FastTrack CISSP Reference

By Jobyer Ahmed(OSCE3, OSCP, CNVP)

Table of Contents

Domain 1 – Security & Risk Management

1. Professional Ethics

Guide decisions when law, business, and security conflict. **(ISC)² Code of Ethics:**

1. Protect society, the common good, public trust, and infrastructure.
2. Act honorably, honestly, justly, responsibly, legally.
3. Provide diligent, competent service to principals.
4. Advance and protect the profession.

2. CIAAN + DAD Opposite

Goal	Essence	Sample Controls	Opposite (DAD)
Confidentiality	Keep data private	Encryption, need-to-know	Disclosure
Integrity	Keep data accurate	Hash, digital sig, change ctrl	Alteration
Availability	Keep systems usable	Redundancy, UPS, DRP	Destruction/DoS
Authenticity	Verify source	Certificates, MFA	Spoofing
Non-Repudiation	Prevent denial	Digital sig + logs	Repudiation

Quick test: “Verify origin?” – Authenticity. “Prove transaction?” – Non-repudiation.

3. The IAAA Chain

Step	Meaning	Example / Cue
Identification	Claim identity	Username, badge ID
Authentication	Prove identity	Password, OTP, biometrics
Authorization	Decide what can be done	RBAC, least privilege
Accountability	Trace actions	Logging, SIEM, time sync

Order never changes. Shared accounts = no accountability.

4. Due Diligence vs Due Care

Term	When	Meaning	Example
Due Diligence	Before	Plan & analyze risk	Vendor assessment
Due Care	After	Act & implement controls	Apply patches
Negligence	Failure to act reasonably	No monitoring after known risk	

Shortcut: Diligence = Think first ; Care = Act after.

5. Governance vs Management

Concept	Governance	Management
Focus	“What & Why” – direction, policy, accountability	“How” – execution, enforcement
Owner	Senior Management / Board	CISO / Ops Teams
Output	Policies, risk appetite, oversight	Standards, procedures, baselines

Policy hierarchy: Policy – Standard – Procedure – Guideline (optional).

Tip “Who is ultimately accountable for security?” **Senior Management.**

6. Legal Systems

Laws differ worldwide; understanding the system determines how accountability and compliance are enforced.

Type	Key Features	Common Regions	Tip
Common Law	Judge-made precedents; flexible interpretation.	United States, United Kingdom, Canada, Australia	"Court rulings or precedent" – Common Law
Civil (or Code) Law	Written codes define everything; judges apply statutes only.	Europe, Asia, South America	"Statute-based, no precedent" – Civil Law
Religious Law	Derived from religious texts (e.g., Sharia, Canon).	Middle East and others	Faith-based jurisdiction
Customary Law	Rooted in community practice or tradition.	Africa, South Pacific	Local customs form part of law

Sub-branches of law (Common Law context):

- **Criminal Law –** Government vs individual; punishment (imprisonment or fine).
- **Civil Law –** Individual vs individual; compensation (damages).
- **Administrative / Regulatory Law –** Government agency enforces rules (Federal Information Security Management Act – FISMA, Health Insurance Portability and Accountability Act – HIPAA, General Data Protection Regulation – GDPR).

FastTrack Tip: "Prosecution / crime" – Criminal. "Damages / lawsuit" – Civil. "Fine / compliance agency" – Administrative.

7. Liability and Negligence

Defines the legal accountability of security professionals and organizations for actions, or inaction, that lead to harm.

Concept	Meaning	Example / Tip
Due Diligence	Investigate before acting (planning and risk assessment).	Vendor security review before contract.
Due Care	Take reasonable action after assessment (control implementation).	Deploy patches, train staff, monitor systems.
Negligence	Failure to act reasonably after risk known.	Ignoring vulnerabilities = liable.
Prudent-Person Rule	Would a reasonable manager have done the same?	Used to judge negligence in court.

FastTrack Tip: Due Diligence = *Think before*; Due Care = *Act after*; Negligence = *Ignored both.*

8. Evidence and Admissibility

In legal or forensic investigations, evidence must meet strict requirements to be accepted in court or internal proceedings. The CISSP exam expects you to recall the five admissibility criteria and evidence types.

Evidence Type	Description	Example
Real / Physical	Tangible items.	USB drive, hardware device.
Documentary	Written or digital records.	System logs, emails, contracts.
Testimonial	Statements from people.	Witness interview.
Demonstrative	Visual illustrations.	Chart showing timeline of attack.

Admissible Evidence must be:

- **Relevant** – Directly relates to the case or claim.
- **Authentic** – Proven origin (chain of custody intact).
- **Accurate** – Collected and preserved correctly.
- **Complete** – Nothing omitted that changes meaning.

- **Convincing** – Persuasive to an impartial observer.

Rules of Evidence

- **Best Evidence Rule:** Use the original whenever possible.
- **Chain of Custody:** Document every person handling evidence; record time/date.
- **Hearsay Rule:** Second-hand statements are inadmissible (except system logs kept in ordinary business).
- **Order of Volatility:** CPU – RAM – Network – Disk – Backups.

