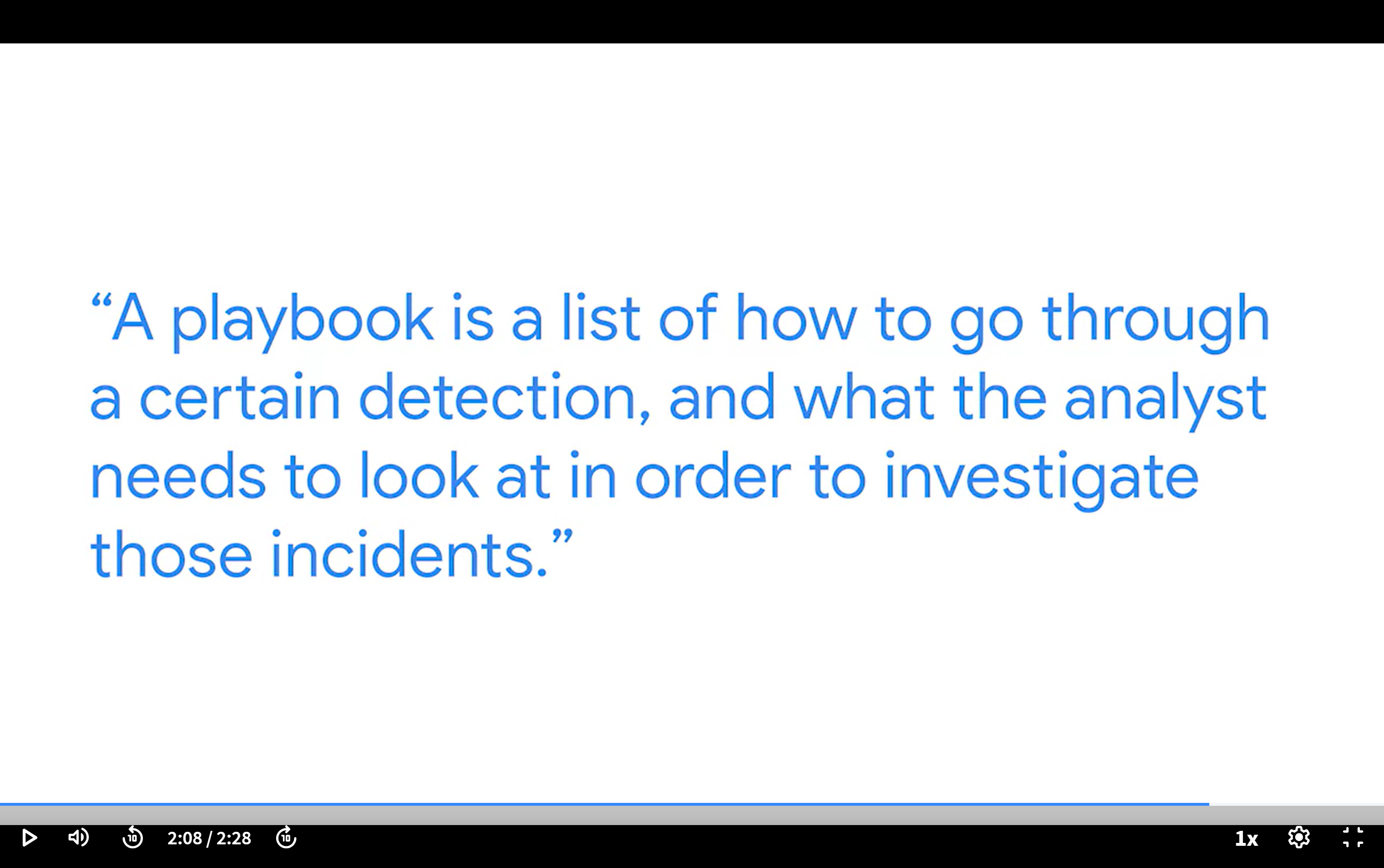
Benefits of cyber security



Roles I can apply



Playbook  


Technical skills

* **Programming languages:** By understanding how to use programming languages, cybersecurity analysts can automate tasks that would otherwise be very time consuming. Examples of tasks that programming can be used for include searching data to identify potential threats or organizing and analyzing information to identify patterns related to security issues.
* **Security information and event management (SIEM) tools:** SIEM tools collect and analyze log data, or records of events such as unusual login behavior, and support analysts’ ability to monitor critical activities in an organization. This helps cybersecurity professionals identify and analyze potential security threats, risks, and vulnerabilities more efficiently.
* **Intrusion detection systems (IDSs):** Cybersecurity analysts use IDSs to monitor system activity and alerts for possible intrusions. It’s important to become familiar with IDSs because they’re a key tool that every organization uses to protect assets and data. For example, you might use an IDS to monitor networks for signs of malicious activity, like unauthorized access to a network.
* **Threat landscape knowledge:** Being aware of current trends related to threat actors, malware, or threat methodologies is vital. This knowledge allows security teams to build stronger defenses against threat actor tactics and techniques. By staying up to date on attack trends and patterns, security professionals are better able to recognize when new types of threats emerge such as a new ransomware variant.
* **Incident response:** Cybersecurity analysts need to be able to follow established policies and procedures to respond to incidents appropriately. For example, a security analyst might receive an alert about a possible malware attack, then follow the organization’s outlined procedures to start the incident response process. This could involve conducting an investigation to identify the root issue and establishing ways to remediate it.

**Cybersecurity (or security):** The practice of ensuring confidentiality, integrity, and availability of information by protecting networks, devices, people, and data from unauthorized access or criminal exploitation

**Cloud security:** The process of ensuring that assets stored in the cloud are properly configured and access to those assets is limited to authorized users

**Internal threat:** A current or former employee, external vendor, or trusted partner who poses a security risk

**Network security:** The practice of keeping an organization's network infrastructure secure from unauthorized access

**Personally identifiable information (PII):** Any information used to infer an individual’s identity

**Security posture:** An organization’s ability to manage its defense of critical assets and data