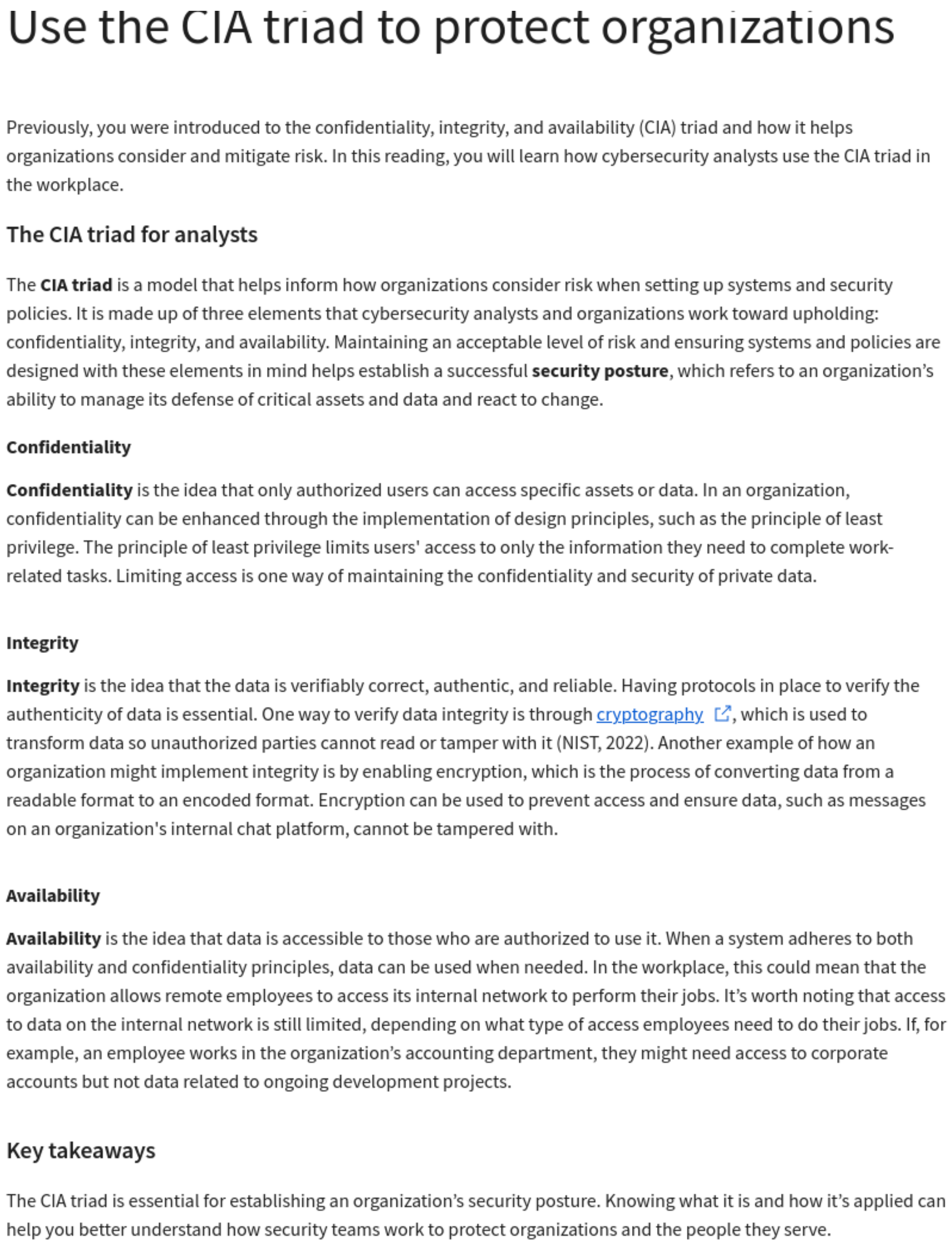
class week 2



Use the CIA triad to protect organizations

Previously, you were introduced to the confidentiality, integrity, and availability (CIA) triad and how it helps organizations consider and mitigate risk. In this reading, you will learn how cybersecurity analysts use the CIA triad in the workplace.

The CIA triad for analysts

The **CIA triad** is a model that helps inform how organizations consider risk when setting up systems and security policies. It is made up of three elements that cybersecurity analysts and organizations work toward upholding: confidentiality, integrity, and availability. Maintaining an acceptable level of risk and ensuring systems and policies are designed with these elements in mind helps establish a successful **security posture**, which refers to an organization’s ability to manage its defense of critical assets and data and react to change.

Confidentiality

Confidentiality is the idea that only authorized users can access specific assets or data. In an organization, confidentiality can be enhanced through the implementation of design principles, such as the principle of least privilege. The principle of least privilege limits users' access to only the information they need to complete work-related tasks. Limiting access is one way of maintaining the confidentiality and security of private data.

Integrity

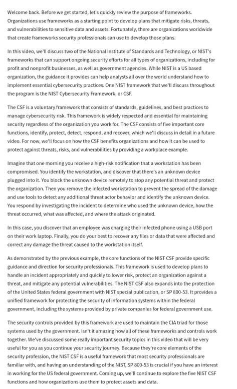
Integrity is the idea that the data is verifiably correct, authentic, and reliable. Having protocols in place to verify the authenticity of data is essential. One way to verify data integrity is through cryptography ↗, which is used to transform data so unauthorized parties cannot read or tamper with it (NIST, 2022). Another example of how an organization might implement integrity is by enabling encryption, which is the process of converting data from a readable format to an encoded format. Encryption can be used to prevent access and ensure data, such as messages on an organization's internal chat platform, cannot be tampered with.

Availability

Availability is the idea that data is accessible to those who are authorized to use it. When a system adheres to both availability and confidentiality principles, data can be used when needed. In the workplace, this could mean that the organization allows remote employees to access its internal network to perform their jobs. It’s worth noting that access to data on the internal network is still limited, depending on what type of access employees need to do their jobs. If, for example, an employee works in the organization’s accounting department, they might need access to corporate accounts but not data related to ongoing development projects.

Key takeaways

The CIA triad is essential for establishing an organization’s security posture. Knowing what it is and how it’s applied can help you better understand how security teams work to protect organizations and the people they serve.



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.

