GOOGLE CYBER SECURITY
Course 1: Play It Safe: Manage Security Risks

SKILLS: Information Systems Security, Risk Management, Security Information and Event Management (SIEM), Incident Response, Security Controls, Vulnerability Management, Auditing, Enterprise Security

Module 1

Security Domains

This module explains the focus of CISSP's eight security domains. Then, primary threats, risks, and vulnerabilities to business operations are identified and defined, along with a discussion of the threats, risks, and vulnerabilities entry-level security analysts focus on most. Additionally, NIST's Risk Management Framework (RMF) is introduced.

What you'll learn

- CISSP's eight security domains
- Security frameworks and controls
- Security audits
- Basic security tools
- Protect assets and data

Overview of the Cybersecurity Program

Purpose of the Program:
The program is designed to equip you with the **knowledge, skills, and tools** necessary to work effectively in the **world of cybersecurity** (also called **security**).

What You'll Learn:

1. **CISSP's 8 Security Domains**
   - You'll get an overview of the **eight core domains** from the **CISSP (Certified Information Systems Security Professional)** framework.
   - These domains represent the **main focus areas** in cybersecurity.
2. **Threats, Risks, and Vulnerabilities**
   - You'll dive deeper into:

   - What **threats** are (potential dangers),
   - What **risks** mean (the chances that a threat will exploit a vulnerability),
   - And what **vulnerabilities** are (weaknesses in systems or processes).
3. **Three Layers of the Web:**
   - **Surface Web** – the part of the internet we use every day.
   - **Deep Web** – data not indexed by search engines (like academic databases, private emails).
   - **Dark Web** – anonymous part of the web often associated with illegal activity.

     You'll see examples to help understand each of these.

4. **Types of Attacks:**
   - You'll be introduced to different kinds of **cyber attacks** (like phishing, malware, ransomware, etc.), which will be explained more later in the course.
5. **Risk Management with NIST RMF:**
   - You'll learn about the **NIST Risk Management Framework** – a structured approach developed by the **National Institute of Standards and Technology (NIST)**.
   - It helps **identify, assess, and manage cybersecurity risks** in organizations.

Why This Matters:

- These topics are considered **foundational** in cybersecurity.
- Gaining a strong understanding will help you:
  - **Prevent attacks**
  - **Reduce risks**
  - **Protect organizations** from daily threats

CISSP security domains:

1. Security and Risk Management

Focus Areas:

- **Defining goals & objectives**: Helps reduce risks to sensitive data like PII (Personally Identifiable Information)
- **Risk mitigation**: Having rules and processes to reduce the impact of security events (e.g., breaches)
- **Compliance**: Developing internal security policies based on laws, standards, and regulations
- **Business continuity**: Ensuring daily operations continue during disruptions using recovery plans
- **Legal and ethical behavior**: Following laws and ethical guidelines to avoid negligence, abuse, and fraud

2. Asset Security

Focus Areas:

- Protecting both **digital and physical assets**
- Ensuring proper:
  - **Storage**
  - **Maintenance**
  - **Retention**
  - **Destruction** of sensitive data (like PII or SPII – Sensitive PII)
- Tracking **who has access** to what data
- Example: Security analysts may oversee the proper destruction of hard drives to prevent data leaks

3. Security Architecture and Engineering

Focus Areas:

- Implementing secure **tools**, **systems**, and **processes** to protect data
- Promoting the idea of **shared responsibility**:
  - Everyone in the organization should actively participate in maintaining security
  - Encouraging users to report suspicious activity or concerns

4. Communication and Network Security

Focus Areas:

- Securing **physical networks**, **wireless networks**, and **cloud communications**
- Protecting remote connections, such as:
  - Insecure Bluetooth
  - Public Wi-Fi
- Example: Security teams may disable risky communication channels to reduce unsafe user behavior

5. Identity and Access Management (IAM)

Purpose:
To control **who can access what** in an organization by using **access and authorization policies**.

Key Goals:

- Ensure users only have access to what they need.
- Prevent unauthorized access.
- Reduce risk to systems and data.

Real-world example:

- If everyone uses the same admin login, you can't track individual actions. This makes it impossible to investigate who did what during a breach.

IAM Core Components:

1. **Identification** – Verifying who a user is (e.g., username, ID card, fingerprint)
2. **Authentication** – Proving identity (e.g., password, PIN)
3. **Authorization** – Granting access based on user roles
4. **Accountability** – Logging and monitoring user actions

6. Security Assessment and Testing

Purpose:
To **evaluate and improve security controls** regularly through testing, auditing, and analysis.

