CISSP Domain 1: Security and Risk Management Notes

How to use these notes: This document serves as a reference compilation, incorporating numerous NIST and other external sources.

The Information Security Triad (C-I-A)

Understanding the foundational principles of information security:

Concept	Meaning	Real-world Example	Key Controls
Confidentiality	Ensures only authorized users can access information.	Lock on a file cabinet / Encryption	Access control, Encryption
Integrity	Ensures information is trustworthy and unaltered.	File checksums / Version control	Hashing, Audit logs, Digital Signatures
Availability	Ensures systems/data are accessible when needed.	Redundant servers / UPS backups	RAID, Backups, Clustering

CISSP Exam Quick Bites:

- Confidentiality: Access control, Least Privilege, Need-to-know

- Integrity: Hashes, Digital Signatures, Checksums

- Availability: Redundancy, RAID, UPS, Failover Systems

Security Governance

Governance

Governance refers to the framework of responsibilities and decision-making practices applied by individuals who oversee an organization's operations.

◆ **Purpose**:

It ensures that **decisions are made strategically and consistently**, in line with the organization's mission, vision, and regulatory obligations.

Governance outlines **how decisions are made** — this includes:

- 📜 **Policies**: "What should be done?"
  - *Example*: A policy that mandates all passwords must be 12 characters or longer.
- 👥 **Roles**: "Who is responsible or accountable?"
  - *Example*: The **Chief Information Security Officer (CISO)** is responsible for implementing security programs.
- □ **Procedures**: "How will it be done?"
  - *Example*: Step-by-step instructions on onboarding employees with system access.

What is Security Governance?

Security governance is the system by which **an organization defines and manages** its security-related decisions. It includes the **policies, responsibilities, and workflows** used to ensure that security supports the organization's broader goals.

Security Governance:

1. **Policies, Roles, and Processes**

   Organizations rely on a structured set of rules and clearly defined roles to guide how they make security decisions.

   🔹 *Example*: A company enforces a "Remote Work Policy" requiring all remote employees to use a VPN.

   🔹 Roles: The IT Security team implements it, and department heads ensure compliance.

---

2. **Strategic Direction for Security**

   Security governance involves **defining the direction** of the security program—like setting objectives and priorities.

   🔹 *Example*: Leadership decides that cloud migration is a priority, so the security team is tasked with creating cloud security controls and policies.

---

3. **Resource Allocation**

It ensures that **adequate funding and personnel** are provided to run the security program effectively.

🔹 *Example*: Based on a recent phishing simulation, the organization invests in employee awareness training and advanced email filtering.

---

4. **Executive Oversight & Visibility**

   Senior leadership must **monitor and evaluate** whether the security program is working and aligns with business risks.

   🔹 *Example*: The board of directors regularly reviews cybersecurity metrics like incident trends, unpatched vulnerabilities, or audit findings to ensure accountability.

💡 Summary:

Security governance ensures that **security decisions are intentional, aligned with business goals**, and have **support from the top** of the organization. It's not just IT’s job—it's a **leadership responsibility**.

Key Functions of Security Governance

---

1. 🔐 Risk Management

Implementing the right controls to **identify, reduce, and control risks** to information systems—ensuring potential threats are managed at an acceptable level.

🔹 *Example*: Using firewalls, DLP tools, and employee training to reduce the risk of data breaches.

2. ⚙️ Resource Management

Making sure that **information security resources—people, technology, and knowledge—are used efficiently** and contribute to the organization's needs.

🔹 *Example*: Deploying a centralized SIEM system to monitor all departments instead of using separate tools.

3. 📊 Performance Measurement

Continuously **track and assess security performance** through metrics and reports to ensure the organization's security goals are being met.

🔹 *Example*: Measuring how fast security incidents are detected and resolved, or how many systems are patched on time.

4. 💰 Value Delivery

Ensuring that **security investments provide measurable benefits**, aligning with and supporting the organization’s business goals.

🔹 *Example*: Investing in cloud security tools not just for compliance, but to safely expand remote work capabilities.

Alignment of Security Function to Strategy, Goals, Mission, and Objectives

Information security management ensures that the **right policies, procedures, standards, and guidelines** are put in place and actively followed, so that business operations are carried out with an **acceptable level of risk**.

🔹 *Example*: Ensuring access control policies are applied across departments to prevent unauthorized data access.

🏛️ Leadership & Governance Go Hand-in-Hand

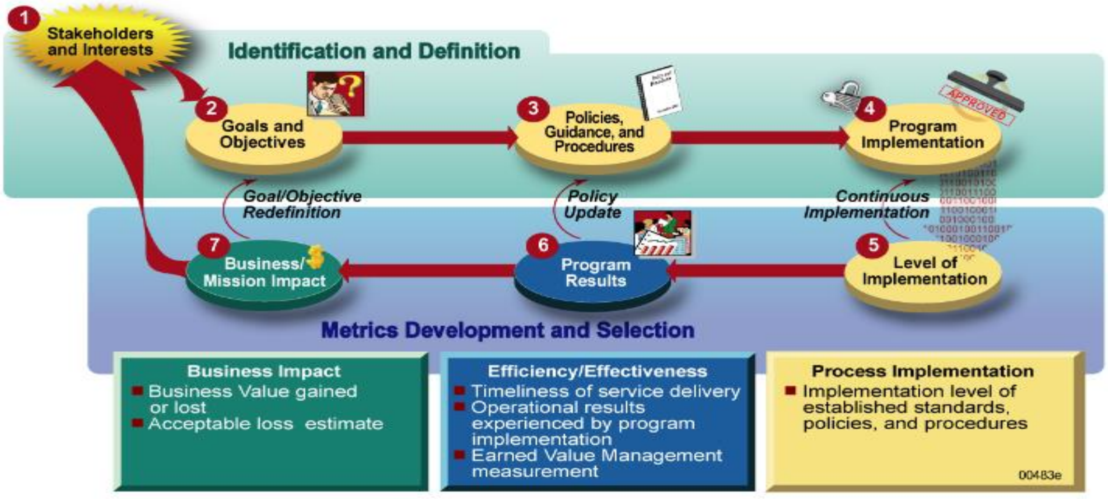
Strong security governance is a sign of **senior leadership’s commitment** to managing risk in a consistent and effective way throughout the organization.

◆ *Example*: When top management reviews and approves security strategy annually, it shows they're actively supporting a secure culture.

🎯 Security as a Business Enabler

The role of security is not just protection—it's to **support and drive the organization’s mission, goals, and vision** by ensuring trust, continuity, and compliance.

◆ *Example*: A financial firm’s security controls enable safe mobile banking, aligning with its digital transformation goals.



1 Stakeholders and Interests
Identification and Definition
2 Goals and Objectives
3 Policies, Guidance, and Procedures
4 Program Implementation
APPROVED
Goal/Objective Redefinition
Policy Update
Continuous Implementation
7 Business/ Mission Impact
6 Program Results
5 Level of Implementation
Metrics Development and Selection
Business Impact
■ Business Value gained or lost
■ Acceptable loss estimate
Efficiency/Effectiveness
■ Timeliness of service delivery
■ Operational results experienced by program implementation
■ Earned Value Management measurement
Process Implementation
■ Implementation level of established standards, policies, and procedures
00483e

Approach to Security Management

Approach to Security Management: Top-Down vs. Bottom-Up

▲ Top-Down Approach – Leadership-Driven Security

In a **Top-Down** approach, **senior management** leads the security program. Decisions, policies, and funding start at the top and flow downward through middle management to technical and operational staff.

✅ Key Characteristics:

- **Leadership-Initiated**: Executives define security strategy.
- **Policy-Driven**: High-level policies are crafted before implementation.
- **Budget Support**: Security gets proper funding and attention.
- **Compliance-Oriented**: More likely to meet regulations and standards.

🏢 Real-World Example:

A CISO presents a risk report to the board showing threats to cloud infrastructure.
▶□ The board approves funding for a new **Cloud Access Security Broker (CASB)**.
▶□ IT then implements the solution organization-wide.

🎯 Why It’s Preferred (CISSP Viewpoint):

Top-down shows **executive commitment** and ensures that security is aligned with the organization’s **mission, goals, and risk appetite**.
□ This is the **ideal approach** for any mature security program.

▼ Bottom-Up Approach – Technician-Initiated Security

In a **Bottom-Up** approach, **technical teams** or IT staff initiate security practices without formal direction or support from leadership.

⚠□ Key Characteristics:

- **IT-Led**: Engineers or admins implement controls they think are needed.
- **Limited Authority**: Security initiatives may lack official endorsement.
- **Low Visibility**: May not align with broader business goals.
- **Reactive**: Often responds to threats after incidents happen.

🔧 Real-World Example:

A system admin installs a firewall without any security policy or guidance from leadership.
▶□ It works technically, but lacks proper change control, documentation, or enterprise alignment.

🚫 Why It’s Risky:

Without **top-level backing**, security lacks direction, consistency, and legitimacy. It's hard to get funding, enforce policies, or integrate security into the business.

Security Budget – Planning and Justifying Investments in Security

---

🏗️ Security is Cheaper When Built-in, Not Bolted-on

Designing security **from the start** is far more cost-effective than adding it later as a patch or fix.

🔧 Example:

- ● **Without planning**: A software application is deployed, and later it’s discovered that it doesn’t encrypt sensitive user data. ▶️ Now the company must re-engineer the software, delaying releases and increasing costs.
- ✅ **With built-in security**: Encryption requirements are included in the design phase. The cost is minimal and no rework is needed.

□ **Takeaway**: **"Shift left" in security**—include it early in the design to reduce risk and cost.

📊 Factors That Influence Security Budgeting

1. ### 👨‍💻 Number of Staff

    More employees = more endpoints, more access controls, more training.

    - *Example*: A startup with 20 users may need only basic endpoint protection, while a company with 2,000 users requires enterprise-level IAM and monitoring tools.

---

2. ### 🔐 Level of Protection Required

The more sensitive the data or critical the systems, the higher the security standards.

- *Example*: A hospital managing electronic health records (EHR) must comply with **HIPAA** and invest in strong encryption and access control systems.

---

3. 📝 Tasks to Be Performed

The complexity and volume of security operations affect the needed tools and staff.

- *Example*: If daily log review and threat hunting are needed, the company may need a **SIEM solution** and analysts to monitor it.

---

4. ⚖□ Regulations to Be Met

Compliance with laws (e.g., GDPR, PCI DSS, SOX) may require specific technologies, audits, or reporting.

- *Example*: A company processing credit cards must invest in tools and processes to comply with **PCI DSS**, like secure storage, logging, and access tracking.

---

5. 🎓 Staff Qualification Level

Highly skilled professionals may demand higher salaries but reduce risks more effectively.

- *Example*: Hiring a certified penetration tester or CISO might be costly, but they can prevent expensive breaches.

---

6. □ Training Required

All employees need awareness training, while technical staff require specialized instruction.

    - *Example*: Regular phishing simulations and training for all employees to reduce social engineering risks.

Organizational Processes – Security Considerations in Business Change

When businesses change structure—whether growing, shrinking, or restructuring—**information security must adapt** to protect assets, data, and people throughout the transition.

🔄 1. Acquisitions and Mergers

In an **acquisition**, one company buys another. In a **merger**, two companies combine to form a new entity.

🔐 Security Concerns:

- Incompatible or conflicting security policies and tools
- Unknown vulnerabilities in the acquired organization’s infrastructure
- Data integration risks (especially PII or regulated data)
- Access control misconfigurations

□ CISSP Example:

Company A acquires Company B, which stores customer data in a non-encrypted format.
▶□ Company A’s security team must:

- Perform a **security risk assessment**
- Align Company B’s infrastructure with its own policies
- Ensure compliance with applicable laws like GDPR or HIPAA

✔ Best Practice:

Always conduct **due diligence** before finalizing a deal—evaluate security posture, compliance status, and third-party risks.

✂□ 2. Divestitures and Spinoffs

A **divestiture** is when a company sells off a part of its business. A **spinoff** is when a unit becomes an independent company.

🔐 Security Concerns:

- Separation of IT systems and access
- Data classification and ownership conflicts
- Retaining confidentiality of intellectual property (IP)
- Ensuring secure transfer or deletion of shared assets

□ CISSP Example:

A large tech company spins off its cloud business into a new entity.
▶□ The security team must:

- Ensure only necessary data is transferred
- Wipe shared servers of old tenant data
- Provide the new company with its own identity management and policies

📌 CISSP Exam Tip:

The **security posture of the merged/spun-off organization must be at least as strong** as the original, or else it's a security downgrade.