FastTrack Tip: "Prove file untampered" – Calculate hash. "Who handled evidence?" – Chain of Custody. "Which to collect first?" – Volatile data.

9. Intellectual-Property (IP) Protections

Safeguards the creations of the mind - inventions, code, designs, and content - giving creators exclusive rights and protecting organizations from legal and ethical violations.

Type	Protects	Duration	Notes / Cue
Copyright	Creative works, software code, documents.	Life of author + 70 years.	Exists automatically upon creation.
Trademark	Brand name, logo, slogan.	Renewable every 10 years.	Must remain in use.
Patent	Novel invention or process.	About 20 years.	Public disclosure required.
Trade Secret	Confidential business information.	While kept secret.	Lose protection if disclosed.

FastTrack Tip: Copyright = creative, Patent = invention, Trademark = brand, Trade Secret = confidential info.
Note: *Reverse engineering* is often restricted under copyright/patent law unless explicitly allowed.

10. Privacy and Data-Protection Laws

Establish rules for how organizations collect, process, store, and share personal data - ensuring individuals' rights are protected and organizations act responsibly.

Core Principles (Across Regulations)
Lawfulness - Fairness - Transparency - Purpose Limitation - Data Minimization - Accuracy - Storage Limitation - Integrity & Confidentiality - Accountability.

Law / Regulation	Region	Focus / Scope	Key Tip
General Data Protection Regulation (GDPR)	European Union	Protects personal data of EU citizens; requires 72-hour breach notification.	"Cross-border EU data transfer."
California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA)**	U.S. – California	Consumer opt-out and data-sale rights.	"Right to opt-out of data sharing."
Health Insurance Portability and Accountability Act (HIPAA)	United States	Protects Protected Health Information (PHI).	"Hospital data breach / patient records."
Gramm-Leach-Bliley Act (GLBA)	United States	Safeguards customer financial information in banks.	"Bank shared customer data."
Sarbanes-Oxley Act (SOX)	United States	Ensures financial reporting accuracy and executive accountability.	"CEO falsified financial statements."
Federal Information Security Management Act (FISMA)	U.S. Federal Agencies	Mandates agency information-security programs.	"Government system compliance."
Payment Card Industry Data Security Standard (PCI DSS)	Global Industry Standard	Protects credit-card data (contracts, not law).	"Merchant storing card numbers."

Roles under GDPR-style laws:

- **Data Controller** – Decides purpose and means of processing.
- **Data Processor** – Processes on controller's behalf.
- **Data Protection Officer (DPO)** – Monitors compliance and reports breaches.

Cross-Border Mechanisms: Standard Contractual Clauses (SCC), Binding Corporate Rules (BCR), Adequacy decisions, EU–U.S. Data Privacy Framework.

FastTrack Tip:

- "Patient data security" – **HIPAA.**
- "EU citizen data transfer" – **GDPR.**
- "Financial integrity / audit" – **SOX.**
- "Bank customer privacy" – **GLBA**.
- "Payment-card breach" – **PCI DSS.**

11. Export Controls and Cybercrime Laws

Law / Convention	Region	Focus	Tip
International Traffic in Arms Regulations (ITAR)	U.S.	Defense and military technology exports.	"Export of encryption to foreign nation."
Export Administration Regulations (EAR)	U.S.	Dual-use technologies (civil + military).	"Advanced chip export restriction."
Computer Fraud and Abuse Act (CFAA)	U.S.	Criminalizes unauthorized system access.	"Unauthorized testing without written approval."
Computer Misuse Act	United Kingdom	Unauthorized access or modification.	"Hacker in London modifies bank data."
Convention on Cybercrime (Budapest Convention)	International	Harmonizes cybercrime laws and cross-border cooperation.	"Global ransomware extradition case."

Enticement vs Entrapment

- **Enticement (legal):** Offers chance to commit crime already intended (e.g., honeypot).
- **Entrapment (illegal):** Induces a person to commit a crime they otherwise wouldn't.

12. Risk Management

Risk management is a **continuous, business-driven process** used to identify, analyze, evaluate, and control anything that could harm organizational objectives, assets, or reputation. The goal is not to eliminate risk but to **reduce it to a level the business is willing to accept**, known as its *risk appetite.*

FastTrack Tip: Risk cannot be eliminated; it can only be managed, transferred, or accepted.

12.1 Key Terminology

Term	Meaning	Example / Tip
Asset	Anything of value to the organization.	Data, systems, people, or brand value.
Threat	Potential cause of an unwanted event.	Hacker, insider, or natural disaster.
Vulnerability	Weakness that a threat could exploit.	Unpatched software or weak password.
Risk	Probability multiplied by impact of a threat exploiting a vulnerability.	Malware exploiting outdated system.
Impact	Negative result if an event occurs.	Downtime, fines, or data loss.
Exposure	Condition of being subject to potential loss.	Lack of backup or recovery site.

Term	Meaning	Example / Tip
Residual Risk	Risk that remains after controls are applied.	Some chance of outage still exists.