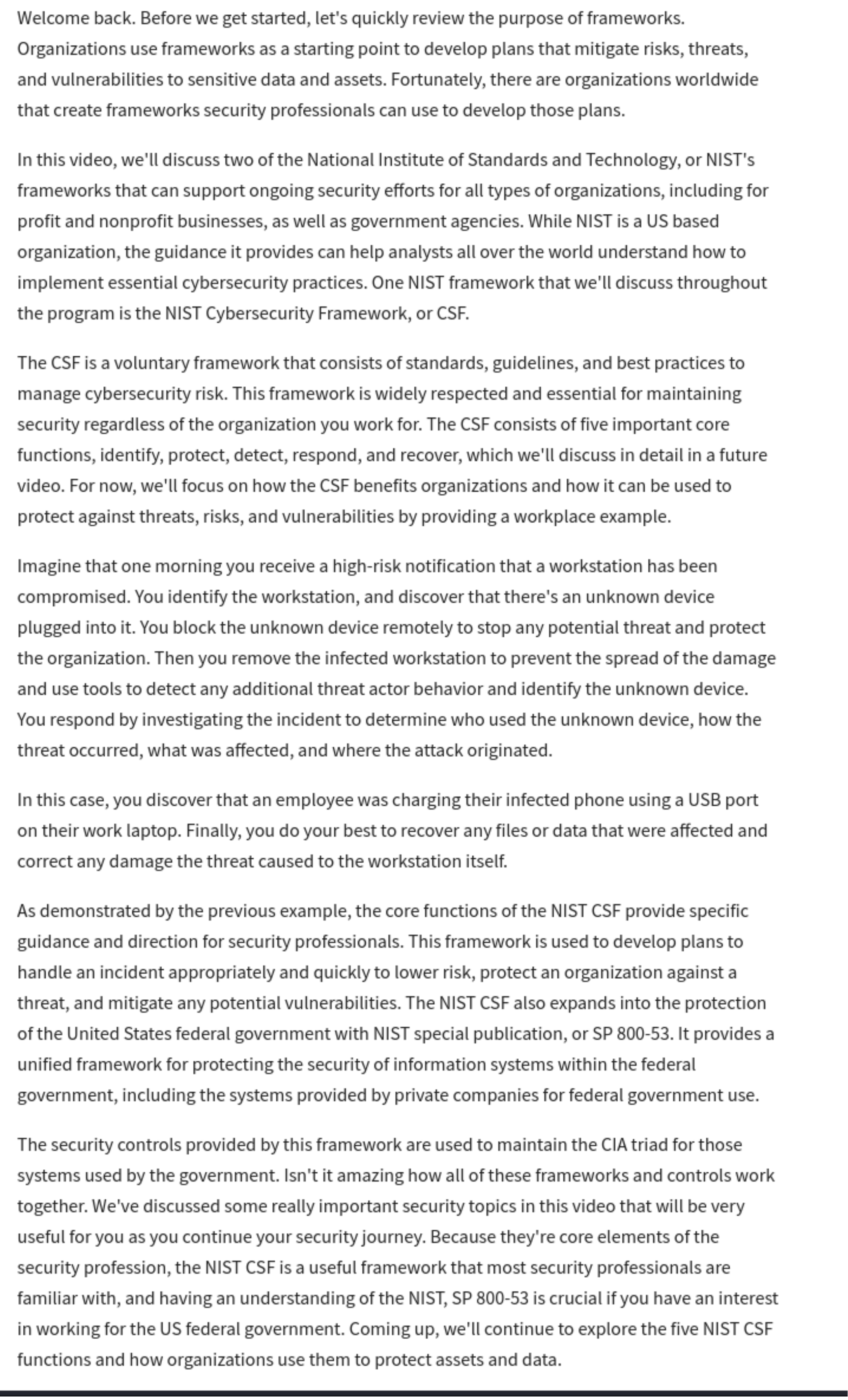
Imagine that one morning you receive a high-risk notification that a workstation has been compromised. You identify the workstation, and discover that there's an unknown device plugged into it. You block the unknown device remotely to stop any potential threat and protect the organization. Then you remove 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.

NIST FRAMEWORK.



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.

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.

NIST CSF focuses on five core functions: identify, protect, detect, respond, and recover. These core functions help organizations manage cybersecurity risks, implement risk management strategies, and learn from previous mistakes. Basically, when it comes to security operations, NIST CSF functions are key for making sure an organization is protected against potential threats, risks, and vulnerabilities. So let's take a little time to explore how each function can be used to improve an organization's security.

The first core function is identify, which is related to the management of cybersecurity risk and its effect on an organization's people and assets. For example, as a security analyst, you may be asked to monitor systems and devices in your organization's internal network to identify potential security issues

The second core function is protect, which is the strategy used to protect an organization through the implementation of policies, procedures, training, and tools that help mitigate cybersecurity threats.

For example, as a security analyst, you and your team might encounter new and unfamiliar threats and attacks. For this reason, studying historical data and making improvements to policies and procedures is essential.

The third core function is detect, which means identifying potential security incidents and improving monitoring capabilities to increase the speed and efficiency of detections. For example, as an analyst, you might be asked to review a new security tool's setup to make sure it's flagging low, medium, or high risk, and then alerting the security team about any potential threats or incidents. The fourth function is respond, which means making sure that the proper procedures are used to contain, neutralize, and analyze security incidents, and implement improvements to the security process.

As an analyst, you could be working with a team to collect and organize data to document an incident and suggest improvements to processes to prevent the incident from happening again.

The fifth core function is recover, which is the process of returning affected systems back to normal operation.

For example, as an entry-level security analyst, you might work with your security team to restore systems, data, and assets, such as financial or legal files, that have been affected by an incident like a breach.

We've covered a lot of information in this video. Hopefully, it helped you understand the value of learning about the NIST CSF and its five core functions.

From proactive to reactive measures, all five functions are essential for making sure that an organization has effective security strategies in place.

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.