🛠□ Key Areas to Review During These Processes:

- Physical Security 🏢 (e.g., access control to new or shared facilities)
- Technical Security 🔐 (e.g., firewalls, encryption, IAM)
- Disaster Recovery 🎁 (e.g., whether BCP/DRP plans are updated)

- Policies & Awareness 📄 (e.g., educating new users on the org's security culture)

Security Officer Reporting Models

Responsibilities of the Chief Information Security Officer

- Accountable for ensuring the protection of all of the business information assets from information assets from intentional and unintentional loss, disclosure, alteration, destruction, and unavailability

Chief Information Security Officer Reporting Models:

The effectiveness of a security program often depends on **where the Security Officer (like a CISO)** reports in the organizational hierarchy. The reporting line impacts **independence**, **authority**, and **visibility** of security operations.

1️⃣ Reporting to the CEO (Chief Executive Officer)

✅ **Best Practice in Mature Organizations**

Pros:

- Direct access to top leadership
- High authority and visibility
- Less conflict of interest

Cons:

- CEO may lack technical background to fully evaluate security decisions

Example:

In a financial firm, the CISO reports directly to the CEO to ensure **executive-level support** and prioritization of cybersecurity initiatives like compliance with SOX or PCI DSS.

2️⃣ Reporting to the IT Department (CIO or CTO)

⚠️ Most common, but not ideal

Pros:

- Easier alignment with IT teams
- Technical collaboration

Cons:

- Potential **conflict of interest**—security decisions may be deprioritized in favor of business convenience
- Lack of independence

Example:

In a small company, the Security Officer reports to the CIO, but struggles to enforce security policies when the IT team resists changes due to project deadlines.

3️⃣ Reporting to the Administrative Services Department

💼 Operational Alignment

Pros:

- Integration with other business support functions like HR, Facilities

Cons:

- May lack adequate technical insight
- Limited strategic alignment

Example:

A university's CISO reports to the head of Admin Services, handling policies like **data privacy training**, but lacks access to drive infrastructure-level decisions.

4️⃣ Reporting to the Insurance and Risk Management Department

🛡️ Good for Risk-Focused Organizations

Pros:

- Aligns security with enterprise risk management (ERM)
- Emphasizes threat prevention and liability reduction

Cons:

- May overlook operational IT realities

Example:

In a healthcare company, the Security Officer reports to the Risk Manager to ensure security investments reduce liability under **HIPAA** and **malpractice risks**.

5️⃣ Reporting to the Internal Audit Department

🔍 Ensures Independence

Pros:

- Strong separation from IT and business units
- Good for compliance monitoring

Cons:

- May lack proactive, hands-on involvement
- Focused more on detection than prevention

Example:

At a multinational bank, the InfoSec Officer reports to Internal Audit, helping conduct **SOX audits** and review controls without influence from operational departments.

6️⃣ Reporting to the Legal Department

⚖️ Focused on Compliance and Incident Liability

Pros:

- Strong alignment with legal obligations and breach response
- Supports data privacy laws (e.g., GDPR, HIPAA)

Cons:

- May treat security purely as a legal checkbox, not a strategic function

Example:

In a tech firm with high privacy risk, the CISO reports to Legal, ensuring all **Data Protection Agreements (DPAs)** and **incident response policies** meet regulatory standards.

📌 CISSP Exam Tip:

The **most effective reporting model** is when the **CISO reports directly to the CEO or Board**, ensuring independence and alignment with organizational goals.

Accountability vs. Responsibility in Information Security:

Concept	Definition	Who?	Action Type
Accountability	Being **ultimately answerable** for outcomes. The one who **owns** the decision or result.	Usually **one person or role**	**Owns the result**
Responsibility	Being **in charge of performing** a task or duty. The one who **executes** or implements.	Often **multiple individuals**	**Executes the task**

🔐 Accountability

Accountability means **ownership**. If something goes wrong, the accountable person is the one who must answer for it—even if they didn't perform the task directly.

✅ **Key Points:**

- Involves **oversight** and **decision-making**
- Includes **setting rules, approving policies**
- Typically lies with **senior roles**: CEO, CISO, Data Owner

□ **Example (CISSP Context):**

- The **CISO** is accountable for the organization's overall security program.
- If a breach occurs due to a missed patch, the CISO must explain **why controls failed**, even if the patching was the IT team's responsibility.

□ Responsibility

Responsibility refers to the **execution** of specific actions or tasks. The responsible party **does the work**, but doesn't own the final outcome.

✅ **Key Points:**

- Involves **implementation and maintenance**
- Assigned to technical or operational staff
- Multiple people can share responsibility

□ **Example (CISSP Context):**

- A **network administrator** is responsible for **configuring firewalls**.
- A **security analyst** is responsible for **monitoring alerts**.

But — neither of them is **accountable** if the security program fails — that falls to leadership.

📌 CISSP Exam Tip:

Accountability cannot be delegated, but **responsibility can**.
You can assign a task to someone, but the person accountable **still owns the outcome**.

Liability, Due Care & Due Diligence:

Liability refers to the organization’s **legal responsibility** to protect its data, systems, and stakeholders.
If an organization **fails to implement reasonable security controls**, and a breach occurs, it could be held **legally liable** for the damages.

Term	What It Means	Real-World Example
Due Diligence	Investigate risks before acting	Reviewing vendor's security audits before contracting
Due Care	Taking responsible protective action	Enforcing security awareness training for all staff
Prudent Man Rule	Act like a reasonable, informed person	Ensuring timely patching and backups are in place

2. Due Care – "Doing the Right Thing"

Due Care is about **taking reasonable action** to protect others. It's the **standard of behavior** expected from a responsible organization or individual in a given situation.

🔍 Key Idea:

What a **prudent person** would do under the same circumstances.

□ Example:

- A company installs **firewalls, antivirus, and user access controls** to protect customer data.
- These are actions taken to show **due care** and fulfill its responsibility to customers and regulators.

🔎 3. Due Diligence – "Investigate Before You Act"

Due Diligence means doing your **homework before making decisions**—you investigate risks and gather facts.

□ Example:

- Before choosing a cloud service provider, a company:
  - Reviews their **security certifications**
  - Reads past **audit reports**

  - Assesses data center locations and legal jurisdiction

That’s **due diligence** — making sure the vendor is trustworthy **before signing the contract**.

COMPLIANCE

GDPR is a comprehensive **data protection and privacy law** implemented by the **European Union (EU)**.
It governs how organizations **collect, store, process, and transfer personal data** of individuals within the EU/EEA.

✓ Applies To:

- All organizations that **handle personal data** of **EU residents**, regardless of where the organization is located (yes, even U.S.-based companies).
- Applies to **data controllers** and **data processors**.

Term	CISSP Definition
Data Subject	The **individual** whose personal data is being collected (e.g., an EU citizen)
Data Controller	The **entity that decides** why and how personal data is processed
Data Processor	The **third party or vendor** that processes data **on behalf of** the controller
Personal Data	Any data that can **identify a person** (e.g., name, email, IP address, photo)
Sensitive Data	Includes race, health info, sexual orientation, religious beliefs, etc.
Consent	Must be **freely given, specific, informed, and unambiguous**
Data Breach Notification	Controllers must notify authorities within **72 hours** of discovering a breach
Right to Be Forgotten	Individuals can request deletion of their personal data
Right to Access	Individuals can request a copy of their data held by the controller

Term	CISSP Definition
Data Protection Officer (DPO)	Mandatory for certain organizations to **oversee GDPR compliance**

Security Requirements under GDPR

- Ensure **confidentiality, integrity, and availability** of personal data
- Implement **appropriate technical and organizational measures** (like encryption, access control)
- Conduct **Data Protection Impact Assessments (DPIAs)** for high-risk processing
- Use **privacy by design and by default** principles

💶 Penalties for Non-Compliance

Organizations can be fined **up to €20 million** or **4% of their global annual revenue**, whichever is higher.

📚 Real-World CISSP Example:

A U.S. e-commerce company collects email addresses and shipping info from EU customers. Under GDPR, they must:

- Get **clear consent**
- Secure the data using **encryption**
- Allow users to **access or delete their data**
- Report any **breach within 72 hours** to EU data authorities

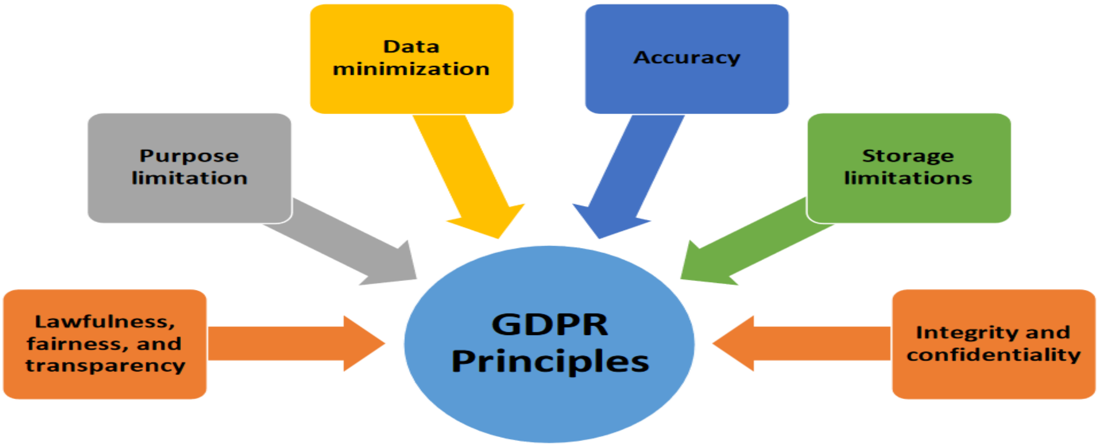
---

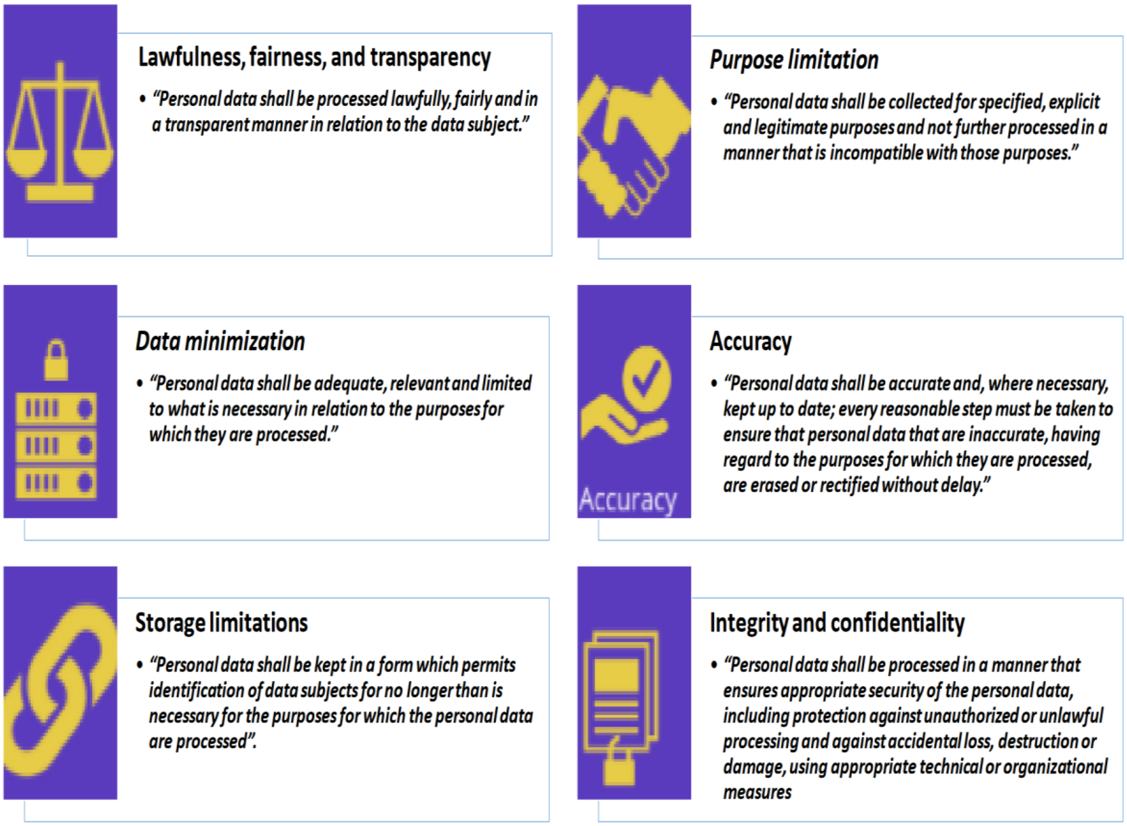
▯ CISSP Exam Tip:

GDPR emphasizes **data subject rights, breach notification**, and **shared responsibility** between controllers and processors.
Expect exam questions around:

- "Who is responsible in a breach?"
- "What is the response window?"
- "Which security measures are considered 'appropriate'?"

