CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL (CISSP)

DAY 01

Michael J Shannon
CISSP, CCSP, CCSK,
ITIL 4 Managing Professional

Class will begin at 10:00 am
Central Standard Time

PROFESSIONAL ETHICS AND SECURITY CONCEPTS

Objectives

- Learn the ISC2 Code of Professional Ethics and the organizational code of ethics
- Examine advanced instances of security principles, including:
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Nonrepudiation

ISC2 CODE OF PROFESSIONAL ETHICS

- According to the ISC2 organization, "All information security professionals who are certified by ISC2 recognize that such certification is a privilege that must be both earned and maintained.
- In support of this principle, all ISC2 members are required to commit to fully support this Code of Ethics."

https://www.isc2.org/ethics

ISC2 CODE OF PROFESSIONAL ETHICS

"ISC2 members who intentionally or knowingly violate any provision of the Code will be subject to action by a peer review panel, which may result in the revocation of certification.

ISC2 members are obligated to follow the ethics complaint procedure upon observing any action by an ISC2 member that breaches the Code. Failure to do so may be considered a breach of the Code pursuant to Canon IV."

https://www.isc2.org/ethics

ISC2 CODE OF PROFESSIONAL ETHICS PREAMBLE

- Keep in mind that this high-level guidance is not intended to be a substitute for the ethical judgment of the security professional
- Preamble: "The safety and welfare of society and the common good, duty to our principals, and duty to each other, require that we adhere, and be seen to adhere, to the highest ethical standards of behavior."
- Therefore, strict adherence to this code is a condition of certification

CODE OF ETHICS CANONS

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

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

3. Provide diligent and competent service to principals

4. Advance and protect the profession

ORGANIZATIONAL CODE OF ETHICS

- A business or organizational code of ethics is a set of core guiding principles to notify how and why decisions are made
- The code informs all stakeholders, including employees, customers, business partners, suppliers, or investors, about how the company delivers the value proposition

ORGANIZATIONAL CODE OF ETHICS

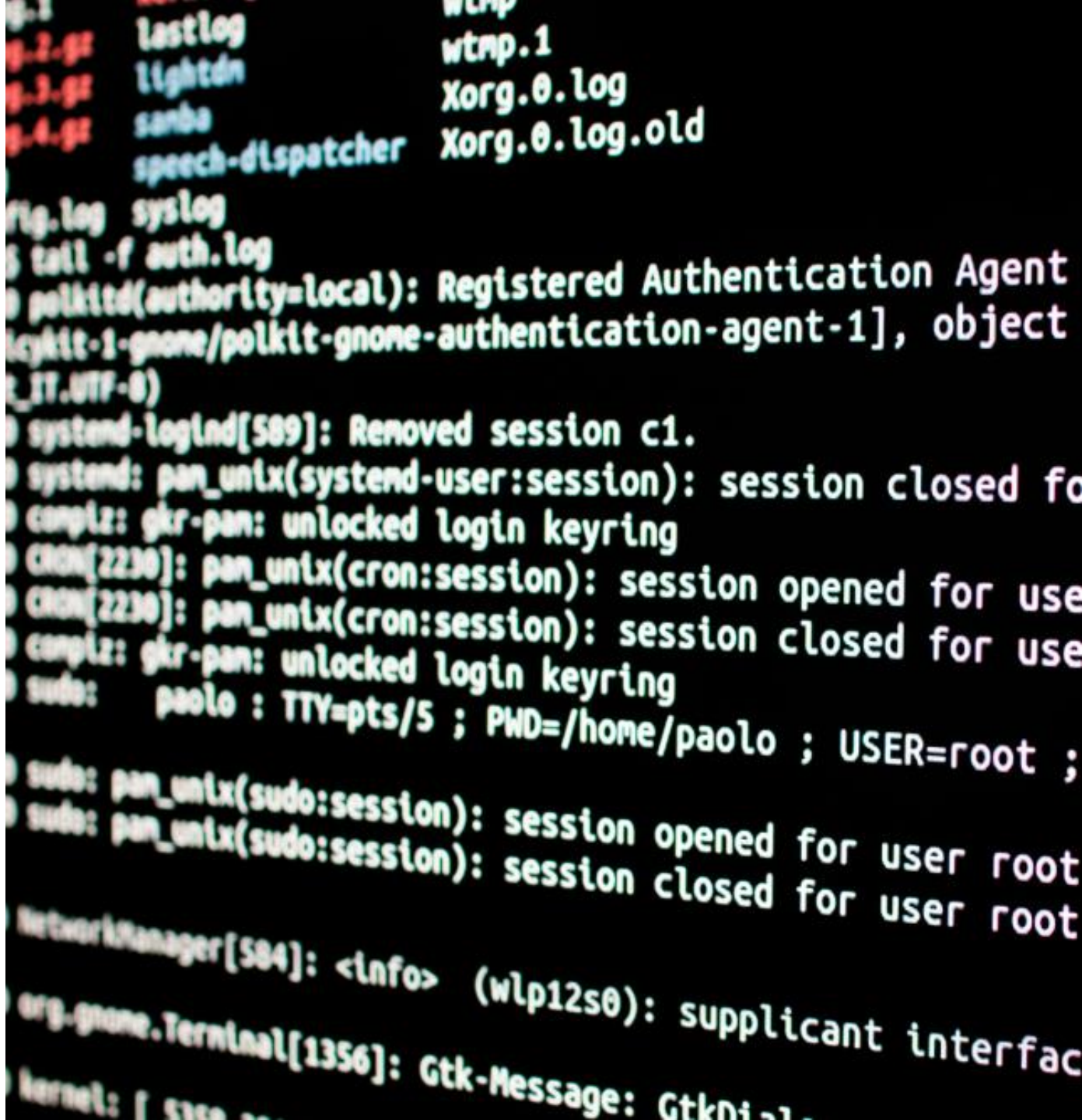
- Organizational codes establish an integral aspect of a mission and model adopted by an organization to underscore:
  - The general ethical principles positively valued by the organization
  - The detailed rules of conduct applicable to parties subject to the code and with which such parties must observe
  - The modes of communication, training, monitoring, and continual improvement of the Code of Ethics

CONFIDENTIALITY

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

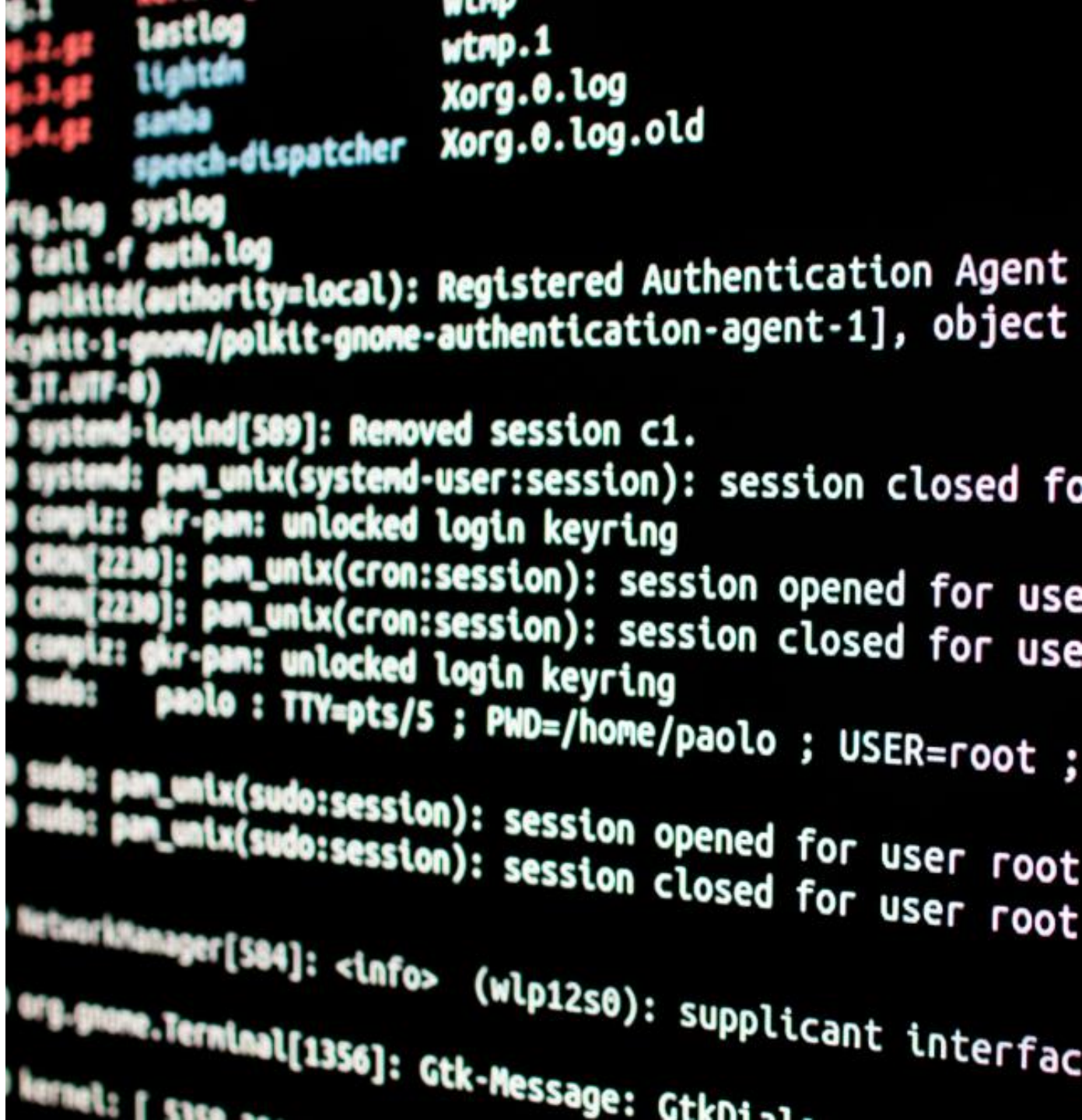
HIGH-LEVEL CONFIDENTIALITY SOLUTIONS

- **WPA3 cryptography**
  - It uses a comparable 192-bit cryptographic mechanism in WPA3-Enterprise mode
  - Specifically, AES-256 in GCM mode with SHA-384 as HMAC
  - Also dictates using CCMP-128 (AES-128 in CCM mode) as the minimum baseline encryption algorithm in WPA3-Personal mode



HIGH-LEVEL CONFIDENTIALITY SOLUTIONS

- **Confidential computing**
  - An AWS Nitro Enclave is a hardened and heavily insulated compute environment that is initiated and connected to the consumer's instance(s) of a virtual machine such as Windows, Linux, and/or macOS
  - No user, including admin or root, nor any application running on the virtual machine has interactive access to the enclave



HIGH-LEVEL CONFIDENTIALITY SOLUTIONS

- **Homomorphic encryption**
  - Homomorphic encryption is an innovative solution that contributes to a zero-trust initiative by protecting data-in-use in untrusted domains (e.g., the cloud) without the need to decrypt
  - The process involves the transformation of data into ciphertext that can be analyzed and worked on as if it were still in its original form
  - Homomorphic encryption utilizes asymmetric algorithms and multifaceted algebraic functions to act upon encrypted data-in-use (i.e., Redis clusters) without affecting the existing encryption

INTEGRITY

- Integrity measures an attacker's ability to manipulate, change, or remove data at rest and data in transit
- It typically involves implementing cryptographic hashing, hash-based message authentication codes (HMACs), and digital signing mechanisms to assure only authorized subjects can change sensitive information
- Protections will counter on-path man-in-the-middle (MITM) attacks, injection or hijacking attacks on data in transit, modifying files, changing access control lists (ACLs), and domain name system (DNS) or Address Resolution Protocol (ARP) cache poisoning