Key Activities:

- Conduct **security control tests**
- Perform **security audits**
- Collect and analyze **security data**

These actions help detect risks and vulnerabilities and improve the organization's defense mechanisms.

Example:
Introducing **multi-factor authentication (MFA)** after a test shows that password-only access is weak.

7. Security Operations

Purpose:
To **detect, respond to, and investigate security incidents** while also preventing future ones.

Key Steps:

1. **Incident response** – Act quickly during an active attack to reduce damage
2. **Forensic investigation** – Collect digital/physical evidence to understand the breach
3. **Post-incident improvement** – Analyze the incident to strengthen future defenses

8. Software Development Security

Purpose:
To integrate **security into every phase of the software development lifecycle (SDLC)**.

Key Practices:

- Use **secure coding guidelines**
- Perform **security reviews** during design, development, testing, and deployment
- Conduct **penetration testing** before releasing the software

Example:

- Do a secure design review early
- Review code for vulnerabilities during development
- Test for security flaws before launching the product

Conclusion:

Understanding all **eight domains** helps you see how organizations build and maintain strong security. These domains also highlight the essential work of cybersecurity teams in defending assets, systems, and data.

Let me know when you're ready to go over threats, risks, vulnerabilities, ransomware, and the layers of the web.

What Are Assets?

- An **asset** is anything valuable to an organization (digital or physical).
- Examples: Computers, office spaces, customer PII (Personally Identifiable Information), patents, and intellectual property.

1. Threats

- A **threat** is anything that can **negatively impact assets**.
- Example: **Social engineering attacks**
  - Specifically, **phishing**: Tricking users (via fake emails or links) into giving up sensitive data like usernames or banking info.

2. Risks

- A **risk** is the **potential for a threat to exploit a vulnerability** and impact an asset's:
  - **Confidentiality** (privacy)
  - **Integrity** (accuracy)
  - **Availability** (accessibility)
- Think of **risk** as the **likelihood** of something bad happening.
- **Example of a risk**: No backup plan for recovering important data in case of a breach or accident.

Risk Levels:

- **Low risk**: Public data (e.g., website content) – no serious impact if exposed.
- **Medium risk**: Sensitive internal data (e.g., unreleased earnings reports) – may hurt reputation or finances.
- **High risk**: Protected data (e.g., SPII, PII, intellectual property) – serious legal, financial, and operational consequences if compromised.

3. Vulnerabilities

- A **vulnerability** is a **weakness** that a **threat can exploit**.
- **Examples:**
  - Outdated firewalls or software
  - Weak passwords
  - Unprotected sensitive data
  - Even people (e.g., unaware employees) can be vulnerabilities
- Important note:
  Both a vulnerability and a threat must exist for a risk to occur.

Role of Entry-Level Analysts

- Educate staff to identify threats (e.g., phishing awareness)
- Use security tools (e.g., access cards to restrict building entry)
- Encourage reporting of suspicious activity
- Monitor and document access to critical assets
- Help the organization **reduce risk** by **managing vulnerabilities**

Ransomware

- **Ransomware** is a type of **malware** used by threat actors to **encrypt an organization's data**.
- Once encrypted:
  - Systems are frozen
  - Devices become unusable
  - Confidential data is locked
- The attacker demands a **ransom payment** in exchange for a **decryption key** (used to unlock the data).
- These events, including negotiations or leaked data, often happen via the **dark web** due to its secrecy.

Three Layers of the Web

1. **Surface Web**
   - Publicly accessible and searchable via standard web browsers
   - Examples: Social media, online shopping, news sites
2. **Deep Web**
   - Not indexed by search engines; requires authorization
   - Example: Company intranet (for internal use only)
3. **Dark Web**
   - Only accessible through special tools like **Tor**
   - Known for anonymous activity; often used for illegal actions like selling stolen data

Three Key Impacts of Threats, Risks, and Vulnerabilities

1. **Financial Impact**
   - High costs from:
     - Production/service interruption
     - Fixing systems
     - Fines due to **non-compliance**
   - Example: After a ransomware attack, restoring operations and paying penalties can be very expensive
2. **Identity Theft**

   - Storing sensitive information like **PII** (Personally Identifiable Information) introduces risk
   - Leaked PII can be sold on the dark web
   - Affects employees, customers, and vendors
3. **Reputational Damage**
   - Loss of customer trust and loyalty
   - Bad publicity and negative media coverage
   - Can lead to long-term harm, customer loss, and even legal penalties

NIST Risk Management Framework (RMF)

What is the NIST RMF?