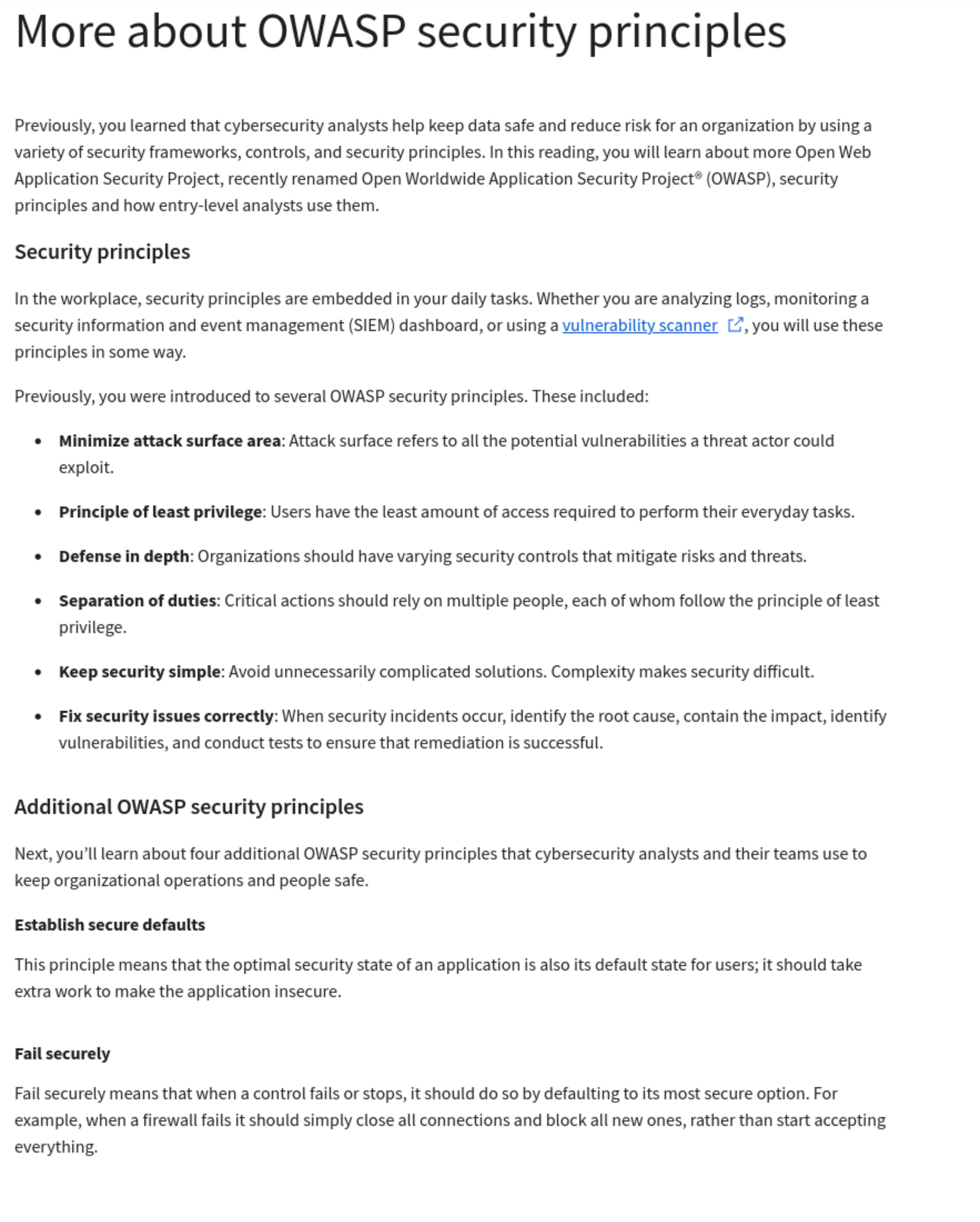
Another principle is separation of duties, which can be used to prevent individuals from carrying out fraudulent or illegal activities. This principle means that no one should be given so many privileges that they can misuse the system. For example, the person in a company who signs the paychecks shouldn't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

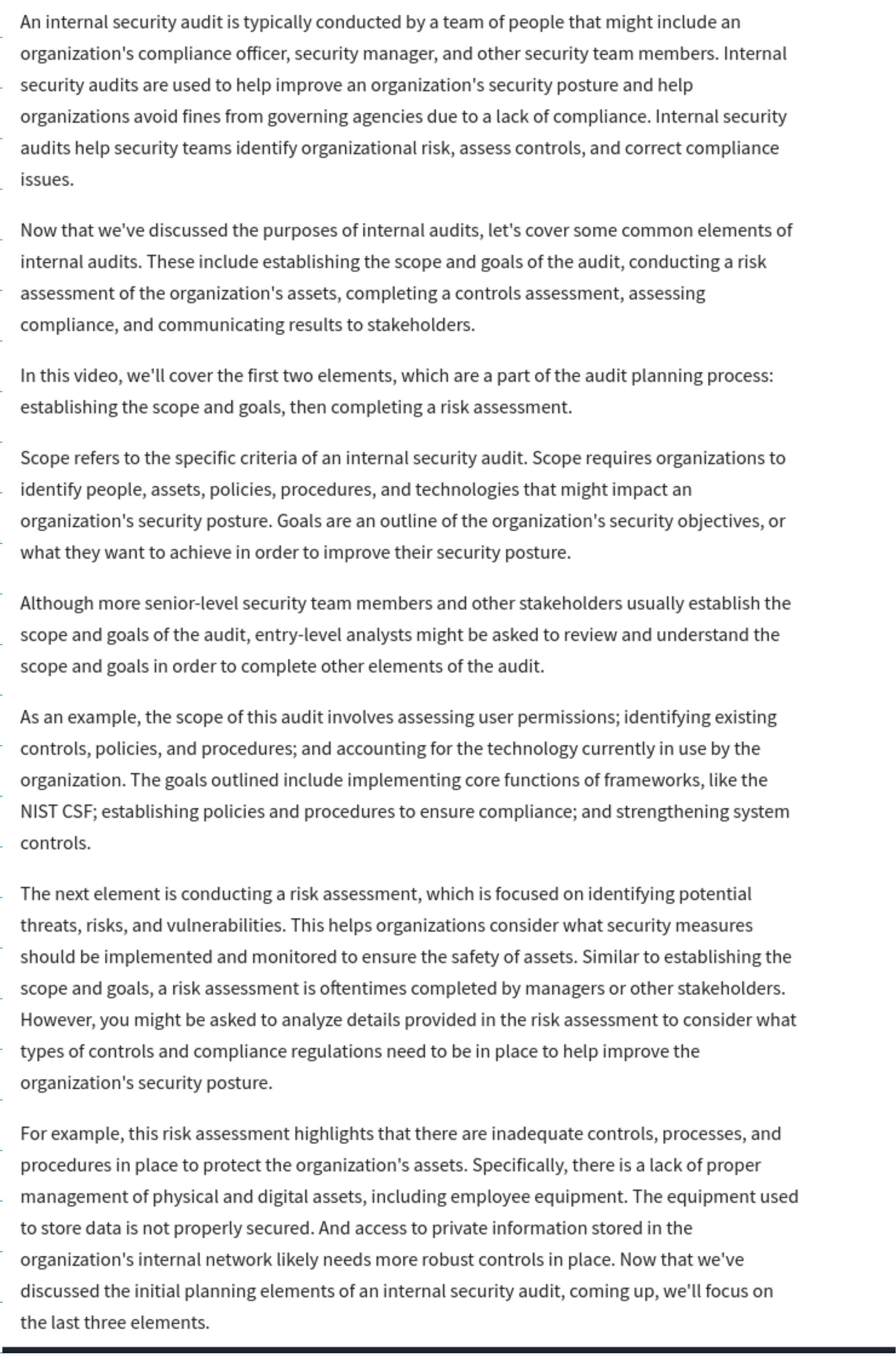
The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):