HIGH-LEVEL INTEGRITY SOLUTIONS

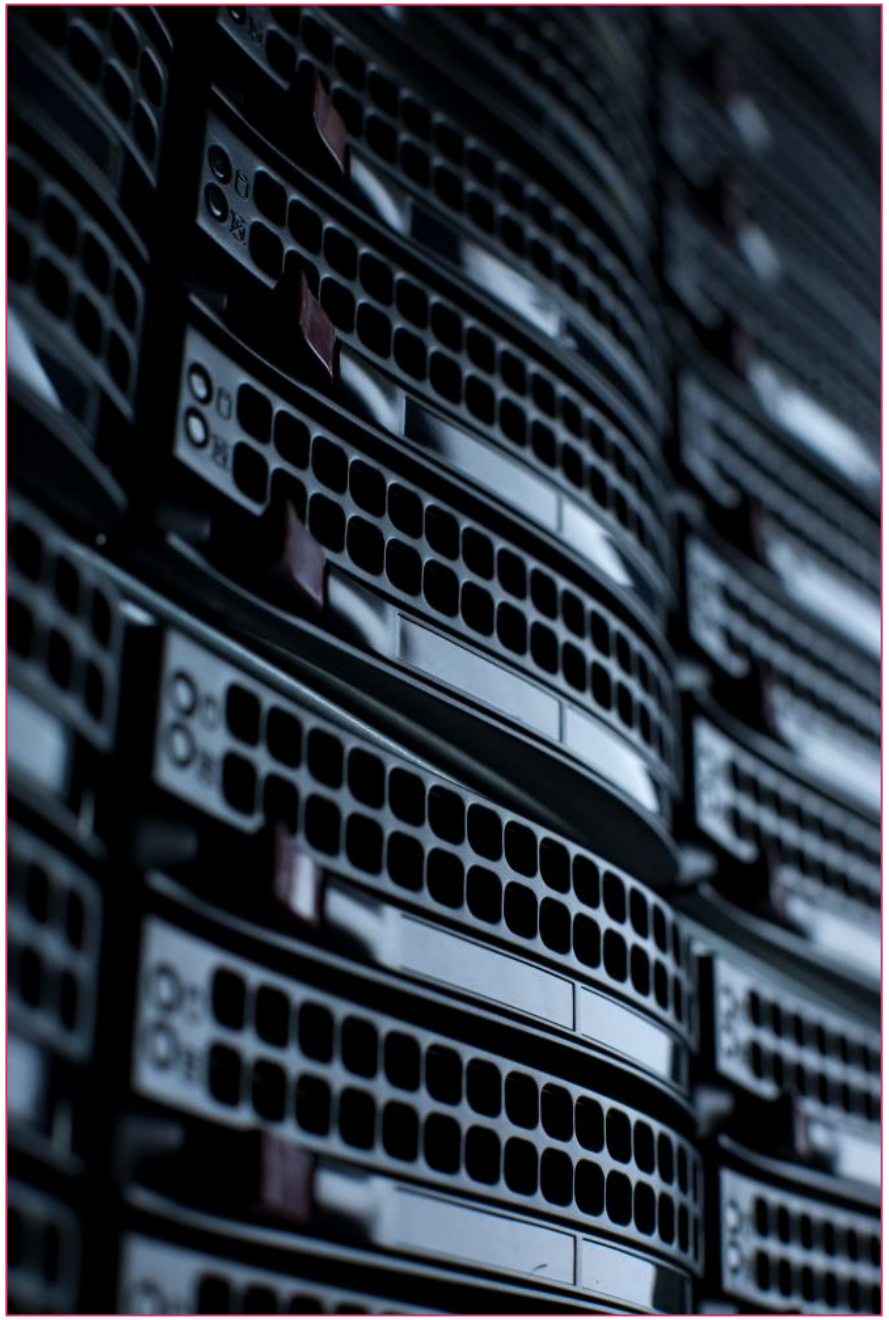
- **Clark–Wilson (CW) integrity model**
  - CW is a mandatory access control model that provides a structure for describing and analyzing an integrity policy for computing systems based on:
    - Established transactions from one reliable state to another reliable state
    - The principle of separation of duties – the guarantor of a transaction and the deployer of the transaction are two separate participants
    - Security policies that relate directly to transaction integrity
  - CW is more appropriate for commercial and industry tasks and procedures where the integrity of the data and information is supreme at any level of classification, whether it be top secret, secret, or classified

HIGH-LEVEL INTEGRITY SOLUTIONS

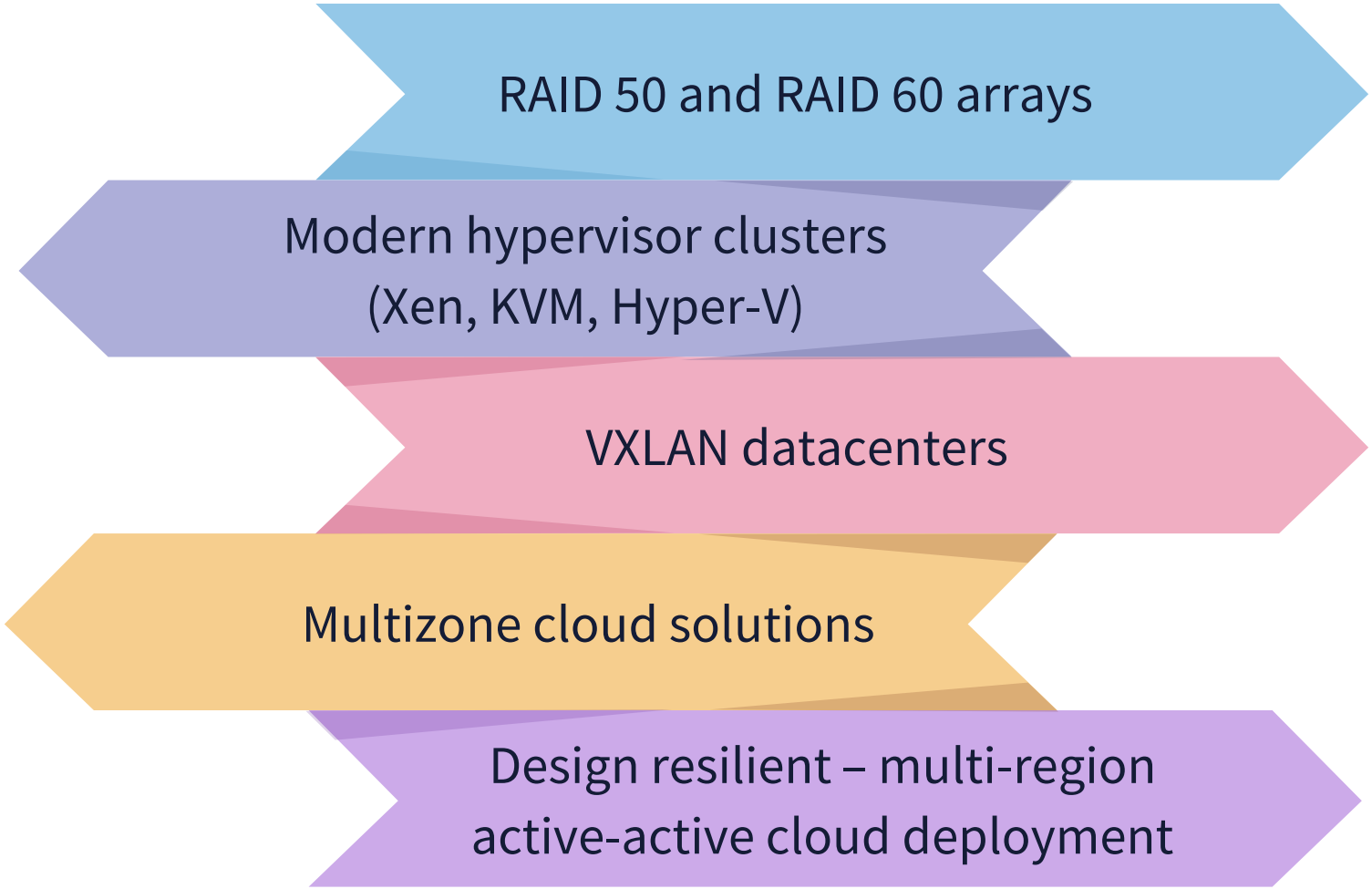
- **Transport Layer Security (TLS) 1.3**
  - In modern environments, TLS 1.2 is habitually not appropriately employed
  - This often renders websites and web applications vulnerable to various threat agent attacks
  - TLS 1.3 eliminates obsolete and unsecure aspects of TLS 1.2, including:
    - SHA-1
    - RC4
    - MD5
    - Arbitrary Diffie-Hellman groups – CVE-2016-0701
  - It also gets rid of obsolete confidentiality contrivances such as DES, 3DES, and AES-CBC

AVAILABILITY

- Availability measures an attacker's ability to disrupt or prevent access to services or data in a client-server or distributed environment
- Vulnerabilities that impact availability can affect hardware, software, and network resources, such as flooding network bandwidth, consuming large amounts of memory, CPU cycles, or unnecessary power consumption
- For a CISSP, availability solutions often involve:
  - Introducing controls against distributed denial-of-service (DDoS) and botnets
  - Assuring that security infrastructure devices are deployed in active-standby or active-active clusters
  - Contributing to business continuity and disaster recovery



HIGH-LEVEL AVAILABILITY



AUTHENTICITY

- According to NIST, authenticity is "The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, message, or message originator."
- Origin authentication is a basic form of authentication, as it only provides a degree of confidence that the correct password, passphrase, or private/secret key was used
- Additional levels of authentication rely on trusted third parties and certificates, digital signatures, and multi-factors, like biometrics

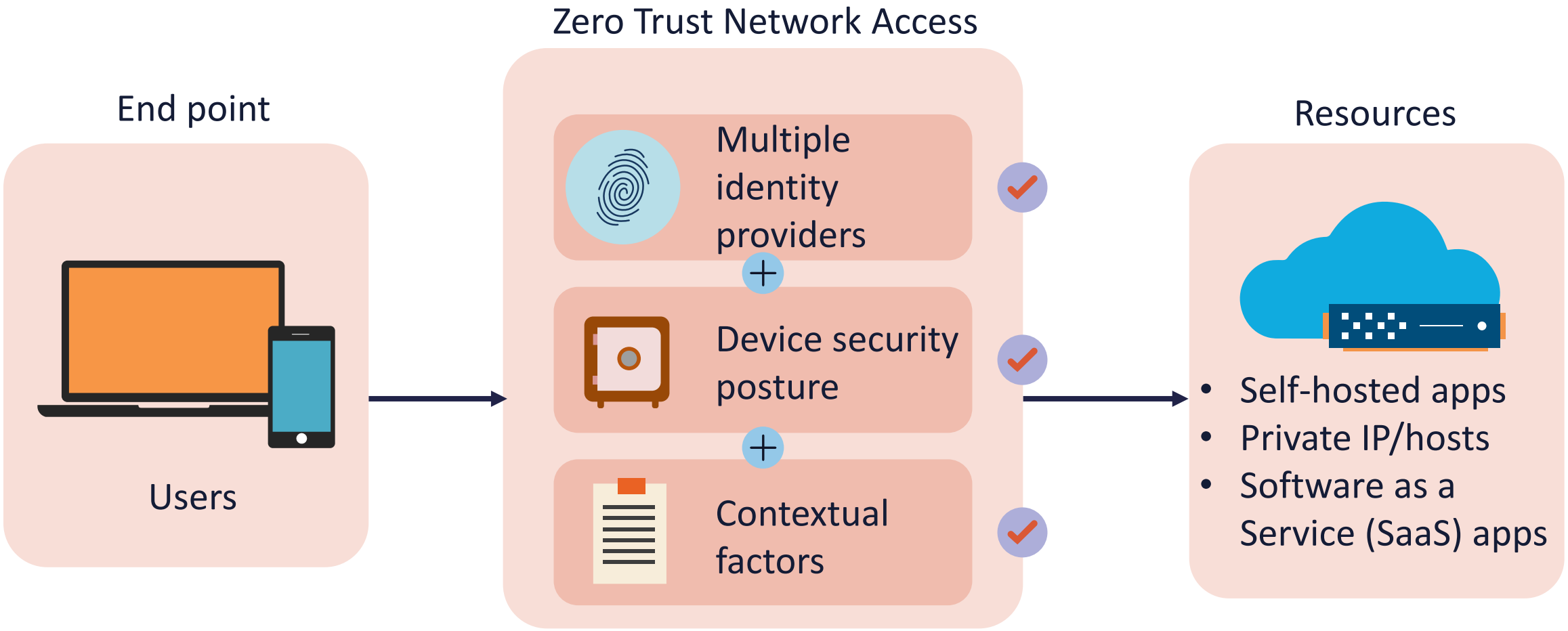
HIGH-LEVEL AUTHENTICITY SOLUTIONS

- **Integrated Identity Platforms**
  - Companies such as IdRamp allow you to manage all systems, services, and applications from one executive dashboard
  - Passwordless (QR codes on endpoints), bring your own identity (BYOI), Zero Trust

HIGH-LEVEL AUTHENTICITY SOLUTIONS

- **Zero Trust Network Access (ZTNA)**
  - This technology makes it feasible to implement a Zero Trust security model
  - Zero Trust is an IT security initiative that accepts that threats exist both inside and outside a network
  - ZTNA demands strict authentication and identification for every subject (principal) before authorizing them to access internal resource objects