- Developed by the **National Institute of Standards and Technology (NIST)**.
- A structured **7-step process** to help organizations **manage risks, threats, and vulnerabilities**.
- While entry-level analysts may not perform all steps, understanding the full process is valuable and can help you stand out during job applications.

The 7 Steps of the NIST Risk Management Framework (RMF)

1. Prepare

- **Goal:** Get ready to manage risks **before** any breach happens.
- **Tasks for analysts:** Monitor for risks, identify helpful controls, and gather information.
- **Example:** Watching for suspicious activity or known vulnerabilities.

2. Categorize

- **Goal:** Understand what's at risk and how it could impact **confidentiality, integrity, and availability (CIA)**.
- **Tasks for analysts:** Follow processes to reduce risks to critical assets, like customer data.
- **Example:** Categorizing data as low, medium, or high risk.

3. Select

- **Goal:** Choose and document security controls.
- **Tasks for analysts:** Help update security documentation like **playbooks** or **guidelines**.
- **Example:** Recording which controls are used to protect employee login data.

---

4. Implement

- **Goal:** Put the selected security controls and privacy plans into action.
- **Tasks for analysts:** Apply security changes to fix observed issues.
- **Example:** Updating password policies if users often request password resets.

5. Assess

- **Goal:** Check if controls are working correctly.
- **Tasks for analysts:** Evaluate how effective tools, procedures, and systems are.
- **Example:** Spotting weaknesses in current defenses and suggesting changes.

6. Authorize

- **Goal:** Accept accountability for risks that remain.
- **Tasks for analysts:** Create reports, write action plans, and help define project goals.
- **Example:** Documenting risk reports to present to management.

7. Monitor

- **Goal:** Continually track system performance and risk levels.
- **Tasks for analysts:** Daily monitoring, identifying any deviation from security goals.
- **Example:** If current systems aren’t keeping risk low, flag it for updates.

Key Reminder:

Even if you don’t set up these processes yourself, your job will involve **ensuring they're functioning correctly** to reduce risk for your organization and its customers.

Let me know if you'd like a simplified visual of the 7 steps or help memorizing them.

Glossary terms from module 1

Assess: The fifth step of the NIST RMF that means to determine if established controls are implemented correctly

Authorize: The sixth step of the NIST RMF that refers to being accountable for the security and privacy risks that may exist in an organization

Business continuity: An organization's ability to maintain their everyday productivity by establishing risk disaster recovery plans

Categorize: The second step of the NIST RMF that is used to develop risk management processes and tasks

External threat: Anything outside the organization that has the potential to harm organizational assets

Implement: The fourth step of the NIST RMF that means to implement security and privacy plans for an organization

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

Monitor: The seventh step of the NIST RMF that means be aware of how systems are operating

Prepare: The first step of the NIST RMF related to activities that are necessary to manage security and privacy risks before a breach occurs

Ransomware: A malicious attack where threat actors encrypt an organization’s data and demand payment to restore access

Risk: Anything that can impact the confidentiality, integrity, or availability of an asset

Risk mitigation: The process of having the right procedures and rules in place to quickly reduce the impact of a risk like a breach

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

Select: The third step of the NIST RMF that means to choose, customize, and capture documentation of the controls that protect an organization

Shared responsibility: The idea that all individuals within an organization take an active role in lowering risk and maintaining both physical and virtual security

Social engineering: A manipulation technique that exploits human error to gain private information, access, or valuables

Vulnerability: A weakness that can be exploited by a threat

Module 2

Security Frameworks and Controls

Security Analyst's Role:

- Not just about protecting organizations — it's also about **protecting people**.
- **Breaches** can damage:
  - Customers' and employees' **financial stability**
  - Their **reputation**
- Your daily work helps ensure the **safety of both people and organizations**.

What's Coming Up in This Section:

- You'll explore:
  - **Security frameworks**
  - **Security controls**
  - **Design principles**
- Learn how they are used in **security audits** to protect systems and data.

