CISSP

LAST MINUTE STUDY GUIDE

DOMAIN 1
SECURITY & RISK MANAGEMENT

JULY 2025

MOS

SECURITY & PRIVACY MADE EASY

CISSP DOMAIN 1: SECURITY AND RISK MANAGEMENT

THE CHANGING ROLE OF SECURITY

Adapting to New Threats

The nature of security threats has significantly evolved. In earlier times, the main goal was to safeguard data stored on internal servers. Now, however, organizations face threats that target a variety of assets, including:

- Smartphones and mobile platforms
- Tablets and portable devices
- Industrial control systems (ICS)
- Smart appliances (IoT), such as connected refrigerators

Social engineering and phishing have also grown more sophisticated, aiming to manipulate human behavior.

Broader Security Responsibilities

Security professionals must now look beyond data protection. The scope has widened to protecting:

- Personnel and human resources
- Hardware and software
- Intellectual property (IP)
- Products and services
- Organizational reputation

They must also ensure compliance with relevant laws and regulations while supporting the company’s mission.

Strategic Integration with Business

Security is now seen as a business enabler rather than just a cost center. Effective security practices:

- Reduce risk exposure
- Protect valuable assets

- Maintain organizational trust
- Enable business objectives

Security teams should align their efforts with executive goals and ensure their initiatives support the overall strategy.

Top-Down Approach

A robust security program begins at the top. The CEO and board members must:

- Champion security initiatives
- Fund and support risk assessments
- Define risk appetites

Ideally, the security team should report directly to executive leadership to avoid conflicts of interest.

Enhancing Organizational Value

Security contributes to organizational value by:

- Maintaining data integrity
- Enabling operational efficiency
- Promoting stakeholder confidence

This shift highlights the transition of security from a reactive function to a proactive, strategic role.

CORE SECURITY PRINCIPLES: THE CIA TRIAD

Confidentiality

Confidentiality ensures that information is only accessed by authorized individuals. Strategies to maintain confidentiality include:

- Implementing strong access control mechanisms
- Encrypting sensitive data
- Enforcing the principle of least privilege
- Promoting the need-to-know basis

Integrity

Integrity guarantees that data is accurate and trustworthy. It protects against unauthorized modifications by:

- Using checksums and hash functions
- Employing digital signatures
- Logging changes and activities
- Implementing version control and audit trails

Availability

Availability ensures that data and services are accessible when needed. It involves:

- Redundant systems and failover clusters
- Disaster recovery planning
- Data backups and offsite storage
- Load balancing and scalability

Expanding to Five Pillars of Security

In addition to CIA, the following two principles complete the modern security framework:

Authenticity

Authenticity verifies the source of information. Techniques include:

- Digital certificates
- Authenticated API connections
- Secure key exchange

Nonrepudiation

Nonrepudiation prevents denial of actions by ensuring individuals cannot deny their involvement. It is achieved through:

- Logging and monitoring
- Digital signatures
- Legal agreements

ACCOUNTABILITY VS. RESPONSIBILITY

Accountability

- **Definition**: The obligation to answer for outcomes and actions.

- **Cannot be Delegated**: A person may delegate tasks, but not the responsibility for results.
- **Example**: A VP is accountable for the financial system, even if IT staff handles technical implementation.
- **Corporate Governance**: Accountability usually lies with senior executives like the CEO, CFO, or Board.

Responsibility

- **Definition**: The duty to perform specific tasks or roles.
- **Can be Delegated**: Tasks can be assigned to others.
- **Multiple Responsible Parties**: Several individuals may be responsible for different components of a task.
- **Example**: The IT administrator is responsible for implementing access controls set by the CISO.

Roles in Security Structure

- **Asset Owner**: Defines security needs, classification, and access.
- **Custodian**: Implements and maintains controls under owner guidance.
- **Processor**: Handles data per owner's instruction.
- **CISO/Security Officer**: Designs and oversees the implementation of security controls.
- **IT Staff**: Execute tasks and manage technical systems.
- **Auditors**: Provide independent assurance that controls meet objectives.