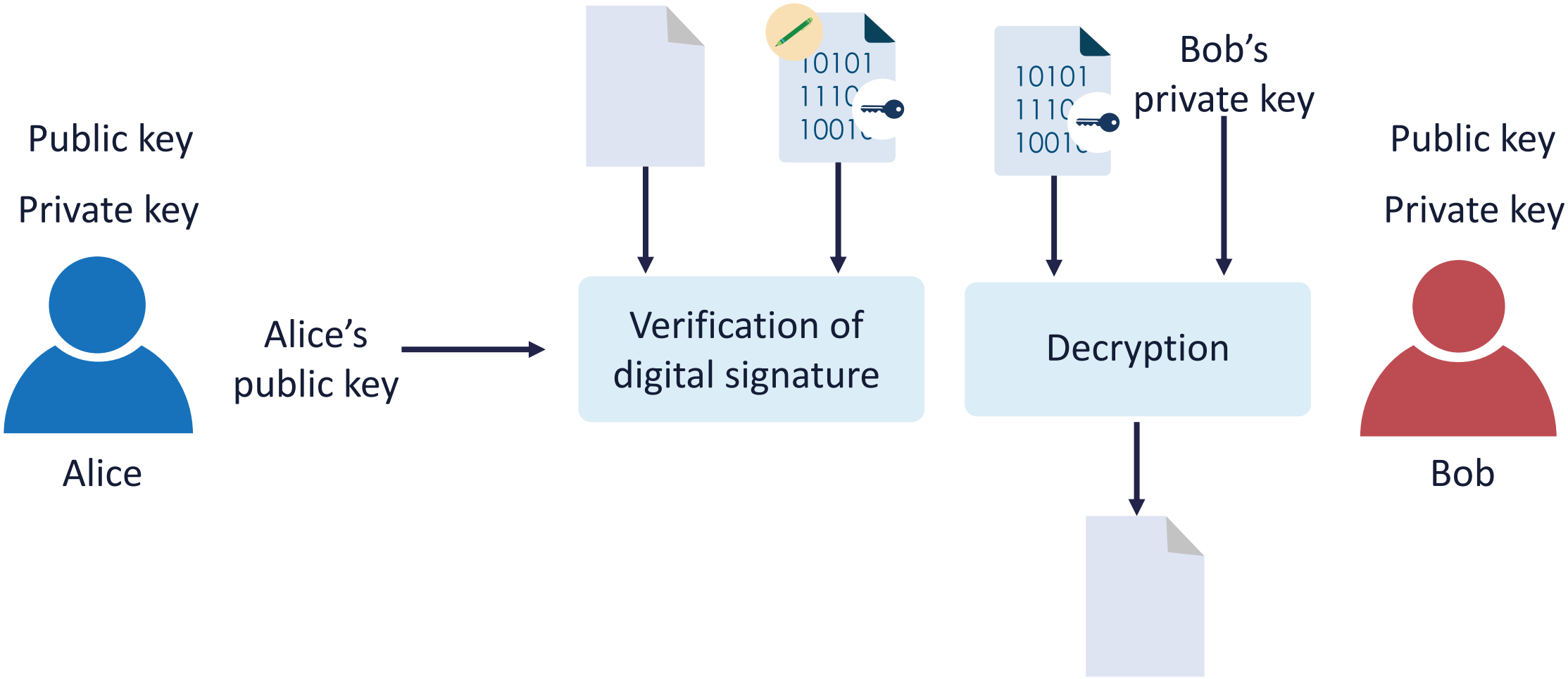
ZTNA ARCHITECTURE



NON-REPUDIATION

- Non-repudiation represents the inability to refuse participation in a digital transaction, contract, or email communication (S/MIME)
- With cryptosystems, a public/private key pair is used
  - The owner/custodian of the private key must protect the key and notify a trusted third party when the key is lost, stolen, or compromised
- Non-repudiation is usually accomplished with digital signatures and digitally signed certificates (X.509v3)

NON-REPUDIATION



SECURITY GOVERNANCE AND COMPLIANCE ISSUES

Objectives

- Align security with strategy, goals, mission, and objectives
- Explore organizational processes, roles, and responsibilities
- Survey security control frameworks
- Compare due diligence to due care
- Examine cybercrimes and data breaches
- Review licensing and intellectual property requirements
- Look at import/export controls and transborder data flow
- Discover privacy, contractual, legal, industry standards, and regulatory requirements

ALIGNING SECURITY WITH STRATEGY, GOALS, MISSION, AND OBJECTIVES

- More than ever, security managers and architects must be sure that security governance, policies, and guidance are closely aligned with the overall organizational strategy, goals, mission, and objectives
- This process has become highly cross-functional and interdisciplinary, involving a blend of skills and competencies that the CISSP-certified person would possess

ALIGN IT SECURITY WITH BUSINESS STRATEGY

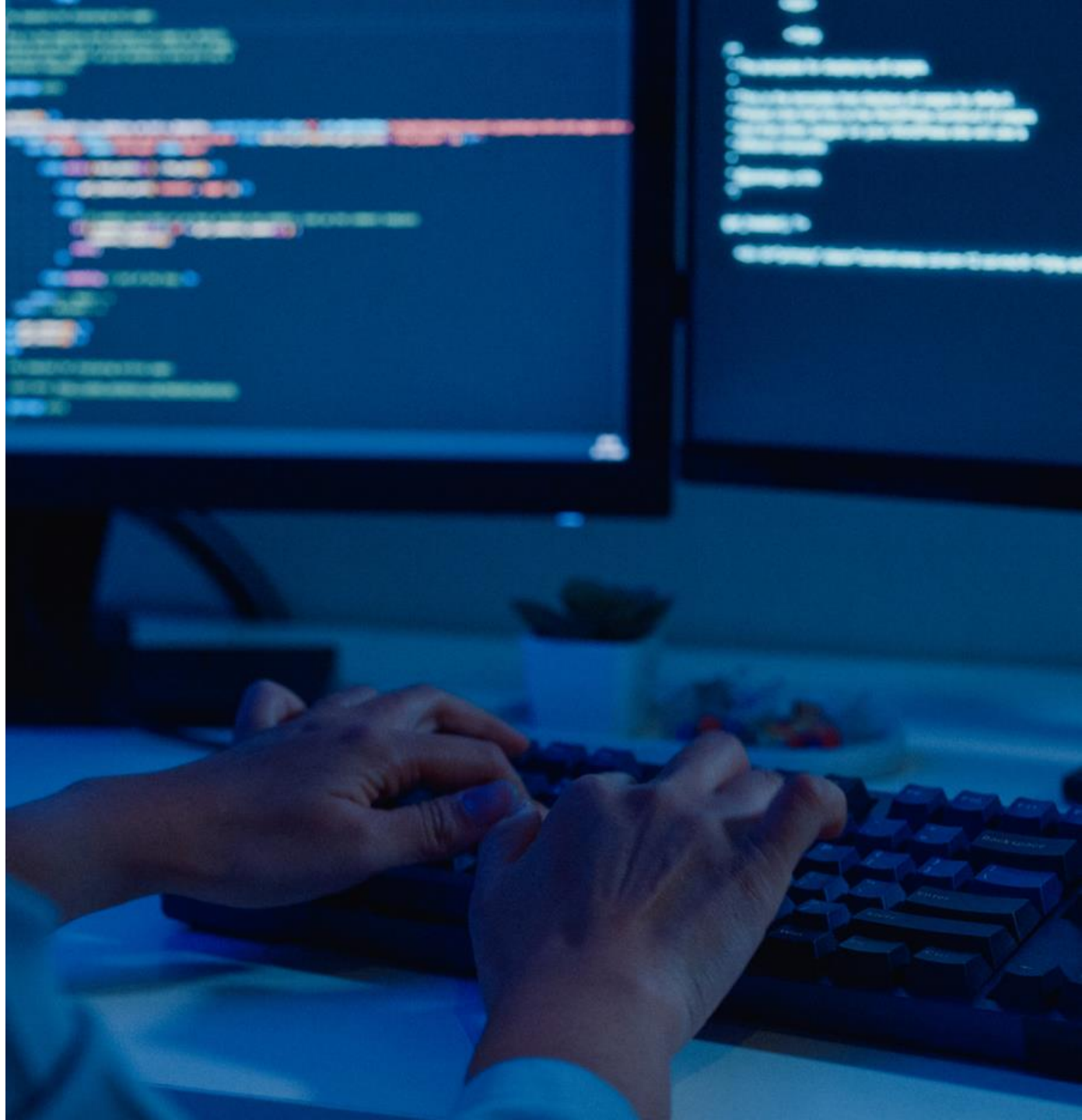
- **Recognize the business goals and risks**
  - Understand the service/product value proposition
  - Know how the organization handles risk for every asset class (mitigate, accept, transfer, etc.)
- **Define your security strategy and metrics**
  - In the words of Sun Tzu in The Art of War: "Tactics without strategy is the noise before defeat"
  - Have access to all relevant and meaningful metrics and key indicators
  - If meaningful metrics do not exist, then they must be accurately generated

ALIGN IT SECURITY WITH BUSINESS STRATEGY

- **Implement and integrate the security solutions** (consider the AWS Well-Architected Framework Operational Excellence principles):
  - Conduct operations as code
  - Make recurrent, small, revocable modifications
  - Improve operations procedures regularly
  - Anticipate and learn from all operational failures
  - Consider fully-managed services when feasible
  - Implement enhanced visibility for actionable insights

ALIGN IT SECURITY WITH BUSINESS STRATEGY

- **Review and improve your security performance**
  - Consider an initiative such as ITIL 4 for continual improvement
  - Implement robust configuration and change management practices
  - Maximize the Service Desk
  - Generate meaningful reports
- **As a security manager or architect continue to add skills and personal experiences**



ORGANIZATIONAL GOVERNANCE

- The need for governance exists anytime a group of people comes together to accomplish an end
- Typically focuses on three attributes or characteristics:
  - Authority
  - Decision-making
  - Accountability
- Governance is focused on the structure and processes for sound decision-making, accountability, management, and conduct at the top of an organization

SECURITY GOVERNANCE

- Security alignment must continually permeate through all organizational processes including governance, steering committee charters, corporate initiatives, and more
- Security strategists must account for any major changes to organizational operations or activity
- The alignment begins with defining organizational and security governance

SECURITY GOVERNANCE

- This initiative directs how an organization's security objectives are determined and achieved
- Determines how risk is controlled and addressed based on the rules to protect the assets and continuity of an organization
- Guides the course and control of organizational security operations, initiatives, and activities
- The security manager's strategy will be derived from effective security governance

SECURITY GOVERNANCE ACTIVITIES

GOVERNANCE COMMITTEES

- A security governance committee is responsible for knowing all security regulations that apply to the organization
- It will document and hold accountable all assigned ownership and custodianship of regulatory compliance within the organization
- The committee process will also oversee the cybersecurity teams who are responsible for mitigating an organization's business risks

GOVERNANCE COMMITTEES

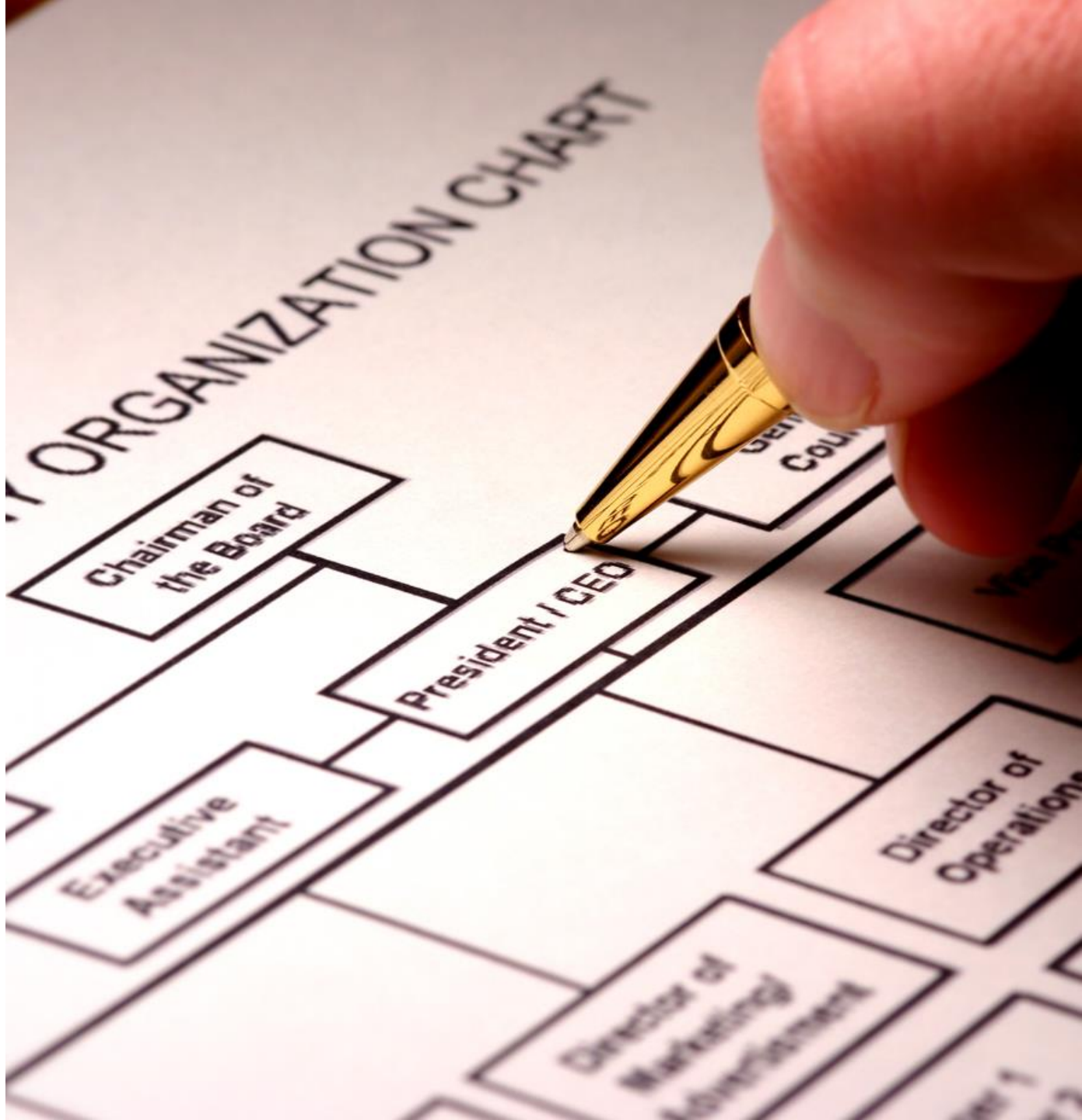
- Security steering committees establish and maintain the security framework (ISO/IEC, NIST, COBIT, CIS, etc.) to assure that security strategies are aligned with and support the objectives of the organization
- The selected security framework should ensure that the activities are consistent with all applicable laws and regulations
- Other activities include ongoing reviews and actions due to macro changes to the organization (acquisitions, mergers, and divestitures)

