or advantages

RISK TREATMENT: TRANSFERENCE

- Risk transference is also referred to as risk sharing and involves passing off all or some risk to a third party or shared party
- Examples include:
  - Using a cloud computing shared responsibility through IaaS, PaaS, or SaaS
  - Signing a reciprocal agreement with another organization to share the cost of a cold/warm disaster recovery site
  - Adding an extra cybersecurity policy to your business policy from an insurance company

RISK TREATMENT: MITIGATION

- Risk mitigation is the strategic and tactical use of technical, administrative, and physical controls to reduce risk to an acceptable level
  - The risk is rarely eliminated, but the impact is reduced
- Examples of mitigating risk include:
  - Implementing next-gen endpoint protection, such as Palo Alto Cortex XDR
  - A startup company employing a cloud access security broker (CASB) or managed security service provider (MSSP)
  - Escalating to a cloud-based SIEM/SOAR solution like Azure
  - 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 nor conservative unless necessary

CATEGORIES OF CONTROLS

Administrative

Managerial security governance, guidance, best practices, policies, and procedures, such as a password policy, hiring policy, screening policy, training and awareness

Physical

Controls to protect people and property, such as fences, gates, locks, guards, video cameras, bollards, lighting, and sensors

Technical

Operational controls that reduce risk using firewalls, access controls, ciphers, IDS/IPS, smartcards, biometrics, EDR, and more

CATEGORIES OF CONTROLS

Administrative	Technical	Physical
Effective hiring practices	Controlled user interfaces	Guards
Effective termination practices	Password, tokens, one-time passwords (OTPs)	Fences
Least privilege	Firewalls	Motion detectors
Acceptable use policies	Routers that filter traffic	Locks
Visibility of employee activity	Antivirus software	Cable conduits
Separation of duties	Access control lists	Swipe cards
Rotation of duties	Intrusion detection/prevention systems	Badges
Mandatory vacations	Smart cards	Dogs
Use of social media	Biometrics	Cameras
Training and awareness	Endpoint protection	Alarms

TYPES OF CONTROLS: PREVENTATIVE

- Preventive controls prevent or delay an external or internal structured or unstructured threat
  - Locks – preventative, although all can be defeated through brute force
  - Barbed and electric fences
  - Gates and tire shredders
  - Firewalls (physical and technical)
  - Intrusion prevention sensors (IPS)

TYPES OF CONTROLS: DETECTIVE

- Detective controls identify an attack, breach, or gap in the environment
  - Security cameras monitored from the security operations center or guard desk
  - Intrusion detection sensors
  - SIEM systems collecting alerts, logs, and other inputs
  - Various sensors that trigger alarms

TYPES OF CONTROLS: CORRECTIVE

- Corrective (recovery) controls return a system, application, or service to a pre-established recovery point
  - A rollback or fallback from a faulty or vulnerable patch or update
  - Restoring a server from backup images and data after a ransomware attack
  - Recovering a configuration error by returning to an infrastructure as code JSON or YAML template or stack
  - Thwarting further spread of a DDoS by the incident response team

TYPES OF CONTROLS: DETERRENT

- A deterrent control will discourage an attacker from carrying out the exploit
  - Signage
  - Bollards
  - Window stickers
  - The visual presence of other controls, such as preventative or detective

TYPES OF CONTROLS: COMPENSATING

- A compensating control aids or augments a control that is already in place
  - Can be a permanent solution or a temporary stop-gap measure
  - Moving to a dual-operator environment
  - Automating a previously manual security task or deployment
  - Adding additional supervisory visibility
  - Adding a DLP engine to Microsoft Exchange implementations

COMPENSATION EXAMPLE: PCI

- With PCI-DSS, an organization is unable to fulfill a particular demand based on legitimate technical or documented constraints
- If unable to meet a certain requirement, the compensating controls must meet three criteria:
  - Match the intent and strength of the original requirement
  - Offer a similar level of defense so that the control adequately offsets the risk of what the original PCI DSS requirement was designed to protect
  - Be "above and beyond" other PCI DSS requirements

CHOOSING SECURITY CONTROLS

- NIST SP 800-30 Risk Management Guide for Information Technology Systems states:
  - If control would reduce risk more than needed, then see whether a less expensive alternative exists
  - If control would cost more than the risk reduction provided, then find something else
  - If control does not reduce risk sufficiently, then look for more controls or a different control
  - If control provides enough risk reduction and is cost-effective, then use it

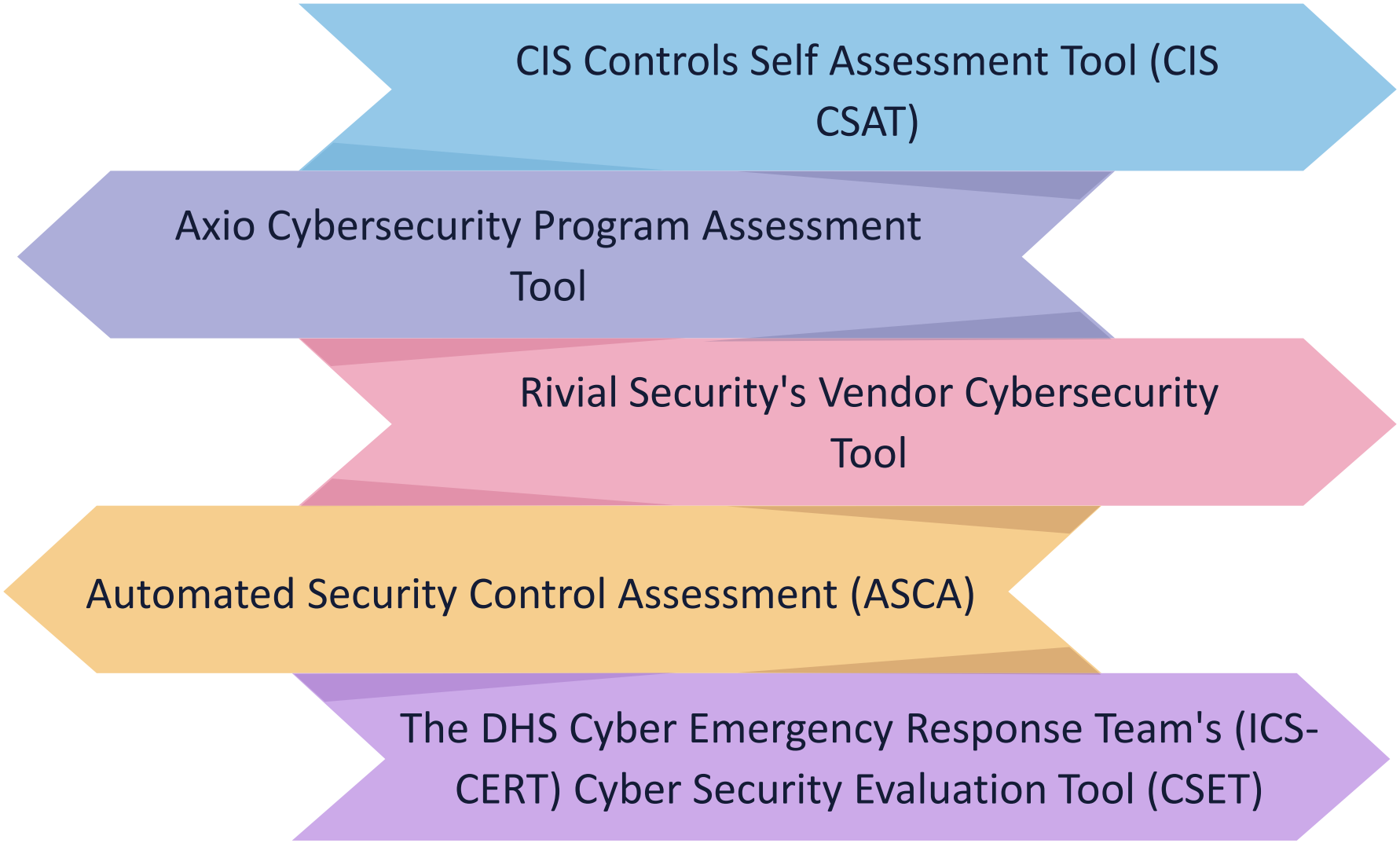
SECURITY CONTROL ASSESSMENTS

- A security control assessment is a methodology for evaluating and improving the implementation of various security controls and countermeasures
- It involves the systematic and often automated processes for gauging, describing, and testing information system security controls before being put into an operational state
- Successful assessments should determine the effectiveness of all implemented security controls and discover any gaps (i.e., gap analysis) that demand further attention (e.g., repair, upgrade, replace, add compensating controls)

SECURITY CONTROL ASSESSMENT (SCA)

- Security control assessment (SCA) is a formal evaluation of a system against a pre-defined set of controls
- It is conducted with, or independently of, a full security test and evaluation (ST&E), which is carried out as part of an official security authorization
- The SCA is often conducted as an audit for an official accreditation or certification process

SECURITY CONTROL ASSESSMENT TOOLS



PENETRATION TESTING FRAMEWORKS

SSAF – a framework provided by Open Information Systems Security Group (OISSG) and a not-for-profit organization based in London

OSSTMM – open-source security testing created by the Institute for Security and Open Methodologies (ISECOM)

OWASP – a popular methodology used widely by security professionals, created by a non-profit organization focused on advancing software security

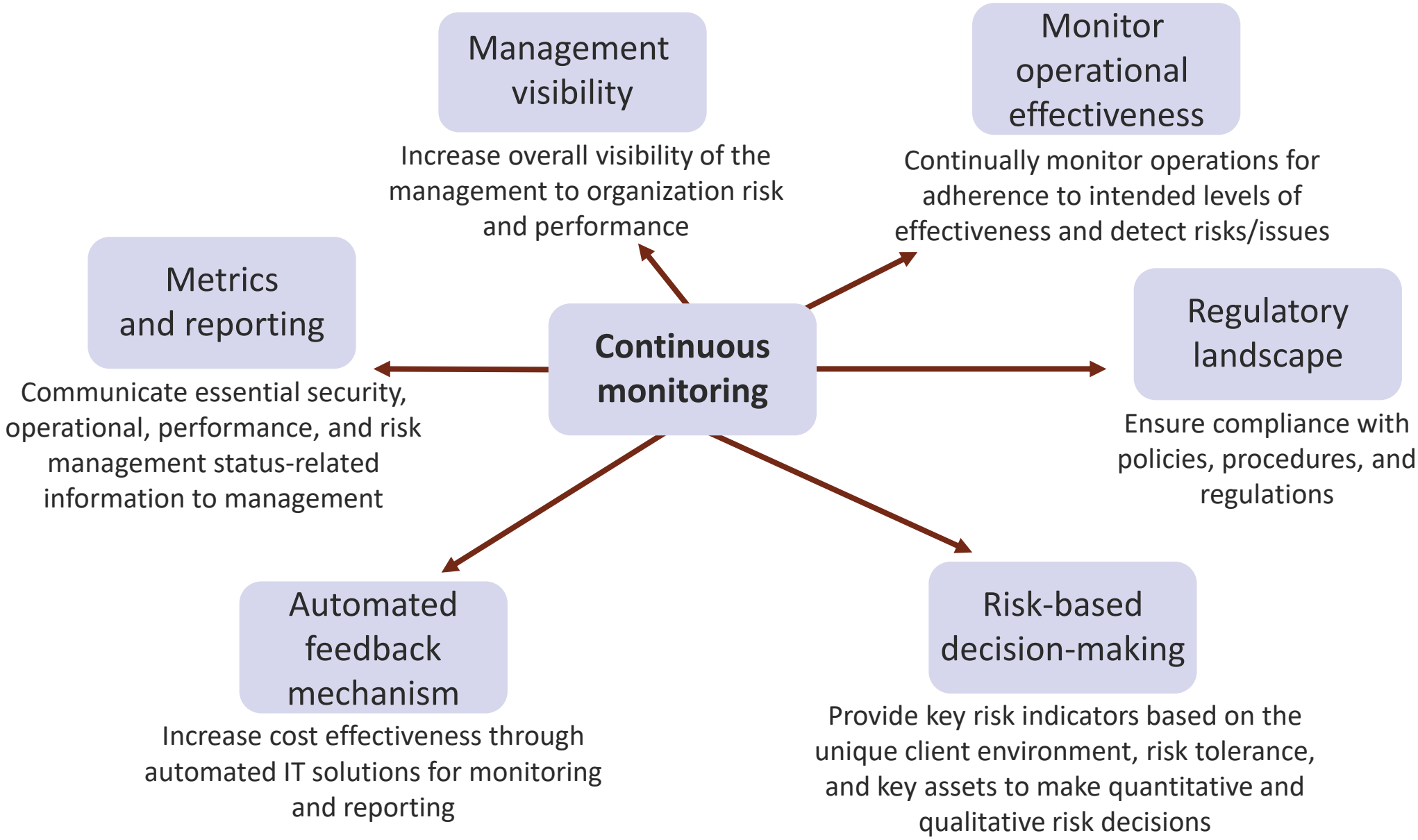
PTES – the Penetration Testing Execution Standard (PTES) methodology was developed to cover the key parts of a penetration test

