# NIST frameworks and OWASP principles and security audits

# NIST frameworks

Welcome back. Before we get started, let's quickly review the purpose of frameworks. Organizations use frameworks as a starting point to develop plans that mitigate risks, threats, and vulnerabilities to sensitive data and assets. Fortunately, there are organizations worldwide that create frameworks security professionals can use to develop those plans.

In this video, we'll discuss two of the National Institute of Standards and Technology, or NIST's frameworks that can support ongoing security efforts for all types of organizations, including for profit and nonprofit businesses, as well as government agencies. While NIST is a US based organization, the guidance it provides can help analysts all over the world understand how to implement essential cybersecurity practices. One NIST framework that we'll discuss throughout the program is the NIST Cybersecurity Framework, or CSF.

The CSF is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity risk. This framework is widely respected and essential for maintaining security regardless of the organization you work for. The CSF consists of five important core functions, identify, protect, detect, respond, and recover, which we'll discuss in detail in a future video. For now, we'll focus on how the CSF benefits organizations and how it can be used to protect against threats, risks, and vulnerabilities by providing a workplace example.

Imagine that one morning you receive a high-risk notification that a workstation has been compromised. You identify the workstation, and discover that there's an unknown device plugged into it. You block the unknown device remotely to stop any potential threat and protect the organization. Then you remove the infected workstation to prevent the spread of the damage and use tools to detect any additional threat actor behavior and identify the unknown device. You respond by investigating the incident to determine who used the unknown device, how the threat occurred, what was affected, and where the attack originated.

In this case, you discover that an employee was charging their infected phone using a USB port on their work laptop. Finally, you do your best to recover any files or data that were affected and correct any damage the threat caused to the workstation itself.

As demonstrated by the previous example, the core functions of the NIST CSF provide specific guidance and direction for security professionals. This framework is used to develop plans to handle an incident appropriately and quickly to lower risk, protect an organization against a threat, and mitigate any potential vulnerabilities. The NIST CSF also expands into the protection of the United States federal government with NIST special publication, or SP 800-53. It provides a unified framework for protecting the security of information systems within the federal government, including the systems provided by private companies for federal government use.

The security controls provided by this framework are used to maintain the CIA triad for those systems used by the government. Isn't it amazing how all of these frameworks and controls work together. We've discussed some really important security topics in this video that will be very useful for you as you continue your security journey. Because they're core elements of the security profession, the NIST CSF is a useful framework that most security professionals are familiar with, and having an understanding of the NIST, SP 800-53 is crucial if you have an interest in working for the US federal government. Coming up, we'll continue to explore the five NIST CSF functions and how organizations use them to protect assets and data.

# OWASP security principles

It's important to understand how to protect an organization's data and assets because that will be part of your role as a security analyst. Fortunately, there are principles and guidelines that can be used, along with NIST frameworks and the CIA triad, to help security teams minimize threats and risks.

In this video, we'll explore some Open Web Application Security Project, or OWASP, security principles that are useful to know as an entry-level analyst.

The first OWASP principle is to minimize the attack surface area. An attack surface refers to all the potential vulnerabilities that a threat actor could exploit, like attack vectors, which are pathways attackers use to penetrate security defenses. Examples of common attack vectors are phishing emails and weak passwords. To minimize the attack surface and avoid incidents from these types of vectors, security teams might disable software features, restrict who can access certain assets, or establish more complex password requirements.

The principle of least privilege means making sure that users have the least amount of access required to perform their everyday tasks. The main reason for limiting access to organizational information and resources is to reduce the amount of damage a security breach could cause. For example, as an entry-level analyst, you may have access to log data, but may not have access to change user permissions. Therefore, if a threat actor compromises your credentials, they'll only be able to gain limited access to digital or physical assets, which may not be enough for them to deploy their intended attack.

The next principle we'll discuss is defense in depth. Defense in depth means that an organization should have multiple security controls that address risks and threats in different ways. One example of a security control is multi-factor authentication, or MFA, which requires users to take an additional step beyond simply entering their username and password to gain access to an application. Other controls include firewalls, intrusion detection systems, and permission settings that can be used to create multiple points of defense, a threat actor must get through to breach an organization.

Another principle is separation of duties, which can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system. For example, the person in a company who signs the paychecks shouldn't also be the person who prepares them.

Only two more principles to go! You're doing great. Keep security simple is the next principle. As the name suggests, when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable. The more complex the security controls are, the harder it is for people to work collaboratively.

The last principle is to fix security issues correctly. Technology is a great tool, but can also present challenges. When a security incident occurs, security professionals are expected to identify the root cause quickly. From there, it's important to correct any identified vulnerabilities and conduct tests to ensure that repairs are successful.

An example of an issue is a weak password to access an organization's wifi because it could lead to a breach. To fix this type of security issue, stricter password policies could be put in place.

I know we've covered a lot, but understanding these principles increases your overall security knowledge and can help you stand out as a security professional.

# More about OWASP security principles

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

## Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event (SIEM) dashboard, or using a vulnerability scanner, you will use these principles in some way.

Previously, you were introduced to several OWASP security principles. These included:

Minimize attack surface area: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.

Principle of least privilege: Users have the least amount of access required to perform their everyday tasks.

Defense in depth: Organizations should have varying security controls that mitigate risks and threats.

Separation of duties: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.

Keep security simple: Avoid unnecessarily complicated solutions. Complexity makes security difficult.