Concept	Key GDPR Requirement
Data Breach Notification	72 hours to report to authorities
Consent	Must be explicit, informed, and clear
Data Subject Rights	Access, Correction, Deletion
Privacy by Design/Default	Security baked into systems from the start
Penalty for Non-compliance	Up to €20M or 4% of global revenue





Lawfulness, fairness, and transparency

- *"Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject."*

Purpose limitation

- *"Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes."*

Data minimization

- *"Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed."*

Accuracy

- *"Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay."*

Storage limitations

- *"Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed".*

Integrity and confidentiality

- *"Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures*

HIPAA is a **U.S. federal law** enacted in 1996 that sets standards for **protecting sensitive patient health information** (PHI – Protected Health Information).

The purpose of HIPAA is to:

- Safeguard the **privacy and security** of health data
- Ensure individuals have **rights over their health information**
- Promote secure **electronic health transactions**

🔍 Who Must Comply with HIPAA?

Role	Definition
Covered Entities	Organizations directly handling PHI — such as **hospitals**, **doctors**, **health insurers**
Business Associates	Vendors that handle PHI **on behalf of covered entities** — e.g., cloud providers, billing companies

What Is Protected Health Information (PHI)?

PHI includes **any health-related data** that can be tied to an individual:

- Name, birth date, SSN
- Medical records, diagnoses, treatments
- Insurance and billing info
- Biometric identifiers (e.g., fingerprints)

□ CISSP Key Components of HIPAA

HIPAA has two major rules CISSP candidates must understand:

□ 1. Privacy Rule

Sets standards for **who can access and share PHI**, and under what circumstances.

- Patients must be informed of their **data rights**
- PHI can't be shared without **consent**, except under specific conditions (e.g., emergencies)
- Applies to both **paper and electronic records**

🔐 2. Security Rule

Requires **administrative, physical, and technical safeguards** to protect **electronic PHI (ePHI)**.

🛠□ Administrative Safeguards:

- Security management process (risk analysis & management)
- Workforce training and management

🏢 Physical Safeguards:

- Facility access controls
- Workstation/device security

💻 **Technical Safeguards:**

- Access control (unique user IDs)
- Audit controls (logging)
- Data encryption
- Integrity controls

□ CISSP Example Scenario:

A healthcare clinic stores patient records in the cloud. To comply with HIPAA, it must:

- Encrypt patient data at rest and in transit
- Restrict access using unique login credentials
- Sign a **BAA** with the cloud provider
- Train employees on PHI handling

⚠□ Non-Compliance Penalties

HIPAA violations can result in:

- Fines ranging from **$100 to $50,000 per violation**
- Criminal charges (in extreme negligence or malicious intent)

📌 CISSP Exam Tip:

HIPAA is about **confidentiality and privacy of health data**.
Expect questions about:

- Responsibilities of **covered entities**
- What qualifies as **PHI**
- What safeguards are required under the **Security Rule**
- **BAA** requirements

Element	Details
Law Name	Health Insurance Portability and Accountability Act (HIPAA)
Primary Focus	Protecting confidentiality, integrity, and availability of PHI
Applies To	Covered Entities + Business Associates
Key Safeguards	Administrative, Physical, Technical

Element	Details
Exam Focus	ePHI protection, BAA, Security/Privacy Rules, breach penalties

The **Gramm-Leach-Bliley Act**, passed in the United States in **1999**, is a federal law that requires **financial institutions** to protect the **privacy and security of customers' personal financial information**.

🏦 Who Must Comply?

Any company that offers financial products or services, including:

- Banks
- Credit unions
- Insurance companies
- Mortgage lenders
- Investment firms
- Some tax preparation and financial advisory services

□ Core Components of GLBA (for CISSP)

GLBA is built around **three main rules** that CISSP candidates must know:

🔐 1. Safeguards Rule

Requires institutions to implement a **comprehensive written information security program** to protect customer data.

✅ Key Requirements:

- Design and enforce **administrative, technical, and physical safeguards**
- Conduct **risk assessments** on systems and data
- Monitor and test security programs regularly
- Train staff and manage vendor security

□ **CISSP Focus:**

Think about this like a **mini security program**—risk management, policies, access controls, audits, etc.

🔒 2. Privacy Rule

Controls how **nonpublic personal information (NPI)** is collected, disclosed, and protected.

✅ **Key Requirements:**

- Inform customers about what personal data is collected
- Explain how data is shared
- Offer customers the **right to opt out** of sharing their information with non-affiliated third parties

□ **CISSP Focus:**

Similar to **data classification and handling**—customers must know how their data is used and be given choices.

📜 3. Pretexting Rule

Prohibits the **use of social engineering** (pretexting) to access private information.

✅ **Example:**

- An attacker pretending to be a bank customer to trick a call center agent into releasing account information.

□ **CISSP Focus:**

Ties into **awareness training, social engineering defense, and identity verification protocols**.

Real-World CISSP Example:

A bank holds sensitive financial data (account numbers, credit scores).
Under GLBA, they must:

- Encrypt sensitive data and restrict access (Safeguards Rule)
- Provide a privacy notice to customers explaining data use (Privacy Rule)
- Train employees to spot phishing or impersonation (Pretexting Rule)

⚠️ Non-Compliance Penalties

- Civil penalties: Up to **$100,000 per violation**
- Officers and directors may be fined **personally up to $10,000** and face imprisonment

---

📌 CISSP Exam Tip:

GLBA = Financial Data + Safeguards + Customer Privacy.
Expect questions like:

- “Which rule requires a security program?” → **Safeguards Rule**
- “Which rule prohibits social engineering?” → **Pretexting Rule**

SOX:

The **Sarbanes-Oxley Act of 2002 (SOX)** is a **U.S. federal law** passed to prevent corporate accounting fraud and improve the accuracy and reliability of **financial disclosures**.

It was enacted in response to high-profile financial scandals (e.g., Enron, WorldCom).

🎯 Purpose of SOX

- Ensure **corporate accountability** and **transparency**
- Prevent **fraudulent financial reporting**
- Improve **internal controls** over financial systems and reporting

While SOX is **not an IT security law**, it significantly affects **information systems** because financial data must be:

- **Confidential**
- **Accurate (Integrity)**
- **Available for auditing**

That ties directly into the **CIA triad**!

FISMA is a **U.S. federal law** that requires all **federal agencies** (and their contractors) to develop, document, and implement an **information security program** to protect sensitive information and systems.

Originally enacted in **2002** as part of the **E-Government Act**, and later updated as **FISMA 2014** to address evolving cyber threats.

🎯 Purpose of FISMA:

- Protect **U.S. government information systems** from threats and vulnerabilities
- Establish a **risk-based approach** to information security
- Ensure agencies are **accountable** for securing their systems
- Provide a framework for **continuous monitoring and compliance reporting**

🏢 Who Must Comply with FISMA?

- All **federal agencies**
- **Contractors** working with federal agencies
- **Third-party service providers** handling federal data

□ **CISSP Insight**: If a private company hosts or manages systems containing U.S. government data, **FISMA compliance applies**.

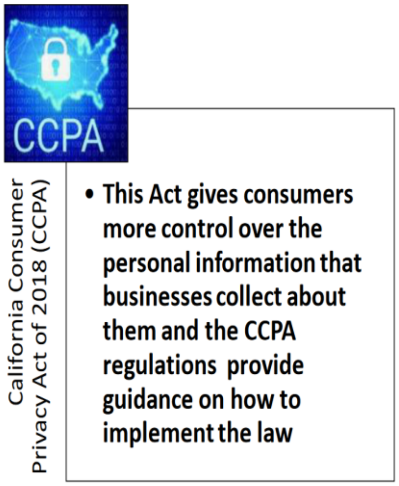
The **California Consumer Privacy Act (CCPA)** is a **state-level privacy law** that grants **California residents** rights over how their personal information is **collected, used, and shared** by businesses.

✓ Who Must Comply with CCPA?

Applies to **for-profit** businesses that:

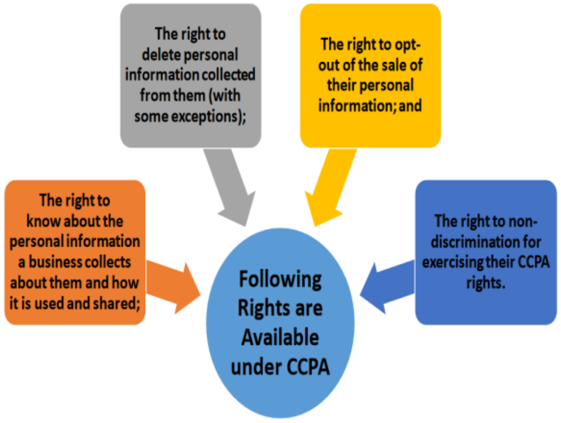
- Collect personal information of **California residents**
- Do business in California
- Meet **one or more** of the following:
    - Have **$25 million+ annual gross revenue**
    - Buy, sell, or share data of **50,000+ consumers, households, or devices**
    - Earn **50%+ of revenue** from selling personal information

Right	Description
Right to Know	Consumers can ask what personal data is collected, used, shared, or sold
Right to Delete	Consumers can request deletion of personal data (with exceptions)
Right to Opt-Out	Consumers can **opt-out of the sale** of their data
Right to Non-Discrimination	Businesses can't discriminate against users for exercising their rights



California Consumer Privacy Act of 2018 (CCPA)

- This Act gives consumers more control over the personal information that businesses collect about them and the CCPA regulations provide guidance on how to implement the law



The right to know about the personal information a business collects about them and how it is used and shared;

The right to delete personal information collected from them (with some exceptions);

The right to opt-out of the sale of their personal information; and

The right to non-discrimination for exercising their CCPA rights.

Following Rights are Available under CCPA

Intellectual Property Laws

Protecting products of the mind is about securing intangible creations — ideas, inventions, brands, etc.
Companies **must actively protect** these resources, or else legal protections may be weakened or lost. For example, if a company doesn't enforce their trademark, they might lose exclusive rights over it.

There are **four major types of Intellectual Property (IP) Laws**:

1. Trade Secret

- **What it protects**: Confidential business information that gives a company a competitive edge.
- **Examples**:
  - Coca-Cola's secret formula

    - Google's search algorithm
    - KFC’s spice blend recipe
- **Key point**: To be a *trade secret*, the company must *actively keep it secret*.
  If it leaks and they haven't taken steps (like NDAs or access controls), they can lose protection.

---

2. Copyright

- **What it protects**: The **expression of ideas**, *not the ideas themselves*.
- **Examples**:
    - A song written by Taylor Swift (lyrics and melody are protected, but "singing about love" isn’t)
    - Software source code
    - Books, paintings, movies
- **Rights granted**:
    - Control over reproduction, distribution, public performance, and derivative works.
- **Important to note**:
    - **Copyright is weaker** in terms of what it protects compared to patents but **lasts longer**.
    - Typical duration: **Lifetime of the author + 70 years** (varies slightly by country).

---

3. Patent

- **What it protects**: New inventions that are **novel**, **useful**, and **non-obvious**.
- **Examples**:
    - Apple's multi-touch iPhone interface
    - Pharmaceutical drugs (e.g., Pfizer's patent on a new vaccine)
    - New manufacturing processes
- **Strongest form of IP protection** but **shortest time**:
    - Generally **20 years** from the application date.
- **Important**:
    - Once a patent expires, anyone can use the invention freely.

---

4. Trademark

- **What it protects**: Marks that distinguish a company's goods or services.
- **Examples**:
  - The Nike "swoosh" logo
  - The McDonald's golden arches
  - The shape of a Coca-Cola bottle
  - Even specific sounds (e.g., Intel's chime sound) and colors (Tiffany Blue)
- **Purpose**: Protect **goodwill and brand identity**.
- **Key point**: Trademarks can last **indefinitely** as long as they are actively used and defended.