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.

Audits



An internal security audit is typically conducted by a team of people that might include an organization's compliance officer, security manager, and other security team members. Internal security audits are used to help improve an organization's security posture and help organizations avoid fines from governing agencies due to a lack of compliance. Internal security audits help security teams identify organizational risk, assess controls, and correct compliance issues.

Now that we've discussed the purposes of internal audits, let's cover some common elements of internal audits. These include establishing the scope and goals of the audit, conducting a risk assessment of the organization's assets, completing a controls assessment, assessing compliance, and communicating results to stakeholders.

In this video, we'll cover the first two elements, which are a part of the audit planning process: establishing the scope and goals, then completing a risk assessment.

Scope refers to the specific criteria of an internal security audit. Scope requires organizations to identify people, assets, policies, procedures, and technologies that might impact an organization's security posture. Goals are an outline of the organization's security objectives, or what they want to achieve in order to improve their security posture.

Although more senior-level security team members and other stakeholders usually establish the scope and goals of the audit, entry-level analysts might be asked to review and understand the scope and goals in order to complete other elements of the audit.

As an example, the scope of this audit involves assessing user permissions; identifying existing controls, policies, and procedures; and accounting for the technology currently in use by the organization. The goals outlined include implementing core functions of frameworks, like the NIST CSF; establishing policies and procedures to ensure compliance; and strengthening system controls.

The next element is conducting a risk assessment, which is focused on identifying potential threats, risks, and vulnerabilities. This helps organizations consider what security measures should be implemented and monitored to ensure the safety of assets. Similar to establishing the scope and goals, a risk assessment is oftentimes completed by managers or other stakeholders. However, you might be asked to analyze details provided in the risk assessment to consider what types of controls and compliance regulations need to be in place to help improve the organization's security posture.

For example, this risk assessment highlights that there are inadequate controls, processes, and procedures in place to protect the organization's assets. Specifically, there is a lack of proper management of physical and digital assets, including employee equipment. The equipment used to store data is not properly secured. And access to private information stored in the organization's internal network likely needs more robust controls in place. Now that we've discussed the initial planning elements of an internal security audit, coming up, we'll focus on the last three elements.

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:

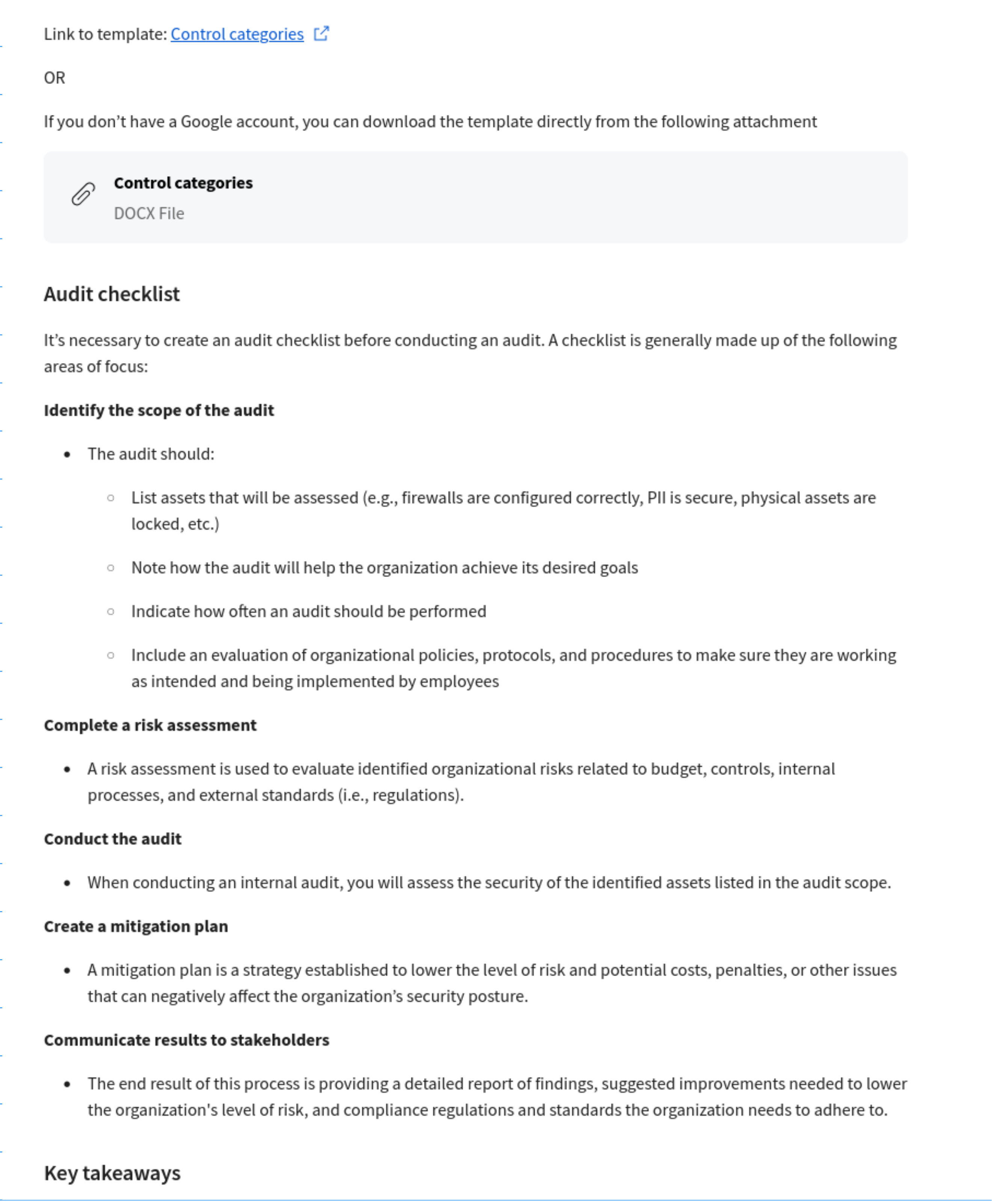
- Industry type
- Organization size
- Ties to the applicable government regulations
- A business's geographical location
- A business decision to adhere to a specific regulatory compliance