ISC2 CODE OF ETHICS

Purpose

CISSPs must adhere to a strict Code of Professional Ethics, which includes four mandatory canons:

1. **Protect society, the common good, and public trust**
2. **Act with honor, honesty, justice, and legality**
3. **Provide competent and diligent service to principals**
4. **Advance and protect the profession**

These canons are listed in order of priority. In case of conflict, higher-order canons override the lower ones.

ORGANIZATIONAL CODE OF ETHICS

Ethical Foundations

Ethical behavior in the workplace is grounded in doing no harm to others. For uniformity, ethics must be defined and documented within corporate policies.

Codified Corporate Ethics

- Organizations develop written codes of ethics to guide behavior.
- These codes align diverse personal values with the company’s expectations.
- Documented ethics create consistency across departments and individuals.

Role of Management

Management plays a crucial part in embedding ethical behavior. Senior leadership:

- Models ethical behavior
- Enforces standards fairly
- Promotes a culture of integrity

A strong ethical foundation improves employee morale, customer trust, and organizational reputation.

SECURITY GOVERNANCE

Understanding Governance

Governance refers to the systems and processes used to oversee and guide an organization’s operations. Its primary aim is to ensure that the organization meets its goals effectively and ethically while maximizing stakeholder value.

In the context of security, governance ensures:

- Proper alignment between security practices and business objectives
- Clear definition of roles, responsibilities, and accountability
- Transparent decision-making and risk management

Corporate Governance

Corporate governance is exercised by executive management, typically the CEO, board of directors, and senior leadership. These individuals:

- Set strategic objectives
- Define acceptable levels of risk
- Allocate resources for compliance and security
- Create policies to guide operational behavior

Security Governance

Security governance is the subset of corporate governance dedicated to managing information security initiatives. It involves:

- Establishing security policies and frameworks
- Aligning security with legal, regulatory, and business requirements
- Prioritizing security investments based on risk assessments
- Promoting a security-first culture

Security Governance vs. Management

Governance is about defining "what" must be done and ensuring oversight. Management focuses on "how" it gets done. For example:

- Governance: Approves a data protection policy
- Management: Implements encryption and access control to comply with that policy

Top-Down Security Governance

An effective security program is built from the top down. Executive management must:

- Provide direction and funding
- Champion a culture of security
- Establish an enterprise-wide security strategy

Without executive sponsorship, security initiatives often lack authority and funding.

Governance Committees

Organizations may establish a governance committee to:

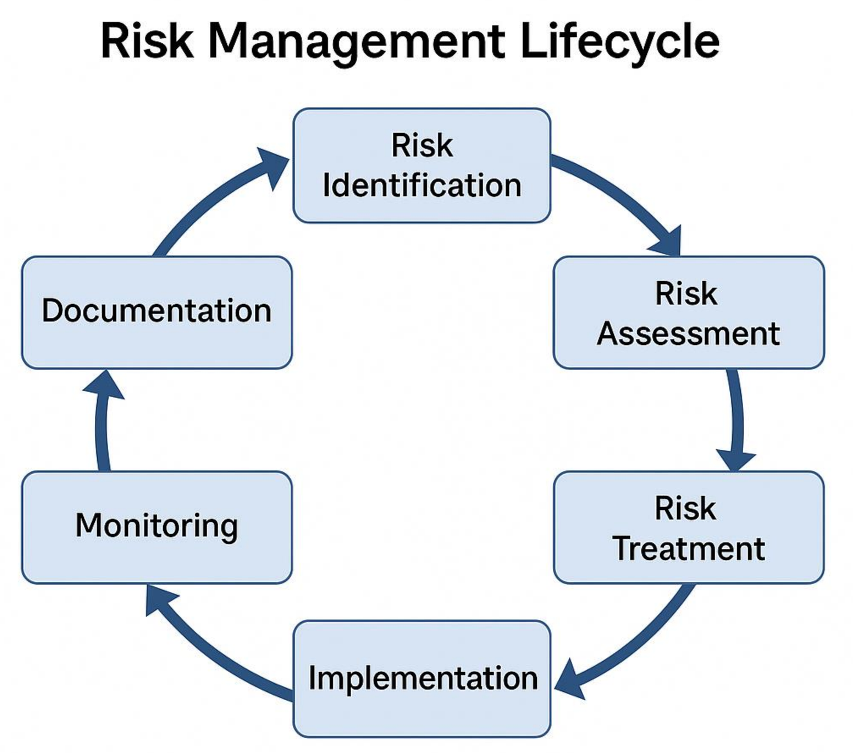
- Review the effectiveness of security programs
- Monitor policy compliance
- Evaluate performance metrics and audits