SECURITY ISSUES FROM ACQUISITIONS

- In challenging economic environments, it is common for organizations to conduct mergers and acquisitions (M&A) to improve their financial posture
- This process can put organizations' sensitive data assets at risk
  - Employees not involved in negotiations may hear about merger talks and possibly leak data to the press or to competitors to hinder the process
- The most significant risk of an M&A is not doing cyber due diligence on the company being acquired

SECURITY ISSUES FROM ACQUISITIONS

- Changing personnel can also create gaps in your security initiatives
- Employees with high-level knowledge may leave the company so that critical processes and procedures must be re-documented and updated
- If departments or groups are understaffed in vital areas, they may take shortcuts that leave sensitive data exposed
- It is important to prioritize security training and update all employees on policies after a merger or acquisition takes place

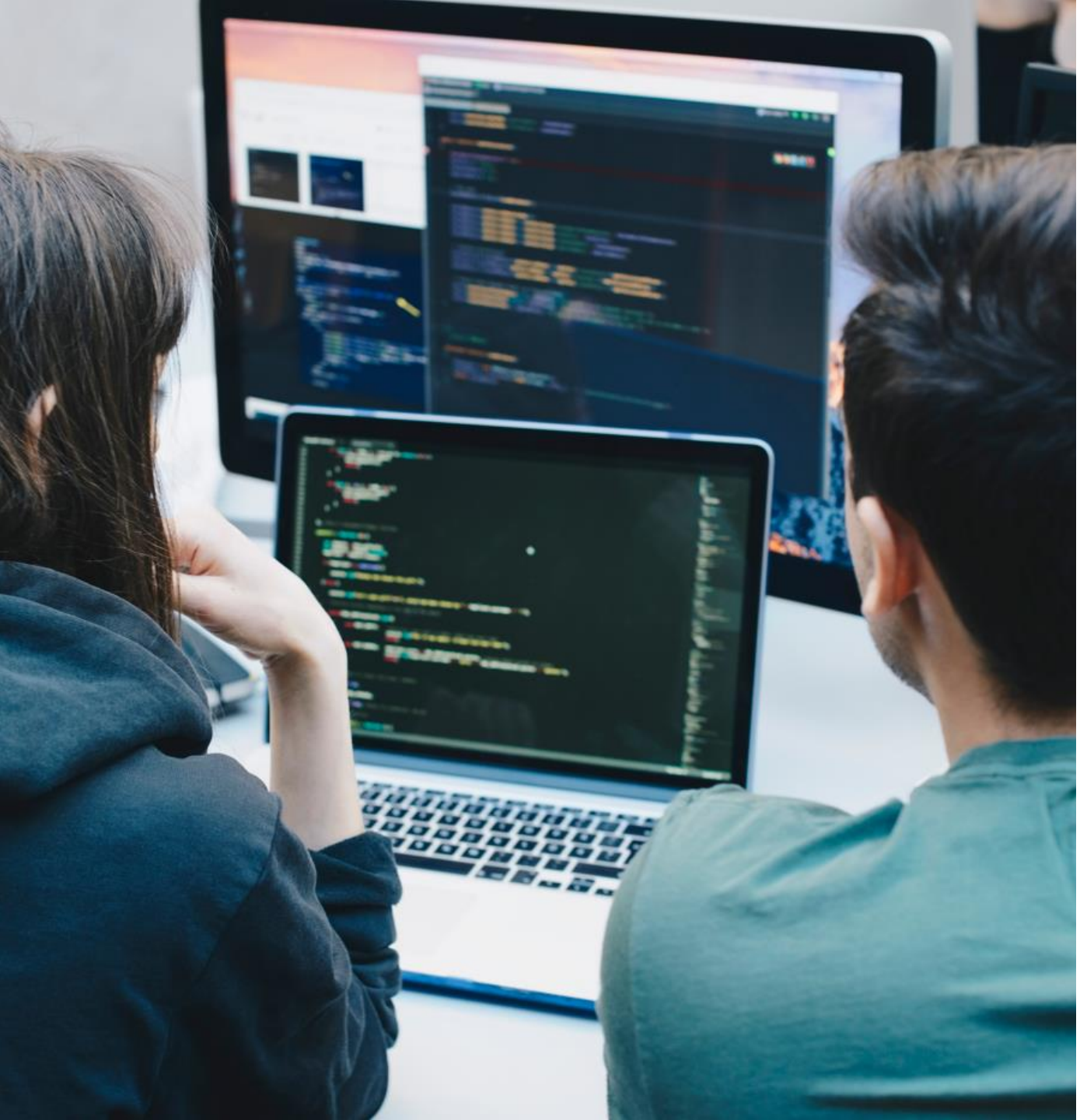


SECURITY ISSUES FROM DIVESTITURES

- Divestitures will introduce many of the same security vulnerabilities as a merger and acquisition
- During divestment, threat actors will use the situation to gain access to sensitive data, trade secrets, and other personal information
- Divestitures tend to increase the number of people, systems, and assets involved, consequently heightening the possibility for human error and negligence
- Divestitures often include mass layoffs which in turn may raise the number of disgruntled ex-employees who become threat agents

ASSET AND DATA OWNERS

- Often the ones to create/acquire the asset or data in the earliest stages of the lifecycle
- May be creators in a discretionary access control (DAC) model
- Owners can determine the classification or sensitivity level of the asset
- Can be the party that tags, labels, or handles the assets
- These are typically highly-privileged or power users in the organization



CUSTODIANS

- This role will typically maintain the assets from a technical perspective
- They often answer directly to an officer or possibly the asset owner
- May be charged with maintaining the confidentiality, authenticity, integrity, and non-repudiation services on behalf of the assets
- Are more involved with the tactical aspects of asset management as opposed to strategic

STEWARDS

- This role usually manages assets from a business or compliance perspective
- They have expertise with interfacing with internal and external customers and stakeholders
- May be tasked with ensuring compliance (standards and controls) and data quality
- Often involved with onboarding and offboarding of assets with joiners and movers

OFFICERS

Chief information officer (CIO)

Chief information security officer (CISO)

Chief privacy officer (CPO)

ROLES AND RESPONSIBILITIES USING RACI

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*

SECURITY CONTROL FRAMEWORKS: ISO

- International Organization for Standardization (ISO) brings global experts together to agree on the best methods for many activities from making a product to managing processes
- ISO has empowered trade and collaboration between people and organizations since 1946
- ISO/IEC 27001 is the international standard for information security detailing specifications for an effective information security management system (ISMS)
- The ISO 27001 guidance helps organizations manage their information security by addressing people, processes, and technology

SECURITY CONTROL FRAMEWORKS: NIST

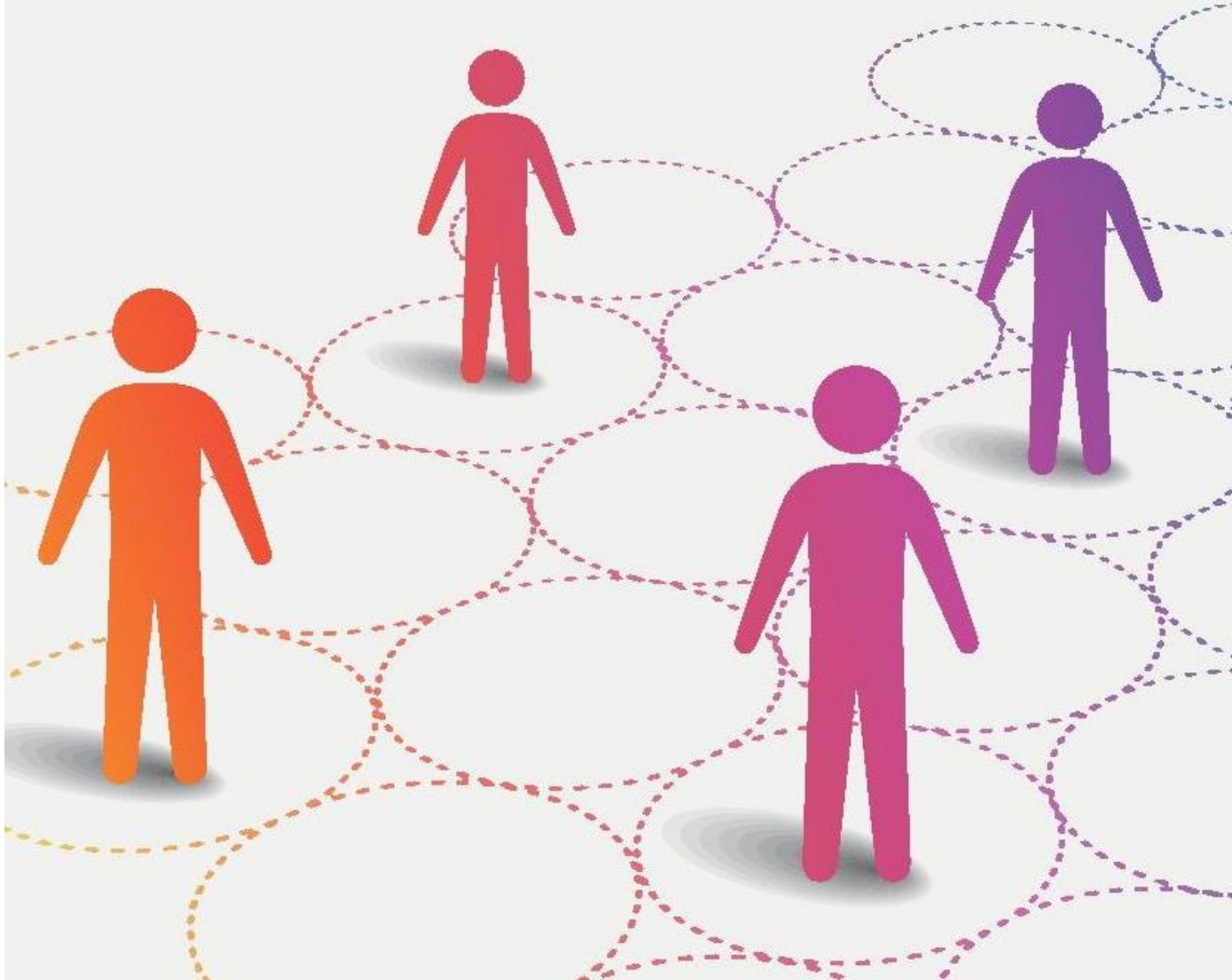
- The National Institute of Standards and Technology (NIST) offers a broad portfolio of services for measurements, standards, and legal scientific studies of measurement
- NIST provides solutions that ensure measurement traceability, support quality assurance, and blend documentary standards with regulatory practices
- SP 800-53 provides a catalog of controls for systems and organizations to manage information security and privacy risk

SECURITY CONTROL FRAMEWORKS: COBIT

- COBIT stands for "Control Objectives for Information and Related Technology"
- It assists organizations in addressing business challenges in regulatory compliance, risk management, and IT strategy alignment with organizational goals
- COBIT 5, the latest iteration of the framework, was released in 2012 and has five principles:
    1. Meeting stakeholder needs
    2. Covering the enterprise end to end
    3. Applying a single integrated framework
    4. Enabling a holistic approach
    5. Separating governance from management

SECURITY CONTROL FRAMEWORKS: SABSA

- Sherwood Applied Business Security Architecture (SABSA) is a well-established framework for constructing business-driven, risk and opportunity focused security initiatives
- It works at both the enterprise and solutions level that support traceable business goals
- It is also widely used for information assurance architectures, Risk Management Frameworks (RMF), and to align and integrate security and risk management into IT architecture methods and frameworks



SECURITY CONTROL FRAMEWORKS: SABSA

- SABSA is made up of several cohesive frameworks, models, methods and processes including:
  - Business Requirements Engineering Framework (known as Attributes Profiling)
  - Risk and Opportunity Management Framework
  - Policy Architecture Framework
  - Security Services-Oriented Architecture Framework
  - Governance Framework
  - Security Domain Framework
  - Through-life Security Service Management & Performance Management Framework

SECURITY CONTROL FRAMEWORKS: PCI

- The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards from 2004 by several public companies
- The compliance structure aims to secure credit and debit card transactions against data theft and fraud
- Although the PCI has no legal authority to force compliance, it is a requirement for any business that processes credit or debit card transactions
- PCI certification is also considered the best way to protect sensitive data and to help businesses build trust with their customers