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

As a reminder, the planning elements of internal security audits include establishing the scope and goals, then conducting a risk assessment. The remaining elements are completing a controls assessment, assessing compliance, and communicating results. Before completing these last three elements, you'll need to review the scope and goals, as well as the risk assessment, and ask yourself some questions. For example: What is the audit meant to achieve? Which assets are most at risk? Are current controls sufficient to protect those assets? If not, what controls and compliance regulations need to be implemented? Considering questions like these can support your ability to complete the next element: a controls assessment.

A controls assessment involves closely reviewing an organization's existing assets, then evaluating potential risks to those assets, to ensure internal controls and processes are effective. To do this, entry-level analysts might be tasked with classifying controls into the following categories: administrative controls, technical controls, and physical controls.

Administrative controls are related to the human component of cybersecurity. They include policies and procedures that define how an organization manages data, such as the implementation of password policies.

Technical controls are hardware and software solutions used to protect assets, such as the use of intrusion detection systems, or IDS's, and encryption.

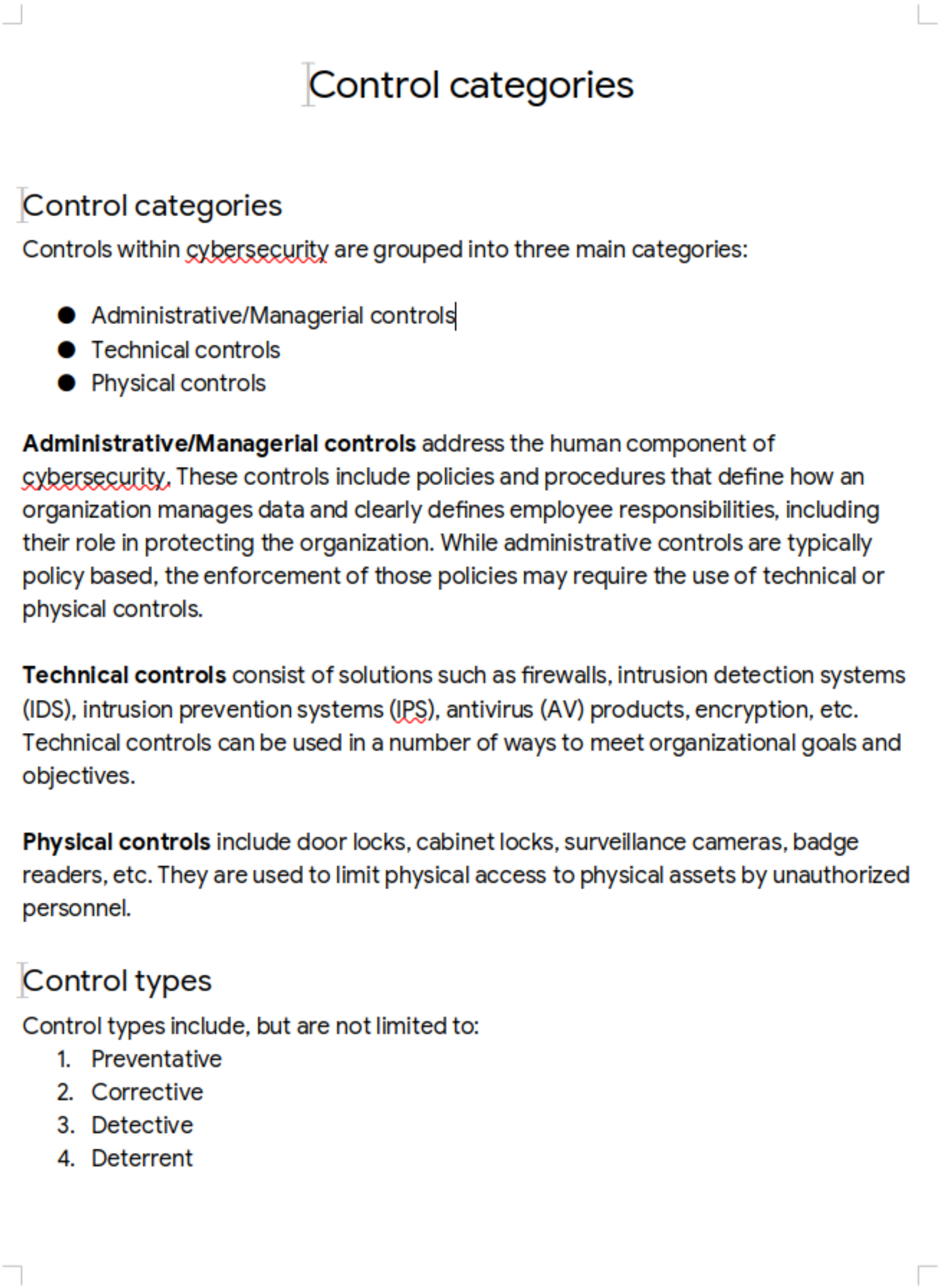
Physical controls refer to measures put in place to prevent physical access to protected assets, such as surveillance cameras and locks.

The next element is determining whether or not the organization is adhering to necessary compliance regulations. As a reminder, compliance regulations are laws that organizations must follow to ensure private data remains secure. In this example, the organization conducts business in the European Union and accepts credit card payments. So they need to adhere to the GDPR and Payment Card Industry Data Security Standard, or PCI DSS.

The final common element of an internal security audit is communication. Once the internal security audit is complete, results and recommendations need to be communicated to stakeholders. In general, this type of communication summarizes the scope and goals of the audit. Then, it lists existing risks and notes how quickly those risks need to be addressed. Additionally, it identifies compliance regulations the organization needs to adhere to and provides recommendations for improving the organization's security posture.