NIST – the National Institute of Standards and Technology (NIST) provides a manual that is best suited to improve the overall cybersecurity of an organization

CONTINUOUS MONITORING AND MEASUREMENT

- Continuous monitoring is a systematic and continuous initiative that often leverages automated tools and cloud technologies to gain visibility into the operation, performance, and security of an organization's systems, applications, services, and user activities
- This tactic enables organizations to detect issues early, mitigate and lower risk, and increase their overall environmental resilience

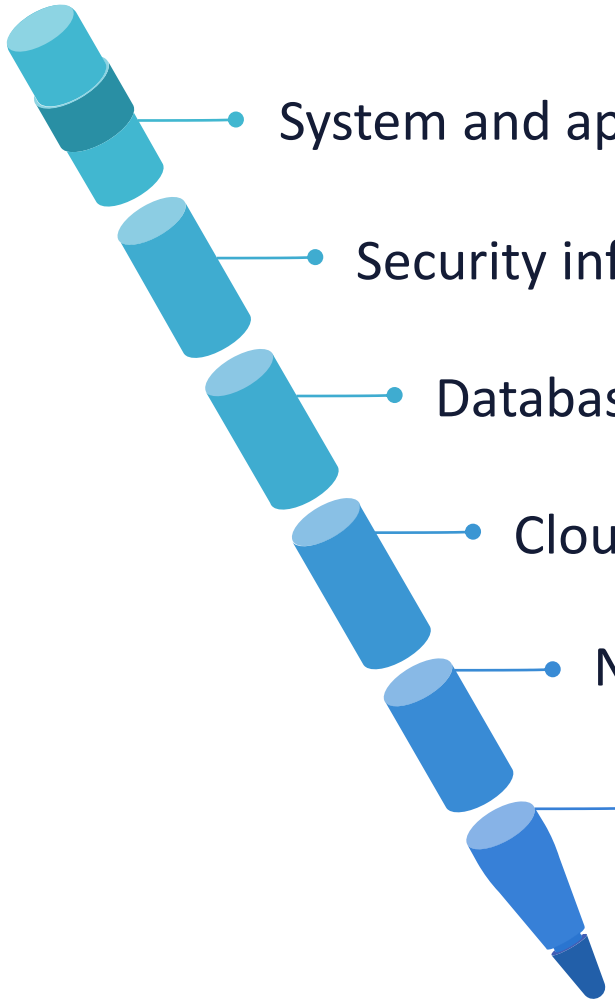
CONTINUOUS MONITORING



EXAMPLE: ISO 9001 QUALITY MANAGEMENT STANDARD

- ISO 9001 focuses on monitoring and measuring organizational processes and activities
- Deploying ISO 9001 can be accomplished using different methods
  - The costs, time, and resource requirements vary based on the approach
- Certification involves adopting the ISO 9001 requirements, then completing an audit by an independent ISO 9001 registrar, then attaining certification

MONITORING AND MEASUREMENTS TOOLS

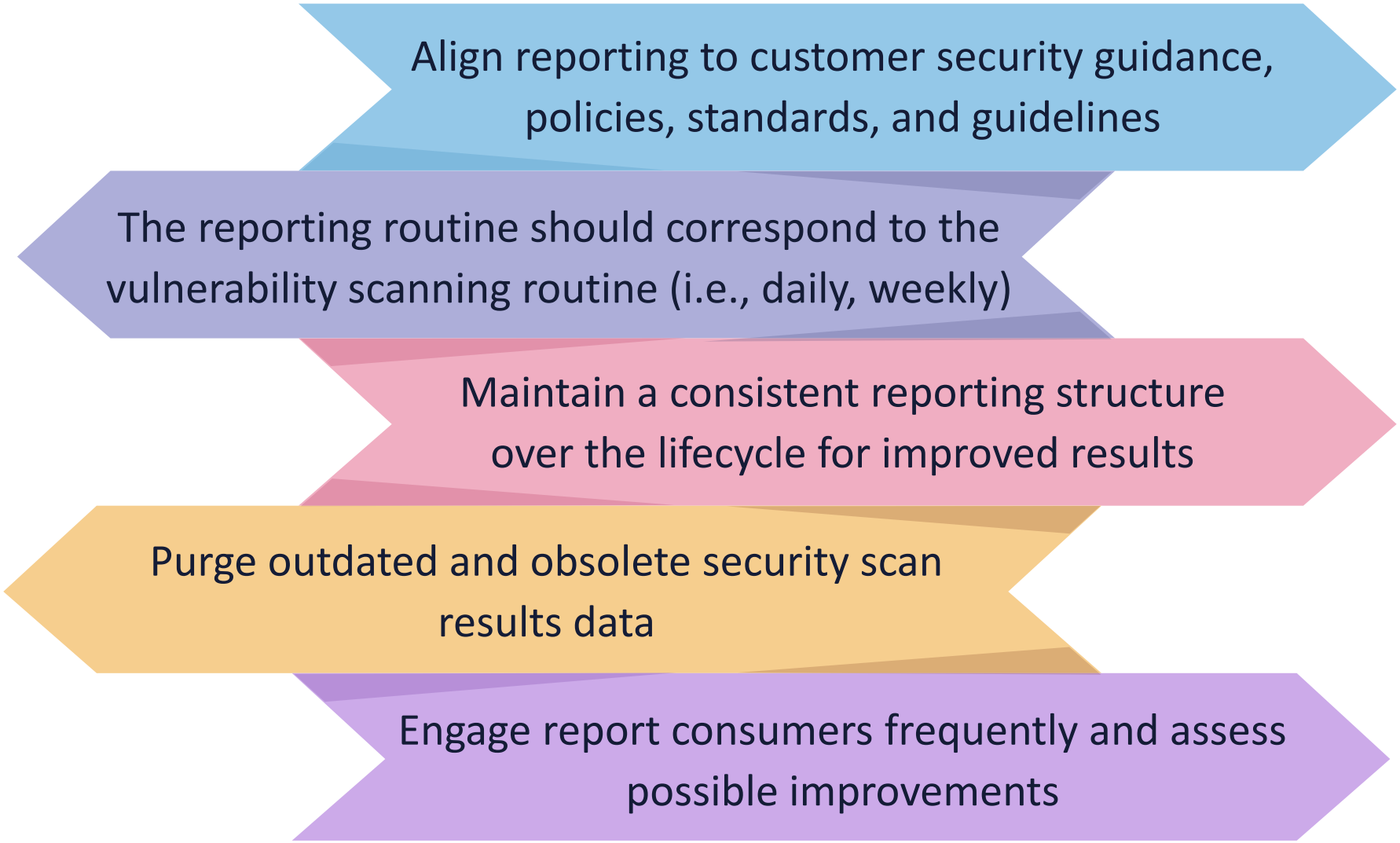


- System and application logs (e.g., Syslog, auditd, NetFlow v9)
- Security information and event management (SIEM)
- Database activity monitoring (DAM)
- Cloud-based API monitoring (e.g., AWS CloudTrail)
- Next-generation endpoint protection (e.g., PA Cortex XDR)
- Hybrid (edge) cloud monitoring with ML/AI engines

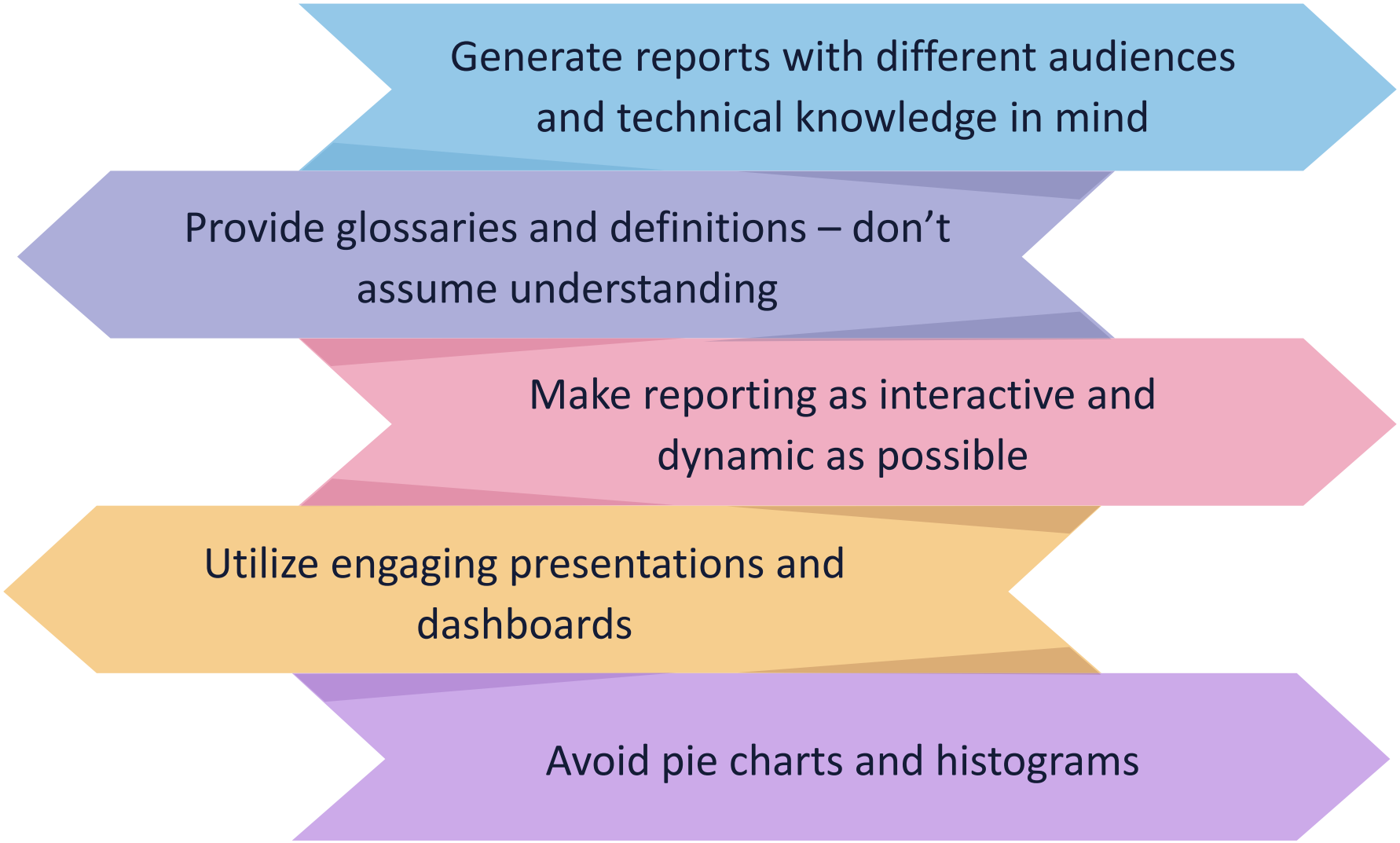
INTERNAL RISK MANAGEMENT REPORTING

- Internal reporting often involves security control assessments to report to decision-makers (i.e., steering committees, executive management)
- The main goal will be to report on the success or failure of programs and initiatives for which resources were allocated
- Reporting may be needed to update stakeholders and decision-makers on changes or new solutions
- The reports will have different formats depending on the type of analysis:
  - Qualitative
  - Semi-quantitative
  - Quantitative

INTERNAL REPORTING BEST PRACTICES



INTERNAL REPORTING BEST PRACTICES



COMMON EXTERNAL REPORTING TARGETS

Partners, vendors, and customers

Press releases and bulletins

Financial reporting

Notices of incidents and breaches (e.g., data, cards)