Quick Comparison Table

Type of IP	Protects	Duration	Examples
Trade Secret	Confidential business info	As long as secret	Coca-Cola recipe, Google's algorithm
Copyright	Expression of ideas	Life + 70 years	Books, movies, source code
Patent	Invention	20 years	New drug formula, new device design
Trademark	Brand identifiers	Indefinite (with use)	Nike logo, Intel sound, Coca-Cola bottle

---

Summary Points:

- Companies must **proactively protect** their IP.
- **Trade Secrets** need **confidentiality**.
- **Copyright** protects **expression**, not the **idea**.
- **Patents** are **strong**, but limited in time.
- **Trademarks** protect **brand image** and can last forever if properly maintained.

Export/Import Restrictions

When dealing with **cryptographic products** (like encryption software, devices, algorithms), governments regulate their movement **across borders** to maintain **national security** and **international stability**.

If companies or individuals fail to follow these regulations, they could face **serious legal penalties**, including heavy fines or criminal charges.

There are **two main areas**:
✅ Export Restrictions
✅ Import Restrictions

Export Restrictions

1. Wassenaar Arrangement (1996)

- **What it is**:
  A voluntary agreement among 42 participating states (like the US, Japan, Germany, etc.)
  It controls the export of **conventional arms** and **dual-use goods and technologies** (technology that can be used both for civilian and military purposes).
- **Purpose**:
  - Prevent the spread of military technology that could threaten **regional or international peace**.
  - Specifically **makes it illegal** to export **munitions** (weapons and military-grade technology) to **terrorist-sponsored nations**.

2. Cryptography and Export Rules

- You **can** export **cryptographic software** to **non-government end-users** (like private companies and individuals) in many countries.
  - **Example**: A U.S. cybersecurity company selling encryption software to a private bank in Germany.
- **You cannot** export **strong encryption technologies** to **terrorist states**.
  - **Example**: No selling encryption tools to countries under sanctions like North Korea or Iran.

Import Restrictions

1. Control on Cryptographic Imports

- Some countries allow import of strong encryption tools **only if** companies give a **copy of private keys** to **law enforcement** (called "key escrow" or "government access").
- Purpose:

    - Helps the government **decrypt** communications if needed for national security investigations.
- **Example**:
  In some Middle Eastern countries, if a company imports strong VPN or encryption software, they might be forced to give the government access keys for surveillance purposes.

2. Understanding Legal Obligations

- Companies must **know the laws** in both their own country and the destination country.
- **Example**:
    - A U.S. company exporting security products to China needs to check if:
        - U.S. law allows it.
        - Chinese law imposes extra requirements.

US Safe Harbor Laws

- (Note: In your points, you mentioned Safe Harbor — here's clarification)
- Originally, **Safe Harbor** was an agreement between the US and Europe to allow **transfer of personal data** between them under privacy protections.
- **However**, it was invalidated and replaced by the **Privacy Shield** and later **other mechanisms**.
- **For CISSP exams**, focus is mainly on **how organizations must comply with privacy and data protection laws across borders**.

Summary Table

Area	Main Idea	Example
Wassenaar Arrangement	Control on military and dual-use exports	No exporting encryption to terrorist states
Exporting Crypto	Allowed to non-government users, not terrorists	US company sells software to Germany, not Iran
Importing Crypto	Some countries require private keys for law enforcement	Importing VPNs in UAE needs government access
Understanding Requirements	Know the import/export laws before doing business	Export control checklist before selling internationally

Key Takeaways

- **Wassenaar Arrangement** controls dangerous tech exports.
- **Cryptography export** is regulated based on who receives it.
- **Import laws** might require handing over **private keys**.
- Companies must **understand international legal requirements** to avoid serious penalties.

Digital Rights Management (DRM)

What is DRM?

- **Digital Rights Management (DRM)** is an **internal security layer** used within organizations to control access to sensitive files and datasets, particularly those containing **proprietary** or **confidential** material.
- It ensures that only **authorized users** can access, use, or modify the protected content.

⍰ **Example:**
A financial firm uses DRM to protect its quarterly earnings reports, ensuring only the board of directors can access them before public release.

DRM Solution Traits

Here are key traits of a **strong DRM solution**:

Trait	Description	Example
Persistency	Protection stays with the file no matter where it goes (email, USB, cloud).	A protected PDF sent via email remains encrypted and restricted.
Continuous Audit Trail	Tracks and logs all user activities related to the file (view, edit, share).	An audit log shows that Manager A accessed the document at 10 AM and printed it.
Dynamic Policy	Admins can **modify or**	If an employee resigns,

Trait	Description	Example
Control	**revoke** permissions **after distribution.**	their access to confidential files is instantly revoked.
Interoperability	DRM works seamlessly across different platforms and devices.	A protected file can be opened securely on Windows, Mac, and smartphones.
Automatic Expiration	Files can be set to **expire** or **become inaccessible** after a set time.	A marketing document becomes unreadable 7 days after it's sent to vendors.

DRM Requires Local Agent

Many DRM systems require a **local agent** (small software) installed on endpoint devices like:

- Laptops
- Desktops
- Mobile devices

▯ **Example:**
A company installs a DRM agent on employees' laptops, ensuring documents can only be accessed through an authenticated, monitored channel.

DRM for Copyright Protection

Beyond internal files, DRM is widely used to **protect copyrighted works**, such as:

- E-books

- Movies
- Music
- Software

It helps to:

- **Prevent unauthorized use**
- **Block illegal modification and distribution**

⍰ **Example:**
Amazon Kindle books use DRM to prevent users from copying or sharing purchased books outside of their accounts.

Digital Watermarks

- **Digital watermarks** are **hidden identifiers** embedded in media files (audio, video, images).
- They **don't stop copying**, but **help detect unauthorized copies** and **prove ownership**.

⍰ **Example:**
A movie studio releases a pre-screening copy of a film to select reviewers, each with a unique invisible watermark.
If the movie leaks online, the watermark helps trace the leak back to the responsible reviewer.

Purpose:

- Copyright enforcement
- Legal prosecution against piracy

UNDERSTAND PROFESSIONAL ETHICS

1. Exercise (ISC)^2 Code of Professional Ethics

As a **CISSP-certified professional**, you are **required** to follow the **(ISC)^2 Code of Ethics**.

- This ensures:
- Public trust
- Integrity
- Ethical behavior across all activities

✓ **Example:**
If you find a critical vulnerability in a client's network, you should **report it honestly** — even if the client might not like hearing it.

(ISC)^2 Code of Ethics Canons

All CISSPs must prioritize these four canons:

Canon	Explanation	Example
Protect society, the commonwealth, and the infrastructure	Ensure your actions benefit the public and secure systems vital to society.	You refuse to work on a project that would create spyware harming citizens privacy.
Act honorably, honestly, justly, responsibly, and legally	Uphold strong moral principles and follow the law.	You refuse to use pirated software in a project, even if it saves money.

Canon	Explanation	Example
Provide diligent and competent service to principals	Serve your employer or clients carefully, skillfully, and truthfully.	You take necessary cybersecurity training to stay updated and provide quality advice.
Advance and protect the profession	Support ethical behavior and promote cybersecurity as a respected field.	You mentor junior cybersecurity professionals to grow ethical expertise in the industry.

SECURITY POLICY, STANDARDS, PROCEDURES

Policy

1. □ Policy

- A **policy** is a **high-level document** that outlines **management's goals, expectations, and security priorities**.
- It’s **mandatory** and **sets the tone** for security governance.

□ **Example:**

> ″All company servers must be properly hardened before being put into production.″

- Policies are the **foundation** for everything else — standards, procedures, baselines, and guidelines.

2. □ Standards

- **Standards** are **mandatory** requirements that specify:
  - ◆ Technologies

  - Configurations
  - Products

- They help ensure **consistency** and **compliance** across the organization.

⍰ **Example:**

> ″All administrators must use Windows Server 2022 as the base operating system for production servers.″

- Standards **support policies** by giving clear, specific mandates.

---

3. □ Procedures

- **Procedures** are **step-by-step instructions** on **how to implement a standard or a policy**.
- They are **mandatory** and provide **explicit, repeatable steps**.

⍰ **Example:**

> ″Apply the Windows 2022 security template using these exact steps whenever a new server is installed.″

- Procedures ensure that tasks are performed **consistently and correctly**.

---

4. ⍰ Baselines

- **Baselines** define the **minimum acceptable level of security** for systems or services.
- They **standardize security settings** and serve as a **starting point**.

⍰ **Example:**

> ″All Windows Server 2022 deployments must match the CIS Level 1 Benchmark.″

- You can always **increase security above the baseline**, but **never go below** it.

5. Guidelines

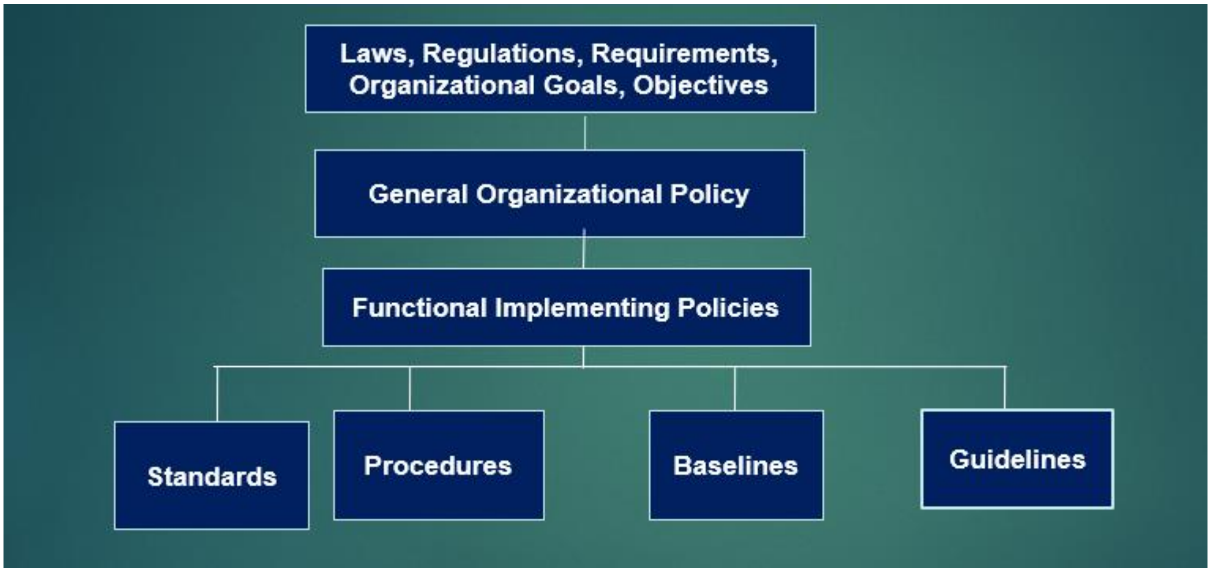
- **Guidelines** are **recommended practices** (not mandatory).
- They offer **advice** to help personnel and system users **secure systems effectively**.

 Example:

> ″It is recommended to use Group Policy Objects (GPOs) to ease the application of security templates.″

- Guidelines are **best practices** — follow them unless there's a good reason not to.

Management’s Security Statement



Laws, Regulations, Requirements, Organizational Goals, Objectives

General Organizational Policy

Functional Implementing Policies

Standards

Procedures

Baselines

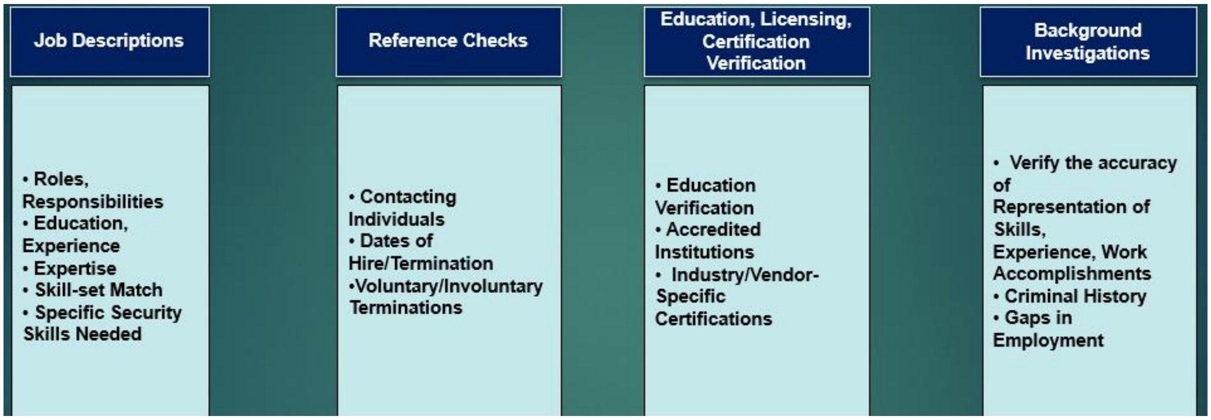
Guidelines

CONTRIBUTE TO PERSONNEL SECURITY POLICIES

Module Topics

Personnel security is **critical** because employees, vendors, and contractors can either **protect** or **threaten** information security.