and react to change

**Sensitive personally identifiable information (SPII):** A specific type of PII that falls under stricter handling guidelines

**Technical skills:** Skills that require knowledge of specific tools, procedures, and policies

**Threat:** Any circumstance or event that can negatively impact assets

**Threat actor:** Any person or group who presents a security risk

**Transferable skills:** Skills from other areas that can apply to different careers

**Module 2**

computer security incident response teams (CSIRTs)

**Phishing**

**Phishing** is the use of digital communications to trick people into revealing sensitive data or deploying malicious software.

Some of the most common types of phishing attacks today include:

* **Business Email Compromise (BEC):** A threat actor sends an email message that seems to be from a known source to make a seemingly legitimate request for information, in order to obtain a financial advantage.
* **Spear phishing:** A malicious email attack that targets a specific user or group of users. The email seems to originate from a trusted source.
* **Whaling:** A form of spear phishing. Threat actors target company executives to gain access to sensitive data.
* **Vishing:** The exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source.
* **Smishing:** The use of text messages to trick users, in order to obtain sensitive information or to impersonate a known source.

**Malware**

**Malware** is software designed to harm devices or networks. There are many types of malware. The primary purpose of malware is to obtain money, or in some cases, an intelligence advantage that can be used against a person, an organization, or a territory.

Some of the most common types of malware attacks today include:

* **Viruses:** Malicious code written to interfere with computer operations and cause damage to data and software. A virus needs to be initiated by a user (i.e., a threat actor), who transmits the virus via a malicious attachment or file download. When someone opens the malicious attachment or download, the virus hides itself in other files in the now infected system. When the infected files are opened, it allows the virus to insert its own code to damage and/or destroy data in the system.
* **Worms:** Malware that can duplicate and spread itself across systems on its own. In contrast to a virus, a worm does not need to be downloaded by a user. Instead, it self-replicates and spreads from an already infected computer to other devices on the same network.
* **Ransomware:** A malicious attack where threat actors encrypt an organization's data and demand payment to restore access.
* **Spyware:** Malware that’s used to gather and sell information without consent. Spyware can be used to access devices. This allows threat actors to collect personal data, such as private emails, texts, voice and image recordings, and locations.