Fix security issues correctly: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

## Additional OWASP security principles

Next, you’ll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

### Establish secure defaults

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

### Fail securely

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

### Don’t trust services

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn’t explicitly trust that their partners’ systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

### Avoid security by obscurity

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):

The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

### Key takeaways

Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.

# Wajih: Stay up-to-date on the latest cybersecurity threats

My name is Wajih and I'm a security engineer at Google working in the digital forensics department. Do you need a background in cybersecurity? No you don't. My past experiences is working at a water park as a snow cone machine guy. I worked at a movie theater selling popcorn in concession stands. During my undergrad, I was a bio major at first like my freshman year. I met someone in a bus who was mentioning about this cool cybersecurity startup that just sounded really cool. Some strategies I leveraged to keep up to date on the latest cybersecurity trends is going on online forums such as Medium to research different security trends and topics. I personally use Medium a lot as I could filter by the tag of like I want to find articles related to cybersecurity and or I want to find articles related to cloud security. Based off their filtering algorithm, I just go on and see like what other people are talking about and then that's what helps me keep up to date. If it's more of like networking that you're looking forward to, then I highly recommend just going out to those like conferences. My advice for people wanting to get into cybersecurity is don't be too overwhelmed with trying to understand every single specialization within cybersecurity. There's so much going on within the cybersecurity field in terms of trends and it's nice to stay up to date with all of those but sometimes you need to take a step back and prioritize what subjects within cybersecurity you are staying most up to date like on. I love this job. I love the challenges. I feel like there is a shortage in cybersecurity professionals out there from just past experiences, hearing from other friends in computer science fields. Most of them say that oh it's too hard, too complicated to get in. Don't listen to those people. I encourage you to push through. It's definitely well worth it. First just get the fundamentals down and be persistent.

# More about security audits

Previously, you were introduced to how to plan and complete an internal security audit. In this reading, you will learn more about security audits, including the goals and objectives of audits.

## Security audits

A **security audit** is a review of an organization's security controls, policies, and procedures against a set of expectations. Audits are independent reviews that evaluate whether an organization is meeting internal and external criteria. Internal criteria include outlined policies, procedures, and best practices. External criteria include regulatory compliance, laws, and federal regulations.

Additionally, a security audit can be used to assess an organization's established security controls. As a reminder, **security controls** are safeguards designed to reduce specific security risks.

Audits help ensure that security checks are made (i.e., daily monitoring of security information and event management dashboards), to identify threats, risks, and vulnerabilities. This helps maintain an organization’s security posture. And, if there are security issues, a remediation process must be in place.

## Goals and objectives of an audit

The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. The objective is to identify and address areas of remediation and growth. Audits provide direction and clarity by identifying what the current failures are and developing a plan to correct them.

Security audits must be performed to safeguard data and avoid penalties and fines from governmental agencies. The frequency of audits is dependent on local laws and federal compliance regulations.

## Factors that affect audits

Factors that determine the types of audits an organization implements include:

- Industry type

- Organization size
- Ties to the applicable government regulations
- A business’s geographical location
- A business decision to adhere to a specific regulatory compliance

To review common compliance regulations that different organizations need to adhere to, refer to the reading about controls, frameworks, and compliance.

## The role of frameworks and controls in audits

Along with compliance, it’s important to mention the role of frameworks and controls in security audits. Frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and the international standard for information security (ISO 27000) series are designed to help organizations prepare for regulatory compliance security audits. By adhering to these and other relevant frameworks, organizations can save time when conducting external and internal audits. Additionally, frameworks, when used alongside controls, can support organizations’ ability to align with regulatory compliance requirements and standards.

There are three main categories of controls to review during an audit, which are administrative and/or managerial, technical, and physical controls. To learn more about specific controls related to each category, click the following link and select “Use Template.”

Link to template: Control categories

OR

If you don’t have a Google account, you can download the template directly from the following attachment

**Control categories**

DOCX File

## Audit checklist

It’s necessary to create an audit checklist before conducting an audit. A checklist is generally made up of the following areas of focus:

**Identify the scope of the audit**

- The audit should:
  - List assets that will be assessed (e.g., firewalls are configured correctly, PII is secure, physical assets are locked, etc.)
  - Note how the audit will help the organization achieve its desired goals
  - Indicate how often an audit should be performed

    - Include an evaluation of organizational policies, protocols, and procedures to make sure they are working as intended and being implemented by employees

**Complete a risk assessment**

- A risk assessment is used to evaluate identified organizational risks related to budget, controls, internal processes, and external standards (i.e., regulations).

**Conduct the audit**

- When conducting an internal audit, you will assess the security of the identified assets listed in the audit scope.

**Create a mitigation plan**

- A mitigation plan is a strategy established to lower the level of risk and potential costs, penalties, or other issues that can negatively affect the organization’s security posture.

**Communicate results to stakeholders**

- The end result of this process is providing a detailed report of findings, suggested improvements needed to lower the organization's level of risk, and compliance regulations and standards the organization needs to adhere to.

## Key takeaways

In this reading you learned more about security audits, including what they are; why they’re conducted; and the role of frameworks, controls, and compliance in audits.

Although there is much more to learn about security audits, this introduction is meant to support your ability to complete an audit of your own for a self-reflection portfolio activity later in this course.

## Resources for more information

Resources that you can explore to further develop your understanding of audits in the cybersecurity space are:

- IT Security Procedural Guide: Audit and Accountability (AU) CIO-IT Security-01-08
- Assessment and Auditing Resources
- IT Disaster Recovery Plan