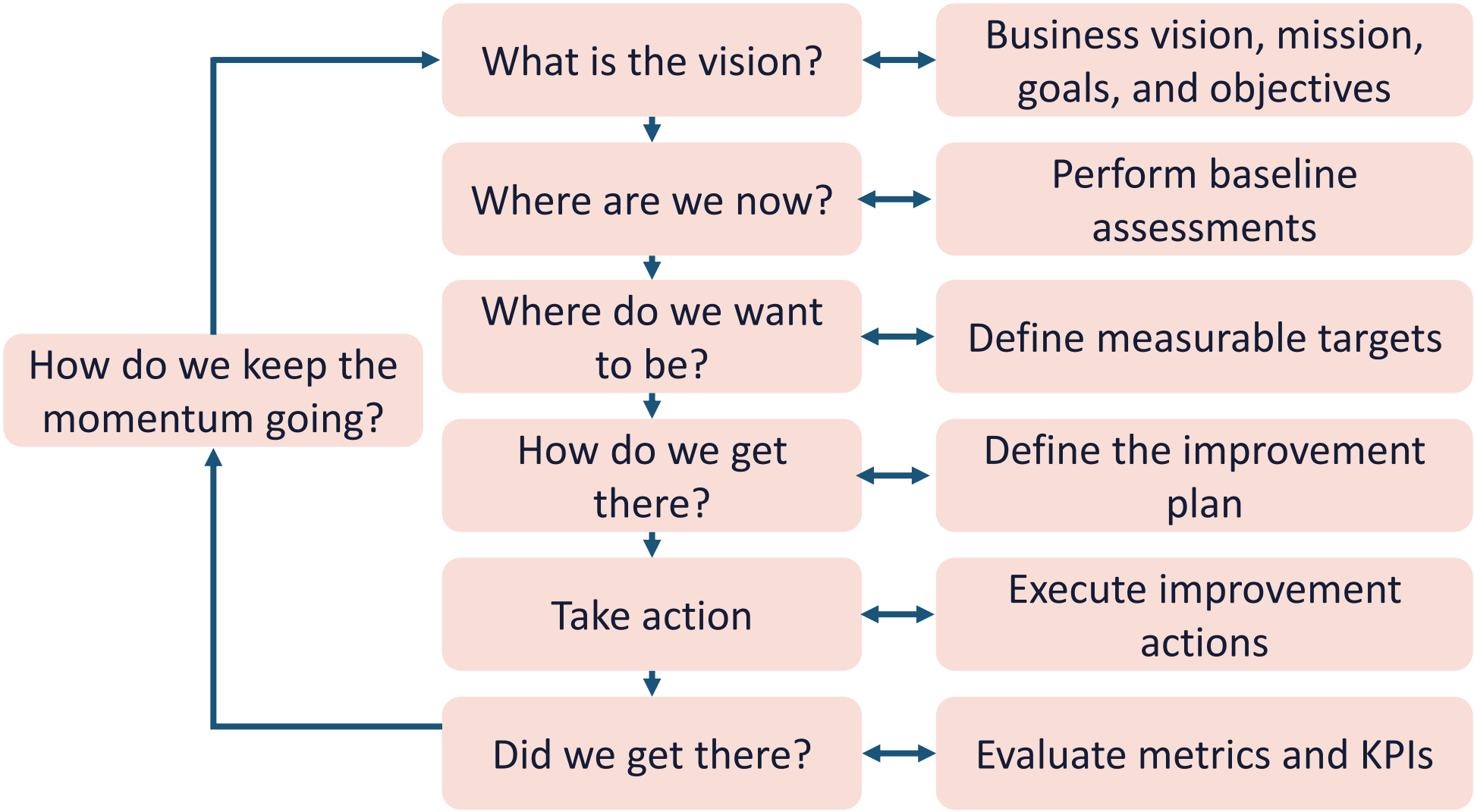
EXTERNAL REPORTING EXAMPLE: SOC 2

- Defines criteria for managing customer data based on five trust service principles: security, availability, processing integrity, confidentiality, and privacy
  - SOC 2 reports are unique to each organization
  - They are aligned with precise business practices, each with its own controls to comply with one or more of the principles
- There are two types of SOC reports:
  - Type I describes a vendor's systems and whether their design is appropriate to meet the applicable trust principles
  - Type II details the operational effectiveness of those systems

CONTINUOUS IMPROVEMENT USING PDCA

- **Plan**: Perform a gap analysis on all areas needing improvement
  - Determine how to best fill the gap, such as improving the knowledge transfer from developers to program managers to customers before the next phases
- **Do**: Complete the plan
  - This may include implementing a knowledge base and automating tasks at certain milestones
- **Check**: Test, monitor, and measure the results of the plan based on the goals it previously initiated
- **Act**: Re-test the improvements before implementation and incorporation into the overall lifecycle

ITIL 4 CONTINUAL IMPROVEMENT MODEL



CAPABILITY MATURITY MODEL (CMM)

- The Capability Maturity Model (CMM) is a methodology used to advance and enhance an organization's software development process
- The model consists of a five-level evolutionary path of progressively prepared and systematically more mature processes
- It is like ISO 9001 standards that specify an effective quality system for manufacturing and service industries

CAPABILITY MATURITY MODELS (CMM)

Initial (chaotic): Chaotic, ad hoc, individual heroics

Level 1

Repeatable (implicit): Process is not codified or defined and is still vulnerable to inconsistency

Level 2

Defined (early explicit): Process is defined and documented as a standard business process

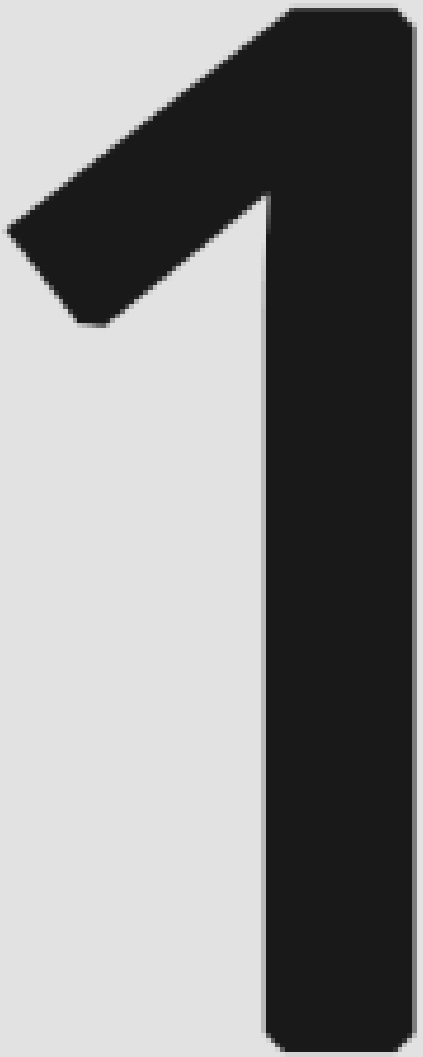
Level 3

Managed (mature explicit): Process is controlled and can be adjusted and adapted to particular projects without measurable losses of quality

Level 4

Optimized (purely explicit): Process management includes deliberate process optimization and improvement

Level 5



CMM LEVEL 1

- At the initial (chaotic) level 1, processes are disorganized and even chaotic
- Success most often depends on individual heroics and is not considered to be repeatable
- Processes are not sufficiently defined or documented for them to be replicated
- Decision-making is a free-for-all and based on intuition and existing experience
- Decision-making authorities are poorly defined, with no key risk indicators (KRIs), key performance indicators (KPIs), critical success factors (CSFs), or real meaningful metrics
- Results are inconsistent and often unaligned with any executive leadership

2

CMM LEVEL 2

- At the repeatable (implicit) level 2, fundamental project management is established, and successes could be repeated
- Decision-making is based on rote adherence to poorly aligned standards and practices and is superficial/not codified
- Roles and responsibilities are unclear, and it is common for people to make decisions outside their level of authority
- Risk is defined purely qualitatively and without much support of expert judgment
- Established KRIs and metrics, if any, are questionable as risk terminology, taxonomy, and policy are superficial or non-existent

CMM LEVEL 3

- At the defined (early explicit) level 3, the enterprise has developed its own standard software process through greater attention to documentation, standardization, and integration
- Visibility is improved as more robust and defensible analysis exists
- Well-established standards, security teams, and steering committees will exist
- Components like service desk and ITIL 4 practices are put in use
- Risk registers, KPIs, and KRIs are defined
- Meaningful metrics and calibrated and more precise semi-quant and quants are evident

CMM LEVEL 4

- At the managed (mature explicit) level 4, the processes are controlled and can quickly be adjusted and adapted for development projects, security initiatives, or other endeavors without measurable loss of quality
- Quality is visible, and risk registers and assessments are up-to-date
- Data is actively used, and risk treatment/handling is adapted accurately
- Indicators and metrics are well-defined and tested
- Accreditation and certification are established
- This is the highest level that most commercial enterprises can hope to meet

CMM LEVEL 5

- At the optimized (purely explicit) level 5, the process management has attained everything at level 4, including deliberate process optimization and continual improvement
- Level 5 is rarely achieved but is still possible with proper leadership and resources
- For example, ITIL 4 mastery and maximum software development proficiency would be demonstrated in this organization

EXPLORING RISK FRAMEWORKS

In this demo…

We will do a web safari and explore several risk frameworks including ISO, NIST, COBIT, SABSA, and PCI

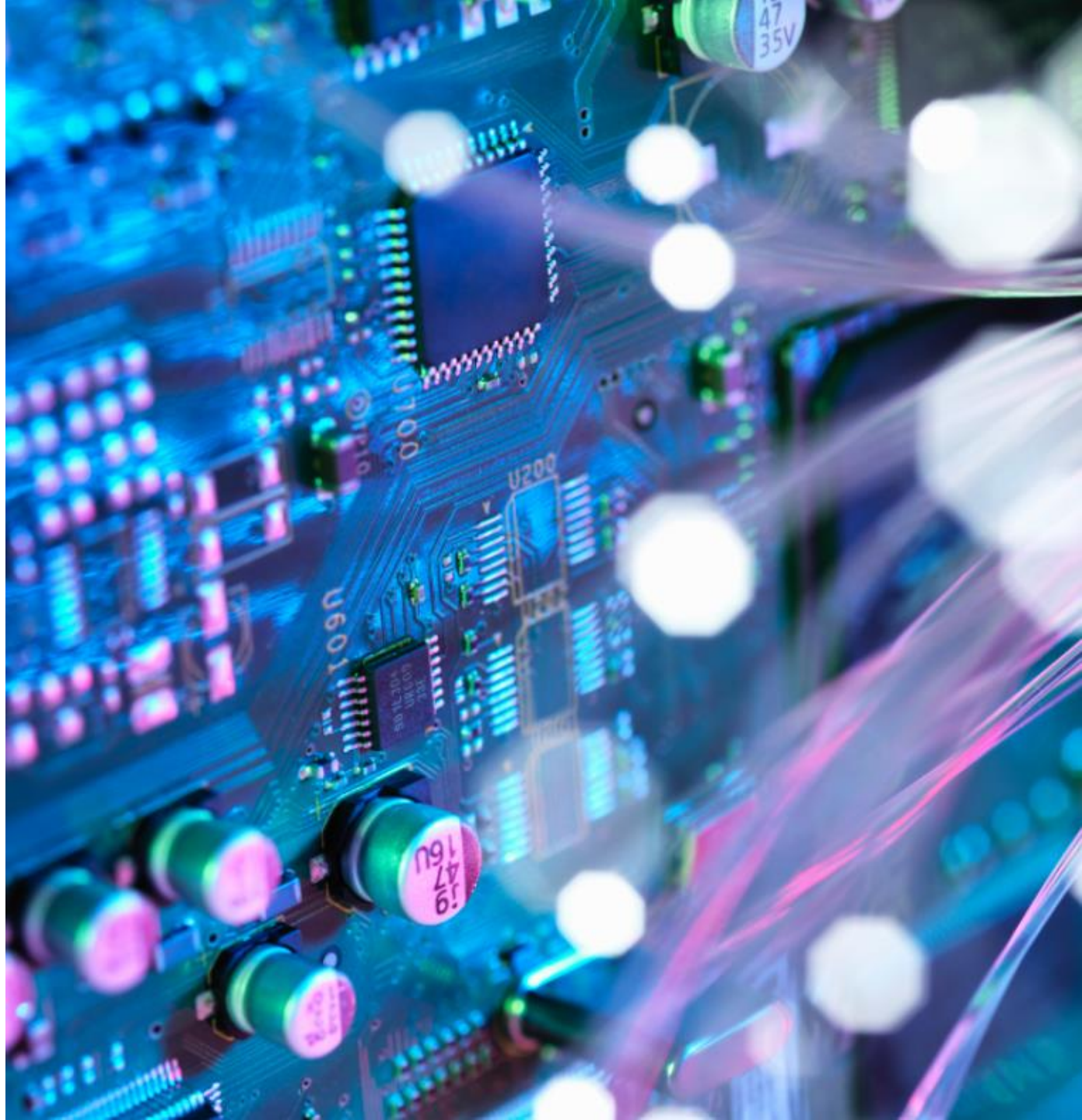
THREAT MODELING, SCRM, AND SECURITY AWARENESS