Candidate Screening



Job Descriptions	Reference Checks	Education, Licensing, Certification Verification	Background Investigations
• Roles, Responsibilities • Education, Experience • Expertise • Skill-set Match • Specific Security Skills Needed	• Contacting Individuals • Dates of Hire/Termination •Voluntary/Involuntary Terminations	• Education Verification • Accredited Institutions • Industry/Vendor-Specific Certifications	• Verify the accuracy of Representation of Skills, Experience, Work Accomplishments • Criminal History • Gaps in Employment

Employment Candidate Screening

- Before hiring, **background checks** are conducted to assess risks.
- Screening might include:
  - ◆ Criminal record checks
  - ◆ Reference verification
  - ◆ Education verification
  - ◆ Employment history

⍰ **Example:**
A finance company screens candidates for any history of fraud or financial misconduct before hiring them.

Employment Agreements and Policies

Every employee should **sign and agree** to several **security-related documents**:

Document	Purpose	Example
Code of Conduct	Defines acceptable and unacceptable behavior at work.	Prohibiting harassment or insider trading.
Conflict of Interest Policy	Ensures employees disclose situations where their personal interests could conflict with company duties.	Disclosing investments in a vendor company.
Gift-Handling Policy	Defines rules around receiving gifts.	Employees may only accept gifts valued under $50.
Ethics Statements	Promotes honesty, integrity, and legal compliance.	Employees must report unethical behavior.
Non-Disclosure Agreement (NDA)	Protects confidential information from unauthorized sharing.	Engineers must not share project designs externally.
Non-Compete Agreement	Restricts employees from working for competitors for a period after leaving.	A developer cannot work for a rival tech firm for one year post-resignation.
Acceptable Use Policy (AUP)	Defines how employees can use company IT resources.	″No personal use of company laptops for illegal downloading.″

Separation of Duties

- **No one person should have complete control** over a critical process.
- Forces **collusion** if someone wants to commit fraud, making fraud harder to execute.

□ **Example:**

- **Network Administrator** handles network access.
- **Firewall Administrator** manages firewall rules.
- **System Administrator** handles application installation.

This way, no single person can control **both access** and **security policies**, reducing risk.

Mandatory Vacations

- **Mandatory vacations** mean employees must take consecutive days off.
- Purpose: during absence, **irregular activities** can be detected by others.

⍰ **Example:**
An employee controlling financial transactions goes on leave. Another employee notices unusual patterns like unauthorized money transfers.

- **Irregularities are more visible** when the main actor is absent.

Job Rotation

- **Switch employees** between different roles **periodically**.
- Benefits:
  - Detect suspicious activities
  - Reduce the risk of collusion
  - Ensure backup capability

- Employee skill development

▯ **Example:**
A systems auditor switches places with a compliance officer for a quarter. The auditor notices that access logs were not properly maintained — something the compliance officer overlooked.

Note:

- **Small organizations** may face difficulties rotating jobs (due to specialized skills).
- Here, stronger **supervision and technical controls** must be applied.

Onboarding and Termination Process

Onboarding

When an employee leaves (resignation, firing, retirement), secure **termination** is **critical**:

1. **Lock User Accounts Immediately:**
▯ Example: HR informs IT, and the user's AD account is disabled at the time of termination.
2. **Recover Property:**
▯ Example: Laptops, phones, ID badges are collected.
3. **Exit Interview:**
▯ Example: Understand reasons for leaving, remind about NDA obligations.
4. **Review NDA Obligations:**
▯ Example: Reiterate that even post-employment, disclosure of company secrets is prohibited.

Termination

When a new employee joins, ensure **secure onboarding**:

1. **Review of Contract Terms & Job Role:**
▯ Example: Explain that the employee must comply with all security policies.

2. **Signing NDA:**
   ⍰ Example: New hire signs confidentiality agreements before being granted access.
3. **Formal Initial Security Training:**
   ⍰ Example: Training sessions on password policies, email security, social engineering awareness.
4. **Secure Access Provisioning:**
   ⍰ Example: Systematically create accounts, issue badges, assign least-privilege access.

ESTABLISH AND MANAGE SECURITY EDUCATION, TRAINING, AND AWARENESS

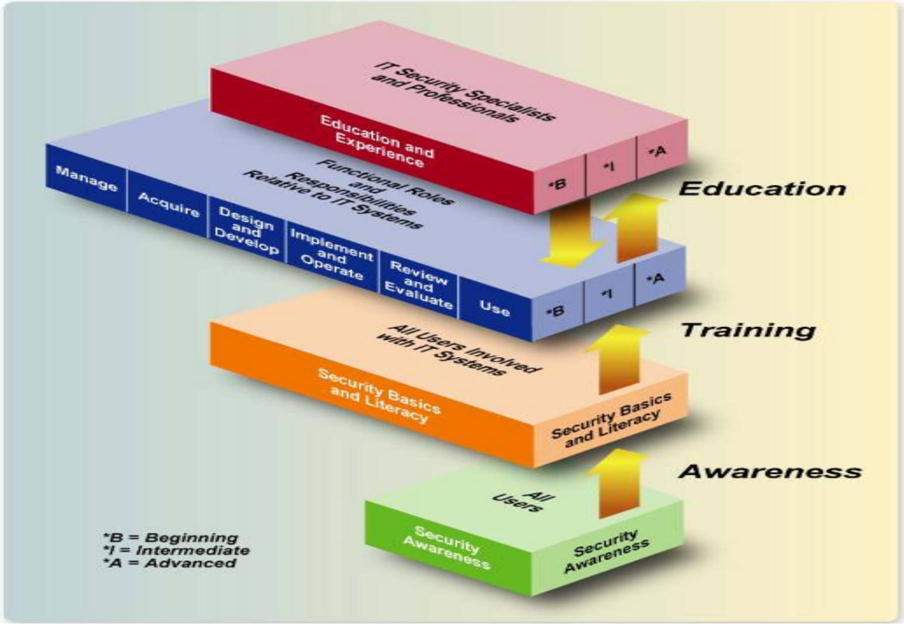
Category	Description	Example
Education	**Formal, structured learning,** often external, through accredited institutions.	A security analyst pursuing a Master's degree in Cybersecurity or CISSP Certification training from an ISC2-accredited center.
Training	**Practical, skill-based sessions** provided internally or by vendors; focuses on specific tasks.	An IT staff member attending an internal session on configuring firewalls.
Awareness	**Informal, lightweight communication**; reminds employees about security behaviors.	Posters reminding users to lock screens; short emails about phishing dangers.

⍰ **Key Points:**

- **Education** ➔Deep Knowledge

- **Training** ➔Task-specific Skills
- **Awareness** ➔Behavioral Reminders

Security awareness and training can often be improved through gamification



Core Areas

Periodic Content Reviews

For **effective security programs**, instruction materials and content must always be **kept current**.

Review and refresh **periodically**:

Area	Why Important	Example
Applicable Laws	Regulations and compliance requirements change over time.	GDPR updates, India’ s DPDP Act, HIPAA updates.

Area	Why Important	Example
Security Tools	New tools, updates, and vulnerabilities emerge.	SIEM updates like Splunk or Microsoft Sentinel improvements.
Organizational Policies	Internal rules must reflect evolving business and risk landscapes.	Updated Remote Work Security Policy after COVID-19.
Recent Attack Styles/Methodologies	Threats evolve (new malware, ransomware variants).	Awareness about phishing campaigns using AI-generated emails.

✓ Example:

Each quarter, the security team updates training materials to include any new phishing techniques seen globally.

Program Effectiveness Evaluation

- **Testing** after security training or education programs is **important** to:
  - Measure effectiveness
  - Confirm understanding
  - Identify gaps for retraining

✓ **Example:**

After VPN usage training, employees take a short quiz to ensure they understand how to connect securely.

UNDERSTAND AND APPLY RISK MANAGEMENT

Risk Management is at the heart of cybersecurity.
It involves **identifying**, **analyzing**, **evaluating**, and **mitigating** risks to protect an organization' s **assets**.

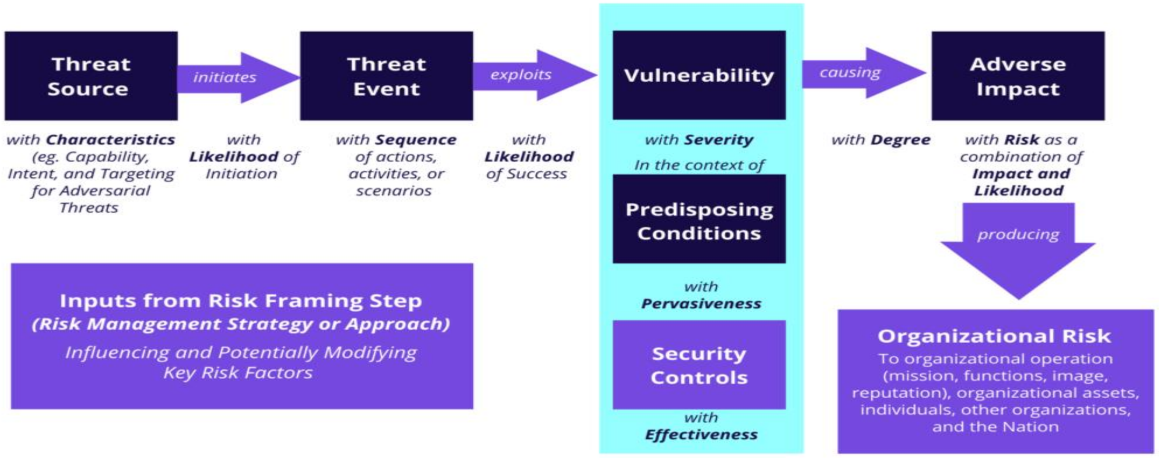
- **Risk Management** = Finding potential dangers and deciding how to deal with them.
- It's about making informed decisions to **balance security and business needs**.

✓ **Example:**
A company recognizes that storing customer data online carries risks and decides to invest in encryption and monitoring.

Risk Management terms:

Concept	Meaning	Example
Threat	Anything that can exploit a vulnerability.	Hacker trying to break into a system.
Vulnerability	Weakness that can be exploited.	Unpatched operating system.
Likelihood	Probability that a threat will exploit a vulnerability.	80% chance a known exploit is used against outdated systems.
Impact	Damage caused if a threat succeeds.	Financial loss, data theft, reputation damage.
Countermeasures	Steps taken to reduce or eliminate risk.	Applying a security patch to fix vulnerabilities.
Residual Risk	Risk that remains even after applying countermeasures.	Even after encrypting data, risk of insider misuse still exists.

Risk Model


Threat Source
initiates
Threat Event
exploits
Vulnerability
causing
Adverse Impact
with Characteristics (eg. Capability, Intent, and Targeting for Adversarial Threats
with Likelihood of Initiation
with Sequence of actions, activities, or scenarios
with Likelihood of Success
with Severity
In the context of
with Degree
with Risk as a combination of Impact and Likelihood
Predisposing Conditions
producing
Inputs from Risk Framing Step
(Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors
with Pervasiveness
Security Controls
with Effectiveness
Organizational Risk
To organizational operation (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation

Risk Management Process

Here’s the **standard process** for risk management:

---

1. Risk Identification

- Finding out **what can go wrong**.

⍰ **Example:**
Identifying that customer data is stored unencrypted.

---

2. Asset Valuation

- **Identify assets** and **assign a value** based on importance to the business.

⍰ **Example:**

- HR database valued at $500,000 due to legal compliance risks if breached.

