# Frameworks and controles

- Secure design
- Introduction to security frameworks and controls
- Controls, frameworks, and compliance
- Heather: Protect sensitive data and information

# Secure design

Hi, welcome back! Previously, we discussed frameworks and controls in general. In this video, you'll learn about specific frameworks and controls that organizations can voluntarily use to minimize risks to their data and to protect users. Let's get started!

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

Confidentiality means that only authorized users can access specific assets or data. For example, strict access controls that define who should and should not have access to data, must be put in place to ensure confidential data remains safe.

Integrity means the data is correct, authentic, and reliable. To maintain integrity, security professionals can use a form of data protection like encryption to safeguard data from being tampered with.

Availability means data is accessible to those who are authorized to access it. As an example, a director may have more access to certain data than a department manager because directors usually oversee more employees.

Let's define a term that came up during our discussion of the CIA triad: asset. An asset is an item perceived as having value to an organization. And value is determined by the cost associated with the asset in question. For example, an application that stores sensitive data, such as social security numbers or bank accounts, is a valuable asset to an organization. It carries more risk and therefore requires tighter security controls in comparison to a website that shares publicly available news content.

As you may remember, earlier in the course, we discussed frameworks and controls in general. Now, we'll discuss a specific framework developed by the U.S.-based National Institute of Standards and Technology: the Cybersecurity Framework, also referred to as the NIST CSF. The NIST Cybersecurity Framework is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. It's important to become familiar with this framework because security teams use it as a baseline to manage short and long-term risk.

Managing and mitigating risks and protecting an organization's assets from threat actors are key goals for security professionals. Understanding the different motives a threat actor may have, alongside identifying your organization's most valuable assets is important.
Some of the most dangerous threat actors to consider are disgruntled employees. They are the most dangerous because they often have access to sensitive information and know where to find it. In order to reduce this type of risk, security professionals would use the principle of availability, as

well as organizational guidelines based on frameworks to ensure staff members can only access the data they need to perform their jobs.

Threat actors originate from all across the globe, and a diverse workforce of security professionals helps organizations identify attackers' intentions. A variety of perspectives can assist organizations in understanding and mitigating the impact of malicious activity.

That concludes our introduction to the CIA triad and NIST CSF framework, which are used to develop processes to secure organizations and the people they serve.

You may be asked in an interview if you know about security frameworks and principles. Or you may be asked to explain how they're used to secure organizational assets. In either case, throughout this program, you'll have multiple opportunities to learn more about them and apply what we've discussed to real-world situations.

Coming up, we'll discuss the ethics of security. See you soon!

# Introduction to security frameworks and controls

Imagine you're working as a security analyst and receive multiple alerts about suspicious activity on the network. You realize that you'll need to implement additional security measures to keep these alerts from becoming serious incidents. But where do you start?

As an analyst, you'll start by identifying your organization's critical assets and risks. Then you'll implement the necessary frameworks and controls.

In this video, we'll discuss how security professionals use frameworks to continuously identify and manage risk. We'll also cover how to use security controls to manage or reduce specific risks.

Security frameworks are guidelines used for building plans to help mitigate risks and threats to data and privacy. Security frameworks provide a structured approach to implementing a security lifecycle. The security lifecycle is a constantly evolving set of policies and standards that define how an organization manages risks, follows established guidelines, and meets regulatory compliance, or laws.

There are several security frameworks that may be used to manage different types of organizational and regulatory compliance risks. The purpose of security frameworks include protecting personally identifiable information, known as PII, securing financial information, identifying security weaknesses, managing organizational risks, and aligning security with business goals.

Frameworks have four core components and understanding them will allow you to better manage potential risks. The first core component is identifying and documenting security goals. For example, an organization may have a goal to align with the E.U.'s General Data Protection Regulation, also known as GDPR. GDPR is a data protection law established to grant European citizens more control over their personal data. A security analyst may be asked to identify and document areas where an organization is out of compliance with GDPR.

The second core component is setting guidelines to achieve security goals. For example, when implementing guidelines to achieve GDPR compliance, your organization may need to develop new policies for how to handle data requests from individual users.

The third core component of security frameworks is implementing strong security processes. In the case of GDPR, a security analyst working for a social media company may help design procedures to ensure the organization complies with verified user data requests. An example of this type of request is when a user attempts to update or delete their profile information.

The last core component of security frameworks is monitoring and communicating results. As an example, you may monitor your organization's internal network and report a potential security issue affecting GDPR to your manager or regulatory compliance officer.

Now that we've introduced the four core components of security frameworks, let's tie them all together. Frameworks allow analysts to work alongside other members of the security team to document, implement, and use the policies and procedures that have been created. It's essential for an entry-level analyst to understand this process because it directly affects the work they do and how they collaborate with others. Next, we'll discuss security controls.

Security controls are safeguards designed to reduce specific security risks. For example, your company may have a guideline that requires all employees to complete a privacy training to reduce the risk of data breaches. As a security analyst, you may use a software tool to automatically assign and track which employees have completed this training.

Security frameworks and controls are vital to managing security for all types of organizations and ensuring that everyone is doing their part to maintain a low level of risk.

Understanding their purpose and how they are used allows analysts to support an organization's security goals and protect the people it serves.

In the following videos, we'll discuss some well-known frameworks and principles that analysts need to be aware of to minimize risk and protect data and users.

# 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.

Integrity of your organization

A triangle representing the CIA (confidentiality, integrity, availability) triad

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 that were introduced previously 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 and NIST RMF, there are several other controls, frameworks, and compliance standards that it is 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. For additional information, review the Executive Order on Improving the Nation's Cybersecurity.

## Key takeaways

In this reading you learned more about controls, frameworks, and compliance. You also learned how they work together to help organizations maintain a low level of risk.

As a security analyst, it’s important to stay up-to-date on common frameworks, controls, and compliance regulations and be aware of changes to the cybersecurity landscape to help ensure the safety of both organizations and people.

# Heather: Protect sensitive data and information

Hello, my name is Heather and I'm the Vice President of Security Engineering at Google. PII has been an important topic on the internet since the beginning of the internet. And we have been talking about increasingly sophisticated ways to protect that data over time. When we think about collecting PII on behalf of another person, we should make sure we're very deliberate about how it's handled and where it's stored, and that we understand where it's stored all the time. Depending on what kind of role you're in, you might also need to protect that data to comply with regulation or law. And so, it's important to understand how the data relates to some of those obligations. If an organization fails to meet their obligations, a number of things might happen. First, you might see a government regulator become more interested in understanding the practices around how a company is handling data. Secondly, consumers, customers, businesses may actually begin to directly inquire of the company how they're handling data. And this may become part of the customer relationship and increasingly important if that data is very sensitive. And third, the last consequence is legal action. And it's not uncommon for us to see victims of cybersecurity incidents now suing companies for mishandling their data. You can keep up to date with compliance, regulation and laws around PII by consulting the relevant website in the jurisdiction that you have a question for. Many government websites now post the laws, regulations, and compliance requirements for data that's being handled. The regulations and laws that govern how PII can be handled are very complex, all over the world, countries, states, counties are regulating it at different levels. It's important to understand and to be aware that these laws exist. However, if you need to ask a question about a specific law, it's important to seek advice from legal counsel for that particular jurisdiction. It may be very different than the jurisdiction that you're in.