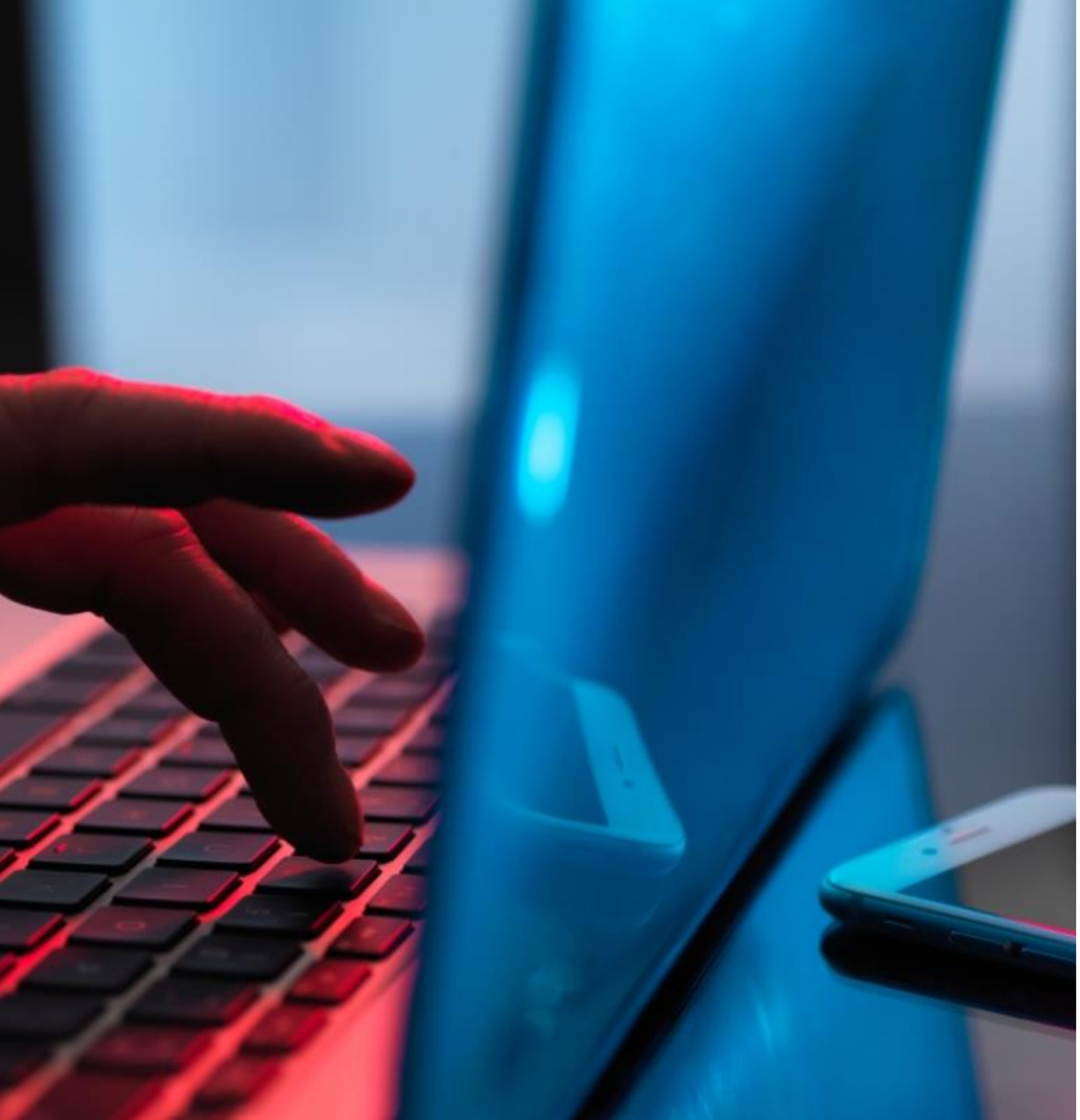
Objectives

- Explore threat modeling concepts and methodologies
- Learn about supply chain risks and mitigation
- Examine security awareness and training, periodic content reviews, and evaluating program effectiveness

THREAT MODELING CONCEPTS AND METHODOLOGIES

- Threat modeling proactively appraises a variety of cybersecurity threat vectors and payloads
- The process entails assessing potential threats and constructing procedures for identifying and answering those threats:
  - It endeavors to understand the granular behavior and steps of the kill chain taken by various forms of malicious code and artifacts
- Typical threat modeling activities include
  - Threat intelligence strategy
  - Asset identification
  - Mitigation capabilities
  - Risk assessment
  - Threat mapping





GOALS OF THREAT MODELING

- Mitigating risk:
  - By recognizing possible exploits and malware before they reach the target(s), security managers can be proactive in reducing risk
- Understanding the behavior of malware attacks:
  - By combining decision-making, human analysis, and machine learning (ML)/artificial intelligence (AI) tools into an art and a science, better risk management is achieved
- Improving security awareness:
  - Improve due care, security hygiene, visibility, continual improvement, and maturity
- Meeting compliance mandates and audits

ADVANTAGES OF THREAT MODELING

- Isolating issues early in the software development lifecycle (Agile, continuous integration (CI)/continuous delivery/deployment (CD)
- Analyzing new attack variants and zero-day code and artifacts:
  - Most organizations contribute to a vendor or cloud ecosystem, security guidance, or vulnerability database to populate with new data
- Understanding more clearly the impact and magnitude of attacks:
  - Both qualitative and qualitative risk analysis are improved
- Categorizing and mapping threat agents, targeted assets, and proper controls into an established matrix

THREAT MODELING LIFECYCLE

1. Make an inventory of all physical and software assets
2. Generate a diagram or topology of a system or service (Infrastructure as Code [IaC], data flow diagrams [DFDs])
3. Establish the scope and goals of the security initiative
4. Carry out the risk assessment and analysis
5. Deploy the optimal and feasible security controls
6. Perform a gap analysis and report for improvement

THREAT MODELING with STRIDE

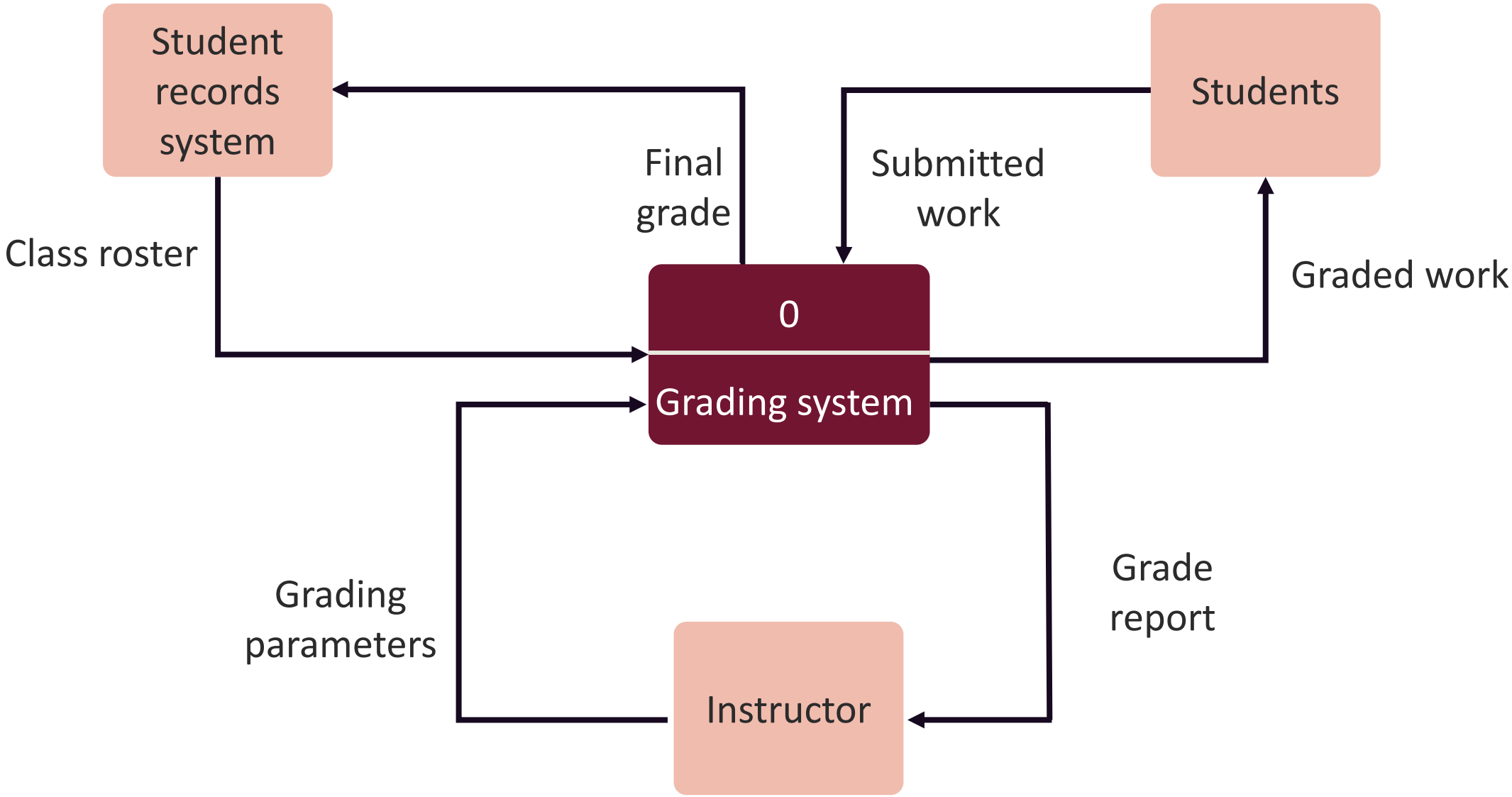
- STRIDE was originally developed to ensure that Microsoft's developers consider security during the initiating and design phases
- The goal is to address confidentiality, integrity, and availability (CIA) along with authentication, authorization, and non-repudiation
- Once the security subject matter expert (SME) builds the DFD-based threat model, system engineers or other experts review the application against the STRIDE threat model classification scheme

STRIDE

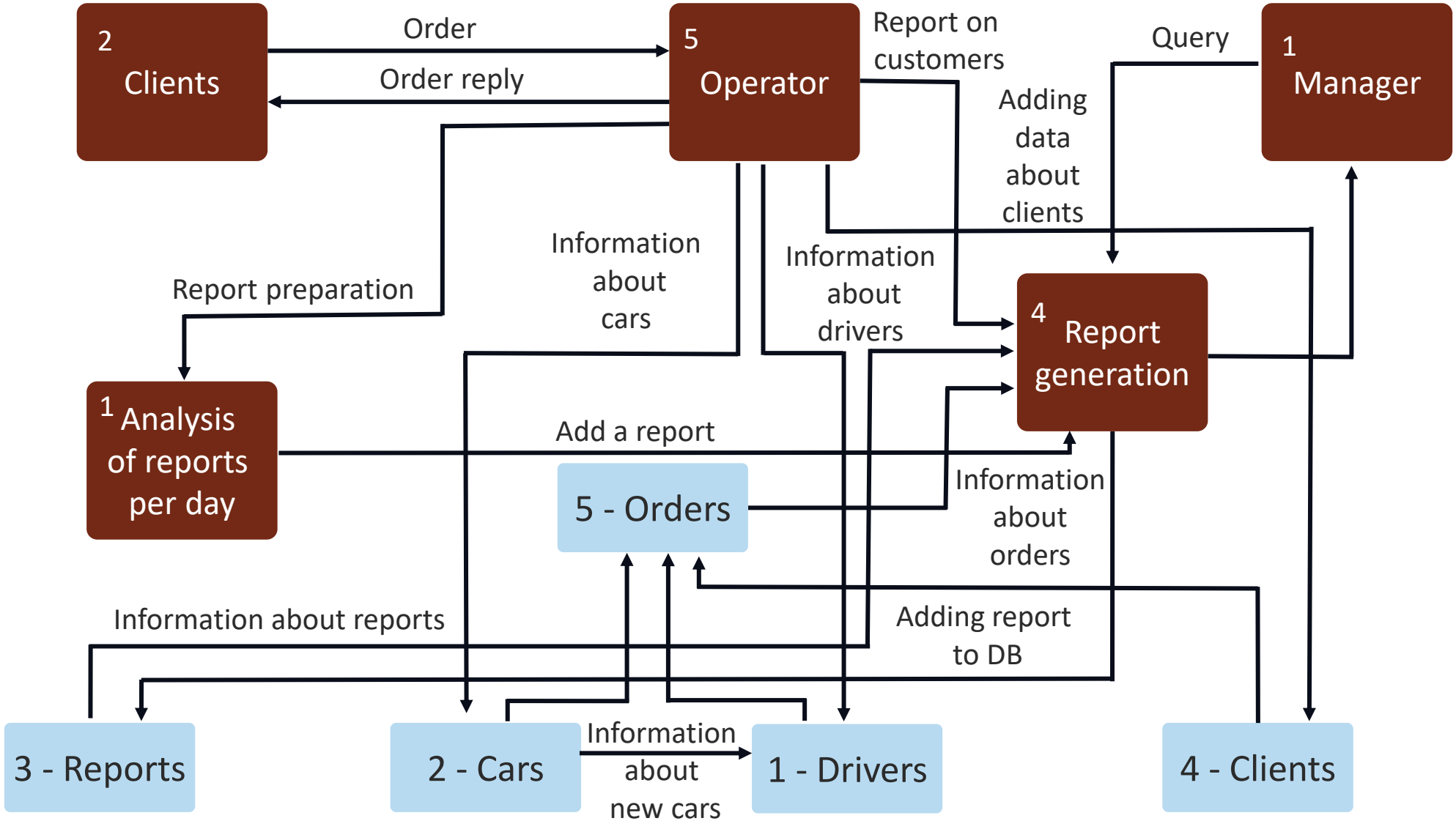
Threat	Definition	Property	Example
Spoofing	Pretending to be someone else	Authentication	Hack victim’s email and to send messages as the victim
Tampering	Changing data or code	Integrity	Software executive file is tampered with by hackers
Repudiation	Claiming not to do a particular action	Non-repudiation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