Formula: Risk = Threat × Vulnerability × Impact
FastTrack Tip: *"what remains after controls,"* the correct term is **residual risk**.

12.2 Risk Categories

Category	Description	Sample Scenario
Strategic	Long-term business or market decisions.	Expanding into an unstable region.
Operational	Day-to-day processes or human error.	Accidental data deletion.
Financial	Market or investment-related loss.	Currency fluctuation, internal fraud.
Compliance / Legal	Violation of laws or regulations.	GDPR non-compliance resulting in fines.
Reputational	Damage to public trust or brand image.	Data breach made public.

FastTrack Tip: Regulatory or fine-related issues indicate **compliance risk**. Loss of customer trust indicates **reputational risk**.

12.3 Risk Analysis Methods

Method	Description	Example / Tip
Qualitative	Uses expert judgment and rating scales such as Low, Medium, High.	"Phishing likelihood is high; impact is medium."
Quantitative	Uses numeric values and monetary cost.	Calculates Annualized Loss Expectancy (ALE).
Hybrid	Combines both methods for a balanced view.	Mix of dollar value and expert scoring.

FastTrack Tip: If management requests a dollar value, use **quantitative analysis**. If the team uses experience or scales, use **qualitative analysis**.

12.4 Quantitative Risk Formulas

Term	Definition	Formula / Example
Asset Value (AV)	Monetary worth of an asset.	Database valued at $100 000.
Exposure Factor (EF)	Percentage of asset value lost per event.	30 percent = 0.3.
Single Loss Expectancy (SLE)	Expected loss from one event.	AV × EF = $30 000.
Annual Rate of Occurrence (ARO)	Estimated frequency per year.	Two incidents per year.
Annualized Loss Expectancy (ALE)	Yearly expected loss.	SLE × ARO = $60 000 per year.

FastTrack Tip: If AV = $100 000, EF = 25 percent, and ARO = 2, then SLE = $25 000 and ALE = $50 000 per year.

12.5 Risk-Treatment Options

Option	Action	Example / Tip
Mitigate (Reduce)	Apply controls to lower likelihood or impact.	Install patches or enable multifactor authentication.
Transfer (Share)	Shift the risk to another party.	Purchase cyber-insurance or outsource services.

Option	Action	Example / Tip
Accept	Acknowledge and document low-impact risk.	Management signs formal acceptance.
Avoid	Eliminate the risky activity entirely.	Disable insecure protocol or cancel the project.
Ignore / Reject	Take no action – generally unacceptable.	-

FastTrack Tip:
Buying insurance means *transferring risk.*
Implementing a control means *mitigating risk.*
Stopping the activity means *avoiding risk.*
Formally approving the risk means *accepting risk.*

12.6 Risk Lifecycle - Continuous Process

1. Identify assets, threats, and vulnerabilities.
2. Assess or analyze likelihood and impact.
3. Prioritize and treat based on severity.
4. Implement appropriate controls.
5. Monitor and review effectiveness and environmental change.

FastTrack Tip: After assessment, the next logical step is to **treat or respond** to the identified risks.

12.7 Risk Metrics and Indicators

Metric	Focus	Example / Tip
Key Performance Indicator (KPI)	Measures how well controls perform.	Patch-compliance rate of 98 percent.
Key Risk Indicator (KRI)	Early signal that risk is increasing.	Phishing-click rate trending upward.
Key Goal Indicator (KGI)	Measures success of business objectives.	Downtime below 1 percent per quarter.

FastTrack Tip:
KPI measures control performance.
KRI provides early warning.
KGI measures business outcome success.

12.8 Roles and Responsibilities

Role	Primary Responsibility
Senior Management / Board	Defines risk appetite and holds ultimate accountability.
Risk Owner	Decides on treatment and acceptance of specific risks.
Chief Information Security Officer (CISO)	Advises management and oversees overall risk posture.
Security Team	Performs assessments and implements controls.
Auditor	Verifies control effectiveness and reporting accuracy.

FastTrack Tip: Senior management is always ultimately accountable. The risk owner is responsible for mitigation or acceptance.

12.9 Appetite, Tolerance, and Threshold

Term	Definition	Example / Tip
Risk Appetite	Overall level of risk the organization is willing to	“Moderate cyber-risk exposure is acceptable.”

Term	Definition	Example / Tip
	accept.	
Risk Tolerance	Acceptable variation within that appetite.	Finance allows 1 percent credit loss.
Risk Threshold	Trigger point for action or escalation.	If phishing-click rate exceeds 10 percent, retraining required.

FastTrack Tip: Risk appetite is the overall limit, risk tolerance is the acceptable range, and risk threshold is the point that demands action.

12.10 Risk Register and Reporting

A **living document** that records and tracks every identified risk, its owner, impact, treatment plan, and review schedule.

Field	Example Entry
ID	R-07
Description	Legacy VPN gateway vulnerable to CVE-2025-1234
Impact	High – remote-access compromise possible
Likelihood	Medium
Owner	Network Manager
Treatment	Mitigate – replace with patched version
Status	In progress
Review Date	Quarterly

FastTrack Tip: The risk register is the official record tracking risk status, owner, and treatment progress.