Internal audits are a great way to identify gaps within an organization. When I worked at a previous company, my team and I conducted an internal password audit and found that many of the passwords were weak. Once we identified this issue, the compliance team took the lead and began enforcing stricter password policies. Audits are an opportunity to determine what security measures an organization has in place and what areas need to be improved to achieve the organization's desired security posture.

Security audits are quite involved, yet of extreme value to organizations. Later in the course, you'll have an opportunity to complete elements of an internal security audit for a fictional company, which you can include in your professional portfolio.



Control categories

Control categories

Controls within cybersecurity are grouped into three main categories:

- Administrative/Managerial controls
- Technical controls
- Physical controls

Administrative/Managerial controls address the human component of cybersecurity. These controls include policies and procedures that define how an organization manages data and clearly defines employee responsibilities, including their role in protecting the organization. While administrative controls are typically policy based, the enforcement of those policies may require the use of technical or physical controls.

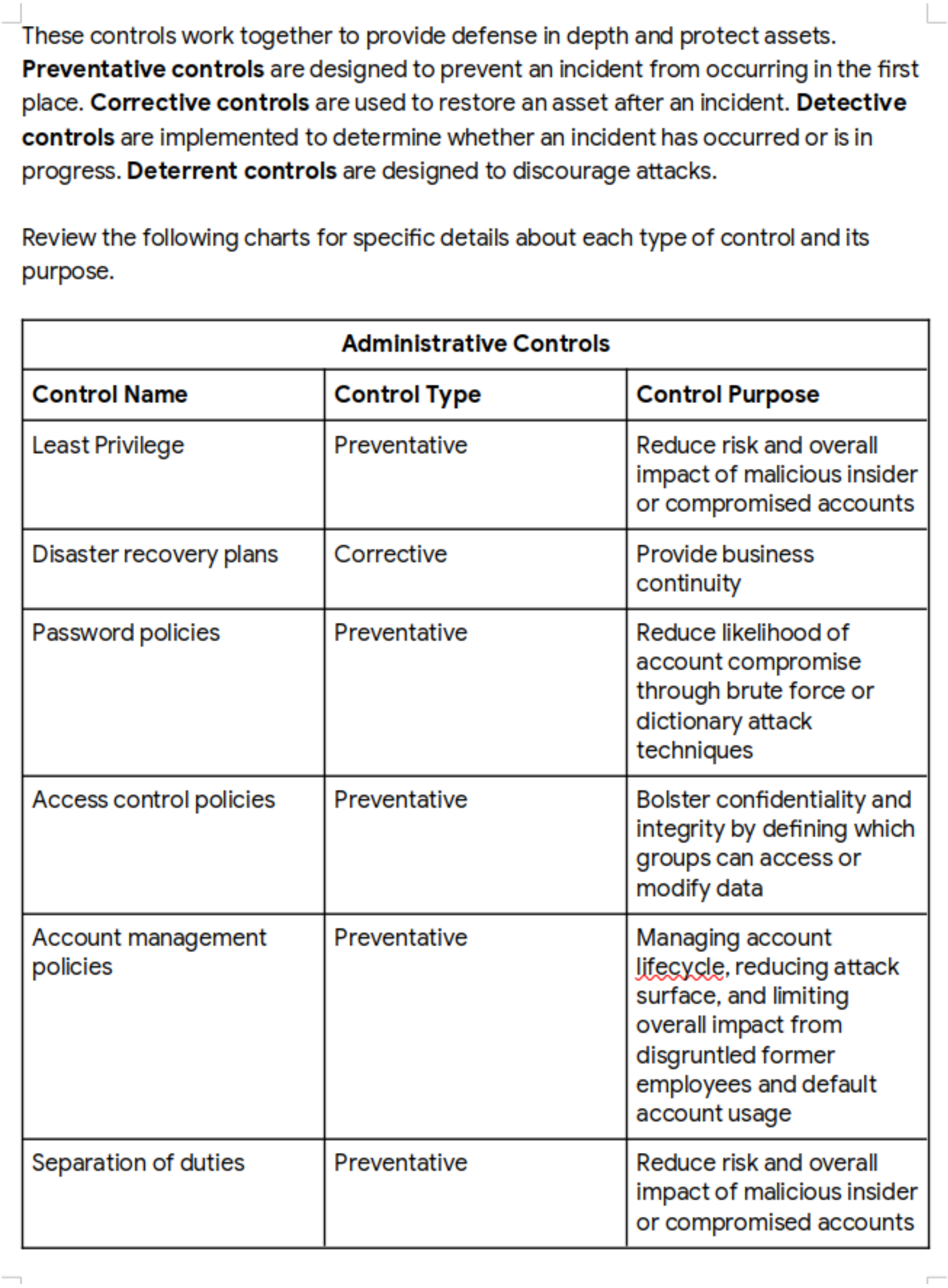
Technical controls consist of solutions such as firewalls, intrusion detection systems (IDS), intrusion prevention systems (IPS), antivirus (AV) products, encryption, etc. Technical controls can be used in a number of ways to meet organizational goals and objectives.

Physical controls include door locks, cabinet locks, surveillance cameras, badge readers, etc. They are used to limit physical access to physical assets by unauthorized personnel.

Control types

Control types include, but are not limited to:

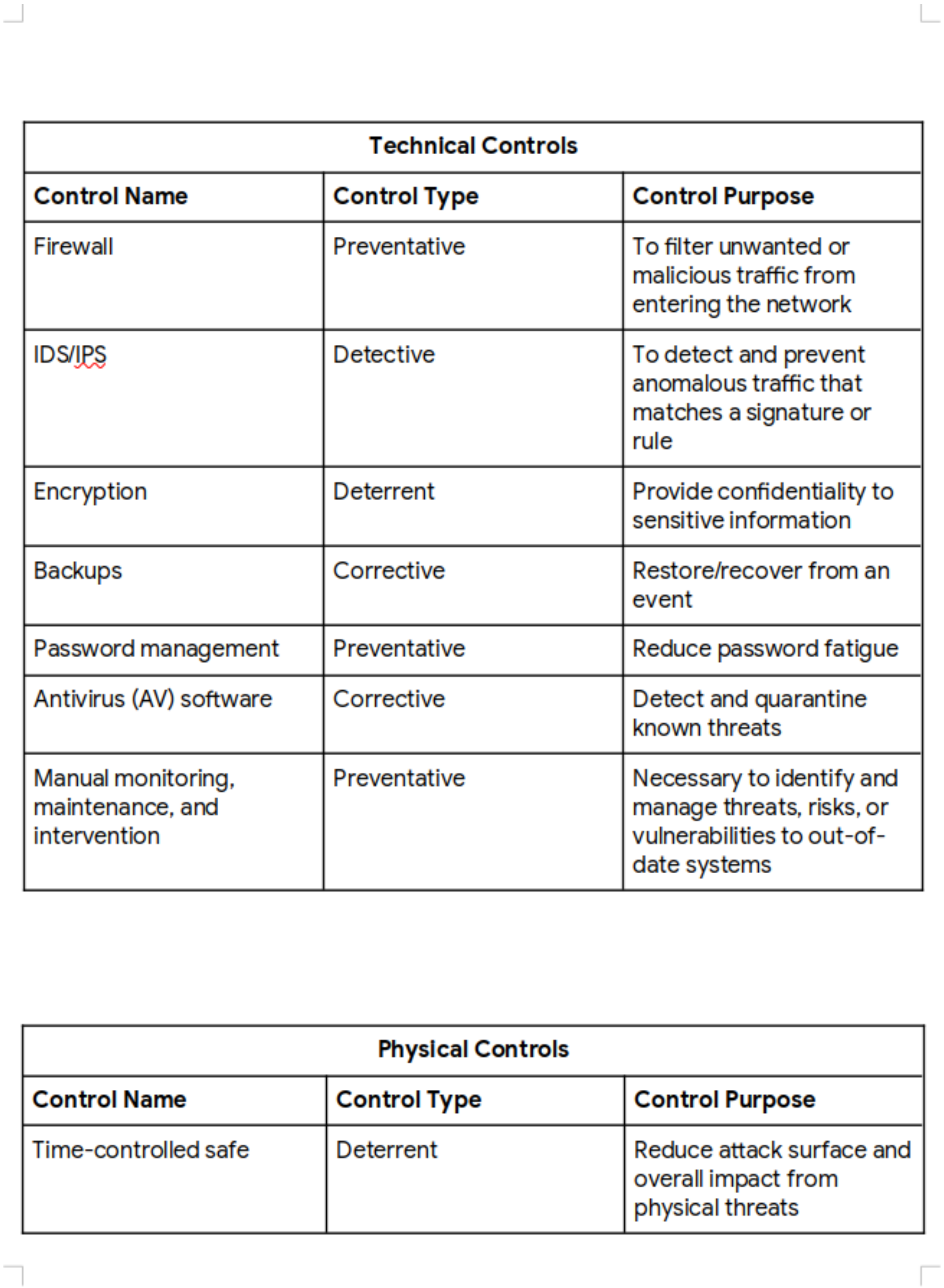
1. Preventative
2. Corrective
3. Detective
4. Deterrent



These controls work together to provide defense in depth and protect assets. **Preventative controls** are designed to prevent an incident from occurring in the first place. **Corrective controls** are used to restore an asset after an incident. **Detective controls** are implemented to determine whether an incident has occurred or is in progress. **Deterrent controls** are designed to discourage attacks.

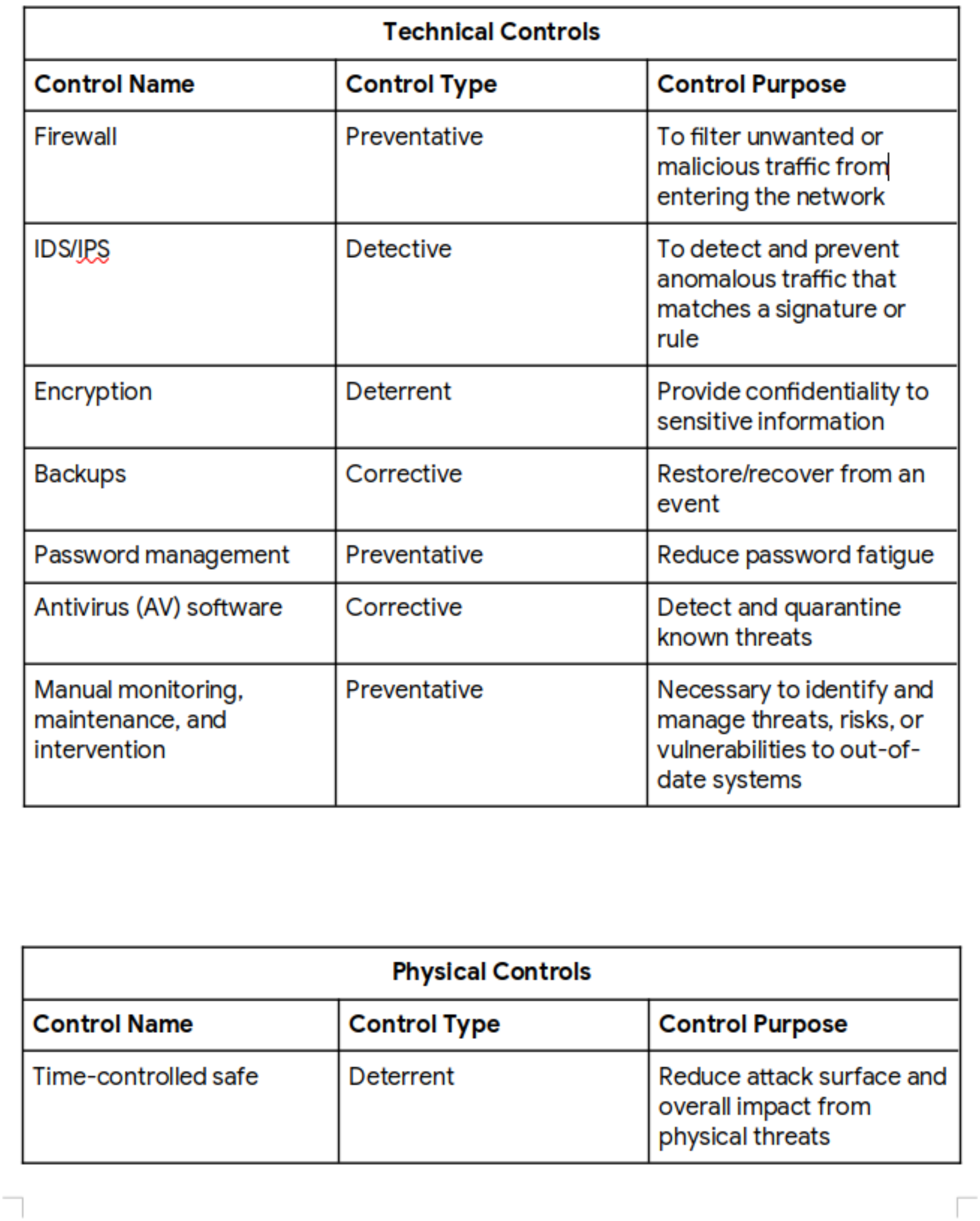
Review the following charts for specific details about each type of control and its purpose.