These committees often include representatives from IT, legal, HR, and senior management.

Tailoring and Scoping

- **Scoping**: Identifies which security requirements are relevant based on organizational needs, legal obligations, and risk appetite.
- **Tailoring**: Adjusts security controls to better fit specific processes or departments. Tailored controls should be cost-effective and provide necessary coverage.

SECURITY RISK MANAGEMENT



Risk management involves identifying, assessing, and minimizing threats to organizational assets. It is essential for protecting business continuity, intellectual property, reputation, and data.

Risk Management Lifecycle

1. **Identify Risks**: Recognize potential threats (e.g., malware, power outage, insider threat)
2. **Analyze Risks**: Evaluate the impact and likelihood of each risk

3. **Prioritize Risks**: Rank risks to determine which need immediate attention
4. **Treat Risks**: Decide on appropriate mitigation strategies (avoidance, transfer, reduction, acceptance)
5. **Monitor and Review**: Continuously track risks and control effectiveness

Asset Valuation

Identifying the value of each asset is a foundational step. Assets include:

- Tangible (servers, buildings)
- Intangible (brand reputation, proprietary code)

Risk Formula Components

- **Asset Value (AV)**: Monetary worth of an asset
- **Exposure Factor (EF):** Percentage of loss if a threat is realized
- **Single Loss Expectancy (SLE)** = AV × EF
- **Annual Rate of Occurrence (ARO)**: Estimated frequency of the threat annually
- **Annual Loss Expectancy (ALE)** = SLE × ARO

This formula helps determine whether the cost of implementing a control is justified.

Types of Risk Assessments

- **Qualitative**: Subjective, based on expert opinion, categorizes risks as high/medium/low
- **Quantitative**: Objective, uses numeric values to assess and compare risks
- **Hybrid**: Combines both methods for a balanced perspective

Risk Treatment Options

1. **Avoidance**: Eliminate activities that introduce risk
2. **Transfer**: Shift responsibility (e.g., through insurance or outsourcing)
3. **Mitigation**: Reduce risk through security controls
4. **Acceptance**: Tolerate the risk if it falls within acceptable limits

Residual Risk

The risk that remains after controls are applied. Organizations must decide if this level is acceptable or requires further action.

Continuous Improvement: PDCA Cycle

- **Plan**: Identify risks and determine required controls
- **Do**: Implement controls
- **Check**: Monitor effectiveness
- **Act**: Make improvements

Triggers for re-assessment include:

- New systems or data
- Changes in regulation
- Discovery of vulnerabilities

DUE CARE AND DUE DILIGENCE

Due Care

Due care refers to the reasonable precautions an organization takes to prevent harm or mitigate risks. It means taking action to protect systems, data, and stakeholders from threats.

Examples:

- Deploying antivirus software
- Conducting employee security awareness training
- Using access control mechanisms

Due Diligence

Due diligence is the ability to demonstrate and document that due care was taken. It provides proof that actions and decisions were appropriate and aligned with organizational policies.

Examples:

- Maintaining audit logs of security events
- Providing records of security training and test results
- Documenting risk assessments and decisions

These concepts help establish legal and regulatory defense if a security incident occurs. Failure to exercise due care or due diligence may result in legal liability or reputational damage.