12.11 Risk Communication and Reporting

Transforms technical findings into clear, actionable insights that management can use for decision-making.

Principles

- **Clarity:** Express risks in business terms such as cost, downtime, or compliance exposure.
- **Relevance:** Relate each risk to organizational objectives.
- **Prioritization:** Highlight the most severe or likely risks first.
- **Actionability:** Include clear, recommended mitigations.
- **Documentation:** Maintain a verifiable audit trail of all reporting.

FastTrack Tip: When briefing executives, present a summarized **risk dashboard** with key metrics and trends instead of raw technical data.

13. Security Frameworks and Standards

Frameworks give structure and consistency to how risk, controls, and compliance are managed.
They define **“what good looks like”** and help align security with business strategy.

Framework	Focus / Scope	Managerial Cue
International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 27001	Builds an Information Security Management System (ISMS) using the Plan–Do–Check–Act (PDCA) cycle.	Use for global certification or governance baseline.
ISO / IEC 27002	Provides control objectives and guidance.	Operational “how-to” companion

		for ISO 27001.
ISO 27005	Defines information-risk management process (aligns with ISO 31000).	Consistent risk documentation across projects.
National Institute of Standards and Technology (NIST) Risk Management Framework (RMF – Special Publication 800-37)	Six-step lifecycle: Categorize – Select – Implement – Assess – Authorize – Monitor.	Mandatory for U.S. federal systems; useful anywhere continuous monitoring is required.
NIST Cybersecurity Framework (CSF)	Outcome-based model: Identify, Protect, Detect, Respond, Recover.	Excellent for maturity assessments and board communication.
NIST SP 800-53	Catalog of security and privacy controls supporting RMF.	Control library for tailoring baselines (Low / Moderate / High).
Control Objectives for Information and Related Technologies (COBIT 2019)	IT-governance and performance-management framework.	Links technology objectives to business value.
Committee of Sponsoring Organizations (COSO Enterprise Risk Management)	Enterprise-wide risk and internal-control framework.	Board-level risk integration and appetite definition.
Sherwood Applied Business Security Architecture (SABSA)	Security-architecture method tracing business drivers to technical design.	Ensures architecture aligns with policy intent.
Payment Card Industry Data Security Standard (PCI DSS)	Protects payment-card data; contractual requirement.	Mandatory for merchants handling cardholder data.

FastTrack Tip:

- Global certification baseline – ISO 27001 + 27002.
- Federal authorization & monitoring – NIST RMF + SP 800-53.
- Board-level risk oversight – COBIT + COSO ERM.
- Architecture traceability – SABSA.

14. Control Maturity and Risk Analysis Models

Defines how effectively an organization's security processes are structured, measured, and continuously improved. These models help assess process maturity and translate risk into measurable, business-aligned terms.

Model	Essence	Professional Use
Capability Maturity Model Integration (CMMI)	Levels 1 to 5 (Initial – Optimized) measure process maturity.	Benchmark repeatability and predictability of security programs.
Factor Analysis of Information Risk (FAIR)	Quantifies risk in financial terms (probable loss exposure).	Converts cyber-risk into business language and ROI.
Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)	Self-directed, qualitative, people-centric risk assessment.	Empowers internal teams; focuses on awareness over audit.

FastTrack Tip: CMMI = Process discipline; FAIR = Financial clarity; OCTAVE = Cultural awareness.

15. Plan–Do–Check–Act (PDCA) Cycle

A continuous improvement framework used in ISO 27001 and NIST RMF to maintain and refine information security management systems. It ensures policies are planned, implemented, reviewed, and enhanced in an ongoing feedback loop.

Phase	Managerial Focus	Example
Plan	Define policies, objectives, risk criteria.	Create ISMS policy and risk register.

Do	Implement and operate controls.	Deploy Multi-Factor Authentication and logging.
Check	Audit, measure, and review results.	Conduct internal audit; track Key Performance Indicators (KPI).
Act	Correct and enhance processes.	Update procedures; refine training.

FastTrack Tip: If audits never change policy = PDCA is broken; improvement occurs in **Act** phase.

16. Governance, Risk, and Compliance (GRC) Integration

Aligns organizational strategy, risk management, and regulatory compliance into a unified framework. GRC ensures that business objectives, security policies, and controls all work together, promoting accountability, consistent decision-making, and efficient use of resources while maintaining compliance with laws and standards.

Element	Objective	Example Practices
Governance	Define authority and accountability.	Board charters, security committees, policy hierarchy.
Risk Management	Identify, assess, and treat threats.	Enterprise risk register, appetite statements, owner assignments.
Compliance	Demonstrate conformity with obligations.	Audit mapping (GDPR, PCI DSS), evidence repositories.

Governance Hierarchy: Policy – Standard – Procedure – Guideline.

Metrics: KPI (control performance), KRI (emerging risk), KGI (goal success).
FastTrack Tip: Governance = Direction Risk = Decision Compliance = Proof. Mnemonic – **GRC = Direction + Protection + Verification.**

17. Threat Modeling Frameworks

Threat modeling proactively identifies possible attack paths before system deployment.