SECURITY CONTROL FRAMEWORKS: FEDRAMP

- The Federal Risk and Authorization Management Program (FedRAMP®) was established to offer a cost-effective, risk-based approach for the adoption and use of cloud services by the federal government
- FedRAMP empowers agencies to use modern cloud technologies, with an emphasis on security and protection of federal information
- In December 2022, the FedRAMP Authorization Act was signed as part of the FY23 National Defense Authorization Act (NDAA)
    - The Act codifies the FedRAMP program as the authoritative standard for security assessment and authorization for cloud computing products and services that process unclassified federal information

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
- Attentiveness may include understanding which framework is required by law or is applicable under vendor due diligence
- This has become a critical initiative with supply chain disruptions and related security gaps

DUE DILIGENCE EXAMPLES

- Examples of due diligence include:
  - Comprehensive background checks and proofing practices before hiring
  - Investigating a cloud service provider (CSP) with the CSA Cloud Controls Matrix or Star Registry before signing a memorandum of understanding (MOU)
  - Testing and evaluating nonrepudiation techniques (digital signatures) before signing contracts or using code
  - When federal agencies mandate how Controlled Unclassified Information (CUI) must reside in a nonfederal system and organization
  - Auditing any changes to the supply chain including new mean time to repair/replace (MTTR) metrics for business impact analysis

DUE CARE

- **Due care** refers to the degree of attention that a reasonable person takes for a particular entity life cycle or program
- It is the level of judgment, attention, and activity that a person would engage in under similar circumstances
- Due care relates to ongoing maintenance activities, operational excellence, and continual improvement (e.g., ITIL 4 initiatives)

DUE CARE EXAMPLES

- Examples of due care include:
  - Performing the necessary maintenance and tested patch management to keep a system or application available and secure
  - Taking all the necessary precautions to ensure that an IP packet arrives with CIA properly applied using various improved controls
  - Using security principles like least privilege, defense in depth, Separation of Duties (SoD), Zero Trust, and more for continual improvement and maturity
  - Updating the security policies and training/awareness to include new threats, technologies (e.g., artificial intelligence, machine learning), and initiatives

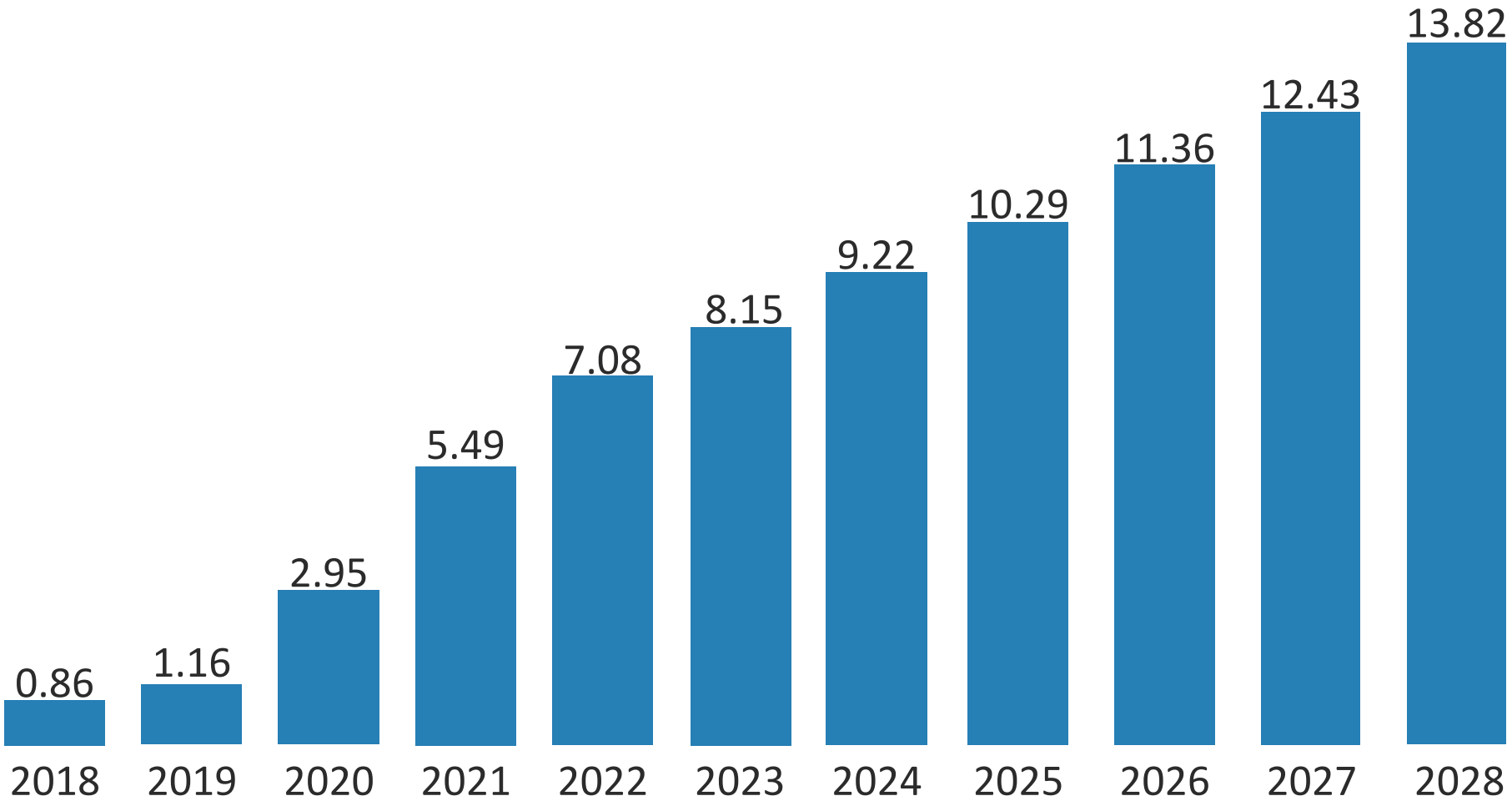
CYBERCRIMES AND DATA BREACHES

- Cybercrime is commonly defined as the following results of threat actors:
  - Harm and destruction of data
  - Stolen financial instruments
  - Productivity loss
  - Theft of intellectual property (IP), personally identifiable information (PII), and other financial data
  - Embezzlement, fraud, and hoaxes
  - Post-attack interruption to the normal course of operations including forensic investigation, restoration and deletion of hacked data and systems, and reputational harm

CYBERCRIMES AND DATA BREACHES

- The costliest cybercrime recently reported by the FBI was business email compromise (BEC) and personal email compromise, which targets businesses and individuals that engage in wire transfers by breaking into their emails
- BEC is a from of cybercrime where the scammer uses email or more elaborate hoaxes to trick someone into sending money or divulging confidential company info
- The costs as of 2024 have stretched into the billions of US dollars

Estimated annual cost of cybercrime worldwide (in trillion U.S. dollars)



https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/

LICENSING ISSUES AND INTELLECTUAL PROPERTY REQUIREMENTS

- Some commercial licenses used on-site do not transfer well to virtual environments or cloud service providers
- Ghost (shadow) IT such as unauthorized Type 2 hypervisors can run unlicensed and pirated software
- Licensing can be different in various countries and regions of the world – even for the same application
- Many organizations have a lack of "licensing management" especially in cloud and Software as a Service (SaaS) environments

OPEN-SOURCE LICENSING ISSUES

- There are over 200 types of open-source licenses that can be used (Apache, GPL, and MIT) – most of which have a lack of warranty for its security, support, or content
  - Many of these licenses are incompatible with each other where certain components cannot be used
  - The more components you use, the more difficult it becomes to track and compare all license stipulations
- Some licenses include "copyleft" clauses that require the release of any software created with the covered components as open-source, in its entirety

INFORMATION RIGHTS MANAGEMENT (IRM)

- Also called digital rights management (DRM) and enterprise digital rights management (E-DRM)
- The goals are to implement controls that work with access controls to protect data and file-level assets
- Example: Must control copying, deleting, and modifying certain PDF documents to protect intellectual property (IP) and copyrights
- DRM is used by publishers, manufacturers, and IP owners for digital content and device monitoring
- Since digital signing and certificates are often used, an enterprise public key infrastructure (PKI) may be part of the policy

IRM/DRM WITH ADOBE DOCUMENTS

Manage document usage	Deny unauthorized sharing	Stop screen captures or printing to files	Enforce expiration	Revoke access based on least privilege
Restrict to specific IP Classless Inter-Domain Routing (CIDR) Ranges	Watermark PDF files	Track document usage	Integrate with command line interface (CLI) for automation	Integrate with e-commerce solutions

IMPORT/EXPORT CONTROLS AND TRANSBORDER DATA FLOW

- The U.S. Department of Commerce's Bureau of Industry and Security (BIS) administers U.S. laws, regulations and policies controlling the export and re-export of commodities, software, and technology placed under the jurisdiction of the Export Administration Regulations (EAR)
- The main objective of BIS is to progress national security, foreign policy, and economic goals by safeguarding an effective export control and treaty compliance system, as well as promote continual U.S. strategic technology leadership

BUREAU OF INDUSTRY AND SECURITY

- BIS is answerable for deploying and enforcing the EAR, which regulates the export, re-export, and transfer (in-country) of items with commercial uses that can also be used in conventional arms, weapons of mass destruction, terrorism, or human trafficking and rights abuses, and less sensitive military items
- The BIS Export Administration (EA) reviews license applications for exports, re-exports, transfers and deemed exports subject to the EAR
- Supply chain security is critical when engaged in import/export activities

TRANSBORDER DATA FLOW

- Transborder data flow (TDF) can be defined as the electronic transmission of data across political borders for processing and storage in file, block, and object storage
- Massive amounts of digital data are processed by businesses, and the data moves globally in ways that have both pros and cons
- For private-sector entities, cross-border data flows reinforce daily operations, logistics, supply chains, and global communications
- Accountable cross-border data flows can reduce human rights abuses, support cybersecurity, promote economic development, financial inclusion, health, sustainability, and more

TRANSBORDER DATA FLOW

- How will companies protect privacy in the target country?
- How will governments seek access to that data for national security and law enforcement auditing and forensic initiatives?
- How do organizations that use the cloud to distribute content to other areas handle different local laws, regional differences, and varying cultural and religious sensitivities?
- Is there a realistic global framework open to democracies operating under the rule of law, that is rights-protective, practicable, and scalable?

GENERAL DATA PROTECTION REGULATION

- The European Union's General Data Protection Regulation (GDPR) is concerned with data protection and privacy in the EU and European Economic Area
- It introduces strict privacy controls for how organizations worldwide collect, use, and store the personal information of EU citizens
- GDPR covers all countries, citizens, **and areas under its jurisdiction** regardless of where the data is created, processed, or stored
- GDPR violations can bring stiff penalties, so organizations everywhere must be mindful of its requirements

GENERAL DATA PROTECTION REGULATION

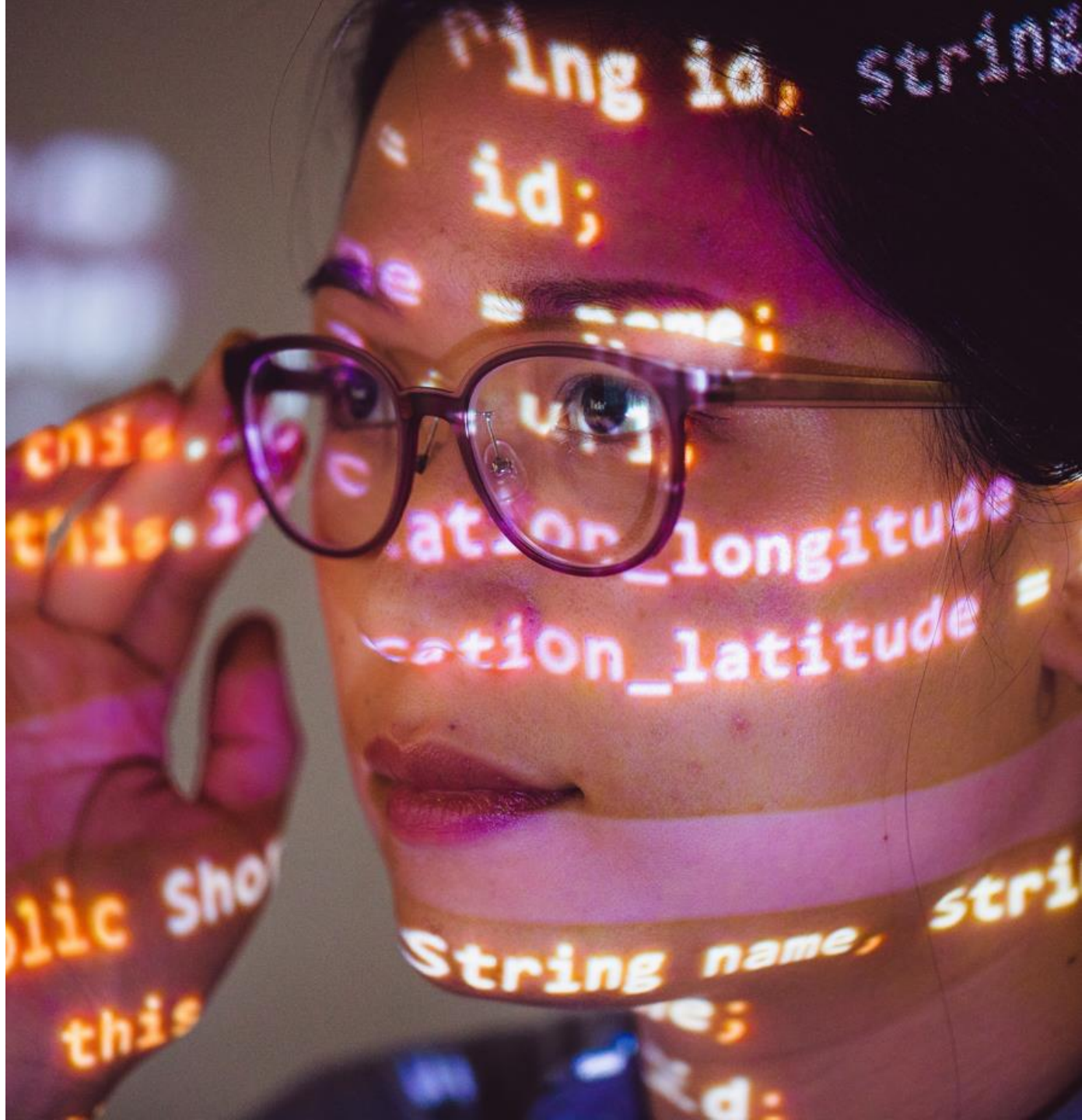
- The Privacy Shield Framework replaced Safe Harbor when on Oct 6, 2015, the European Court of Justice (ECJ) – Europe's highest court – concluded that the US-EU Safe Harbor agreement between the European Commission and the U.S. Department of Commerce was invalid
- Although the Court of Justice subsequently invalidated the Privacy Shield framework in 2020, participants are still obliged to comply with some of its requirements
- The GDPR is a continually evolving and changing organism (AI protections) so security managers must constantly monitor changes