LEGAL, REGULATORY, AND COMPLIANCE REQUIREMENTS

Legal Systems

Organizations must comply with the legal system in the jurisdictions in which they operate. The primary types of legal systems include:

- **Civil Law**: Based on written codes (e.g., France, Japan)
- **Common Law**: Based on precedent and judicial rulings (e.g., US, UK)
- **Religious Law**: Based on religious texts and principles
- **Customary Law**: Based on traditional practices

Key Regulatory Categories

- **Laws**: Enforceable rules (e.g., GDPR, HIPAA, SOX)
- **Regulations**: Rules issued by government bodies (e.g., SEC, FDA)
- **Industry Standards**: Best practices adopted voluntarily or required by contracts (e.g., PCI DSS)
- **Contractual Obligations**: Agreements requiring compliance with specific controls

Cross-Border Data Issues

When data flows between countries, organizations must:

- Understand local and international privacy regulations
- Comply with data localization laws
- Apply transfer mechanisms such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs)

CONTROL FRAMEWORKS

Security frameworks provide a structured approach to managing risks and implementing controls. They help ensure consistency, compliance, and efficiency across the organization.

NIST (National Institute of Standards and Technology)

The NIST Cybersecurity Framework (CSF) and NIST SP 800 series are widely adopted in both government and private sectors.

- **NIST CSF**: Focuses on five core functions – Identify, Protect, Detect, Respond, Recover
- **SP 800-53**: Provides detailed security and privacy controls
- **SP 800-37**: Guides risk management using the Risk Management Framework (RMF)

ISO/IEC 27000 Series

Internationally recognized standards for information security management systems (ISMS).

- **ISO 27001**: Specifies requirements for establishing, implementing, and maintaining an ISMS
- **ISO 27002**: Provides implementation guidance for controls
- **ISO 27701**: Focuses on privacy information management
- **ISO 27005**: Addresses risk management practices

COBIT (Control Objectives for Information and Related Technologies)

Developed by ISACA, COBIT provides a governance and management framework for enterprise IT.

- Aligns IT goals with business objectives
- Offers maturity models to assess control effectiveness
- Encourages performance measurement and accountability

ITIL (Information Technology Infrastructure Library)

Primarily a service management framework, ITIL aligns IT services with business needs.

- Emphasizes service lifecycle: Strategy, Design, Transition, Operation, and Improvement
- Addresses incident, change, and problem management

TOGAF (The Open Group Architecture Framework)

An enterprise architecture methodology used to design, plan, implement, and govern business information systems.

SECURITY POLICIES, STANDARDS, PROCEDURES, AND GUIDELINES

Security Policy

A high-level document that outlines the organization's security philosophy, rules, and responsibilities.

- Approved by executive leadership
- Supports compliance with laws and standards
- Acts as the foundation for security planning and behavior

Standards

Standards define specific, mandatory rules to support policies.

- Example: All passwords must be a minimum of 12 characters
- Ensures consistency in technology and processes

Procedures

Detailed, step-by-step instructions to perform tasks or implement controls.

- Example: Steps to provision new user access
- Ensures repeatability and reduces errors

Guidelines

Recommendations that offer flexibility and allow judgment.

- Not mandatory, but help meet best practices
- Example: Suggesting tools or techniques for secure coding

Each of these documents should be reviewed regularly and updated as necessary to remain relevant.

PRIVACY FUNDAMENTALS

Definition of Privacy

Privacy refers to the right of individuals to control how their personal information is collected, used, and shared. Organizations must uphold this right while meeting business and regulatory requirements.

Personally Identifiable Information (PII)

PII includes any information that can be used to identify an individual, such as:

- Name, address, phone number
- Social Security number or government ID
- Financial, health, or biometric data

Privacy Principles

- **Consent**: Data subjects must be informed and agree to data processing
- **Purpose Limitation**: Collect data only for specific, legitimate purposes
- **Data Minimization**: Only gather data necessary for the intended use
- **Accuracy**: Keep data up to date and correct
- **Storage Limitation**: Retain data only as long as necessary
- **Integrity and Confidentiality**: Protect against unauthorized access or alteration
- **Accountability**: Demonstrate compliance with privacy laws

Data Subject Rights

Under regulations like GDPR or CCPA, individuals have:

- Right to access their data
- Right to rectification and erasure
- Right to object or restrict processing
- Right to data portability