**Social Engineering**

**Social engineering** is a manipulation technique that exploits human error to gain private information, access, or valuables. Human error is usually a result of trusting someone without question. It’s the mission of a threat actor, acting as a social engineer, to create an environment of false trust and lies to exploit as many people as possible.

Some of the most common types of social engineering attacks today include:

* **Social media phishing:** A threat actor collects detailed information about their target from social media sites. Then, they initiate an attack.
* **Watering hole attack:** A threat actor attacks a website frequently visited by a specific group of users.
* **USB baiting:** A threat actor strategically leaves a malware USB stick for an employee to find and install, to unknowingly infect a network.
* **Physical social engineering:** A threat actor impersonates an employee, customer, or vendor to obtain unauthorized access to a physical location.

**Social engineering principles**

Social engineering is incredibly effective. This is because people are generally trusting and conditioned to respect authority. The number of social engineering attacks is increasing with every new social media application that allows public access to people's data. Although sharing personal data—such as your location or photos—can be convenient, it’s also a risk.

Reasons why social engineering attacks are effective include:

* **Authority:** Threat actors impersonate individuals with power. This is because people, in general, have been conditioned to respect and follow authority figures.
* **Intimidation:** Threat actors use bullying tactics. This includes persuading and intimidating victims into doing what they’re told.
* **Consensus/Social proof:** Because people sometimes do things that they believe many others are doing, threat actors use others’ trust to pretend they are legitimate. For example, a threat actor might try to gain access to private data by telling an employee that other people at the company have given them access to that data in the past.
* **Scarcity:** A tactic used to imply that goods or services are in limited supply.
* **Familiarity:** Threat actors establish a fake emotional connection with users that can be exploited.
* **Trust:** Threat actors establish an emotional relationship with users that can be exploited *over time*. They use this relationship to develop trust and gain personal information.
* **Urgency:** A threat actor persuades others to respond quickly and without questioning.

**Password attack**

A **password attack** is an attempt to access password-secured devices, systems, networks, or data. Some forms of password attacks that you’ll learn about later in the certificate program are:

* Brute force
* Rainbow table

Password attacks fall under the communication and network security domain.

**Social engineering attack**

**Social engineering** is a manipulation technique that exploits human error to gain private information, access, or valuables. Some forms of social engineering attacks that you will continue to learn about throughout the program are:

* Phishing
* Smishing
* Vishing
* Spear phishing
* Whaling
* Social media phishing
* Business Email Compromise (BEC)
* Watering hole attack
* USB (Universal Serial Bus) baiting
* Physical social engineering

Social engineering attacks are related to the security and risk management domain.

**Physical attack**

A **physical attack** is a security incident that affects not only digital but also physical environments where the incident is deployed. Some forms of physical attacks are:

* Malicious USB cable
* Malicious flash drive
* Card cloning and skimming

Physical attacks fall under the asset security domain.

**Adversarial artificial intelligence**

**Adversarial artificial intelligence** is a technique that manipulates [artificial intelligence and machine learning](https://www.nccoe.nist.gov/ai/adversarial-machine-learning) technology to conduct attacks more efficiently. Adversarial artificial intelligence falls under both the communication and network security and the identity and access management domains.

**Supply-chain attack**

A **supply-chain attack** targets systems, applications, hardware, and/or software to locate a vulnerability where malware can be deployed. Because every item sold undergoes a process that involves third parties, this means that the security breach can occur at any point in the supply chain. These attacks are costly because they can affect multiple organizations and the individuals who work for them. Supply-chain attacks can fall under several domains, including but not limited to the security and risk management, security architecture and engineering, and security operations domains.

**Cryptographic attack**

A **cryptographic attack** affects secure forms of communication between a sender and intended recipient. Some forms of cryptographic attacks are:

* Birthday
* Collision
* Downgrade

Cryptographic attacks fall under the communication and network security domain.

