**How Frameworks, Controls, and Principles Work Together: The Role of Security Audits**

Security audits play a critical role in ensuring that the **frameworks**, **controls**, **principles**, and **compliance regulations** we've discussed actually work together to protect an organization’s data and assets. Conducting a security audit is an essential step in reviewing how well an organization’s security measures align with industry best practices and regulatory requirements.

There are two main types of security audits: **external** and **internal**. While external audits are often done by third-party entities, **internal audits** are the ones that entry-level analysts are most likely to contribute to. Let’s take a closer look at what internal security audits involve and how they help organizations stay secure.

**Internal Security Audits:**

An **internal security audit** is a comprehensive review of an organization's security practices to ensure they meet internal goals, compliance regulations, and industry standards. These audits are typically conducted by a team that includes the **compliance officer**, **security manager**, and other security team members.

**Key purposes of an internal audit** include:

* **Improving security posture**: Identifying weaknesses and strengthening overall security measures.
* **Avoiding compliance fines**: Ensuring that the organization complies with relevant regulations and standards.
* **Risk management**: Identifying organizational risks and correcting vulnerabilities in controls or procedures.

**Common Elements of Internal Audits**

Let’s break down some of the **core elements** of an internal security audit. These are the tasks and steps that auditors follow to assess the organization's security posture.

1. **Establishing the Scope and Goals of the Audit**
   * **Scope**: This refers to the specific criteria that define what the audit will cover. This could include identifying **people**, **assets**, **policies**, **procedures**, and **technologies** that are relevant to the organization’s security.
     + Example: The scope of the audit could include assessing **user permissions**, reviewing existing **controls**, evaluating **policies and procedures**, and assessing the **technologies** in use by the organization.
   * **Goals**: The goals of the audit outline the organization’s security objectives and what the audit aims to achieve. The goals focus on improving the security posture and meeting **compliance requirements**.
     + Example: The goals could include implementing core functions of frameworks like the **NIST Cybersecurity Framework (CSF)**, ensuring **compliance**, and strengthening **system controls**.
2. **Conducting a Risk Assessment** A **risk assessment** helps the organization identify potential **threats**, **risks**, and **vulnerabilities**. The goal is to determine what security measures need to be implemented and monitored to protect assets and ensure business continuity.
   * In a risk assessment, auditors consider various risk factors, such as:
     + **Inadequate controls or processes**: For example, the lack of proper management of **physical and digital assets** could be a risk.
     + **Unsecured equipment**: Issues like storing sensitive data on poorly secured devices could be highlighted.
     + **Weak access controls**: Not having robust **access controls** for private information or internal networks is another risk.
   * Even though **senior-level security team members** often complete the risk assessment, **entry-level analysts** might be asked to **review** and understand the findings. They will need to help analyze the information and suggest which **controls** and **compliance regulations** need to be improved or implemented.

**Next Steps: Audit Planning to Execution**

So far, we've focused on the initial planning stages of the audit: establishing the **scope** and **goals** and conducting the **risk assessment**. These steps help set the foundation for a thorough internal audit.

In the next part of the audit process, auditors will conduct:

* **A controls assessment**, to evaluate whether existing controls are effective.
* **A compliance assessment**, to ensure that all regulations and standards are being met.
* **Communication of results**, which involves reporting findings to stakeholders and suggesting improvements.

As you continue in your role as a **security analyst**, understanding the audit process is crucial. You'll likely be involved in conducting audits, reviewing results, or contributing to **risk assessments** and **controls evaluations** to help strengthen the organization's security posture.

**Final Elements of an Internal Security Audit**

As we continue our journey into the world of **internal security audits**, we now move into the **final elements** that an **entry-level analyst** might be involved in. Previously, we discussed the initial stages of an audit: **establishing the scope and goals** and **conducting a risk assessment**. Now, we will focus on the **controls assessment**, **compliance assessment**, and **communication of results**.