Example from Google:

- At Google, keeping **customer information confidential** is a top priority.
- The **NIST Cybersecurity Framework** helps ensure:
  - Protection of tools and data
  - Compliance through **security controls**

What Are Security Frameworks?

- **Security frameworks** are **guidelines** organizations use to create **policies and procedures** that help:
  - **Mitigate threats, risks, and vulnerabilities**
  - Protect **data, privacy**, and **people**
- They are used as **starting points** for developing customized security strategies.

Types of Protection Covered

- Frameworks address both:
  - **Virtual threats** (e.g., ransomware, phishing)
  - **Physical threats** (e.g., unauthorized building access)
    - Example: Requiring **key cards** or **badges** to enter offices

Purpose of Frameworks

- Help **prevent, detect, and respond** to security breaches.
- Especially useful against **social engineering attacks** that target human behavior (like phishing).

Why People Matter Most

- **Human error** is the biggest security threat.
- Frameworks include guidance to:
  - **Increase employee awareness**
  - **Train staff** to recognize red flags and suspicious behavior
  - **Report issues** quickly and effectively

Your Role as an Analyst

- Understand and help implement the **security plans** based on frameworks.
- Contribute to keeping the **organization, employees, and customers** safe from attacks and breaches.

What Are Security Controls?

- **Security controls** are **safeguards** or measures designed to reduce **specific security risks**.
- Without proper controls, organizations face **financial loss** and **reputation damage** due to risks like:
  - **Trespassing**
  - **Fake employee accounts**
  - **Unauthorized access to benefits or resources**

Three Common Types of Security Controls

1. Encryption

- Converts **plaintext** into unreadable **ciphertext**.
- Ensures **confidentiality** of sensitive data (e.g., Social Security numbers, customer accounts).
- Data must be **decrypted** back into readable form to be useful.

2. Authentication

- Verifies **who someone is** before granting access.
- Example: Logging in with a **username and password**.
- **Multi-Factor Authentication (MFA)** adds another layer:
  - Requires an additional proof like a **code**, **fingerprint**, **voice**, or **face scan**.

3. Authorization

- Determines **what someone is allowed to access** after authentication.
- Ensures only approved users access specific **resources or data**.
- Example: A government analyst having access to **deep web** internal data that others can't see.

Note on Biometrics & Social Engineering

- **Biometrics** (like fingerprint, eye scan) are used for authentication.
- **Vishing** (voice phishing) is a social engineering attack that can **mimic someone's voice** to bypass biometric verification.

Relationship between frameworks and controls

What Are Frameworks?

- **Security frameworks** are **guidelines** to help organizations **plan** for managing **risks, threats, and vulnerabilities**.
- They help with **compliance** (e.g., HIPAA in healthcare).
- Example: NIST RMF, NIST CSF, ISO/IEC 27001, and Cyber Threat Framework (CTF).

What Are Controls?

- **Security controls** are **actions or tools** used to reduce specific risks.
- They are used **alongside frameworks** to achieve security goals.
- Example: Using **multi-factor authentication (MFA)** to protect medical records.

Types of Controls

Type	Description	Examples
Physical	Protect physical spaces	Locks, security guards, CCTV, access cards
Technical	Protect systems & data	Firewalls, MFA, antivirus
Administrative	Define roles, rules, and processes	Authorization, separation of duties, asset classification

---

Examples of Frameworks

- **CTF (Cyber Threat Framework)**: Developed by U.S. intelligence to create a **common language** for sharing info about cyber threats.
- **ISO/IEC 27001**: Global framework for managing **information security** (financial data, IP, employee info). It provides a **list of controls**, but they're optional.

Key Takeaways

- **Frameworks = plans**
- **Controls = tools/actions**
- Together, they:
  - Help meet **compliance** laws (like HIPAA)
  - Reduce **risks and threats**
  - Strengthen an organization's **security posture**

CIA Triad – Core Security Model

It stands for:

1. **Confidentiality**

   → Only **authorized users** can access data.

   → Data is shared on a **need-to-know** basis.

   Example: A bank protects customers' financial info from unauthorized access.

2. **Integrity**

   → Data must be **correct, authentic, and reliable**.

   → Any change should be **intentional and authorized**.

   Example: Bank blocks suspicious activity to ensure account data isn't tampered with.

3. **Availability**

   → Data must be **accessible** to authorized users **when needed**.

   → Systems and apps must run reliably.

   Example: Bank ensures customers can always access their accounts online.