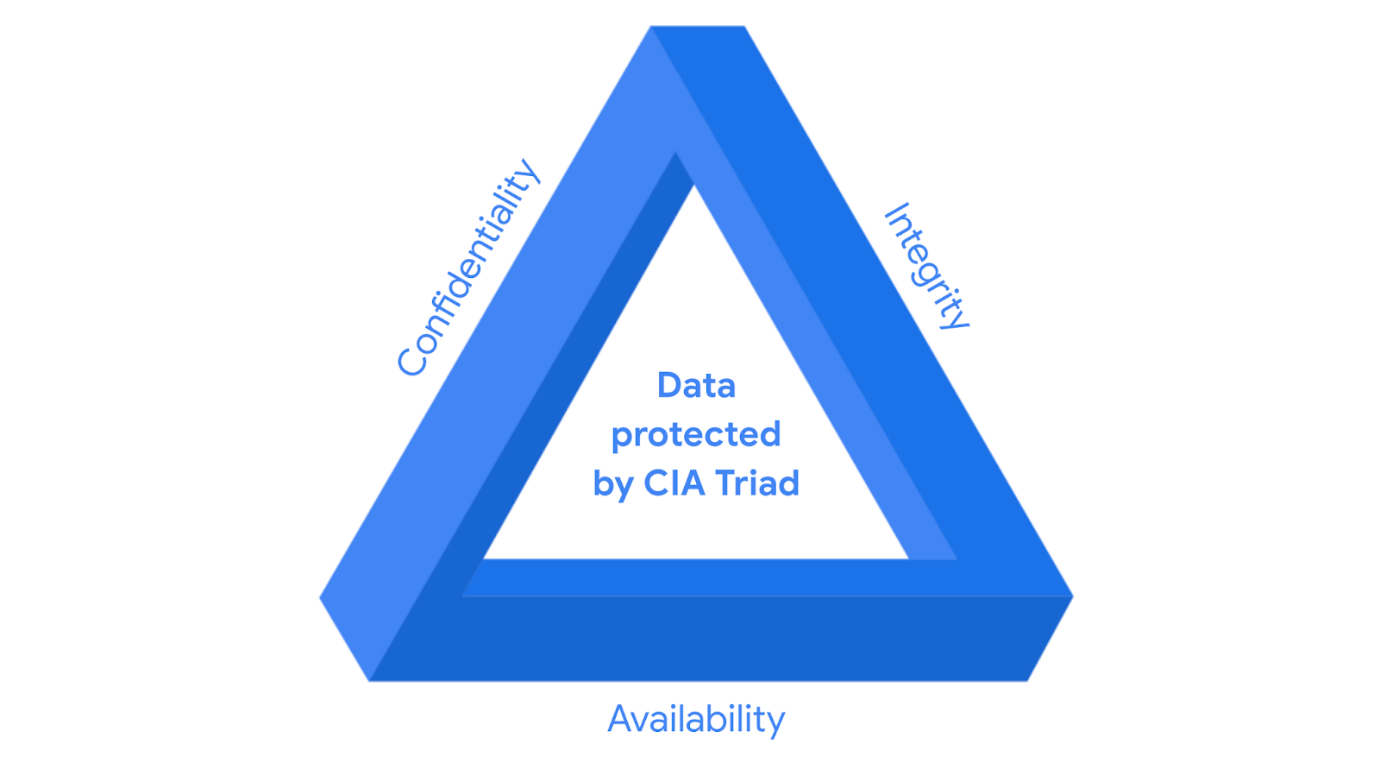
**Model 3**

**Controls, frameworks, and compliance**

Previously, you were introduced to security frameworks and how they provide a structured approach to implementing a security lifecycle. As a reminder, a security lifecycle is a constantly evolving set of policies and standards. In this reading, you will learn more about how security frameworks, controls, and compliance regulations—or laws—are used together to manage security and make sure everyone does their part to minimize risk.

**How controls, frameworks, and compliance are related**

The **confidentiality, integrity, and availability (CIA) triad** is a model that helps inform how organizations consider risk when setting up systems and security policies.



CIA are the three foundational principles used by cybersecurity professionals to establish appropriate controls that mitigate threats, risks, and vulnerabilities.

As you may recall, **security** **controls** are safeguards designed to reduce specific security risks. So they are used alongside frameworks to ensure that security goals and processes are implemented correctly and that organizations meet regulatory compliance requirements.