CALIFORNIA CONSUMER PRIVACY ACT

- The California Consumer Privacy Act (CCPA) is a privacy law that controls how businesses can gather, use, and share the personal information of California residents
- The law also grants consumers the right to know what data companies collect about them, to request destruction of their data, and to opt out of sharing or selling their data
- The law applies to businesses that have customers in California, **regardless of their location or operation**

PERSONAL INFORMATION PROTECTION LAW

- The China Personal Information Protection Law (PIPL) is a relatively new data privacy law in China that is aimed at personal information protection and challenges with personal data leakage and loss
- PIPL applies not only to entities physically located in mainland China that handle PII, but also to entities located outside mainland China that engage in certain activities involving the personal information of persons physically located in China



PROTECTION OF PERSONAL INFORMATION ACT

- The Protection of Personal Information Act (PoPIA or the PoPI Act) is a set of laws that govern data protection and privacy in South Africa
- The act was passed to regulate the right to privacy, as enshrined by section 14 of the Constitution of South Africa and functions in concert with the Promotion of Access to Information Act

CONTRACTUAL, LEGAL, INDUSTRY STANDARDS, AND REGULATORY REQUIREMENTS

- In cloud computing, for instance, the legal responsibility for data processing falls to the consumer or user who solicits the services of a CSP
- As in all other cases in which a third party is given the task of processing personal data, the user, or data controller, is responsible for ensuring that the relevant requirements for the protection and compliance with requirements for PII and Protected Health Information (PHI) are satisfied or met

CONTRACTUAL PII

- Contractual PII is where an organization or entity processes, transmits, or stores PII as part of its business or services
- This information is required to be adequately protected in line with relevant local, state, national, regional, federal, or other laws
- The relevant contract should list the applicable rules and requirements from the organization who "owns" the data and the applicable laws to which the provider should adhere

REGULATED PII

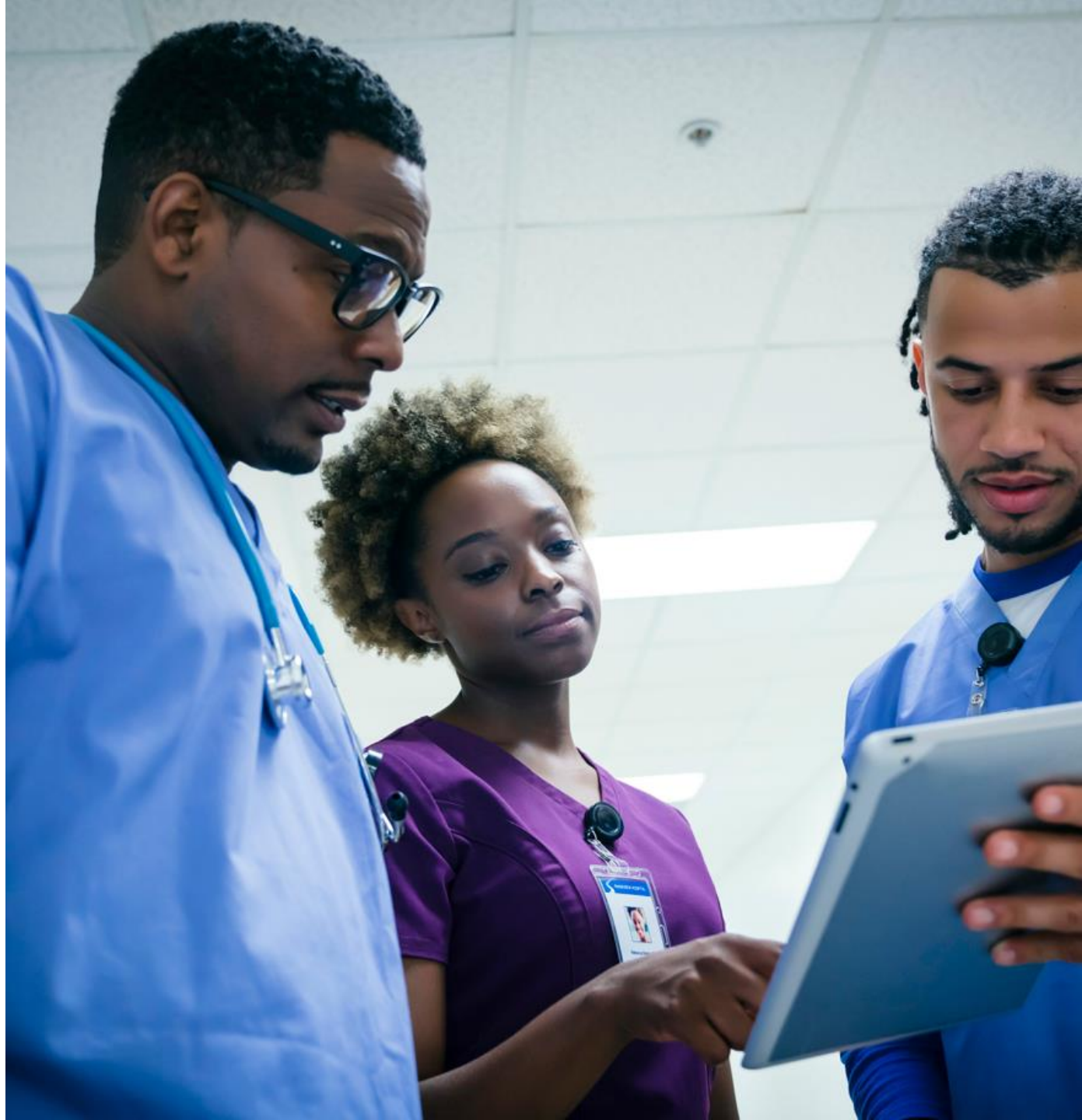
- With regulated PII, the key focus and distinct criteria to which the regulated PII must adhere is required under law and statutory requirements
  - PCI-DSS
  - GDPR
  - Sarbanes-Oxley
- This is different than the contractual criteria that may be based on best practice or organizational security policies

HIGHLY REGULATED INDUSTRIES: NERC/CIP

- To reinforce the cyber resilience of the U.S., the government created the North American Electric Reliability Corporation (NERC) framework that is directed at protecting a portion of the U.S. utility infrastructure
- The NERC Critical Infrastructure Protection (CIP) Standards deal specifically with the cybersecurity attributes of the Bulk Electric System and its capable and steady supply

HIGHLY REGULATED INDUSTRIES: HIPAA/HITECH

- The HITECH Act updated HIPAA and is focused on promoting the implementation of secure and private **electronic** health records and meaningful use of health information technology, and is part of the American Recovery and Reinvestment Act of 2009
- HIPAA predates the HITECH Act by 13 years and deals with the portability of health insurance (ensuring employees do not lose coverage while between jobs), and the privacy/security of health data



INVESTIGATIONS AND POLICIES

Objectives

- Explore requirements for investigation types
- Develop, document, and implement security policy elements
- Examine candidate screening and hiring
- Survey employment agreements, policy-driven requirements, onboarding, transfers, and termination processes
- Learn about vendor, consultant, and contractor agreements and controls

ADMINISTRATIVE INVESTIGATIONS

- The main goal of administrative investigations is to collect and scrutinize data and information regarding incidents or allegations of wrongdoing, policy abuses, or other assorted reckless behaviors
- These investigations assist in:
  - Lowering organizational risk or harm
  - Preventing future occurrences of incidents
  - Maintaining organizational mission and integrity
  - Helping to maintain compliance and accreditation

REQUIREMENTS FOR ADMINISTRATIVE INVESTIGATIONS

- The investigative team must ensure that when witnesses are deposed, they have certain rights:
  - They can be attended, represented, and counseled by legal parties
  - Counsel for a witness can instruct on objections about the scope and range of questions
  - Counsel cannot interrupt the questioning beyond permissible objections
  - Once the process concludes, counsel may appeal for clarification of the answers

CASE STUDY: DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

- The Department of Defense Office of Inspector General (DoD OIG) conducts administrative investigations to:
  - Investigate claims of misconduct by senior officials
  - Report on whistleblower reprisal cases
  - Manage the DoD Hotline and Contractor Disclosure Program
  - Offer ongoing training and awareness on whistleblower protections
  - Accelerate the voluntary resolution of retaliation allegations

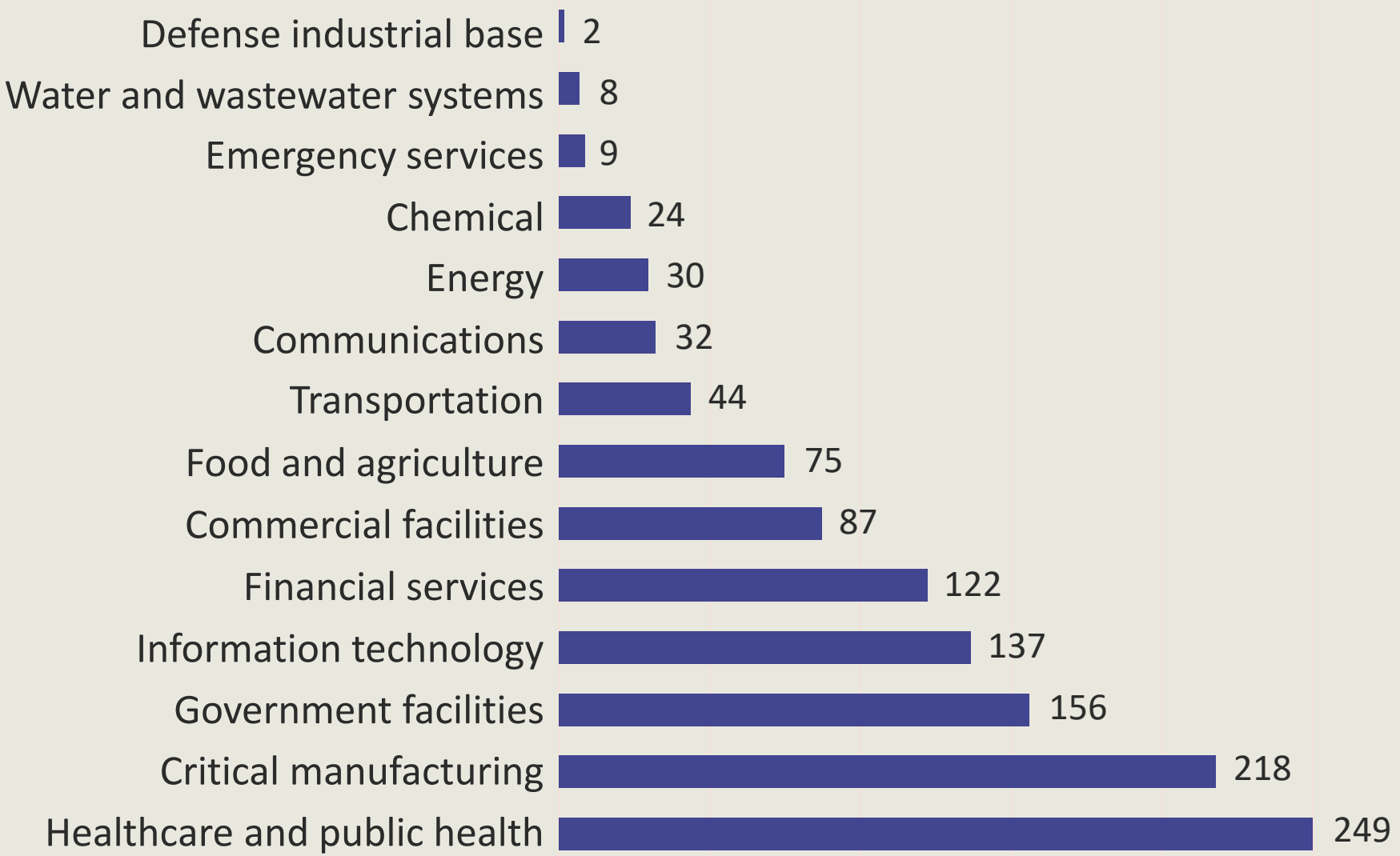
CRIMINAL INVESTIGATIONS

- There are several requirements for the security manager to conduct proper criminal investigations:
  - Possess practical knowledge of applicable criminal laws
  - Be able to recognize and examine electronic and possibly physical evidence
  - Possess skills and expertise with interviews, interrogations, and cross-examinations
  - Adhere to high-level standards and ethics
  - Have proficiency in specialized software applications and data and statistical analysis