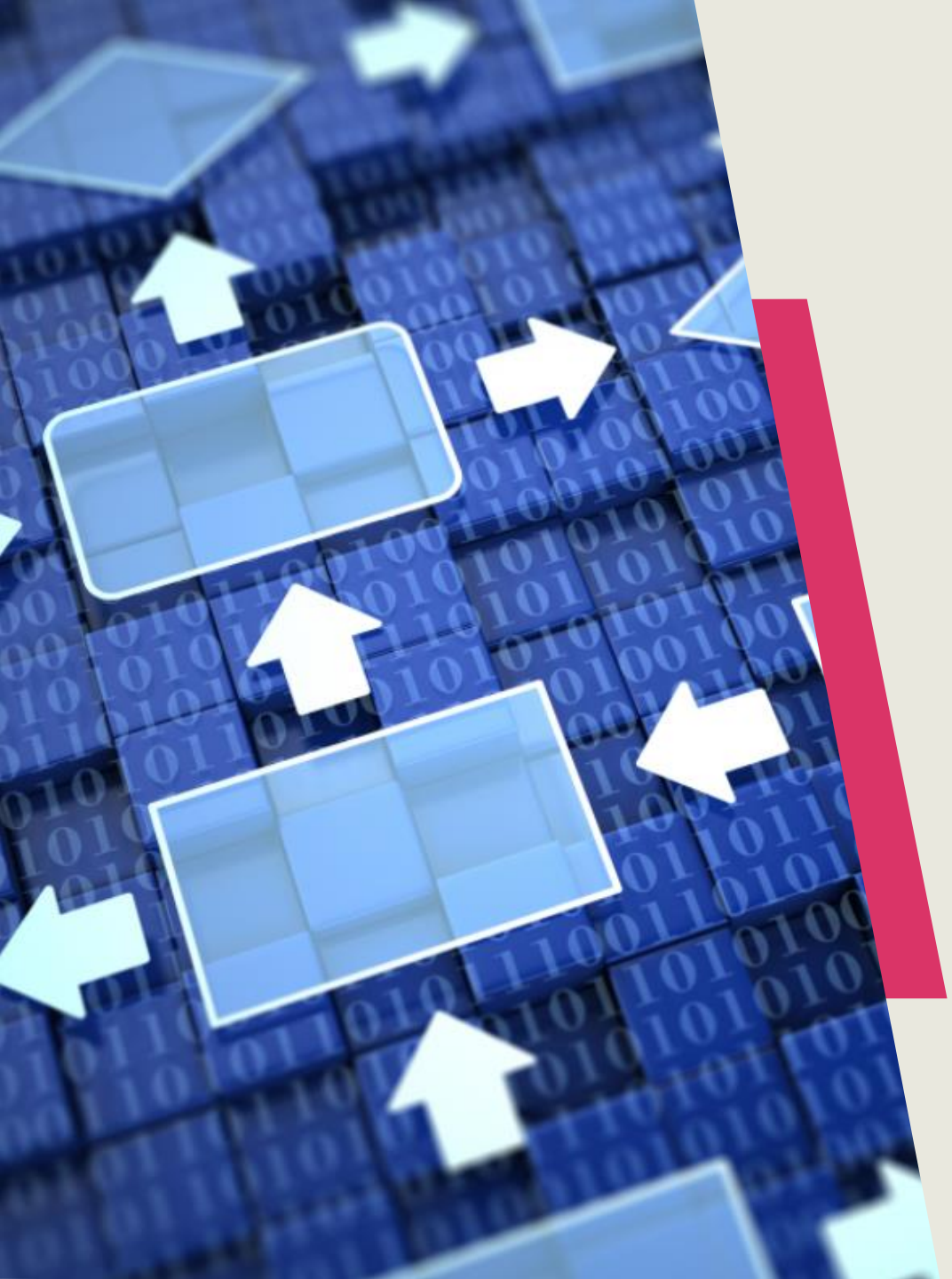
"STRIDE: Acronym of Threat Modeling System." All About Testing, February 21, 2019. https://allabouttesting.org/stride-acronym-of-threat-modeling-system/.

BASIC DATA FLOW DIAGRAM



COMPLEX DATA FLOW DIAGRAM

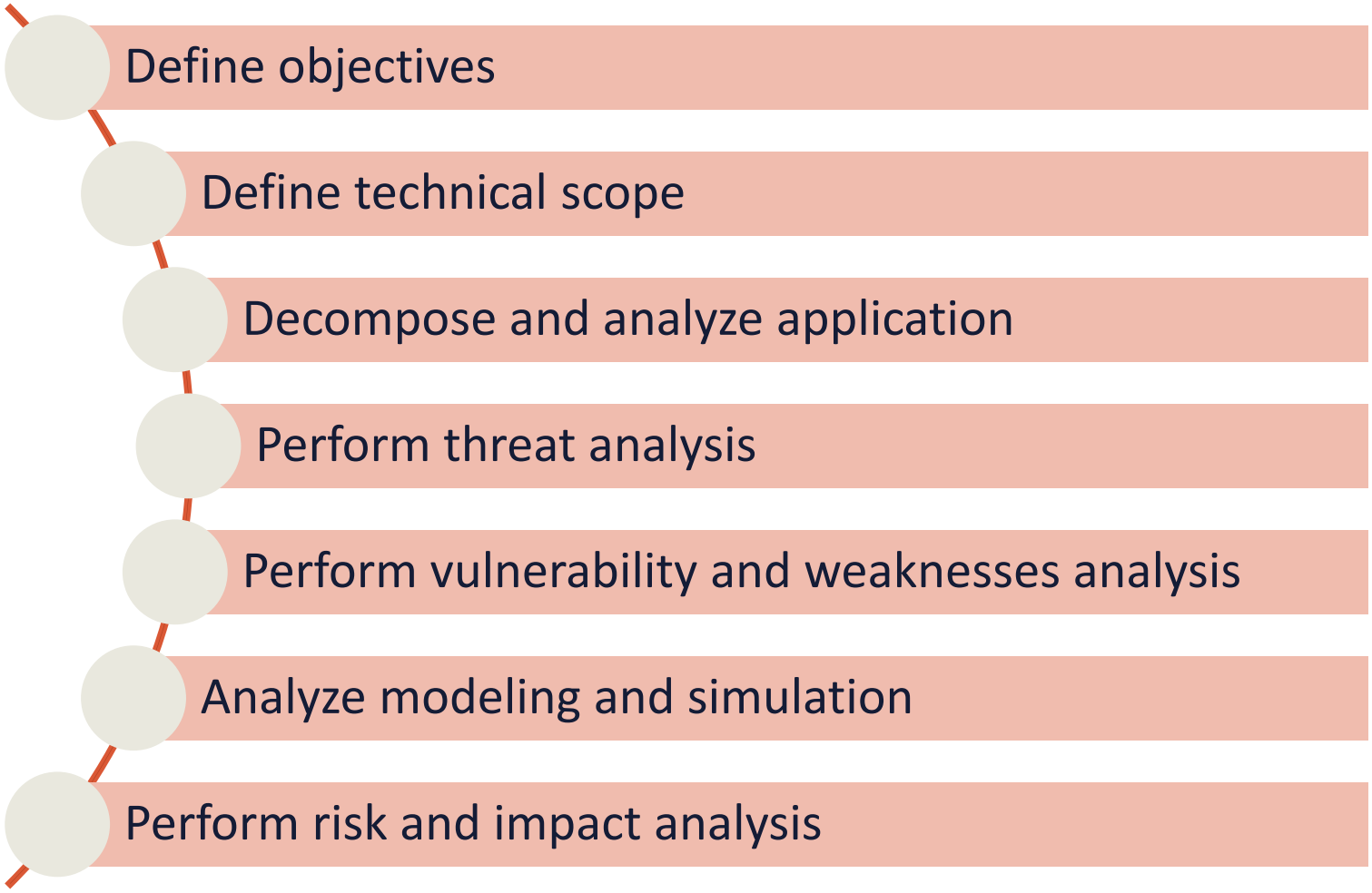




PROCESS FOR ATTACK SIMULATION AND THREAT ANALYSIS (PASTA)

- PASTA is a relatively new application threat modeling approach
- It offers a seven-step platform-independent process for risk analysis
- The objective is to align business goals with technical security needs while allowing for business impact analysis and compliance
- PASTA combines an attacker-centric perspective on potential threats with asset-centric risk and impact analysis
- It is most suitable organizations that must align threat modeling with strategic objectives

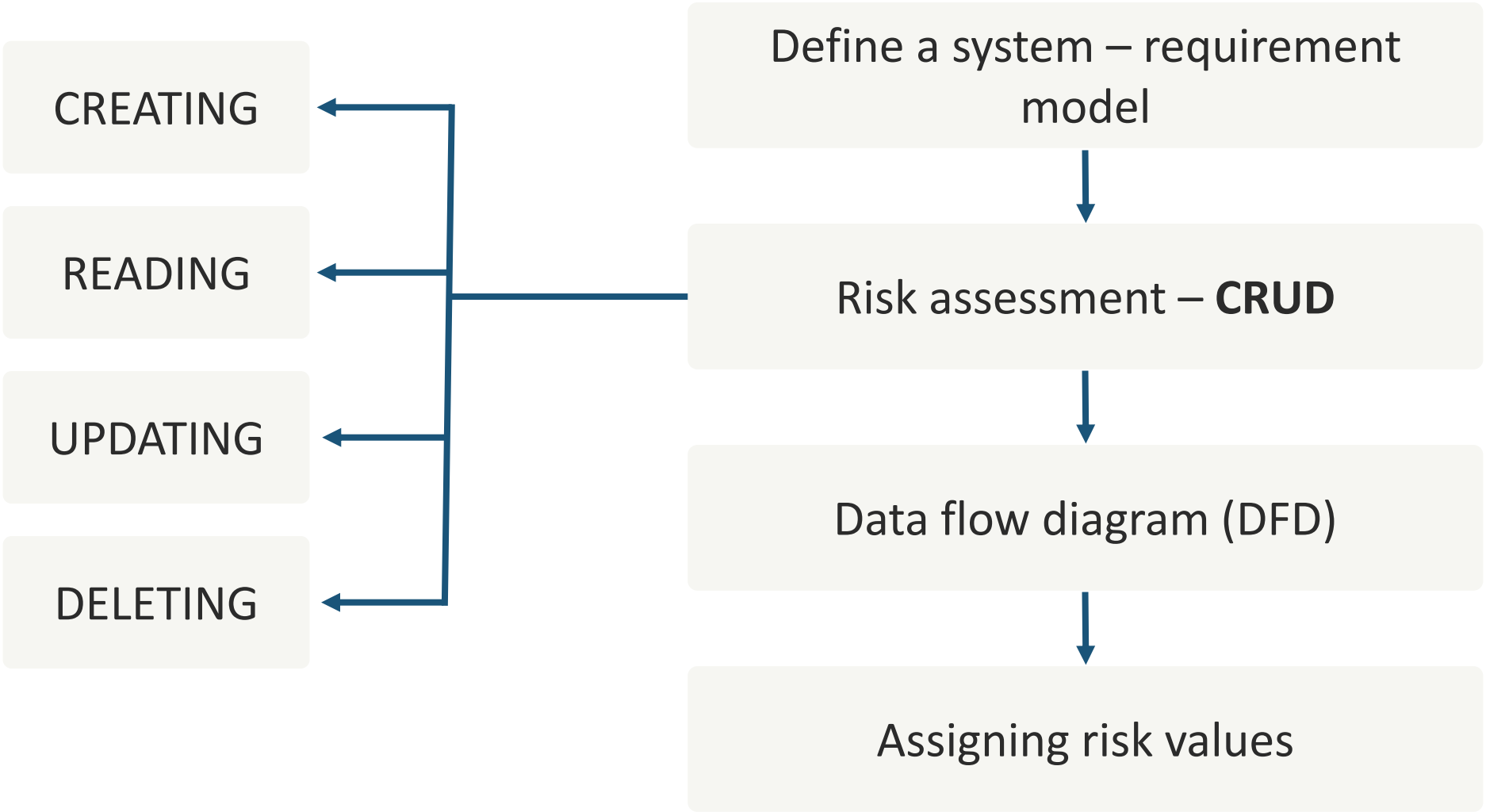
SEVEN STAGES OF PASTA



TRIKE

- Trike is an open-source option that emphasizes enabling the security auditing process with a cyber risk management angle
- It combines a risk-based approach with a unique implementation and risk modeling process
- The foundation of the approach is a requirements model that endeavors to ensure the assigned level of risk for each asset is acceptable to the various stakeholders
- With the requirements model in place, the next step in Trike threat modeling is to create a DFD:
  - In the Trike threat methodology, DFDs are used to illustrate data flow in an implementation model and the actions users can perform within a system state