INTELLECTUAL PROPERTY (IP) PROTECTIONS

Copyright

- Protects original works of authorship (e.g., software code, documentation)
- Grants exclusive rights to reproduce, distribute, and modify
- Automatically applies upon creation

Trademarks

- Protect symbols, logos, and names that distinguish goods/services
- Prevents others from using similar branding that causes confusion

Patents

- Protect inventions and processes that are novel and useful

- Grant exclusive rights for a limited period

Trade Secrets

- Protect confidential business information (e.g., algorithms, formulas)
- Must be actively protected through access controls and NDAs

Licensing Agreements

- Define how IP can be used, modified, and distributed
- Can be open source (e.g., GPL, MIT) or proprietary

Misuse of intellectual property may result in legal actions, fines, and reputational damage.

THREAT MODELING

Threat modeling is a structured process to identify, assess, and prioritize potential threats to a system or process. It helps in designing effective security controls during the system development lifecycle (SDLC).

Key Steps in Threat Modeling

1. **Identify Assets**: Determine what needs to be protected (data, applications, services)
2. **Create an Architecture Overview**: Understand the system's layout and components
3. **Decompose the Application**: Break down the system to analyze attack surfaces and trust boundaries
4. **Identify Threats**: Use structured methods like STRIDE or PASTA
5. **Document and Rate Threats**: Assess likelihood and impact
6. **Determine Mitigations**: Design security controls to reduce risk

STRIDE Threat Categories

- **Spoofing**: Impersonating another user
- **Tampering**: Unauthorized data modification
- **Repudiation**: Denying actions or transactions
- **Information Disclosure**: Exposing confidential data
- **Denial of Service (DoS)**: Interrupting availability

- **Elevation of Privilege**: Gaining unauthorized access rights

Common Tools for Threat Modeling

- Microsoft Threat Modeling Tool
- OWASP Threat Dragon
- ThreatModeler

SECURITY ROLES AND RESPONSIBILITIES

Senior Management

- Sets security goals and approves budgets
- Establishes risk tolerance and strategic direction
- Ensures regulatory and legal compliance

Data Owner

- Determines data classification and access rights
- Ultimately accountable for data protection

Data Custodian

- Implements and manages security controls as per data owner's direction
- Maintains system backups, logs, and updates

Security Administrator

- Configures and monitors security technologies
- Enforces policy and manages user permissions

Users

- Must follow acceptable use policies (AUPs)
- Responsible for practicing safe computing behaviors

Auditors

- Independently evaluate security controls
- Ensure compliance with internal policies and external regulations

COMPLIANCE

Internal Compliance

Ensures adherence to the organization's own policies, procedures, and control frameworks.

- Example: Following internal data retention policies

External Compliance

Ensures alignment with legal, contractual, and regulatory requirements.

- Examples: GDPR, HIPAA, PCI DSS, SOX

Failure to meet compliance obligations can result in:

- Regulatory penalties
- Civil or criminal liability
- Loss of reputation

PROFESSIONAL ETHICS

Importance of Ethics

Ethics guide behavior and decision-making in the absence of formal laws. Security professionals must:

- Avoid conflicts of interest
- Respect privacy and confidentiality
- Uphold trust and integrity

ISC2 Code of Ethics (Recap)

1. Protect society and the common good
2. Act honorably, honestly, and legally
3. Provide competent services to principals
4. Advance the profession

Violations of the Code of Ethics can result in suspension or revocation of CISSP certification.

SECURITY AWARENESS, TRAINING, AND EDUCATION

Security Awareness

Designed to inform users of basic security principles and the risks associated with negligent behavior.

- Delivered via emails, posters, newsletters
- Focused on recognizing phishing, social engineering, password hygiene

Security Training

Provides users with practical skills to perform their roles securely.

- Targeted to specific job functions
- Includes hands-on exercises and assessments

Security Education

Delivers long-term, in-depth knowledge to professionals and specialists.