COMMON CYBERCRIME INVESTIGATIONS

- According to the U.S. FBI, the most common cybercrimes categories in 2023 were:
  - **Phishing and business email compromise (BEC)**
  - Intellectual property rights (IPR) theft
  - Computer intrusions (hacking)
  - Economic espionage (theft of trade secrets)
  - Online extortion
  - International money laundering
  - Identity theft
  - Child pornography
  - Ransomware

INFRASTRUCTURE SECTORS AFFECTED BY RANSOMWARE (FBI-2023)



CIVIL INVESTIGATIONS

- A civil investigation is an inquiry to gather data and supporting evidence for a civil legal matter such as:
  - A lawsuit claiming damages due to a company vehicle accident
  - Both sides of a case performing an investigation to collect materials they will use to pursue the case or contest claims, depending on the scenario
- Security managers may need to seek outside counsel for attorneys who specialize in civil matters if their legal department doesn't have the expertise

REGULATORY INVESTIGATIONS

- This form of investigation will force security managers and officers to contend with external auditors and investigators who are seeking damages such as fines and penalties for regulatory breaches
- For example, after investigations, these companies were given the following GDPR fines:
  - Google – €50m in 2019 for violating GDPR
  - H&M – €35.3m in 2020 for secretly monitoring hundreds of its employees
  - Telecom Italia – €27.8m
  - British Airways – £20m
  - Marriott International Hotels – £18.4m

REGULATORY INVESTIGATIONS

- Security professionals must realize that data incident investigations may take months or years until resolution
- They will have to interface with state attorney generals, federal regulators, and state administrative agencies
- The more regulators involved, the longer the investigation takes, especially with bigger cases
- Regulatory investigations usually get resolved in one of four ways:
  - Litigation
  - Settlement
  - Closing notice
  - Silence

LIST OF COMMON INDUSTRY STANDARDS

- ISO 27001 information security management systems (ISMS)
- ISO 27701 GDPR compliance
- ISO 9000 family – quality management
- CMMC – Cybersecurity Maturity Model Certification
- OSHA Fall Protection in Construction
- NIST 800-53 family

DEVELOP, DOCUMENT, AND IMPLEMENT SECURITY POLICY

- Most security professionals will rely upon existing templates to construct and implement security policy elements
- A good example for the CISSP candidate would be the SANS.org security policy templates site
  - In collaboration with information security subject-matter experts and volunteer leaders with security policy experience, SANS has developed and posted a set of security policy templates for public use

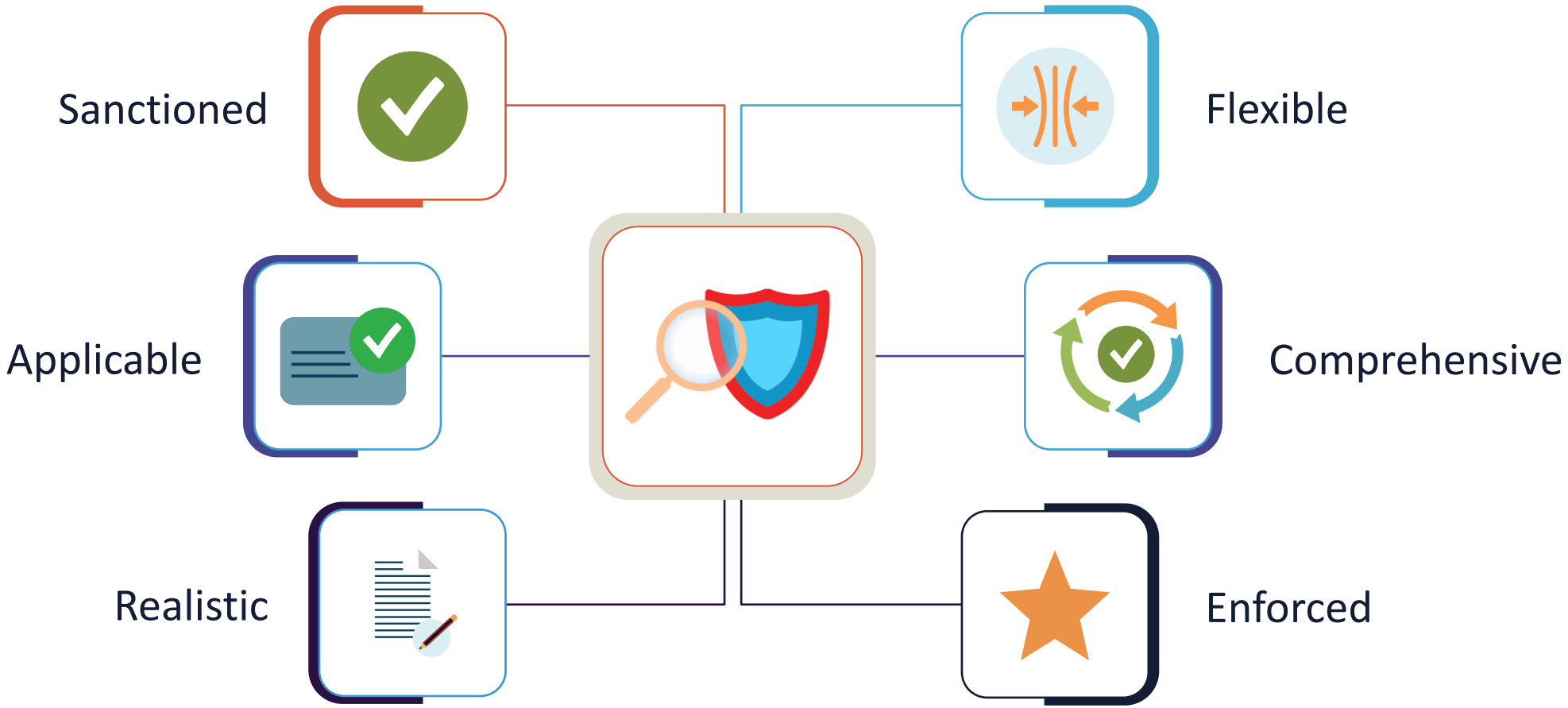
SECURITY POLICIES

- Policies, especially security policies, institute a general framework within which to function
- They are also a guiding direction in which to move forward in the future
- The function of a policy is to categorize guiding principles, steer proper behavior, and provide a roadmap for implementing various security controls
- An information security policy is a directive that outlines how an organization plans to protect its data, applications, services, and systems

SECURITY POLICIES

- Security policies and procedures help 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 EFFECTIVE INFORMATION SECURITY POLICIES



POLICIES SHOULD BE SANCTIONED

- The policies must be authorized
- A policy requires the support of executive management or the C-suite
- There is often one owner or accountable entity
  for the security policy (i.e., RACI)
- **This demands visible involvement and ongoing activities such as communication, funding, championing, prioritization, due diligence, and**
  due care

POLICIES SHOULD BE APPLICABLE

- The policies must be appropriate and relevant to the organization
- They must be in concert with the charters, missions, strategies, and value propositions of the enterprise
- Strategically, the information security policy must support the guiding principles (i.e., ITIL4) and objectives of the organization
- Tactically, policies must be closely related to those stakeholders and principals who must conform
- **Templates should be customized as needed to meet this objective**

POLICIES SHOULD BE REALISTIC

- In actuality, the policies can be effectively executed
- Policies must mirror the actual state of the environment in which they will be applied
- Information security policies and procedures should only demand what is possible in the given time frame
- If the assumption is that the policy goals are to reduce risk and advance the organization’s guiding principles, then a positive result is anticipated
- **Policies (i.e., mock phishing campaigns) should never set up principals for failure or retribution but rather offer a clear track for success**

POLICIES SHOULD BE FLEXIBLE

- Polices must be agile and changeable
- An information security policy should accommodate sudden and rapid modifications when necessary
- An adaptable set of policies will realize that information security is not a static, point-in-time initiative
- **This ongoing process designed to support the organizational mission must adapt to new opportunities, technologies, competitors, and business continuity challenges (i.e., pandemics)**

POLICIES SHOULD BE COMPREHENSIVE

- The scope of information security policies must be inclusive **and include all applicable internal and external parties (stakeholders)**
- The policies must consider :
  - Customers (internal and external)
  - Shareholders
  - Organization objectives
  - Laws and regulations
  - Cultural norms of employees and consumers
  - Business and strategic partners
  - Vendors and suppliers (supply chain)
  - Environmental impacts and sustainability
  - Global cyber threats

POLICIES SHOULD BE ENFORCED

- The information policies should first be **enforceable** and then subsequently be **enforced**
- Enforceable entails that countermeasures have been implemented to support the policy and adherence to policies is measurable
- When necessary, proper actions will be taken:
  1. Email or phone call reminder
  2. Verbal and/or written warning
  3. Sanctions or removal of privileges
  4. Suspension with pay
  5. Suspension without pay
  6. Termination
  7. Criminal or civil legal action (incarceration, reimbursement, and/or restitution)

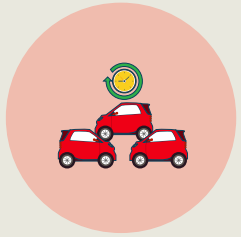
SAMPLE PERSONNEL POLICIES (AUP)

Endpoint use policy

Rotation of duties

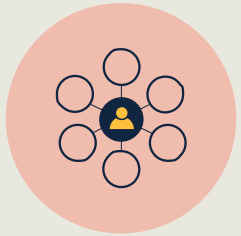
Corporate vehicle policy

Clean desk



Mandatory vacations

No piggybacking/tailgating



Social media usage

Web surfing sites

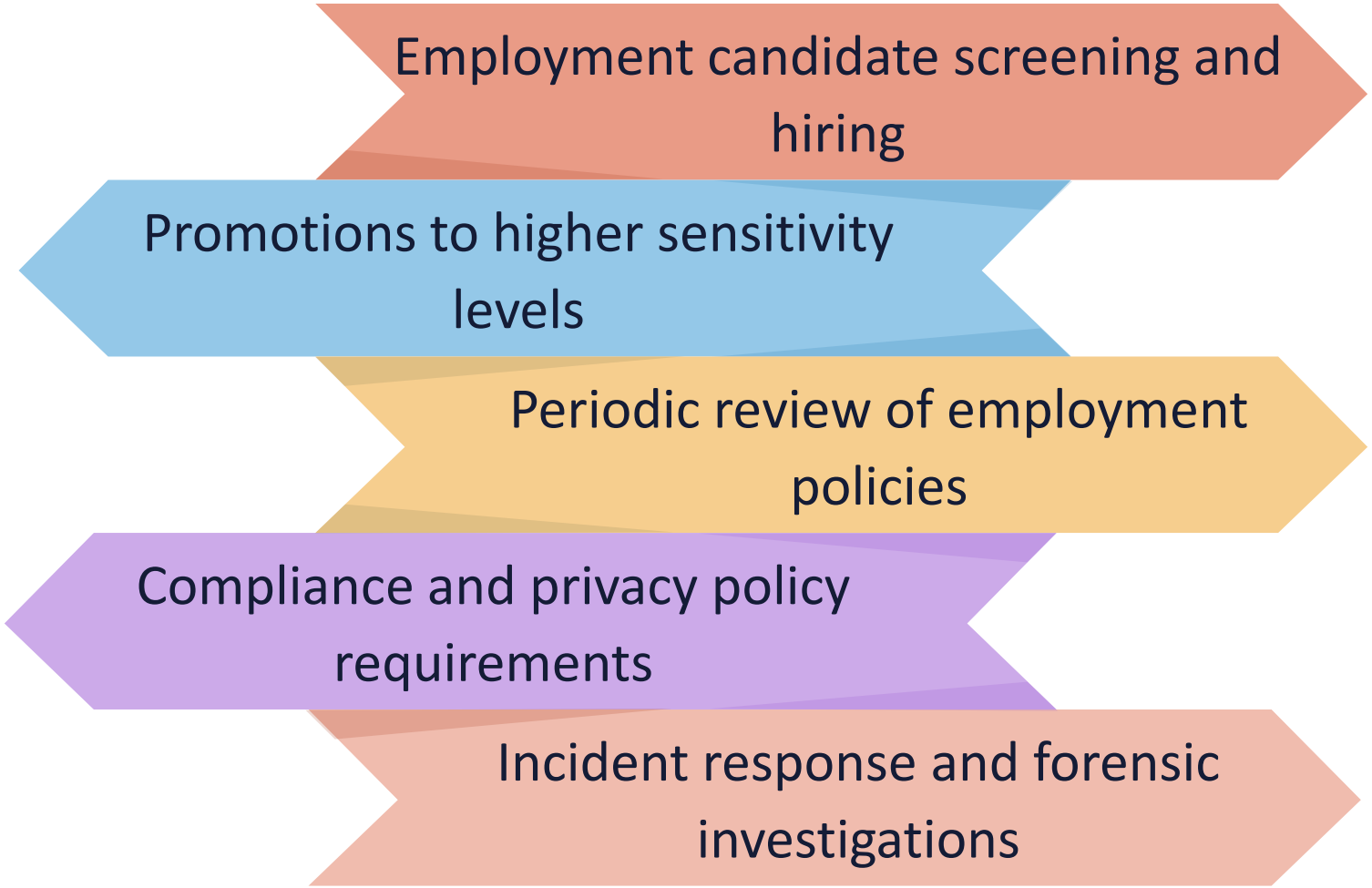
CANDIDATE SCREENING & HIRING

- Security policy steering committees must work closely with HR and legal departments to determine best practices for candidate screening and hiring (joiners and movers)
- At the start of an interview, it is not uncommon to sign a non-disclosure or confidentiality agreement
- Many organizations will have employees sign an additional employment contract that may include non-compete clauses or extended NDAs
- New employees should sign off on all security policies as well as the acceptable use policy