Model	Focus / Purpose	CISSP Cue
STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege)	Microsoft model to categorize threats by violated security property.	“Systematic identification of potential threats.”
Process for Attack Simulation and Threat Analysis (PASTA)	Seven-stage, business-driven, risk-aligned methodology.	Connects technical threats to business impact.
Damage, Reproducibility, Exploitability, Affected Users, Discoverability (DREAD)	Quantitative scoring (0–10 per factor) to prioritize risks.	“Rank severity numerically.”
Attack Trees	Visual graph from attacker goal (root) to possible steps (branches).	“Visualize attacker paths and counter-measures.”
Cyber Kill Chain / MITRE ATT&CK	Describes attack lifecycle (Reconnaissance – Exfiltration).	“Phase-based view of attacker behavior.”

Typical Kill Chain Phases Reconnaissance – Weaponization – Delivery – Exploitation – Installation – Command & Control – Actions on Objectives.

18. Applying Threat Modeling

Steps to evaluate any system design:

1. **Identify Assets and Data Flows** – What needs protection?
2. **Define Trust Boundaries** – Where control shifts between entities.
3. **Identify Threats** – Use STRIDE categories.
4. **Find Vulnerabilities and Existing Controls.**
5. **Prioritize Risks** – Rate by impact or DREAD score.
6. **Mitigate and Validate** – Implement and test defenses.

FastTrack Tip: Threat Modeling = “Predict attacks before they happen.”

19. Business Continuity and Disaster Recovery Planning (BCP / DRP)

keep critical business functions running during disruption and restore them within acceptable limits. Continuity = people + process + technology + resilience.

19.1 Planning Lifecycle

1. **Initiation** – Obtain senior-management approval and funding.
2. **Business Impact Analysis (BIA)** – Identify critical processes, dependencies, and allowable downtime.
3. **Risk Assessment** – Analyze threats to those processes.
4. **Strategy Development** – Select recovery strategies (alternate sites, cloud, redundancy).
5. **Plan Development** – Document roles, procedures, and communication paths.
6. **Testing and Exercises** – Validate plan effectiveness.
7. **Maintenance** – Update after changes or tests.

FastTrack Tip: “If never tested – plan = theory.”

19.2 Key Recovery Metrics

Defines the time-based objectives used in business continuity and disaster recovery planning. These metrics establish how long systems can be down, how much data loss is acceptable, and the total time needed to restore normal operations after a disruption.

Metric	Definition	Example
Recovery Time Objective (RTO)	Maximum downtime tolerable before impact.	“4 hours.”
Recovery Point Objective (RPO)	Maximum acceptable data loss (in time).	“1 hour.”
Maximum Tolerable Downtime (MTD)	Latest time before business failure.	“48 hours.”
Work Recovery Time (WRT)	Time to resume normal operations after systems recovered.	“2 hours.”
Formula	MTD ≥ RTO + WRT	

FastTrack Tip: If RTO + WRT > MTD – Plan fails.

19.3 Site Types and Testing

Outlines the different recovery site options and how continuity plans are validated through testing. Site types determine recovery speed and cost, while progressive testing methods ensure readiness without unnecessary disruption.

Category	Description	Typical RTO
Hot Site	Fully operational duplicate; instant switchover.	Minutes
Warm Site	Pre-configured, partial data.	Hours
Cold Site	Power + space only.	Days
Mobile / Cloud	Portable or virtual alternative.	Varies

Testing Methods: Checklist, Table-top, Simulation, Parallel, Full Interruption.
FastTrack Tip: Test escalation should progress from non-disruptive to realistic.

20. Personnel Security and Lifecycle Management

Phase	Primary Controls	Purpose
Pre-Employment	Background checks, verification, NDA	Ensure trustworthiness

Onboarding	Account provisioning, policy acknowledgment	Establish accountability
During Employment	Job rotation, mandatory vacation, least privilege	Detect fraud & enforce resilience
Transfer / Role Change	Access review and re-authorization	Prevent privilege creep
Termination	Immediate access revocation + exit interview	Eliminate lingering risk

FastTrack Tip: Mandatory vacation – fraud detection indicator.

21. Security Awareness and Training

Level	Goal	Example
Awareness	Shape attitude and attention.	Posters, emails, phish-tests.
Training	Build specific skills.	Incident-response drill, secure coding.
Education	Deep knowledge and career growth.	Professional certifications (CISSP, CISM).

Measurement Metrics: Phish-click rate ↓ Report rate ↑ Completion % ↑
FastTrack Tip: “Security culture ≠ training session - it’s behavior change.”

22. Supply-Chain Risk Management (SCRM)

Ensure that vendors and suppliers do not introduce vulnerabilities into your environment.

Principle	Practice
Visibility	Maintain inventory of suppliers and software components (Software Bill of Materials – SBOM).
Verification	Request audits (SOC 2 reports, ISO 27036 certification).
Integrity	Require signed code, tamper-evident packaging, and trusted delivery.
Resilience	Establish alternate suppliers and redundant channels.
Governance	Include SCRM clauses in contracts and risk register.