- Example: Pursuing CISSP, CISM, or other advanced credentials

Program Best Practices

- Tailor content to audience roles
- Use real-life examples and simulations
- Measure effectiveness with quizzes and metrics

BUSINESS CONTINUITY AND DISASTER RECOVERY

Business Continuity Planning (BCP)

Business Continuity Planning ensures that critical business operations can continue during and after a disruption. The goal is to minimize downtime and reduce operational losses.

Key Components:

- **Business Impact Analysis (BIA)**: Identifies critical business functions and the impact of their disruption.
- **Risk Assessment**: Identifies threats and vulnerabilities affecting operations.
- **Continuity Strategies**: Defines actions to maintain or quickly resume operations.
- **Plan Development**: Documents roles, responsibilities, procedures, and contact lists.
- **Testing and Maintenance**: Ensures the plan is effective and current.

Disaster Recovery Planning (DRP)

Disaster Recovery is a subset of BCP focusing on the recovery of IT systems, applications, and data.

DR Elements:

- **Backup Solutions**: Regular backups and offsite storage
- **Recovery Sites**:
  - **Hot Site**: Fully equipped, ready-to-go
  - **Warm Site**: Partially equipped, some setup required
  - **Cold Site**: Basic infrastructure, setup needed before use
- **DR Procedures**: Step-by-step instructions to restore services

KEY METRICS IN BCP/DRP

Recovery Time Objective (RTO)

The maximum acceptable amount of time that a system, application, or function can be down after a disaster before causing significant damage to the business.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss measured in time. It refers to the point in time to which data must be restored after a disaster.

Business Impact Analysis (BIA)

A critical component of BCP that identifies:

- Critical functions and processes
- Dependencies and interconnections
- Potential impacts of disruptions (financial, reputational, operational)

The BIA helps prioritize systems and processes for recovery efforts.

TABULAR SUMMARY: BCP/DRP CORE CONCEPTS

Term	Definition	Purpose
RTO	Recovery Time Objective – Max time system/process can be down before causing major disruption	Defines acceptable downtime before full recovery

RPO	Recovery Point Objective – Max age of data loss acceptable in disaster	Determines backup frequency and tolerable data loss
BIA	Business Impact Analysis – Identifies critical systems and their interdependencies	Guides resource prioritization and recovery planning
DRP	Disaster Recovery Plan – Technical plan to recover IT infrastructure after disruption	Ensures continuity of IT services
BCP	Business Continuity Plan – Broad strategy to maintain operations during and after a crisis	Ensures continued business functionality, not just IT
SLA	Service Level Agreement – Agreement with vendors detailing recovery responsibilities and timing	Ensures expectations and responsibilities are clearly defined

SERVICE LEVEL AGREEMENTS (SLA)

An SLA is a contract between a service provider and a customer that outlines expected performance metrics and responsibilities.

Key Elements:

- **Uptime Guarantee**: Availability commitment (e.g., 99.9%)
- **Response Times**: Timeframes for acknowledging and resolving issues
- **Penalties**: Consequences for not meeting targets
- **Support Scope**: What is covered (hardware, software, network)

SLAs ensure accountability and measurable service standards for both internal and external service providers.

SECURITY DOCUMENTATION

Importance of Documentation

Well-maintained security documentation supports compliance, guides response efforts, and enables continuity of operations. It should be:

- Clear, concise, and accessible
- Regularly reviewed and updated
- Mapped to controls and policies

Key Types:

- **Policies**: High-level intent and direction (e.g., Information Security Policy)
- **Standards**: Mandatory control specifications (e.g., encryption protocols)
- **Procedures**: Operational steps for consistent implementation (e.g., patching process)
- **Guidelines**: Flexible recommendations (e.g., secure coding best practices)
- **Plans**: Detailed guidance for incident response, disaster recovery, and business continuity

PERSONNEL SECURITY POLICIES

Personnel security policies are a critical part of an organization's overall security program. These policies focus on managing human risk by ensuring that individuals with access to sensitive assets are properly vetted, trained, monitored, and managed throughout their tenure. Proper personnel security helps reduce the risk of insider threats, fraud, social engineering attacks, and negligence.