---

3. Threat Analysis

- Define and understand **potential threats**.

▯ **Example:**

- Threat: Cybercriminals launching phishing attacks.
- Threat Frequency: Monthly attacks observed.
- Consequences: Credential theft, data loss.

---

4. Vulnerability Assessment

- Identify **internal weaknesses** that threats could exploit.

▯ **Example:**
Finding unpatched operating systems during a security scan.

---

5. Risk Analysis

- Two types:

Type	Meaning	Example
Qualitative Risk Analysis	Subjective, ranks risks (High/Medium/Low).	A ransomware threat ranked "High Risk".
Quantitative Risk Analysis	Numbers-based financial risk calculation.	Loss of $50,000 expected annually from potential breaches.

---

6. Risk Evaluation

- Decide **how serious** each risk is, and **prioritize** handling.

⍰ **Example:**
Rank insider threats as "Critical" due to high impact and likelihood.

---

7. Risk Treatment

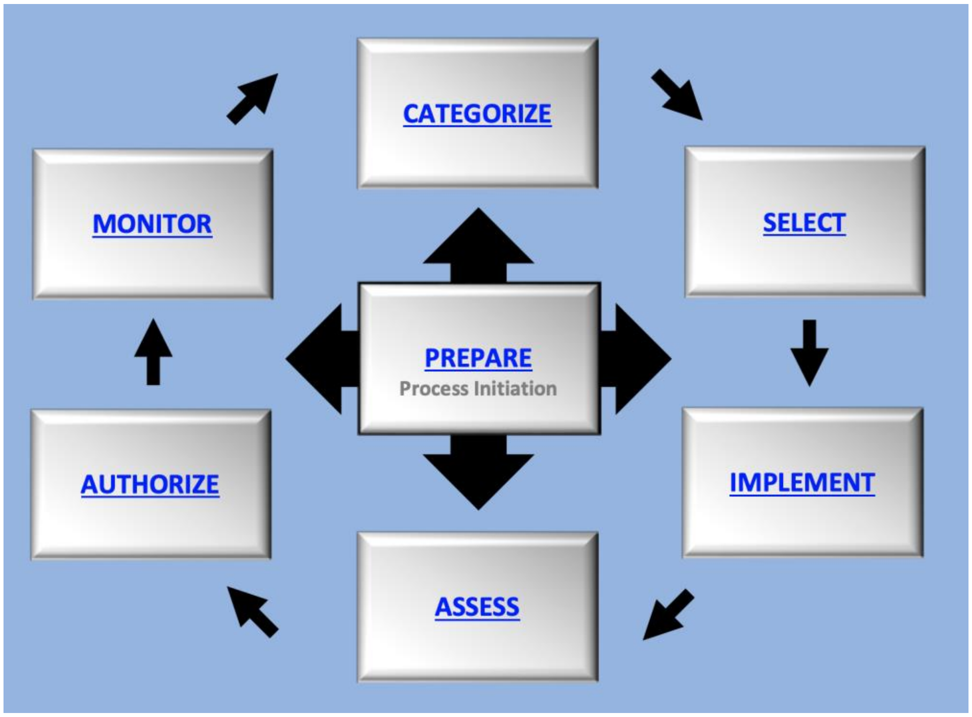
Different ways to manage risk:

Method	Meaning	Example
Risk Reduction	Apply controls to lower the risk.	Install antivirus and firewalls.
Risk Transfer	Shift the risk to a third party.	Buy cybersecurity insurance.
Risk Avoidance	Eliminate the activity causing risk.	Cancel a risky cloud migration plan.
Risk Acceptance	Accept the remaining risk without further action.	Accept risk of non-critical system downtime during updates.

RISK FRAMEWORK

Frameworks guide **structured risk management** in organizations.

NIST SP 800-37 RMF



NIST SP 800-37 - Risk Management Framework (RMF)

Focus: **Federal and critical systems security**
7-Step Process:

Step	Action	Example
Prepare	Set up roles, strategy.	Assign risk officers, establish risk appetite.
Categorize	Identify assets and value.	Mark customer database as High-Impact Asset.
Select	Choose security controls.	Require encryption at rest and MFA.

Step	Action	Example
Implement	Apply selected controls.	Deploy encryption tools and access controls.
Assess	Test effectiveness.	Conduct penetration tests and audits.
Authorize	Senior official accepts residual risk.	CIO approves the launch with documented risks.
Monitor	Continuous evaluation of controls.	Monthly vulnerability scans, update policies annually.

□ **Memory Tip:**

> Prepare ➔ Categorize ➔ Select ➔ Implement ➔ Assess ➔ Authorize ➔ Monitor

ISO 31000 - RISK MANAGEMENT

- **International Standard** for any type of risk, in any industry.
- **8 Principles** focus on:
  - ◆ Structured approach
  - ◆ Integration into all business processes
  - ◆ Continual improvement
  - ◆ Decision-making support

□ **Example:**
An airline company uses ISO 31000 to manage operational risks like flight delays and cybersecurity risks like DDoS attacks.

Risk Identification

Asset valuation

Asset Valuation (Business Impact Analysis - BIA)

- Measures:
  - **Value of assets**
  - **Threats**
  - **Risks**
  - **Impact if asset is affected**

⍰ **Example:**
If a payroll system outage would delay employee salaries and trigger legal penalties, it's classified as a **critical** asset.

Threat analysis

- **Define actual threats.**
- **Predict consequences.**
- **Estimate frequency.**
- **Assess probability.**

⍰ **Example:**
Threat: Phishing
Consequence: Credential theft
Frequency: High (weekly attempts)
Probability: High (employees frequently targeted)

Vulnerability assessment

- **Baseline scan** to find weaknesses.

- Helps choose **appropriate safeguards**.

⍰ **Example:**
Regular vulnerability assessments find:

- Unencrypted devices
- Poor access control
- Outdated SSL/TLS certificates

Likelihood Determination

Risk Fundamentals

What is Risk?

- **Risk** = Likelihood of a threat exploiting a vulnerability, causing impact to business.

⍰ **Example:**
A hacker exploiting an outdated firewall (vulnerability) leads to a data breach (impact).

Acceptable Risk

- The **level of risk** an organization is willing to **accept** in exchange for business benefits.

⍰ **Example:**
A small retailer accepts the minor risk of payment system downtime during Black Friday, rather than spending millions on redundant systems.

Risk is rated using three factors:

Factor	Meaning	Example
Impact	Harm caused if the risk occurs.	Reputation damage, legal fines.
Likelihood	Chance the threat will happen.	High if many phishing emails

Factor	Meaning	Example
		detected.
Exposure	How much and how often the organization faces the threat.	High if running multiple exposed servers without patching.

▯ Remember:

$$\text{Risk} = \text{Likelihood} \times \text{Impact}$$

Identify Threats and Vulnerabilities

Element	Meaning	Example
Threat	External conditions that cause risk.	Hackers, malware, natural disasters.
Vulnerability	Internal weaknesses that allow threats to succeed.	Weak passwords, missing patches.

▯ Important Tip:

- **We can control vulnerabilities** (patch systems, strong passwords).
- **We cannot control threats** (natural disasters will happen).

ANALYSIS OF RISK

Risk Analysis / Assessment

- Risk analysis involves:
- Thoroughly examining **sources of risk.**
- Understanding **how exposed** assets are.

- Identifying the **potential impact** if exploited.

⍰ **Example:**
Analyzing risk of ransomware encrypting customer databases:

- Impact = Severe business disruption
- Likelihood = High if anti-malware tools are outdated.

Metrics for Risk Management

Qualitative Risk Assessment

- **Subjective**, uses expert opinion.
- Fast and useful when numbers aren't available.
- Uses **risk matrices** like High/Medium/Low.

⍰ **Example:**
A security team rates insider threats as "High Risk" based on interviews.

- **Senior management owns the risks.**
- Risk identification may involve business unit managers, data owners, custodians.

⍰ **Example:**
IT Manager helps identify risks with cloud services; senior executives decide whether to accept or mitigate them.

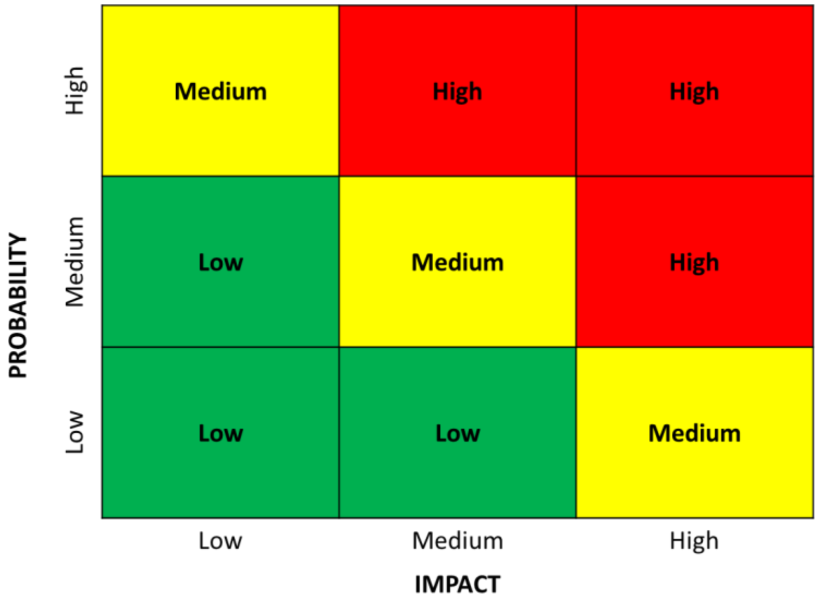
- Risk is evaluated based on:

  - ◆ High/Medium/Low probability
  - ◆ High/Medium/Low impact

- Uses interviews, expert opinions, workshops.

⍰ **Example:**
A team rates "ransomware attack" as **High Probability** and **High Impact**, while "fire damage to server room" is **Low Probability** but **High Impact**.

Qualitative Example



PROBABILITY	Low	Medium	High
High	Medium	High	High
Medium	Low	Medium	High
Low	Low	Low	Medium

IMPACT

Quantitative Risk Assessment

- **Objective**, uses **numerical data.**
- Calculates financial impacts using formulas.

⍰ Important Metrics:

Metric	Meaning	Formula	Example
SLE (Single-Loss Expectancy)	Loss for one incident.	Asset Value × Exposure Factor	$10,000 × 40% = $4,000 loss.
EF (Exposure Factor)	% of asset value lost per incident.	Expressed as %	Fire damages 40% of asset.
ARO (Annualized Rate of Occurrence)	Frequency per year.	Frequency ÷ Years	Event happens every 5 years → ARO = 0.2.
ALE (Annualized	Expected annual	SLE × ARO	$4,000 × 0.2 =

Metric	Meaning	Formula	Example
Loss Expectancy)	loss.		$800/year loss.

⍰ Summary Formula Chain:

$$\text{SLE} = \text{Asset Value} \times \text{EF}$$

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

⍰ Example:
If data breach could cost $100,000 (SLE) and is likely once every 5 years (ARO = 0.2),
then ALE = $20,000 annually.

Risk Response

Method	Meaning	Example
Risk Reduction	Apply controls to lower the risk.	Install antivirus and firewalls.
Risk Transfer	Shift the risk to a third party.	Buy cybersecurity insurance.
Risk Avoidance	Eliminate the activity causing risk.	Cancel a risky cloud migration plan.
Risk Acceptance	Accept the remaining risk without further action.	Accept risk of non-critical system downtime during updates.

Access Control Types

Access controls protect assets by limiting who can access resources and how.

Control Type	Description	Examples
Physical	Protect the physical environment.	Door locks, security guards, CCTV cameras, fences.
Administrative (Managerial)	Policies, training, hiring, and access management.	Security awareness programs, hiring background checks, access approval forms.
Logical (Technical)	Computerized controls.	Firewalls, password systems, encryption, VPN access.

Administrative Controls

Examples:

- **Policies and Procedures:** Set rules for security operations.
- **Personnel Security:** Background checks, role-based access.
- **User Access Management:** User provisioning/de-provisioning.
- **Privilege Management:** Ensuring users have "least privilege" access only.
- **Monitoring:** Conducting audits, security log reviews.

Logical (Technical) Controls

Examples:

- **Network Access:** Firewalls controlling traffic.
- **Remote Access:** VPN secured access.
- **System Access:** Role-based access to databases.
- **Application Access:** Login authentication for apps.
- **Malware Control:** Anti-virus, endpoint protection.
- **Cryptography:** Encryption of data at rest and in transit.