Why it Matters

As a **security analyst**, you'll apply the CIA triad daily to:

- Set security policies
- Reduce risk from **malware**, **social engineering**, and **data breaches**
- Protect both **organizations** and the **people they serve**

CIA Triad in the Workplace

1. Confidentiality

- **Goal:** Ensure only **authorized users** can access sensitive data.
- **How analysts apply it:**
  - Use the **principle of least privilege** (give users access only to what they need).
  - Example: An HR employee can access employee records, but not company financials.
- **Tools/Methods:**
  - Access controls
  - Encryption
  - User authentication

2. Integrity

- **Goal:** Keep data **correct**, **authentic**, and **trustworthy**.
- **How analysts apply it:**
  - Use **cryptographic techniques** to prevent unauthorized changes.
  - Example: Chat messages are **encrypted** so they can't be altered in transit.
- **Tools/Methods:**
  - Encryption
  - Hashing (to detect tampering)
  - Checksums

3. Availability

- **Goal:** Ensure **authorized users** can access data **when needed**.
- **How analysts apply it:**
  - Maintain system uptime and fast recovery from disruptions.
  - Example: Remote employees get secure access to internal networks.
- **Tools/Methods:**
  - Firewalls
  - Redundant systems
  - Backups and disaster recovery plans

Key Point

The **CIA triad** supports a strong **security posture**, meaning the organization:

- Can defend its critical assets
- Can respond effectively to changes and threats
- Keeps employees, customers, and data protected

NIST frameworks

Purpose of Frameworks

- Frameworks help organizations **create plans** to reduce **risks, threats, and vulnerabilities** to sensitive **data** and **assets**.
- Used by all types of organizations — **for-profit**, **non-profit**, and **government**.

NIST Cybersecurity Framework (CSF)

- **Voluntary** and **globally respected**.
- Provides **standards**, **guidelines**, and **best practices** to manage cybersecurity risk.
- Applies to **any industry**, not just government.

Five Core Functions of CSF:

1. **Identify** – Know your assets, risks, and who has access.
2. **Protect** – Implement safeguards (like access controls).
3. **Detect** – Identify if a threat or breach has occurred.
4. **Respond** – Take steps to investigate and contain.
5. **Recover** – Restore systems and data, learn from the incident.

Example (From Video):

- You detect a **high-risk** alert on a workstation.
- An **unknown device** is plugged in — you **block it**, **analyze the threat**, and find it's an **infected phone**.
- You then take steps to **recover files**, fix the system, and learn how it happened.

NIST SP 800-53

- A special publication of NIST used for **federal government systems**.
- Provides **security controls** to ensure **confidentiality**, **integrity**, and **availability** (CIA triad).
- Applies to **government systems** and also **private companies** working with the government.

Key Takeaway

- **CSF** helps handle incidents quickly and efficiently.
- **SP 800-53** helps protect **U.S. federal systems**.
- Together, they ensure security plans are in place to **prevent**, **respond to**, and **recover from** attacks.

Five core functions of the NIST Cybersecurity Framework (CSF)

NIST CSF – 5 Core Functions

These five functions help organizations **manage cyber risks**, **respond to incidents**, and **recover from damage**:

1. Identify

- Understand what needs protection: **people, systems, assets, and data**.
- Example: You monitor your internal network to **spot weaknesses** or **suspicious activity**.

2. Protect

- Use **policies**, **training**, **tools**, and **procedures** to defend against threats.
- Example: Improve old security policies based on **lessons learned from past attacks**.

3. Detect

- **Find** cybersecurity events quickly using **monitoring tools**.
- Example: Check if a new tool **correctly flags threats** and **alerts the team**.

4. Respond

- **Take action** when an incident happens — contain and analyze it.
- Example: Help document what happened and **suggest improvements** to avoid future attacks.

5. Recover

- **Restore systems and data** after a security incident.
- Example: Help your team **bring services back online**, including restoring **legal or financial files**.

Key Takeaway

From **planning** to **response and recovery**, all five functions work together to:

- Reduce risks,
- Improve security processes,
- And help the organization **bounce back quickly** after an attack.