Frameworks: **NIST Special Publication 800-161 Revision 1**, **ISO 27036**.
FastTrack Tip: “Third-party risk = Your risk.”

23. Continuous Monitoring and Improvement

Continuous monitoring ensures security posture remains effective over time.

Phase	Objective	Example
Define	Select metrics and data sources.	Logs, tickets, patch status.
Collect	Automate data gathering.	SIEM (Security Information and Event Management), Vulnerability Scanner.
Analyze	Correlate events and trends.	Detect anomalies or control failures.
Respond	Take corrective actions.	Adjust rules, patch systems.
Report	Communicate status to management.	Dashboards, risk heat maps.

Maturity Models: Capability Maturity Model Integration (CMMI) Levels 1–5; NIST Cybersecurity Framework (CSF) Tiers 1–4; ISO PDCA cycle.

FastTrack Tip: Monitoring = “Measure - Adapt - Improve.”

24. Security Culture and Organizational Maturity

Measures how deeply security values are embedded across people, processes, and leadership. A mature security culture prioritizes accountability, learning, and continuous improvement over mere compliance.

Element	Indicator of Success
Leadership Support	Executives model secure behavior and allocate budget.
Accountability	Clear ownership for risk and controls.
Learning Culture	Near-miss sharing without blame.
Metrics and Feedback	Regular KPI / KRI review drives actions.

FastTrack Tip: “Culture eats policy for breakfast - make security a habit, not a rule.”

25. Threat Actors and Motives

Classifies the various individuals or groups behind cyber incidents, explaining why they attack and how they operate. Understanding their motives helps prioritize defenses and tailor threat intelligence.

Actor Type	Motivation	Common Behavior
Script Kiddies	Fun, fame	Use existing tools.
Hacktivists	Ideology	Defacement, leaks.
Insiders	Negligence or revenge	Data theft, sabotage.
Cybercriminal Groups	Profit	Ransomware, fraud.
Nation-States / Advanced Persistent Threat (APT)	Espionage	Long-term, stealth campaigns.
Competitors	Advantage	Trade-secret theft.
Supply-Chain Attackers	Indirect compromise via vendors.	Tampered updates.

FastTrack Tip: Insiders = most difficult to detect; APT = most persistent.

Domain 2 – Asset Security

1. What Asset Security Really Means

Asset Security makes sure every piece of information - and every system that stores, processes, or transmits it - gets protection proportional to business value, sensitivity, and criticality from creation to destruction.

FastTrack Tip: Classify first, then control. Protection without classification is guesswork.

2. Understanding Assets

Asset = anything of value. Track both tangible and intangible.

Type	Examples	Why it matters
Information	Databases, source code, contracts	Primary breach target
Software	Applications, Application Programming Interfaces, firmware	Vulnerabilities live here
Hardware	Servers, laptops, network gear	Loss = data exposure
People	Employees, admins, contractors	Privileged knowledge/credentials
Intellectual	Trade secrets, patents, algorithms, brand	Competitive edge
Facilities	Data centers, power/HVAC/links	Availability backbone

Inventory of record: Configuration Management Database (CMDB).

3. Ownership and Accountability

Defines who owns, implements, or verifies security controls - the backbone of governance and data responsibility.

Role	Responsibility	Exam Focus
Senior Management	Ultimate accountability; sets risk appetite; approves risk acceptance.	Overall accountability (CISSP default answer).
CISO	Implements strategy; reports effectiveness; advises on risk.	Not a data owner.
Business / Mission Owner	Owns the process; defines criticality and uptime needs.	Defines business impact.
Data / Information Owner	Assigns classification, handling, retention, and disposal.	Who defines classification – Data Owner.
System Owner	Ensures hosting environment matches classification.	Confirms proper control enforcement.
Data Custodian / System Admin	Implements controls (encryption, backup, ACLs).	Who implements controls – Custodian.
Security Administrator	Runs IAM, firewall, logging, and account management.	Operates, not decides.
Privacy Officer / DPO	Ensures compliance (GDPR, HIPAA).	Legal + privacy governance.
Users / Operators	Follow policy, report incidents.	Everyone’s responsibility.
Auditor / Assessor	Independently verifies control effectiveness.	Independence = assurance.

FastTrack Tip: Accountable = Senior Management · Defines classification = Data Owner · Implements = Custodian.

4. Classification of Information and Assets

Defines how data is categorized by sensitivity to ensure proper protection, handling, and disposal throughout its lifecycle.

Typical Levels	Example Handling Focus
Top Secret / Highly Confidential	National security, trade secrets
Secret / Confidential	Internal customer data
Internal Use Only	HR or internal documents
Public	Marketing materials

4.1 Classification Process

Outlines the structured steps to identify, evaluate, label, and periodically review information based on business impact. Key:

1. Identify asset.
2. Assess impact (Confidentiality, Integrity, Availability).
3. Assign classification level.
4. Define handling rules.
5. Label visibly and via metadata.
6. Review periodically.