Security Control Categories

To defend systems effectively, we categorize controls based on their **intended function**:

Control Category	Purpose	Example
Directive	Mandate or policy that tells what to do.	Company Acceptable Use Policy.
Deterrent	Discourages unwanted behavior.	Warning signs: ″Area Under Surveillance.″
Preventative	Stops incidents before they happen.	Firewalls, password requirements.
Compensating	Alternative control when the ideal control isn't possible.	Enhanced monitoring when MFA isn't available.
Detective	Identifies and alerts after an event occurs.	Intrusion Detection Systems (IDS), audit logs.
Corrective	Fixes problems after detection.	Patching vulnerabilities after discovery.
Recovery	Restores systems to normal after serious disruption.	Disaster recovery site, restoring data backups.

Tip:
Use **Defense in Depth** = multiple types of controls across layers.

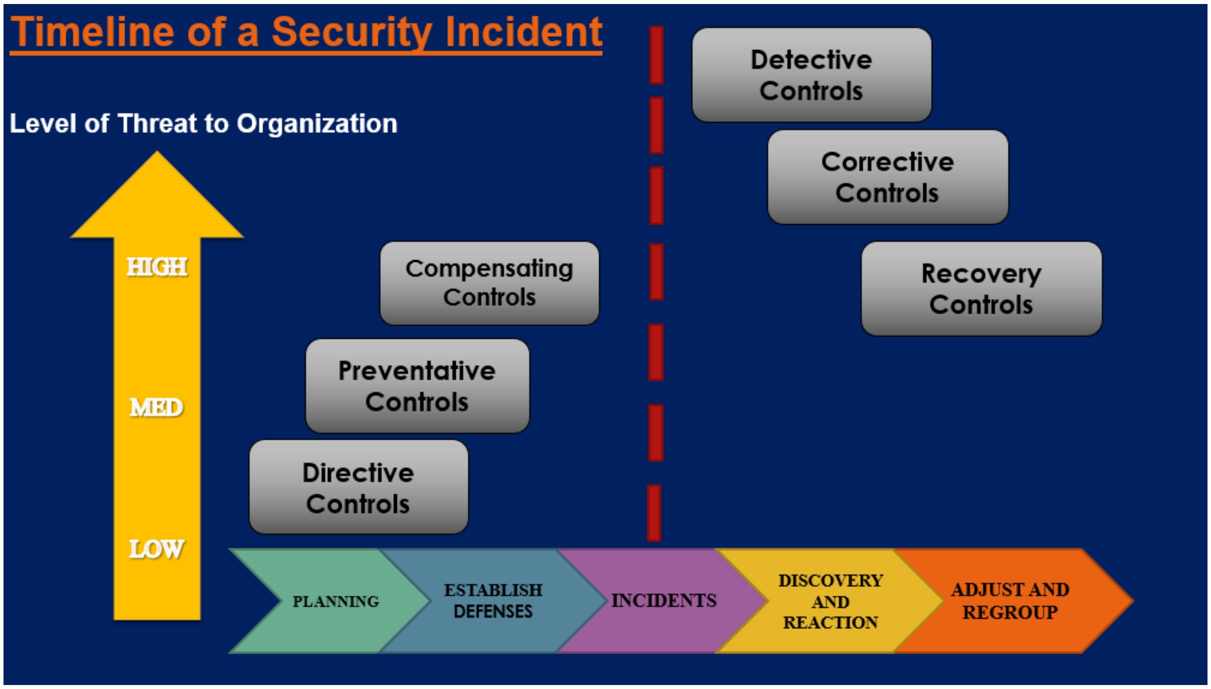
Key Concept: Defense in Depth

- **Single-layer defense** is dangerous — if that one control fails, you are exposed.

- **Layered defense** (multiple controls) makes it harder for an attacker to succeed.

⍰ **Example:**

- **Physical Security:** Lock doors to server room.
- **Administrative Security:** Define policies for access.
- **Logical Security:** Require 2FA to log into servers.



Timeline of a Security Incident

Vulnerability Assessment

⍰ **Steps:**

1. **Vulnerability Scanning:**
   Use tools (e.g., Nessus, OpenVAS) to scan systems for known vulnerabilities.
2. **Finalize Analysis:**
   Analyze the scan results — prioritize vulnerabilities based on severity (Critical, High, Medium, Low).
3. **Communicate Results:**
   Report findings to stakeholders with **risk levels and recommendations**.

⍰ **Example:**
A vulnerability scan reveals outdated Apache server versions vulnerable to CVEs. IT patches the servers.

Penetration Testing

⍰ **Purpose:**
Simulate **real-world attacks** on systems to understand **risk exposure**.

⍰ **Key Points for Successful Pen Test:**

- **Clear Objectives:** What are we testing? (Web app? Network perimeter?)
- **Scope:** Which systems? How deep can testing go?
- **Rules of Engagement:** What is allowed? What isn't?
- **Limitations:** No destructive attacks unless explicitly permitted.
- **Acceptable Activities:** List of authorized test actions.

⍰ **Real-World Example:**
A penetration test identifies a SQL Injection vulnerability in a company's online payment portal.

Penetration Test Strategies

Strategy	Meaning	Example
External Testing	Test from outside organization’s network (simulates outsider attack).	Hacker trying to breach through exposed web servers.
Internal Testing	Test from inside organization’s network (simulates insider threat).	Malicious employee attempts.
Blind Testing	Tester has little or no info (realistic attacker simulation).	Red Team gets only IP address.
Double-Blind Testing	Neither defenders nor testers know test timing/details.	Full surprise attack simulation.

Categories of Penetration Testing

Type	Meaning	Example
Zero Knowledge	Tester knows nothing about the target.	Only IP address given.
Partial Knowledge	Tester knows limited details.	Tester has network diagrams.
Full Knowledge	Tester knows all about the target systems.	Tester is given admin credentials to identify deep weaknesses faster.

▯ **Tip:**

- **Zero Knowledge** = Simulates external attacker.
- **Partial/Full Knowledge** = Simulates insider or detailed threat actor.

Penetration Test Methodology

▯ **5 Steps:**

1. **Reconnaissance:**
   Gather public info (whois, DNS, Google hacking).
2. **Enumeration:**
   Identify systems, ports, services, usernames.
3. **Vulnerability Analysis:**
   Find and map known vulnerabilities to the systems.
4. **Execution/Exploitation:**
   Exploit vulnerabilities to gain unauthorized access.
5. **Document Findings:**
   Write clear report: vulnerabilities found, data accessed, recommendations.

▯ **Example:**
Reconnaissance finds a public FTP server. Enumeration identifies open access. Exploitation uploads a backdoor file. Document and fix.

THREAT MODELING

Introduction to Threat Modeling

Threat modeling is **thinking like an attacker** — identifying possible ways to compromise a system **before** an attack happens.

□ **Main Goal:**

Identify threats early

Understand how existing controls behave

Prioritize risks

Implement better defenses

□ **Scope of Threat Modeling Can Include:**

Network (e.g., corporate LAN, cloud VPC)

System (e.g., a server or IoT device)

Application (e.g., banking app)

Data (e.g., customer records)

Threat Modelling

Step	Meaning	Example
Identify Threat Agents	Who might attack you?	Hackers, insiders, competitors
Identify Possible Threats	What can go wrong?	SQL injection, ransomware
Understand Current	What defenses are in	Firewalls, encryption

Step	Meaning	Example
Controls	place?	
Identify Vulnerabilities	Gaps in protection	Outdated software
Prioritize Risks	Rank by impact and likelihood	Focus on most critical
Implement Controls	Add protections to lower risk	MFA, updated patches

STRIDE

STRIDE helps you systematically identify six main types of threats.

Letter	Threat	Definition	Property Violated	Example
S	Spoofing	Pretending to be someone else	Authentication	Attacker logs in as a user
T	Tampering	Changing data	Integrity	Hacker modifies bank transfer data
R	Repudiation	Denying actions	Non-Repudiation	User claims they didn’t send a payment
I	Information	Exposing private	Confidentiality	Data breach

Letter	Threat	Definition	Property Violated	Example
	Disclosure	data		leaking emails
D	Denial of Service (DoS)	Crashing system	Availability	DDoS attack on a website
E	Elevation of Privilege	Gaining unauthorized access	Authorization	Normal user gains admin rights

□ Tip:

```
STRIDE = Spoof, Tamper, Repudiate, Inform, Deny, Elevate
```

Defining security requirements.

The Threat Modeling Tool enables any developer or software architect to:

□ Define Security Requirements

What are the rules to protect data/systems?

□ Create an Application Diagram

Draw system architecture: servers, users, data flows.

□ Identify Threats

Use STRIDE or other models.

□ Mitigate Threats

Add controls: encryption, authentication, logging.

□ Validate Mitigations

Pen testing, security reviews, audits.

PASTA

2. □ PASTA (Process for Attack Simulation and Threat Analysis)

A structured, **7-step** process:

Step	Meaning	Example
1. Define Objectives	What’s important?	Protect customer data.
2. Define Technical Scope	What systems?	Mobile app + backend.
3. Application Decomposition	Break down system parts.	App modules: login, payment.
4. Threat Analysis	Identify threats.	Brute-force attacks.
5. Vulnerability Analysis	Find weaknesses.	Weak password policies.
6. Attack Enumeration	List attack paths.	Password spray attack.
7. Risk and Impact Analysis	Calculate and prioritize.	Financial loss from breach = $1M risk.

□ Focus:

Detailed modeling, simulating realistic attacks.

Cyber Kill Chain

Cyber Kill Chain (Lockheed Martin)

The **Cyber Kill Chain** describes **how attackers move** through stages to breach a target.

Stage	Meaning	Example
1. Reconnaissance	Research target.	Finding public emails.
2. Weaponization	Create attack tool.	Crafting malware.
3. Delivery	Send payload.	Phishing email with attachment.
4. Exploitation	Execute payload.	User opens infected file.
5. Installation	Install malware.	Install Remote Access Trojan (RAT).
6. Command & Control (C2)	Remote control victim system.	Hacker communicates with infected laptop.
7. Actions on Objectives	Achieve goal.	Steal data or disrupt services.

▯ **Goal:**

Break attacker chain early to prevent full compromise.

SECURITY RISK CONSIDERATIONS INTO ACQUISITIONS STRATEGY AND PRACTICE

✅ **Definition:**
When acquiring products, services, or partnerships, you must **analyze security risks** early in the **planning phase**, not after purchase.

□ **Focus Areas:**

- Understand potential risks from vendors or suppliers.
- Define clear **security and service expectations**.
- Monitor third parties continuously.

□ **Example:**
Before purchasing a cloud-based CRM system, a company requires the vendor to show SOC 2 Type II certification.

Apply Risk-Based Management Concepts to the Supply Chain

The **supply chain** is a major risk area!
Vendors, contractors, suppliers — all can introduce vulnerabilities.

□ **Risk Management Applied To Supply Chain Includes:**

- **Governance Review:** Ensure third parties follow good security governance.
- **Site Security Review:** Visit vendor sites and check their security controls.
- **Formal Security Audit:** Request ISO 27001 audit reports.
- **Penetration Testing:** Validate their systems by testing for weaknesses.

□ **When Direct Review Isn't Possible:**
Use trusted **third-party assessments**:

- **ISO certifications**
- **CSA STAR** (Cloud Security Alliance program)

AICPA SSAE 16 SOC Reports (SOC 1, SOC 2, SOC 3)

⍰ **Example:**
A SaaS vendor cannot be physically visited, so the customer reviews the vendor's SOC 2 report instead.

Regular Third-Party Assessment

Ongoing reviews are critical — not a "one-time" check!

Method	Description	Example
On-Site Assessment	Visit vendor location, interview staff, inspect physical security.	Checking firewall, badge access, clean desk policy.
Document Exchange and Review	Exchange policies, security procedures, contracts.	Vendor sends encryption policy for review.
Process/Policy Review	Evaluate their incident response, patching, and access controls.	Vendor demonstrates their incident handling SOP.

Tip:
Periodic reassessment is necessary because vendor security postures can change!