**1. Controls Assessment**

After reviewing the **scope**, **goals**, and **risk assessment**, you'll be tasked with evaluating the organization’s existing controls. This process involves classifying the **types of controls** in place and determining whether they are adequate for the risks and assets they are meant to protect.

There are three main categories of controls to review:

* **Administrative Controls**: These are policies and procedures that help manage the human side of cybersecurity. Examples include:
  + **Password policies** that set rules for complexity and frequency of password changes.
  + **Access control policies** that define who has access to what data.
* **Technical Controls**: These involve hardware and software solutions designed to protect the organization's assets. Examples include:
  + **Intrusion Detection Systems (IDS)**, which monitor network traffic for suspicious activity.
  + **Encryption** of data both at rest and in transit to protect sensitive information from unauthorized access.
* **Physical Controls**: These refer to the physical barriers or measures that protect assets from unauthorized physical access. Examples include:
  + **Surveillance cameras** in secure areas.
  + **Locked doors** to prevent unauthorized personnel from accessing sensitive areas.

As an **entry-level analyst**, you may be tasked with reviewing these categories to assess whether the existing controls are sufficient to protect the organization's critical assets.

**2. Assessing Compliance**

After reviewing the organization’s controls, the next step is to ensure that the organization is **adhering to necessary compliance regulations**. **Compliance regulations** are laws and standards that organizations must follow to ensure data security, privacy, and the protection of sensitive information.

Some common regulations that might come into play include:

* **GDPR (General Data Protection Regulation)**: If the organization operates in the **European Union**, it must follow GDPR, which sets strict rules on data privacy and handling personal information.
* **PCI DSS (Payment Card Industry Data Security Standard)**: If the organization accepts **credit card payments**, they must comply with PCI DSS to ensure secure handling of payment information.

As an entry-level analyst, you may need to **verify that the organization is in compliance** with these regulations by reviewing policies, procedures, and systems in place. Ensuring compliance helps mitigate legal and financial risks for the organization.

**3. Communicating Results**

Once the internal security audit is complete, the results and **recommendations** need to be **communicated to stakeholders**. This step is crucial because it ensures that the audit findings are properly understood, and corrective actions can be taken.

Key elements to include in the communication of results:

* **Summary of the audit’s scope and goals**: Recap what was covered in the audit and the objectives the audit aimed to achieve.
* **Identification of risks**: List the existing **risks** and categorize them based on **severity** (e.g., high, medium, or low risk). Highlight any risks that need to be addressed immediately.
* **Compliance status**: Indicate whether the organization is meeting required **compliance standards** (e.g., GDPR, PCI DSS) and whether any changes are needed.
* **Recommendations for improving security posture**: Provide suggestions on **how to address the identified risks**, including implementing better controls, updating policies, or ensuring stricter adherence to compliance requirements.

**Practical Example: Internal Password Audit**

As an example, think about a scenario where your team conducts an **internal password audit**. During the audit, you might find that many passwords are weak (e.g., short, simple, or reused across multiple accounts).

Once this issue is identified, the **compliance team** may step in and **enforce stricter password policies**—requiring longer, more complex passwords and regular password changes. This is an example of how an internal audit can identify weaknesses and drive positive changes within the organization.

**Conclusion**

Security audits are comprehensive and valuable tools for improving an organization’s **security posture**. They help identify gaps, **assess controls**, ensure **compliance**, and improve the overall security framework of an organization.

As an **entry-level analyst**, you’ll likely be involved in **collecting data**, **evaluating controls**, and **assessing compliance** during internal security audits. Your contribution will help the organization stay secure, compliant, and prepared for any threats or vulnerabilities that may arise.

In the next part of this course, you'll get a chance to apply what you’ve learned by completing elements of a **fictional company’s internal security audit**. This will be a great opportunity to gain hands-on experience and add a valuable project to your professional portfolio!

# 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](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/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](https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA)

OR

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

## 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:

* [Assessment and Auditing Resources](https://www.nist.gov/cyberframework/assessment-auditing-resources)



 [IT Disaster Recovery Plan](https://www.ready.gov/it-disaster-recovery-plan)