TRIKE THREAT MODELING



VISUAL, AGILE, AND SIMPLE THREAT (VAST)

- The VAST method was introduced after analyzing the inadequacies and challenges in other legacy models
- The core principle is that effective threat modeling must be scalable over the infrastructure and entire DevOps portfolio:
  - Specifically, it should effortlessly integrate seamlessly into an Agile and/or CI/CD environment
- VAST delivers meaningful, precise, and reliable outputs for developers, security teams, and the C-suite alike
- A key differentiator is its real-world approach that realizes that the security issues of development teams are diverse from those of the data center or infrastructure group

VAST

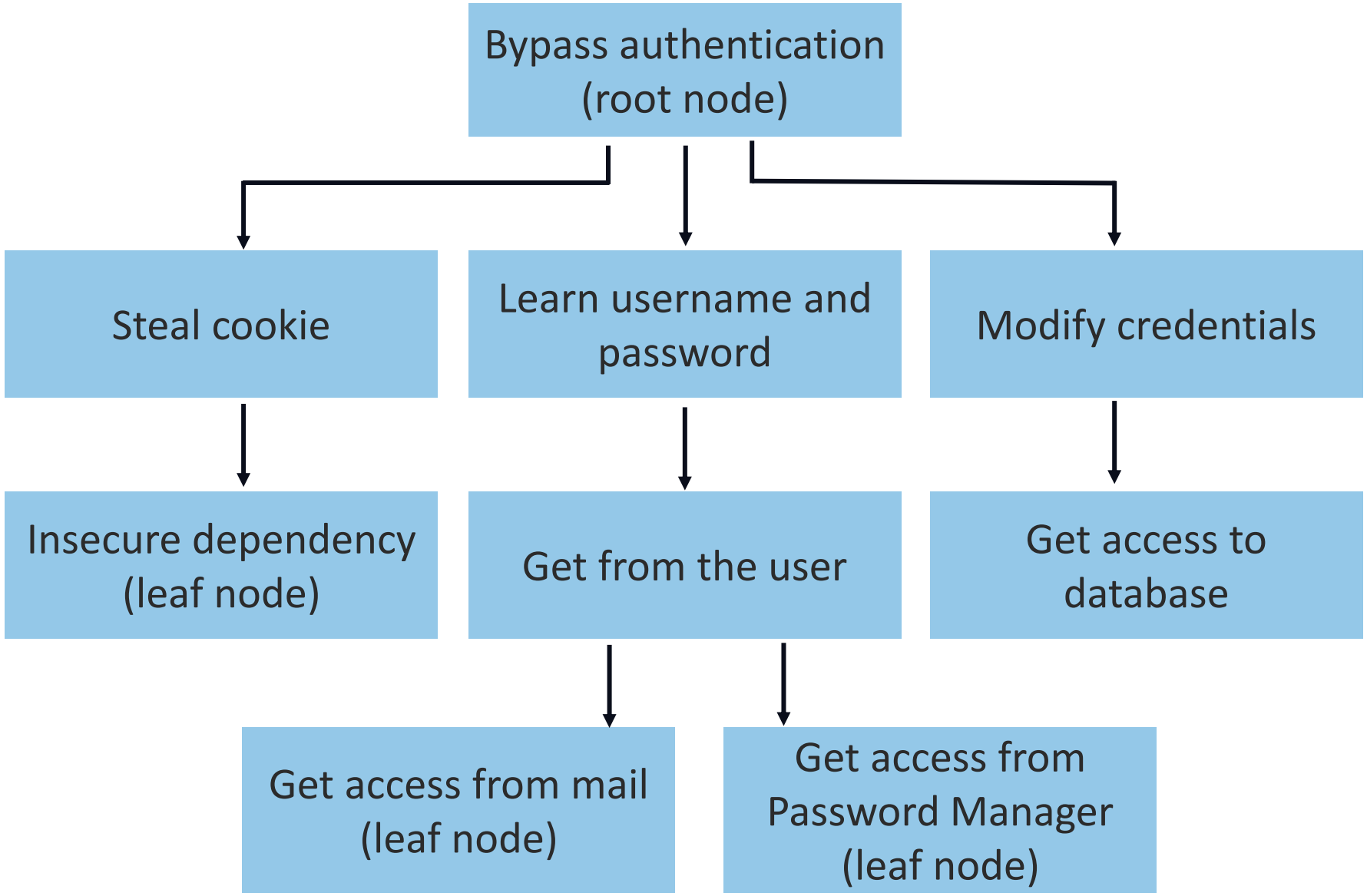
	OCTAVE	Trike	PASTA	Microsoft	VAST
Implement application security at design time	✓	✓	✓	✓	✓
Identify relevant mitigating controls	✓	✓	✓	✓	✓
Contribute directly to risk management	✓	✓	✓		✓
Prioritize threat mitigation efforts	✓	✓	✓		✓
Encourage collaboration among all stakeholders	✓	✓			✓
Provide outputs for all stakeholders	✓	✓			✓
Offer consistent repeatability		✓			✓
Automate the threat modeling process					✓
Integrate into an Agile DevOps environment					✓
Scale across thousands of threat models					✓

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

ATTACK TREES

- Are used to determine how a threat actor might attempt to access an asset like a network, application, or system
- Help security professionals recognize the possible hazards to various targets
- Graphically outline threat agent techniques to conduct a successful kill chain
- Help security administrators better understand the methodologies of their attackers and the controls to counter them

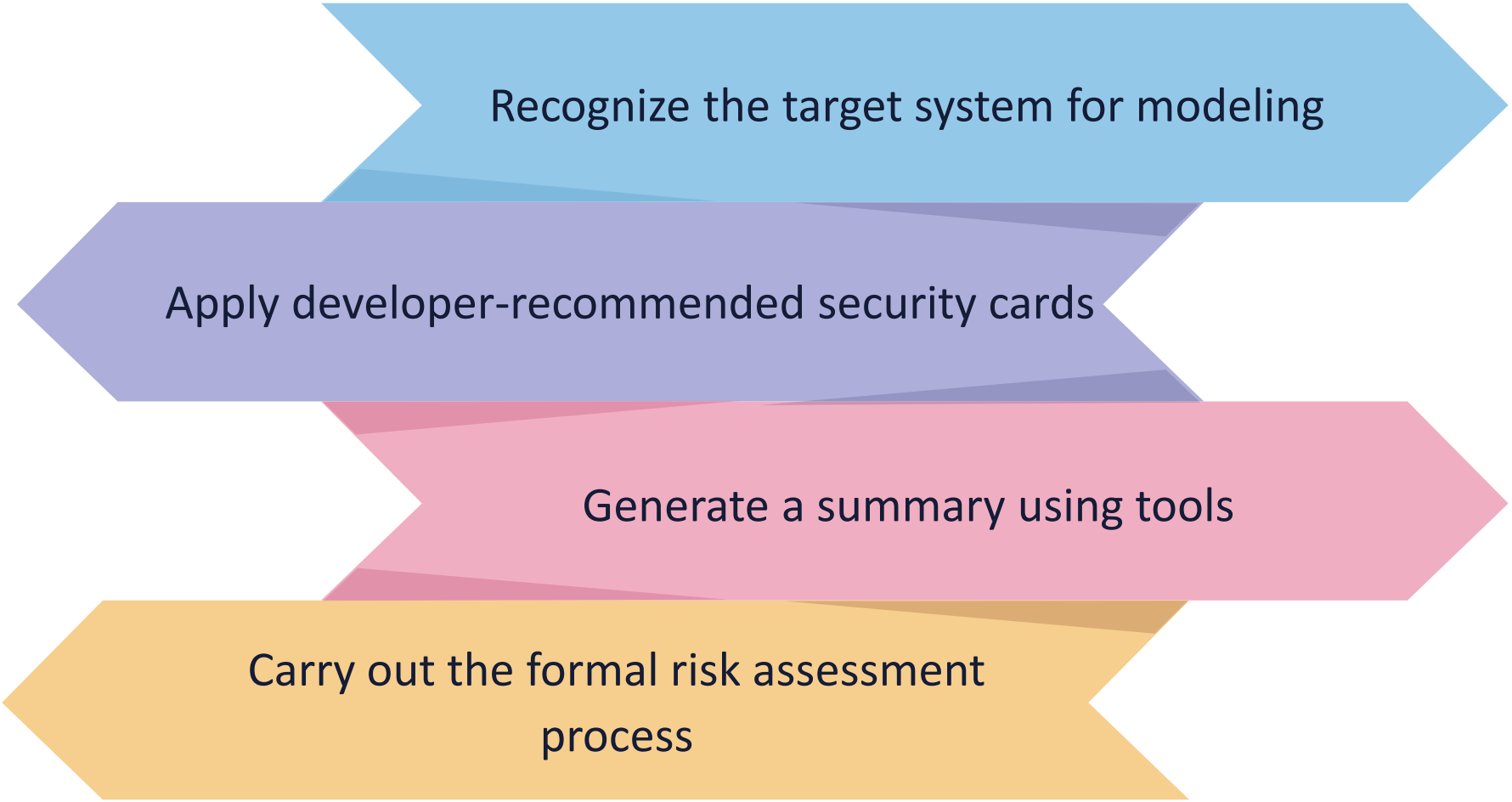
SAMPLE ATTACK TREE



hTMM

- Hybrid threat modeling method (hTMM) was created by the Software Engineering Institute (SEI) in 2018
- It is a combination of the Security Quality Requirements Engineering Method (SQUARE), security cards, and persona non grata (PNG) tasks
- The goals of the method include
  - No false positives
  - No unnoticed threats
  - A consistent result regardless of the cost and participants

hTMM ACTIVITIES



SUPPLY CHAIN RISKS: GLOBAL UNREST

- According to the World Economic Forum, in 2024, the global supply chains faced their worst shortages in 50 years due to the pandemic and global conflict
- A rebound in consumer demand, fueled by stimulus spending, was stronger than anticipated, which also put pressure on supply chains
- Another contributing factor is that China shut down production facilities and even entire cities

SUPPLY CHAIN RISKS: ECONOMIC INSTABILITY

- Economic events that can disrupt the supply chain:
  - Vendors, distributors, and suppliers going bankrupt
  - National or global economic recessions
  - A work stoppage at a key manufacturing partner due to strikes or other issues
  - Sudden spikes in demand for parts or components causing backorders
  - Price and currency volatility

SUPPLY CHAIN RISKS: CLIMATE-DRIVEN DISRUPTIONS

- Hurricanes and monsoons
- Superstorms and tornadoes
- Solar events
- Flooding
- Wildfires started by lightning
- Mudslides
- Hailstorms

SUPPLY CHAIN RISKS: ESG NON-COMPLIANCE

- The organization may decide to abandon certain points in the supply chain due to lack of attention or non-compliance in reducing their global impact
- The social aspect looks at how an organization treats people and exists as a member of supply chains, including
  - Employee engagement and diversity, equity, and inclusion (DEI)
  - Health, safety, and social sustainability
  - Privacy, data protection, and cyber security
  - Product safety
  - Labor standards
  - Human rights issues