Administrative Controls		
Control Name	**Control Type**	**Control Purpose**
Least Privilege	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts
Disaster recovery plans	Corrective	Provide business continuity
Password policies	Preventative	Reduce likelihood of account compromise through brute force or dictionary attack techniques
Access control policies	Preventative	Bolster confidentiality and integrity by defining which groups can access or modify data
Account management policies	Preventative	Managing account lifecycle, reducing attack surface, and limiting overall impact from disgruntled former employees and default account usage
Separation of duties	Preventative	Reduce risk and overall impact of malicious insider or compromised accounts



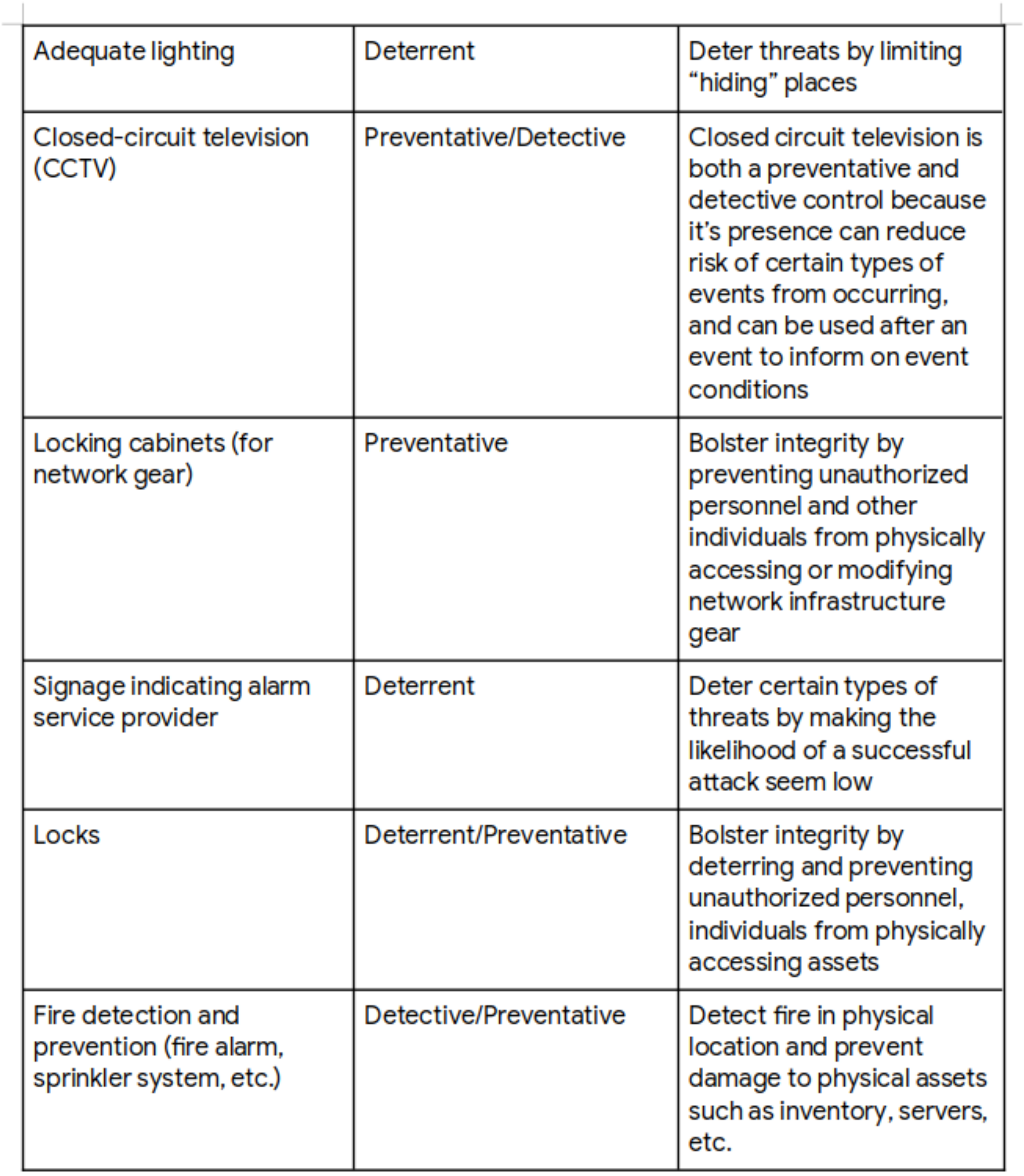
Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Corrective	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical Controls		
Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats



Technical Controls		
Control Name	**Control Type**	**Control Purpose**
Firewall	Preventative	To filter unwanted or malicious traffic from entering the network
IDS/IPS	Detective	To detect and prevent anomalous traffic that matches a signature or rule
Encryption	Deterrent	Provide confidentiality to sensitive information
Backups	Corrective	Restore/recover from an event
Password management	Preventative	Reduce password fatigue
Antivirus (AV) software	Corrective	Detect and quarantine known threats
Manual monitoring, maintenance, and intervention	Preventative	Necessary to identify and manage threats, risks, or vulnerabilities to out-of-date systems

Physical Controls		
Control Name	**Control Type**	**Control Purpose**
Time-controlled safe	Deterrent	Reduce attack surface and overall impact from physical threats



Adequate lighting	Deterrent	Deter threats by limiting "hiding" places
Closed-circuit television (CCTV)	Preventative/Detective	Closed circuit television is both a preventative and detective control because it's presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions
Locking cabinets (for network gear)	Preventative	Bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear
Signage indicating alarm service provider	Deterrent	Deter certain types of threats by making the likelihood of a successful attack seem low
Locks	Deterrent/Preventative	Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative	Detect fire in physical location and prevent damage to physical assets such as inventory, servers, etc.