Service Level Agreements (SLAs) vs. Assurance

Term	Meaning	Example
SLA	Formal agreement describing	"99.9% uptime guarantee"

Term	Meaning	Example
	expected service performance.	
Assurance	Actual evidence that the SLA terms are being met.	SLA monthly reports, vulnerability scans

⍰ **Key Point:**

SLAs = Promises

Assurance = Proof that promises are kept

⍰ **Penalty Clause:**
If vendors don't meet SLA terms (e.g., uptime drops), there can be **financial penalties**.

Minimum Security Requirements

Before any acquisition or project:

⍰ **Best Practices:**

Involve stakeholders early to set security expectations.

Specific, Realistic, Measurable security requirements.

Document discussions and agreed outcomes.

Validate understanding (repeat back requirements).

Avoid picking tools before understanding needs.

Use diagrams and prototypes to visualize systems.

□ **Example:**
Before signing a contract for a database hosting service, clearly define encryption standards (AES-256), backup frequency (daily), and compliance needs (HIPAA).

Service Level Requirements (SLR)

□ **SLR:**

Captures client-specific **service expectations**.

Forms the basis for the eventual SLA.

□ **SLR Must Include:**

Detailed service level targets (e.g., backup recovery time <4 hours).

Mutual responsibilities (customer must also maintain their part).

□ **Example:**
Customer demands that any critical incident must be **resolved within 2 hours** — this requirement becomes part of the SLR.

Service Level Agreement (SLA)

□ **SLA:**
A **formal agreement** between the service provider and customer that:

Describes the service.

Documents service level targets (availability, response time).

Details provider and customer responsibilities.

□ **Example:**
SLA for a cloud service provider states:

99.95% uptime

Response within 30 minutes for critical incidents

Data backups daily

Service Level Report

□ **Service Level Report:**

Tracks actual service performance.

Compares **agreed** vs **achieved** service levels.

Identifies **areas for improvement**.

Reports **exceptional events** (e.g., service outages).

□ **Example:**
Monthly report shows cloud provider achieved only 99.5% uptime (below promised 99.9%).

Silicon Root Of Trust

Silicon Root of Trust:
Hardware-embedded security anchors that ensure the device boots securely and is tamper-resistant.

Feature	Meaning	Example
Tamper Resistance	Detect if hardware is modified.	Server motherboard detects tampering.
Secure Boot	Only trusted code can run at startup.	Prevent malware at boot time.
Cryptographic Operations	Hardware security modules store keys.	Keys are secured inside a secure element.
Remote Attestation	Device remotely proves its integrity.	IoT device proves it hasn’t been hacked.

Software Bill Of Materials(SBOM)

Physically Unclonable Functions (PUF)

□ PUF:

Hardware-based fingerprints (like DNA for devices).

Unclonable due to manufacturing randomness.

□ PUF Uses:

Device Authentication: Ensures only trusted devices connect.

Encryption Keys: Hardware generates keys.

Security Activities: Anti-counterfeit protections.

□ Example:
Smartphones use PUF to generate encryption keys that are **unique** to each device and impossible to replicate.

Software Bill of Materials (SBOM)

□ SBOM = Inventory list of software components.

Lists libraries, frameworks, and dependencies used in a software product.

Essential for understanding supply chain risk in software.

□ Example:
If a vulnerability is found in OpenSSL, organizations can check their SBOMs to identify all software affected.

□ Benefits:

Faster vulnerability response

Regulatory compliance (e.g., Executive Order 14028 in U.S.)

Quick Visual Summary

Risk in Acquisition:- Early Risk Analysis- Vendor Security Reviews- Third-Party Assessments

Supply Chain Risk:- Review | Audit | Monitor Continuously- Use ISO, SOC, CSA reports

SLR vs SLA:- SLR: Customer viewpoint requirements- SLA: Formal contract- Service Reports track actual performance

Silicon Root of Trust:- Tamper Protection- Secure Boot- Hardware Key Storage- Remote Attestation

SBOM:- Know your software components- Find vulnerable libraries quickly

BCP/DRP

▯ Definitions:

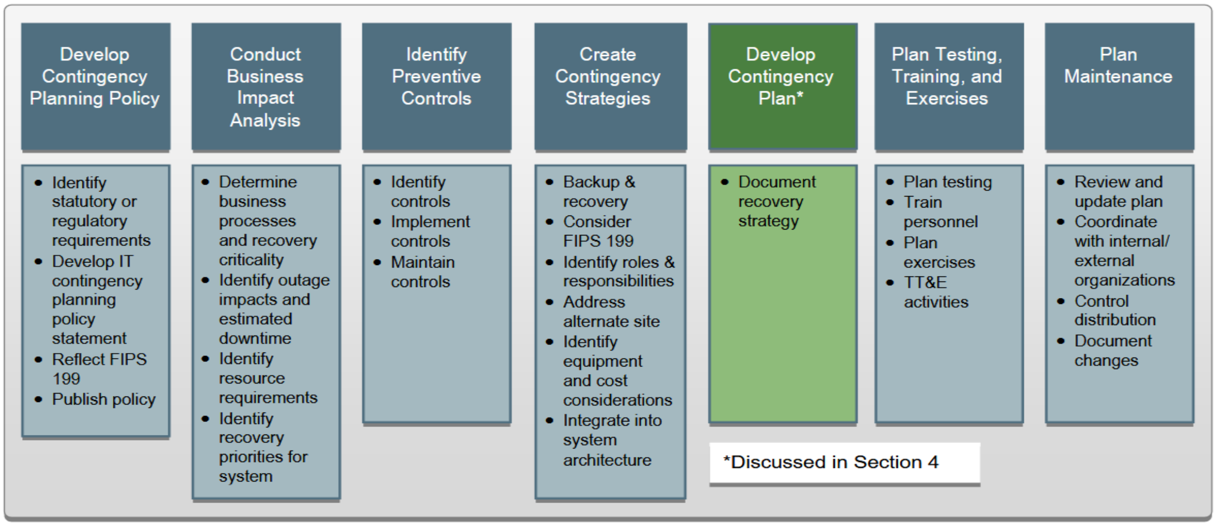
Term	Meaning	Focus
BCP	Plan to **continue business** operations during/after disruption.	Business Processes
DRP	Plan to **recover IT systems** after major failure.	IT Systems

▯ BCP = Focuses on maintaining operations
▯ DRP = Focuses on recovering IT services

▯ Example:

BCP: Moving staff to another office after a fire.

DRP: Restoring the backup data center after a server room fire.



Develop Contingency Planning Policy	Conduct Business Impact Analysis	Identify Preventive Controls	Create Contingency Strategies	Develop Contingency Plan*	Plan Testing, Training, and Exercises	Plan Maintenance
• Identify statutory or regulatory requirements • Develop IT contingency planning policy statement • Reflect FIPS 199 • Publish policy	• Determine business processes and recovery criticality • Identify outage impacts and estimated downtime • Identify resource requirements • Identify recovery priorities for system	• Identify controls • Implement controls • Maintain controls	• Backup & recovery • Consider FIPS 199 • Identify roles & responsibilities • Address alternate site • Identify equipment and cost considerations • Integrate into system architecture	• Document recovery strategy	• Plan testing • Train personnel • Plan exercises • TT&E activities	• Review and update plan • Coordinate with internal/ external organizations • Control distribution • Document changes

*Discussed in Section 4

Figure 3-1: Contingency Planning Process

Absolutely! The NIST framework for contingency planning is one of the most comprehensive and structured approaches available. The picture you're referring to likely comes from **NIST Special Publication 800-34 Rev. 1**, titled:

"Contingency Planning Guide for Federal Information Systems"

This document outlines **seven key phases** of a robust **Business Continuity Plan (BCP) / Disaster Recovery Plan (DRP)** under the broader umbrella of **Contingency Planning**.

◆ 1. Develop the Contingency Planning Policy

- **Purpose:** Define the organization's contingency planning objectives, scope, and structure.
- **Includes:** Roles, responsibilities, and authority for the planning process.

◆ 2. Conduct the Business Impact Analysis (BIA)

- **Purpose:** Identify and prioritize critical IT systems and components.
- **Outcome:** Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) are determined here.

◆ 3. Identify Preventive Controls

- **Purpose:** Implement measures to reduce the effects of disruptions.
- **Includes:** Fire suppression, UPS systems, RAID, system hardening, etc.

◆ 4. Create Contingency Strategies

- **Purpose:** Develop recovery strategies for system downtime or failure.
- **Examples:** Redundant systems, alternate sites (hot/warm/cold), cloud backups.

◆ 5. Develop an Information System Contingency Plan

- **Purpose:** Create the actual plan document.
- **Includes:** Detailed roles, responsibilities, communication protocols, and recovery procedures.

◆ 6. Ensure Plan Testing, Training, and Exercises

- **Purpose:** Validate the plan and improve staff readiness.
- **Activities:** Tabletop exercises, functional tests, full-scale simulations.

◆ 7. Ensure Plan Maintenance

- **Purpose:** Keep the plan up-to-date as systems and business requirements evolve.
- **Includes:** Regular reviews, updates, and change management.

BCP/DRP PHASES AS PER CBK

◆ 1. Project Initiation

Goal: Establish the foundation for the BCP/DRP process.

- **Actions:**
  - Obtain senior management support.
  - Define the scope and objectives.
  - Appoint a BCP/DRP coordinator and form a planning team.
- **Example:**
  A bank forms a BCP team to create a recovery plan for their online banking platform, with buy-in from the CIO.

◆ 2. Business Impact Analysis (BIA)

Goal: Identify critical business processes and assess the impact of disruptions.

- **Key Concepts:**
    - Determine **Maximum Tolerable Downtime (MTD)**, **Recovery Time Objective (RTO)**, **Recovery Point Objective (RPO)**.
    - Analyze financial, operational, and legal impacts.
- **Example:**
  An e-commerce company finds that downtime of its payment gateway beyond 1 hour results in $50,000/hour loss, setting RTO at 60 minutes.

Metric	Meaning	Example
Maximum Tolerable Downtime (MTD)	Maximum time a function can be down before severe impact.	Payroll MTD = 2 days.
Recovery Time Objective (RTO)	Time to recover function after disruption.	Restore payroll system in 1 day (RTO < MTD).
Recovery Point Objective (RPO)	Maximum acceptable data loss (how old last backup can be).	RPO for payroll = 12 hours (backup every 12 hours).

◆ 3. Risk Assessment

Goal: Identify threats, vulnerabilities, and evaluate risk to business operations.

- **Actions:**
    - Perform threat modeling.
    - Map vulnerabilities to critical systems.
    - Calculate risk level (likelihood × impact).
- **Example:**
  A data center identifies power outages and ransomware as top risks and rates them based on past incidents.

◆ 4. Strategy Development

Goal: Define recovery and continuity strategies to meet RTO/RPO.

- **Options Include:**
  - Redundancy, alternate processing sites (hot, warm, cold), cloud failover, mobile recovery units.
  - Manual workarounds for business functions.
- **Example:**
  A financial firm chooses a **hot site** for real-time failover of its trading systems and sets up a **manual cheque writing** process in case of server failure.

◆ 5. Plan Design and Development

Goal: Document the procedures and roles required for recovery.

- **Components:**
  - Emergency response plan
  - Communication plan
  - Incident response, system recovery, and restoration procedures
  - Resource lists and vendor contacts
- **Example:**
  The BCP document includes who to call if the primary site is down, how to switch to backup systems, and how to notify stakeholders.

◆ 6. Plan Testing and Exercises

Goal: Validate the effectiveness of the plan and train staff.

- **Types of Testing:**
  - **Checklist Review:** Paper-based check.
  - **Tabletop Exercise:** Discussion-based scenario.
  - **Simulation:** Real-time scenario test.
  - **Parallel Test:** Recovery systems are run alongside production.
  - **Full Interruption Test:** Complete failover (rarely used).
- **Example:**
  An insurance firm conducts a **tabletop test** where a simulated fire disrupts the data center, and staff must follow the response plan.

◆ 7. Plan Maintenance

Goal: Ensure the plan remains current and effective.

- **Actions:**
  - Update after changes in systems, business structure, or incidents.
  - Review at least annually.
  - Maintain version control.
- **Example:**
  After migrating to a new cloud provider, an organization updates contact information, system dependencies, and test scripts.

◆ 8. Awareness and Training

Goal: Ensure staff are familiar with their roles in the BCP/DRP.

- **Actions:**
  - Train employees on response roles.
  - Include BCP overview in onboarding.
  - Conduct awareness campaigns.
- **Example:**
  Quarterly drills are conducted for customer support teams to ensure they know how to access systems from the alternate site.