**Security frameworks** are guidelines used for building plans to help mitigate risks and threats to data and privacy. They have four core components:

1. Identifying and documenting security goals
2. Setting guidelines to achieve security goals
3. Implementing strong security processes
4. Monitoring and communicating results

**Compliance** is the process of adhering to internal standards and external regulations.

**Specific controls, frameworks, and compliance**

The National Institute of Standards and Technology (NIST) is a U.S.-based agency that develops multiple voluntary compliance frameworks that organizations worldwide can use to help manage risk. The more aligned an organization is with compliance, the lower the risk.

Examples of frameworks include the NIST Cybersecurity Framework (CSF) and the NIST Risk Management Framework (RMF).

**Note:** Specifications and guidelines can change depending on the type of organization you work for.

In addition to the [NIST CSF](https://www.nist.gov/cyberframework) and [NIST RMF](https://csrc.nist.gov/projects/risk-management/about-rmf), there are several other controls, frameworks, and compliance standards that are important for security professionals to be familiar with to help keep organizations and the people they serve safe.

**The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

FERC-NERC is a regulation that applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. These types of organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. They are also legally required to adhere to the Critical Infrastructure Protection (CIP) Reliability Standards defined by the FERC.

**The Federal Risk and Authorization Management Program (FedRAMP®)**

FedRAMP is a U.S. federal government program that standardizes security assessment, authorization, monitoring, and handling of cloud services and product offerings. Its purpose is to provide consistency across the government sector and third-party cloud providers.

**Center for Internet Security (CIS®)**

CIS is a nonprofit with multiple areas of emphasis. It provides a set of controls that can be used to safeguard systems and networks against attacks. Its purpose is to help organizations establish a better plan of defense. CIS also provides actionable controls that security professionals may follow if a security incident occurs.

**General Data Protection Regulation (GDPR)**

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. residents’ data and their right to privacy in and out of E.U. territory. For example, if an organization is not being transparent about the data they are holding about an E.U. citizen and why they are holding that data, this is an infringement that can result in a fine to the organization. Additionally, if a breach occurs and an E.U. citizen’s data is compromised, they must be informed. The affected organization has 72 hours to notify the E.U. citizen about the breach.

**Payment Card Industry Data Security Standard (PCI DSS)**

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment. The objective of this compliance standard is to reduce credit card fraud.

**The Health Insurance Portability and Accountability Act (HIPAA)**

HIPAA is a U.S. federal law established in 1996 to protect patients' health information. This law prohibits patient information from being shared without their consent. It is governed by three rules:

1. Privacy
2. Security
3. Breach notification

Organizations that store patient data have a legal obligation to inform patients of a breach because if patients' **Protected Health Information** (PHI) is exposed, it can lead to identity theft and insurance fraud. PHI relates to the past, present, or future physical or mental health or condition of an individual, whether it’s a plan of care or payments for care. Along with understanding HIPAA as a law, security professionals also need to be familiar with the Health Information Trust Alliance (HITRUST®), which is a security framework and assurance program that helps institutions meet HIPAA compliance.

**International Organization for Standardization (ISO)**

ISO was created to establish international standards related to technology, manufacturing, and management across borders. It helps organizations improve their processes and procedures for staff retention, planning, waste, and services.

**System and Organizations Controls (SOC type 1, SOC type 2)**

The American Institute of Certified Public Accountants® (AICPA) auditing standards board developed this standard. The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels such as:

* Associate
* Supervisor
* Manager
* Executive
* Vendor
* Others

They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

**Pro tip**: There are a number of regulations that are frequently revised. You are encouraged to keep up-to-date with changes and explore more frameworks, controls, and compliance. Two suggestions to research: the Gramm-Leach-Bliley Act and the Sarbanes-Oxley Act.

**United States Presidential Executive Order 14028**

On May 12, 2021, President Joe Biden released an executive order related to improving the nation’s cybersecurity to remediate the increase in threat actor activity. Remediation efforts are directed toward federal agencies and third parties with ties to U.S. [critical infrastructure](https://csrc.nist.gov/glossary/term/critical_infrastructure#:~:text=Definition(s)%3A,any%20combination%20of%20those%20matters.). For additional information, review the [Executive Order on Improving the Nation’s Cybersecurity](https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/).