FastTrack Tip: Classification must be owner-driven, consistent, and reviewed - not IT-driven.

4.2 Labeling and Metadata

- **Documents:** Header/footer labels + IRM/DLP tags.
- **Databases:** Field-level tags (“Contains PII”).
- **Cloud:** Metadata drives CASB and policy enforcement.
  FastTrack Tip: Labels must *trigger* controls (encryption, DLP) - not just decorate files.

4.3 Handling by Classification

Specifies how each classification level must be stored, transmitted, accessed, and destroyed to maintain confidentiality and compliance.

Level	Data at Rest	Data in Transit	Access Controls	Contracts / Compliance	Retention / Disposal
Public	Standard storage	HTTP	Basic access	–	Policy-based
Internal	Encrypted disk (AES-256)	TLS 1.2+	Authenticated users	NDA	Standard retention
Confidential	AES-256 + Key Mgmt Control	TLS 1.3 / IPsec / SFTP	Least privilege	DPA / audit clauses	Secure purge
Restricted	HSM / KMS with dual control	Mutual auth only	VDI / DLP restrictions	Vendor audit	NIST 800-88 destroy

5. Asset Inventory and Configuration Management

Maintains a complete record of all organizational assets and their configurations to ensure accountability, change control, and security integrity.

Inventory Records:
Asset ID, Owner/Custodian, Classification, Location, Criticality, Dependencies, Support status, Retention/Disposal evidence.

Maintain Accuracy:
Automated discovery · Reconciliation · Lifecycle flags · Integration with Change Management.

Configuration Management:
Approved baseline – Authorized change – Drift detection – Version control – Patch/Vulnerability linkage.

Manager Scenarios:
- Unknown device – isolate, identify owner, classify.
- Unsupported system – replace or isolate, accept risk formally.
- Unapproved change – treat as incident, rollback.

FastTrack Tip: If it's not in the CMDB, it's untrusted until proven otherwise.

6. Information Lifecycle and Secure Provisioning

Protects data from creation to destruction by enforcing ownership, classification, and secure deployment practices before production.

Lifecycle: Create – Use – Store – Transmit – Retain – Destroy.

Golden Rule: assign owner and classify at creation.

6.1 Secure Provisioning (before production)

- **Baseline hardening:** Gold images, remove unused services, patch, disable weak protocols (SMBv1, TLS 1.0).
- **Ownership & labeling:** Assign Data Owner, register in CMDB, set retention/disposal.
- **Access & identity:** Least privilege, MFA, separate admin accounts, break-glass approval.
- **Endpoints:** Full-disk encryption, Secure Boot, EDR, remote wipe.
- **Keys & secrets:** Store in HSM / KMS only; dual control; define cryptoperiods.
- **Pre-go-live checks:** Vulnerability/config scan, certificate review, CAB approval.
  FastTrack Tip: No system goes live unclassified or unhardened.

6.2 Data Minimization and Quality

- Collect only what is necessary and lawful.
- Ensure accuracy and integrity (input validation, hash/checksum).
- Enable Right to Rectification.
- Maintain immutable audit logs.
  FastTrack Tip: The less you keep, the less you can lose.

6.3 Location and Sovereignty

- Map where data resides (primary, replica, third party).
- Respect local laws of data location.
- Use Standard Contractual Clauses / Binding Corporate Rules for cross-border transfer.
- Keep encryption keys within region.
  FastTrack Tip: Data location defines law - keep keys where you control the jurisdiction.

7. Data Retention, Archival, and Disposal

Ensures data is retained only as long as needed, securely archived for audits, and permanently destroyed when no longer required.

7.1 Retention Policy

Defines how long each data type must be kept based on legal, regulatory, and business requirements.

- Define **purpose** (legal / business need).
- Specify **duration** per data type and region.
- Assign **owner** approval + legal validation.
- Maintain **readable format** until disposal.
- Automate via lifecycle rules.
  FastTrack Tip: Retention prevents premature deletion; destruction prevents unnecessary liability.

7.2 Archival Controls

Separates and secures long-term data storage to ensure accessibility, integrity, and traceability for audits.

- Separate archives from production (read-only).
- Encrypt and log access; test restore regularly.
- Apply hash or digital signature to verify integrity.
- Record every retrieval event.
  Tip: “Old data needed for audit” – restore from archive, not backup.

7.3 Legal Hold

Temporarily suspends data deletion during investigations or litigation to preserve evidence.

- Suspend deletion when litigation or investigation is active.
- Freeze records in production and backups.
- Document scope, start date, release authorization.
- Maintain chain of custody.
  FastTrack Tip: Deleting under legal hold = evidence destruction – legal liability.

7.4 Secure Destruction

Applies approved sanitization or destruction methods to eliminate data remnants and prevent unauthorized recovery.