SUPPLY CHAIN RISKS: CATASTROPHIC EVENTS

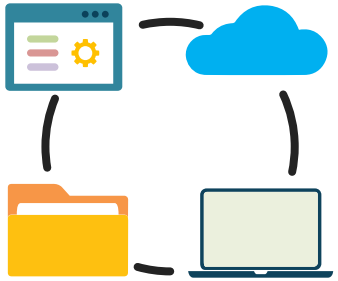
- Catastrophes and natural disasters should be handled with the disaster recovery aspect of business continuity (BCP) or continuity of operations (COOP)
- There are quite a few possible events:
  - Active shooters
  - Internal chemical or gas leak
  - Internal fires or flooding
  - Earthquakes and other seismic activity
  - Ransomware attacks
  - Theft of intellectual property (IP)

SUPPLY CHAIN RISKS: PRODUCT TAMPERING

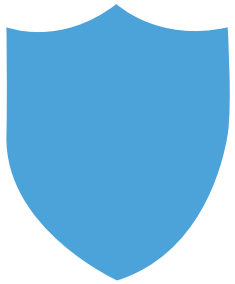
- Tampering is a critical risk for visibility in the supply chain, although quite difficult
- Compromised privileged insiders can inject into a product component or by changing firmware:
  - These exploits often generate a back door link between the device and external command and control (C2) systems that the attacker manages
  - When the device or integrated component reaches the final customers, it leverages the back door to get access or exfiltrate data

SUPPLY CHAIN RISKS: PRODUCT TAMPERING

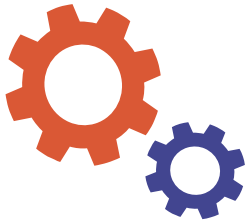
Start up



Unified Extensible Firmware Interface (UEFI)



Secure launch



Windows

Securely operate Windows 10

Malicious code

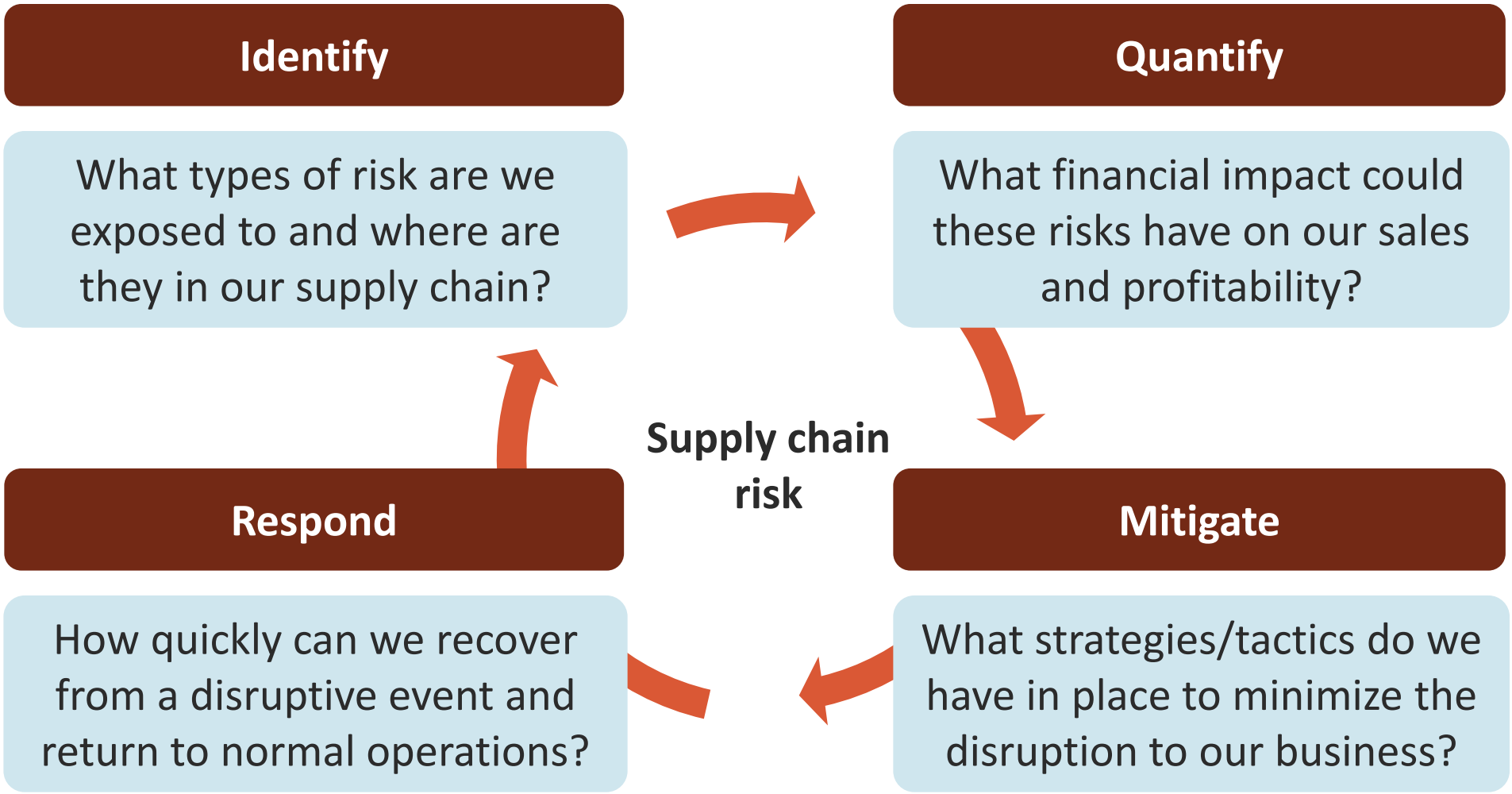
SUPPLY CHAIN RISKS: COUNTERFEITS

- Vendors and consumers face a huge challenge with the origin or authenticity of hardware and software products moving through global supply chains
- Counterfeiters progressively have access to the same quality code, parts, and technology used by original equipment manufacturers (OEMs)
- Counterfeits can be categorized into two forms from the customer's perspective:
  - **Non-deceptive** counterfeits are ones that customers can effortlessly distinguish from the real ones based on things like price, quality, and aspects of the sale
  - **Deceptive** counterfeits are sold under comparable conditions and almost undistinguishable from the original

SUPPLY CHAIN RISKS: IMPLANTS

- Hardware trojan attacks on integrated circuits (ICs) and printed circuit boards (PCBs) have gained attention recently
- These are at risk of malicious modification by untrusted parties in the manufacturing supply chain
- Also, attackers can install implants or tamper with PCBs when they are in transit or the field
- Hardware trojans cause financial harm, loss of reputation, privacy breaches, and even threaten human safety and national security

SUPPLY CHAIN RISK MANAGEMENT



THIRD-PARTY ASSESSMENT AND MONITORING

- A third-party risk assessment and monitoring initiative is an ongoing analysis of all risks and vulnerabilities visible to an organization based on all relationships in the supply chain
- It can relate to assessing and monitoring all third parties IN the chain as well as having the assessment and monitoring PERFORMED by an external entity
- These tools are a critical aspect of every third-party risk management (TPRM) program

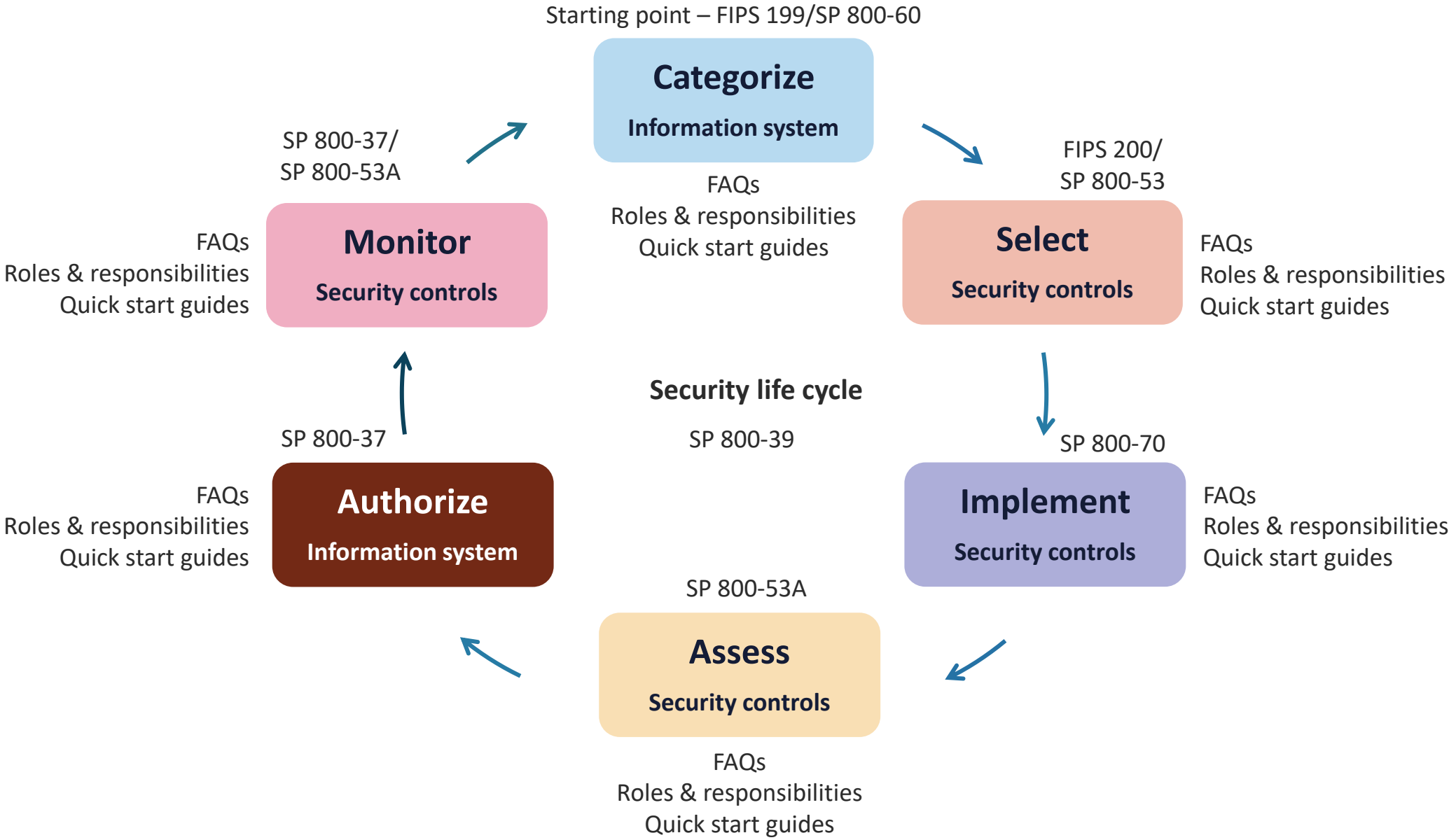
IMPLEMENTING MINIMUM SECURITY REQUIREMENTS

- Implementing baselines and guidance:
  - CIS Best Practices (Top 18)
  - AWS Well-Architected Framework
  - NIST Risk Framework
- Infrastructure as Code (IaC):
  - Terraform
  - AWS CloudFormation
- Zero Trust initiatives
- Software assurance
- Capability Maturity Model (CMM)

NIST CYBERSECURITY FRAMEWORK

IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER
• Asset management • Business • Environment • Risk assessment • Risk management	• Awareness control • Awareness and training • Data security • Information protection and procedures • Maintenance • Protective technology	• Anomalies and events • Security continuous monitoring • Detection process • Communication	• Response planning • Communications • Analysis • Mitigation • Improvements	• Recovery planning • Improvements • Communication