Objectives of Personnel Security

- Ensure trustworthiness and reliability of personnel
- Mitigate insider threats and enforce accountability
- Align human resources practices with security policies
- Promote a secure organizational culture

Key Elements of Personnel Security:

1. Pre-Employment Screening

Before hiring, organizations must assess the risk posed by prospective employees.

- **Background Checks**:
  - Criminal history checks
  - Employment and professional reference verification
  - Financial and credit checks (where legally allowed)
  - Drug screening (depending on the organization's policies)
- **Verification of Identity**: Confirming legal documents, citizenship, and work authorization

- **Position Sensitivity Classification**: Aligning the level of screening with job sensitivity (e.g., access to classified information)

2. Employment Agreements

Employees should sign formal agreements that clearly state:

- **Non-Disclosure Agreements (NDAs)** to protect confidential and proprietary information
- **Acceptable Use Policy (AUP)** covering allowed use of systems, internet, devices, etc.
- **Security Responsibilities**: Awareness of obligations regarding data protection and compliance
- **Intellectual Property (IP) Agreements**: Assigning ownership of work products

3. Onboarding and Security Orientation

- Initial security training: Data handling, password hygiene, phishing awareness
- Provide employees with access rights based on the principle of least privilege
- Familiarization with incident reporting procedures

4. Access Control and Monitoring

- Implement **Role-Based Access Control (RBAC)** or Attribute-Based Access Control (ABAC)
- **Access Reviews**: Conduct periodic reviews to ensure access is still appropriate
- Use logging and monitoring tools to detect suspicious activities (SIEM systems)
- Identity lifecycle management: provisioning, de-provisioning, and changes

5. Ongoing Monitoring and Supervision

- Regular feedback and performance reviews
- Behavior monitoring for signs of discontent or insider threat indicators
- Technical controls like screen monitoring, email filtering, and endpoint detection

6. Job Rotation and Mandatory Vacations

- Helps uncover fraud or improper activity
- Cross-trains employees to reduce knowledge silos
- Encourages transparency and accountability

7. Disciplinary Process and Enforcement

- Clearly documented disciplinary process for violations
- Tiered response structure (warning, suspension, termination)
- Ensure actions are consistent, fair, and legally sound

8. Termination and Offboarding

- **Immediate Termination Actions**:
  - Disable all system access
  - Retrieve devices, ID cards, tokens, access badges
  - Escort from premises (in high-risk cases)
- **Exit Interview**:
  - Reiterate NDA obligations
  - Understand reasons for leaving and gather feedback
- Document all termination-related actions for audit purposes

These security measures extend beyond IT—they depend heavily on collaboration between HR, Legal, IT Security, and Management.

TABULAR SUMMARY: PERSONNEL SECURITY POLICIES

Security Phase	Controls/Activities	Purpose
Pre-Employment	Background checks, identity verification, position sensitivity classification	Validate trustworthiness and reduce initial risk
Employment Agreements	NDA, AUP, IP ownership clauses, code of conduct	Set legal and behavioral expectations
Onboarding	Security training, assigning least-privilege access, familiarization with policies	Prepare employee to act securely from day one
Access Monitoring	RBAC, access review, logging, identity lifecycle controls	Ensure access is appropriate and traceable

Ongoing Monitoring	Performance reviews, anomaly detection, email/screen monitoring	Identify potential insider threats early
Job Rotation/Vacation	Cross-training, mandatory leave, control review during absence	Reduce fraud and improve organizational resilience
Disciplinary Actions	Clear consequences, escalation procedures, documentation	Enforce accountability and consistency
Termination	Revoke access, recover assets, exit interview, document actions	Prevent post-exit threats and maintain records

INTEGRATING SECURITY IN THE SOFTWARE DEVELOPMENT LIFECYCLE (SDLC)

Software security must be an integral part of every stage in the Software Development Lifecycle (SDLC). Failing to do so leads to insecure systems, compliance violations, and increased remediation costs.