OWASP Security Principles

OWASP Security Principles

1. **Minimize the Attack Surface Area**
    - Reduce the number of ways attackers can break in.
    - Example: Disable unused features, block phishing emails, and use strong password policies.
2. **Principle of Least Privilege**
    - Give users **only the access they need** — nothing more.
    - Example: You can view logs but **not change permissions**, so if your account is hacked, damage is limited.
3. **Defense in Depth**
    - Use **multiple layers of protection**.
    - Example: Combine MFA, firewalls, intrusion detection, and permissions to block attackers at many points.
4. **Separation of Duties**
    - **No one person should control everything** — this prevents abuse or fraud.
    - Example: One person writes paychecks; another signs them.
5. **Keep Security Simple**
    - **Don't overcomplicate** controls — complexity leads to mistakes and poor collaboration.
    - Example: Use clear, manageable policies everyone understands.
6. **Fix Security Issues Correctly**
    - Identify the **real cause** of a problem and fix it completely.
    - Example: Weak Wi-Fi password? Fix it by enforcing **strong password rules** and test after fixing.

Why This Matters

Understanding and applying these principles:

- **Reduces risk**
- **Prevents breaches**
- **Makes you a smarter and more effective security analyst**

OWASP Security Principles Summary

Previously Covered Principles:

1. **Minimize Attack Surface Area**
   Reduce the number of potential vulnerabilities that threat actors can exploit.
   Example: Disable unnecessary features or services.
2. **Principle of Least Privilege**
   Users should only have the minimum access necessary to perform their job.
   Example: A user can view logs but cannot modify configurations.
3. **Defense in Depth**
   Use multiple layers of security controls to protect assets.
   Example: Combine firewalls, antivirus software, and multi-factor authentication.
4. **Separation of Duties**
   Distribute critical tasks among multiple individuals to prevent abuse of power.
   Example: One person prepares payroll, another approves it.
5. **Keep Security Simple**
   Avoid overly complex security solutions that are difficult to manage.
   Example: Use standardized access rules instead of custom code.
6. **Fix Security Issues Correctly**
   Address the root cause of a security issue and verify the fix works.
   Example: Patch a vulnerability rather than just restarting the system.

Newly Introduced Principles:

7. **Establish Secure Defaults**
   The most secure settings should be the default configurations.
   Example: New user accounts start with limited permissions.
8. **Fail Securely**
   When a system fails, it should do so in a secure manner.
   Example: If a firewall fails, it blocks all traffic rather than allowing it.
9. **Don't Trust Services**
   External services or third-party vendors should not be assumed secure. Always verify their data and behavior.
   Example: Validate data from a vendor before sharing it with customers.
10. **Avoid Security by Obscurity**
    Security should not rely solely on secrecy of implementation or hidden details.
    Example: Use proper access controls rather than relying on hidden URLs.

Plan a Security Audit

How Everything Works Together: Security Audits

What is a Security Audit?

A **security audit** is a detailed review of an organization's **security controls**, **policies**, and **procedures** to ensure they meet established expectations, like industry frameworks and legal regulations.

Types of Security Audits:

- **External Audits** – Performed by third parties (e.g., regulatory bodies).
- **Internal Audits** – Conducted by internal security teams and stakeholders.

Purpose of Internal Security Audits

- Improve **security posture**
- Identify **risks and vulnerabilities**
- Verify **compliance** with regulations
- Recommend fixes for weaknesses before external audits occur

Five Key Elements of an Internal Security Audit

1. Establish Scope and Goals

- **Scope**: Defines what will be audited (people, assets, systems, policies, etc.)
- **Goals**: Security objectives like improving controls or meeting compliance standards

Example:

- **Scope** includes: reviewing user permissions, identifying current controls, analyzing policies
- **Goals** include: applying NIST CSF functions, improving compliance, and strengthening system security

2. Conduct Risk Assessment

- Identify **threats**, **risks**, and **vulnerabilities**
- Helps determine which **controls**, **frameworks**, and **regulations** to focus on

Example:

- Audit reveals lack of asset management, insecure storage devices, and weak access controls

3. Controls Assessment

- Evaluate the **effectiveness of current controls**
- Identify gaps (e.g., outdated antivirus, no MFA)

4. Compliance Assessment

- Ensure policies align with legal and industry frameworks (e.g., HIPAA, NIST, ISO/IEC 27001)

5. Report Findings to Stakeholders

- Share results clearly
- Suggest improvements
- Help guide future security investments

How Everything Connects

Concept	Role in Audit
Frameworks	Guide what to assess (e.g., NIST CSF)
Controls	Are reviewed and tested
Security Principles	Are used to evaluate and recommend changes
Compliance Regulations	Are checked for violations or risks