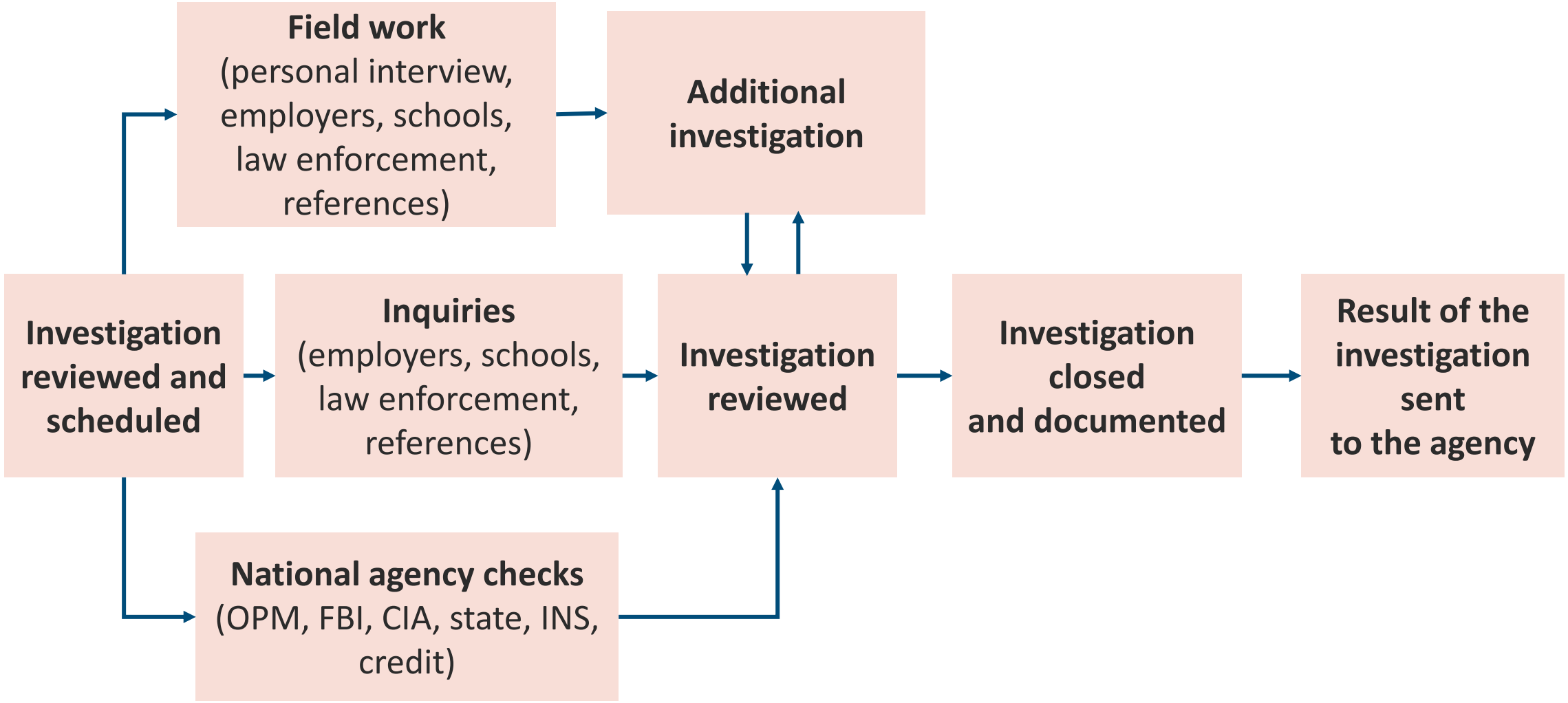
EMPLOYMENT CANDIDATE ACTIVITIES

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

CONDUCTING INVESTIGATIONS



NATIONAL BACKGROUND INVESTIGATIONS BUREAU (NBIB)



NON-DISCLOSURE AGREEMENTS (NDAS)

- Also called "confidentiality agreements"
- A legal contract between two or more parties representing a confidential relationship that is often strictly enforced
- Can be business-to-business and/or business-to-employee
  - Identifies confidential information they wish to share with each other
  - For example, IP, trade secrets, technologies, campaigns, ideas, new processes, new products, and services
- Also restricts the sharing of that information
- Commonly used during the interview process

SERVICE-LEVEL AGREEMENTS (SLAS)

- A settlement that defines the detailed responsibilities of the service provider or vendor in setting customer expectations
- It also explains the support system (i.e., service desk and or tech support) response to problems or outages for an agreed level of service
- Although it can be internal between business units or departments, it is usually external
- SLAs should be used with new third-party vendors or cloud providers (i.e., SaaS, IaaS, PaaS) for 24-hour support

ORGANIZATIONAL-LEVEL AGREEMENTS

- An OLA documents the relevant information for regulating the relationship between internal service recipients and an internal IT area (service provider)
- The difference between an SLA and an OLA is what the service provider is promising the customer (SLA) vs. what the functional IT groups promise each other (OLA)
- An OLA often corresponds to the structure of an SLA with a few specific differences based on the enterprise
- These were recently used for outlining usage of private and hybrid cloud resources as management uses chargebacks (or showbacks) against the budgets of departments, organizational units, and business units

MEMORANDUM OF UNDERSTANDING

- Memorandum of Understanding (MOU), also called a Memorandum of Agreement (MOA)
- It is a more official term for the historic "letter of intent"
- A formal MOU usually precedes the more formal and final contract-signing processes
- It defines common courses of action and high-level roles and responsibilities in the management of a cross-domain connection
- It will usually terminate the customer's provider search process so that subsequent time and resources can be dedicated to the next steps of the formal contract process

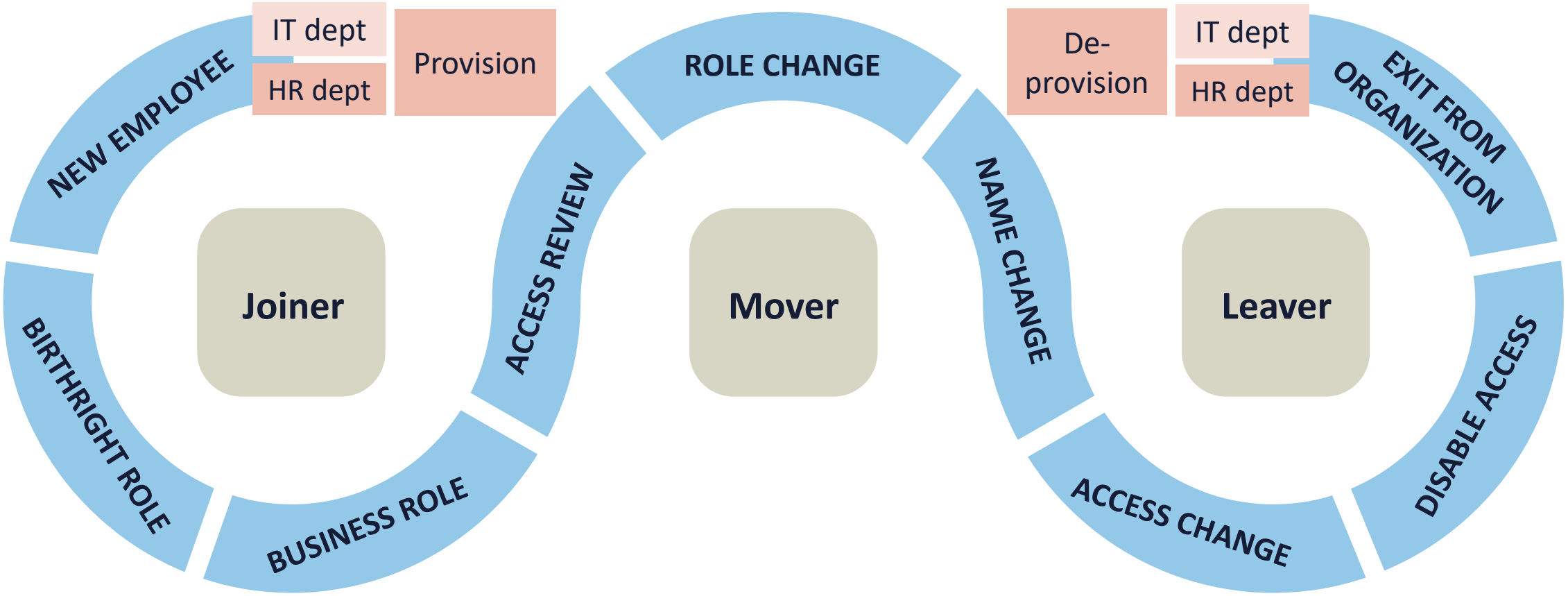
RECIPROCAL AGREEMENTS

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

INTEROPERABILITY AGREEMENT (IA)

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

IDENTITY MANAGEMENT EMPLOYEE LIFECYCLE



ONBOARDING

- A process also called "provisioning" where assets, guidance, knowledge, skills, and behavior are distributed to joiners and movers
  - Provisioning all devices and equipment
- Initial training and awareness will include videos, printed material, computer-based training (CBT), lectures, formal and informal meetings, and organizational mentors
- Involves team member introductions and explanation of standards and practices (standard operating procedures [SOPs])
  - Clearly define roles and responsibilities
- Elaborate on AUP expectations and additional human resources activities
- **Managers must remove any ambiguity and uncertainty**

AUTOMATING ONBOARDING

- Offboarding and de-provisioning is the reverse process and is typically LESS automated than onboarding
- Enterprises often deploy systems that involve self-service onboarding of personal devices (i.e., bring your own device [BYOD], choose your own device [CYOD], corporate owned personally enabled [COPE])
- An employee registers a new device, and the native supplicant is automatically provisioned for that user and device and installed using a supplicant profile that is preconfigured to connect the device to the corporate network
- Startup companies will often use a Software-as-a-Service provider or a cloud access security broker (CASB)

HANDLING ORGANIZATIONAL MOVERS

- A mover is an employee who is granted a promotion, changes departments or teams, or moves across the organization because of a restructuring strategy
- Inter-departmental collaboration between IT, HR, and operations empowers enterprises to reduce risk with movers
- Many organizations will utilize an automated proxy platform involving local or cloud-based auditing with databases, servers, clusters, and web apps
  - For example, attribute-based access controls with Okta or IdRamp

EMPLOYMENT TERMINATIONS

- Termination will be driven by a variety of circumstances
- Organizations must test and document all procedures for revoking outgoing employee access before termination
- Need to monitor and audit the employee closely in the last weeks, days, or even hours of service
- If possible, terminate face-to-face and with a witness from security or human resources

EMPLOYMENT TERMINATIONS

- It is imperative to meet all regulatory requirements such as the Worker Adjustment and Retraining Notification Act (WARN) and Sarbanes-Oxley Act (SOX)
- Establish a policy for:
  - Deleting/disabling accounts
  - Revoking certificates and digital signatures
  - Returning property (physical and IP)
- Mangers should modify/update corporate-controlled social media
- **Former employees must be added to the risk ledger of potential threat agents**
- Do follow-up interviews, if possible, to learn about vulnerabilities

EMPLOYEE RELEASE & EXIT INTERVIEWS

- **If possible, conduct exit and follow-up interviews to gather intel about potential unknown vulnerabilities and weaknesses**
- Possibly identify factors that led to an employee leaving voluntarily
  - How can the organization improve to keep employees, if applicable?
- Remind leavers of their agreements and responsibilities
  - Review NDAs and non-competes
- Conduct all activities with respect and dignity of the ex-employee