NIST RISK FRAMEWORK



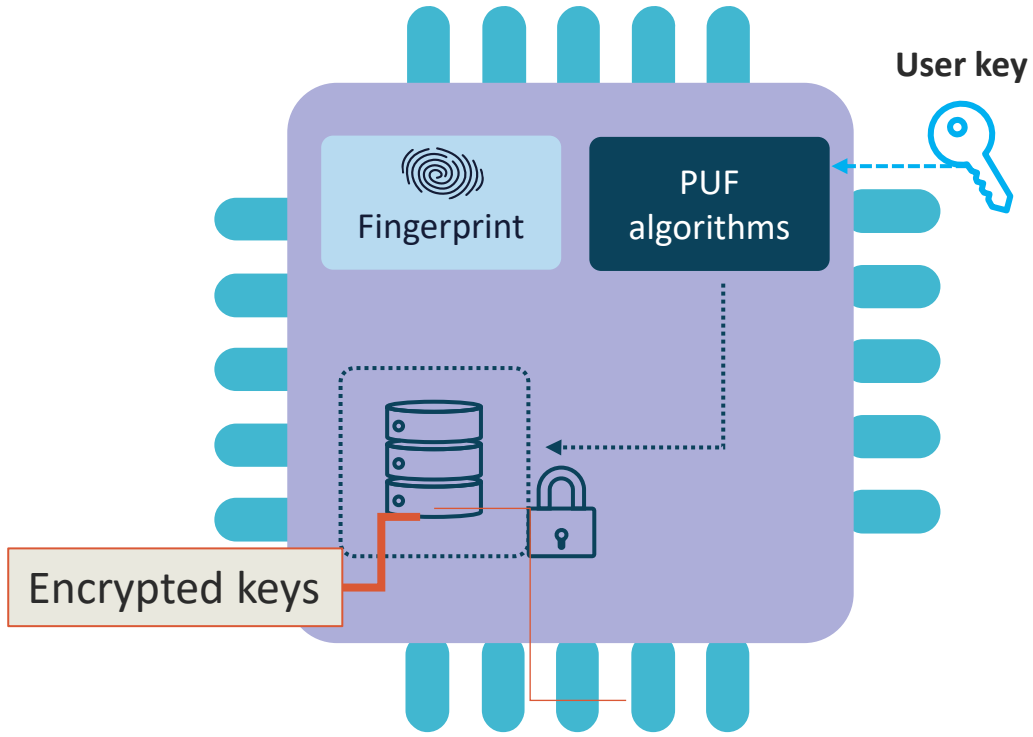
SERVICE LEVEL REQUIREMENTS

- The availability goal of security with the supply chain is often measured by service level requirements
- These are critical success factors (CSFs) that measure the percentage of delivered goods from an order compared to the total order, intending to meet demand and fulfill customer requirements:
  - Having high supply chain service levels requires effort across all phases of the chain
- For example, a 93% fill rate denotes that the vendor successfully delivered orders on time 93% of the time

SILICON ROOT OF TRUST

- Silicon-based security for emergent hardware-based functions is critical for mitigating an unrelenting epidemic of new and evolving cyber threats
- Silicon Root of Trust integrates security straight into the hardware level of servers
- Explicitly, the integrated lights-out (iLO) chip that makes secure out-of-band management of servers (for example, remote controlling and monitoring) feasible
- This solution successfully generates an immutable fingerprint in the silicon, delivering unparalleled levels of protection against new firmware attacks and previously undetected firmware exploits

PHYSICALLY UNCLONABLE FUNCTION (PUF)



- Physically unclonable functions (PUFs) are a hardware security method that utilizes inherent device variations to generate an unclonable, distinctive response to various inputs:
  - Think of a PUF as comparable to a human biometric factor
  - They are intrinsic and unique identifiers for each piece of silicon
- Since silicon processing techniques are imperfect, every single IC ever produced varies physically from each other:
  - These distinctions manifest in ways such as different path delays, transistor threshold voltages, voltage gains, and many others that are not crucial for a security manager to understand

SOFTWARE BILL OF MATERIALS (SBoM)

- An SBOM is an organized list of components, libraries, and dependencies used in a software system, such as an application container
- It is not unlike a bill of materials used when manufacturing a physical product like an automobile:
  - A list of all the materials and components used to build such a product
- SBOMs are valuable building blocks in software security and software supply chain risk management since they itemize all the open-source and third-party components that exist in a codebase, as well as licenses, versions, and patching/update states

INCREASING AWARENESS AND TRAINING

Awareness	Training and education

• Commonly under-utilized
• Can often be overdone
• Increases awareness through:
  • Self-paced computer-based training (CBT) modules, videos, and classroom training
  • Posters, newsletter articles, email, and bulletins
  • Combination of the carrot and stick
  • Reminders to 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
	• **"Champion(s)"**

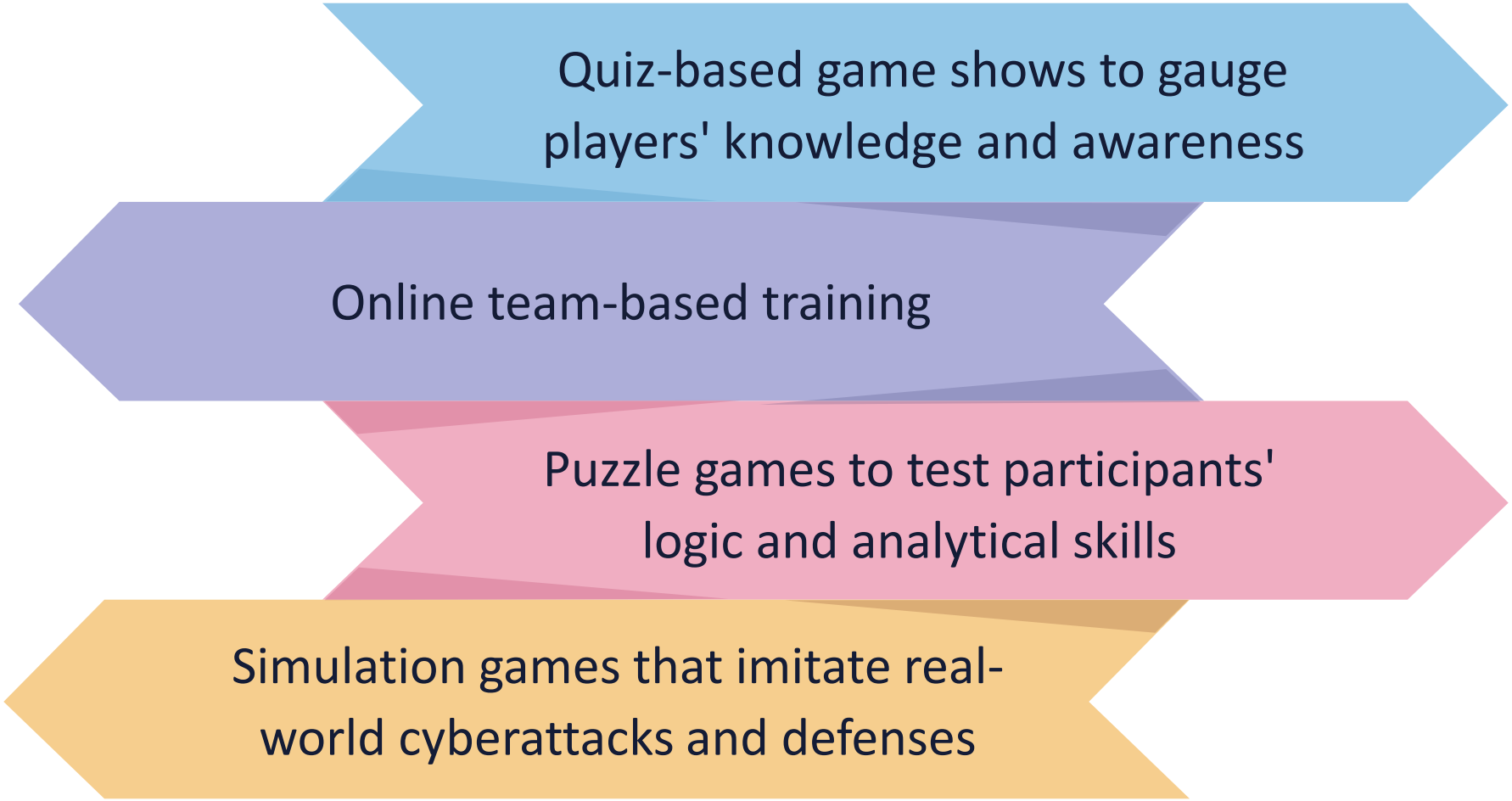
TRAINING AND AWARENESS CAMPAIGNS

- Adhering to acceptable use policies (AUP)
- No tailgating (piggybacking) access controls
- Social engineering awareness:
  - Handling phone calls
  - Social media threats
  - Spoofing and hoaxes
  - Reporting to security guards and teams
- Mock phishing and business email compromise (BEC) campaigns
- Incident and disaster recovery plan (DRP) drills and exercises

SECURITY TRAINING THROUGH GAMIFICATION

- Gamification and simulations enable employee engagement (buy-in) and enthusiasm
- It makes it easier for stakeholders to remember the training and awareness initiatives that they learn
- Simulated environments embolden learners to ramp up quickly on privacy and security mandates as well as to help develop new technical skills

CYBERSECURITY GAMIFICATION EXAMPLES



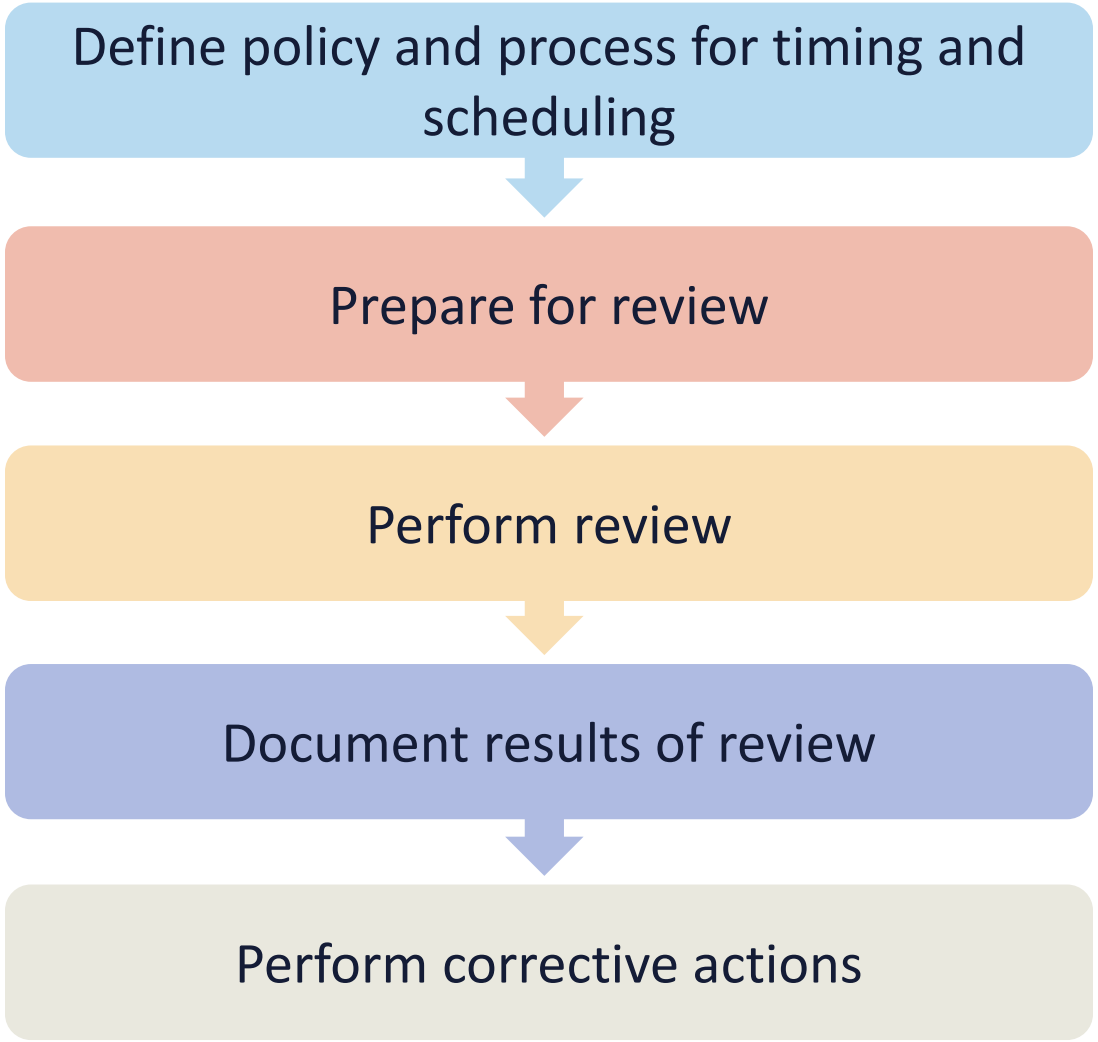
PERIODIC CONTENT REVIEWS

- Regardless of the security program, training, awareness, or initiative, periodic content reviews must be conducted
- Periodic reviews assist content creators and instructional designers with tools to
  - Recognize outmoded information
  - Evaluate keyword optimization
  - Certify alignment with current industry technologies and trends
- This should be a continual, proactive approach to affirm that your content is still pertinent and meaningful to the learning audience

PERIODIC CONTENT REVIEWS

- Regardless of the security program, training, awareness, or initiative, periodic content reviews must be conducted to address emerging technologies and trends:
  - New and changing regulations
  - Shifts in business structure (mergers, initial public offerings)
  - Cryptocurrencies and smart contracts
  - Augmented reality
  - Generative AI
  - Blockchain and ledgers
  - Graph databases
  - Quantum computing and post-quantum reaction
  - Serverless technologies

PERIODIC CONTENT REVIEWS



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
  - Technical security
  - Security management
  - Compliance

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
- Peer and supervisory evaluations should be performed to offer valuable critique and to reinforce 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