Core Objectives

- Build secure applications from the ground up
- Identify and fix vulnerabilities early
- Comply with legal and industry regulations (e.g., GDPR, PCI-DSS)

Secure SDLC Phases in Detail:

1. Initiation / Requirements Gathering

- Define **security functional requirements** (e.g., access control, encryption)
- Perform **regulatory impact assessments** (HIPAA, GDPR, etc.)
- Document threat environment and business objectives

2. System Design

- Perform **architectural risk analysis** and **threat modeling**
- Define **security architecture components** (firewalls, IDAM, audit logging)
- Use secure design patterns (e.g., segmentation, input validation)
- Establish secure trust boundaries and data flow diagrams

3. Implementation / Development

- Follow **secure coding guidelines**:
  - Avoid SQL injection, XSS, CSRF, buffer overflows
  - Validate input and sanitize output
- Use tools like:
  - **Static Application Security Testing (SAST)**
  - **Software Composition Analysis (SCA)** to check for third-party library vulnerabilities
- Conduct **code reviews and peer validation**

4. Testing and Validation

- **Dynamic Application Security Testing (DAST)**: Analyzes running apps for vulnerabilities
- **Interactive Application Security Testing (IAST)**: Combines SAST and DAST features
- **Penetration Testing**: Simulates real-world attacks
- **Fuzz Testing**: Tests input handling with random data
- Ensure regression testing does not introduce new vulnerabilities

5. Deployment

- Harden deployment environments (e.g., OS, web servers)
- Apply **Change Management**: All changes are tested and approved
- Secure configurations (disable default accounts, close unused ports)

6. Maintenance & Operations

- Continuous monitoring of logs and alerts (SIEM integration)
- Patch management: Timely updates for OS and app vulnerabilities
- Perform **post-release security assessments**
- Conduct regular **vulnerability scans and audits**

Secure SDLC Methodologies

- **Waterfall**: Linear progression—security reviews at each phase
- **Agile**: Iterative development—embed security in each sprint
- **DevSecOps**:

- Integrates security into DevOps pipelines
- Automates security checks (SAST/DAST tools during CI/CD)
- Encourages collaboration across development, security, and operations

Secure SDLC Phases in Detail:

Tabular Summary for Quick Understanding

Phase	Security Activities	Tools/Practices
1. Requirements Gathering	- Define security goals- Identify legal & compliance needs- Perform risk assessments	- Security requirement checklists- Data classification tools
2. Design	- Threat modeling- Define secure architecture- Set trust boundaries	- STRIDE, PASTA- DFD tools- Security architecture reviews
3. Development	- Apply secure coding standards- Conduct peer code reviews- Use vetted libraries	- SAST (e.g., SonarQube)- OWASP ESAPI- Code linters
4. Testing & Validation	- Conduct DAST/IAST- Penetration & fuzz testing- Validate regression tests	- DAST (e.g., OWASP ZAP)- IAST tools- Burp Suite, Fuzzers
5. Deployment	- Enforce secure configurations- Implement change controls- Validate environments	- CIS Benchmarks- IaC scanning tools- Config checklists
6. Maintenance & Monitoring	- Patch systems- Monitor logs- Audit controls and vulnerabilities	- SIEM (e.g., Splunk)- Nessus, Qualys- Log analyzers

Standards and Frameworks

- **OWASP Software Assurance Maturity Model (SAMM)**
- **NIST Secure Software Development Framework (SSDF)**
- **ISO/IEC 27034**: Guidelines for application security

A secure SDLC improves quality, lowers costs, reduces risk exposure, and helps meet audit requirements.

FINAL THOUGHTS ON DOMAIN 1

Security and Risk Management forms the foundation of the CISSP curriculum. It emphasizes:

- Aligning security with business strategy
- Understanding governance, compliance, and law
- Implementing a risk-based approach to security
- Protecting the CIA triad (Confidentiality, Integrity, Availability)
- Promoting ethics, awareness, and training

A strong grasp of Domain 1 principles enables professionals to build secure, resilient, and compliant information systems while supporting the goals of the organization.

Thank You

Want to learn CISSP?
Get trained for just
₹4,999/- at MoS!

MINISTRY OF
MOS
SECURITY

WWW.MINISTRYOFSECURITY.CO