Media Type	Method	Example
Magnetic (HDD)	Purge	Degauss or multi-pass overwrite
Solid-State (SSD / Flash)	Destroy	Crypto-erase or physical shred
Optical (CD / DVD)	Destroy	Pulverize or incinerate
Paper	Clear	Cross-cut shred, pulp, or burn

Maintain a **destruction certificate** tied to the asset ID for audit traceability.
FastTrack Tip: When in doubt - purge more, not less.

8. Data Backup and Recovery Alignment

Ensures data availability by creating secure, encrypted, and tested backups aligned with business recovery objectives.

8.1 Backup Principles

- Align frequency and scope to classification and RPO (Recovery Point Objective).
- Encrypt in transit and at rest (AES-256 minimum).
- Store keys separately in HSM / KMS.
- Perform regular restore tests - untested backups = false assurance.

- Protect backup indexes and metadata (they can reveal user paths or systems).
- Maintain segregation of duties between backup and production admins.
  FastTrack Tip: CISSP expects backups that are **encrypted, tested, isolated, and auditable.**

8.2 Off-Site and Cloud Backups

- Verify provider controls (Service Organization Control 2 / ISO 27001).
- Map data sovereignty - know which country retains each backup.
- Include encryption, retention, and destruction clauses in the SLA.
- Use dedicated accounts and least privilege access for backup operations.
- Ensure off-site backups are physically and logically isolated from production (to resist ransomware).
  FastTrack Tip: A “backup available but also encrypted by ransomware” – lack of isolation control.

8.3 Backup Validation Metrics

Measure how reliable and recoverable the backup process is.

- **Restore success rate (%)** – valid recoveries per attempt.
- **RTO (Restoration time)** – measured vs target.
- **Last verification date.**
- **Encryption compliance rate.**
- **Retention accuracy (under/over retention).**
  FastTrack Tip: What gets measured gets secured - validate backups like you validate firewalls.

9. Media and Physical Asset Handling

Protects information stored on physical media through controlled access, transport, and destruction processes.

9.1 Handling Rules by Sensitivity

Applies graduated physical security controls based on data classification and criticality.

Classification	Physical Protection
Public	Normal office controls
Internal	Locked cabinets / restricted areas
Confidential	Locked storage, limited keys, signed check-out
Restricted	Safe or vault, dual access control, chain-of-custody log

FastTrack Tip: Physical classification mirrors data classification - stronger label = stronger control.

9.2 Media Movement

Ensures secure transport, logging, and verification when media is transferred between locations or entities.

- Log all hand-offs and transport details.
- Use tamper-evident seals and encrypt data before shipment.
- Approve courier vendors and obtain delivery receipts.
  Scenario: “Tape lost in transit” – policy violation due to missing encryption + custody log.

9.3 Media Reuse and Disposal

Specifies sanitization and certified destruction practices to prevent data leakage from reused or discarded media.

- Re-classify before reuse; sanitize per original classification.
- Maintain destruction certificate for each asset.
- Never discard storage media with residual data in regular trash.

FastTrack Tip: Media handling = secure storage + controlled movement + safe reuse + verified destruction.

10. Privacy and Personally Identifiable Information (PII) Protection

Establishes safeguards for lawful and transparent handling of personal data while maintaining compliance and individual rights.

10.1 PII Lifecycle

1. **Collect** only necessary information (data minimization).
2. **Use** it for declared and lawful purposes (purpose limitation).
3. **Store** securely (encryption, access control, segregation).
4. **Allow rights** of access, rectification, deletion ("right to be forgotten").
5. **Dispose** securely once no longer needed.
   FastTrack Tip: CISSP scenarios expect "minimize, protect, honor user rights, and delete securely."

10.2 Privacy Laws and Frameworks

Summarizes global and regional privacy regulations that define how personal data must be collected, processed, and reported in case of breaches.

Law / Framework	Region / Scope	Key Requirement
GDPR	EU	Lawful basis, explicit consent, 72-hour breach notification
CCPA/CPRA	California (US)	Disclosure, opt-out, deletion rights
HIPAA	US (Healthcare)	Protect health info with administrative / technical safeguards
COPPA	US	Parental consent for data of children < 13
ISO/IEC 27701	Global	Privacy Information Management extension to ISO 27001

FastTrack Tip: "72 hours to report a breach" – think GDPR.

10.3 Privacy Impact Assessment (PIA)

Evaluates privacy risks before processing personal data to ensure compliance, transparency, and privacy by design.

- Map data flows (end to end including vendors).
- Identify risks to privacy rights and freedoms.
- Apply controls (anonymization, pseudonymization, consent management).
- Obtain approval from the Data Protection Officer (DPO).
  FastTrack Tip: New system collecting PII – run PIA before design approval ("privacy by design").

10.4 Additional Exam-Relevant Privacy Concepts

Covers essential GDPR-related roles, rights, and response requirements that define accountability in data protection.

- **Data Controller:** Determines why and how data is processed.
- **Data Processor:** Processes data on behalf of controller.
- **Consent Requirements:** Freely given, specific, informed, and revocable.
- **Data Subject Rights:** Access, Rectification, Erasure, Portability, Restriction, Objection.
- **Breach Response:** Detect – Notify – Document – Remediate – Report (within 72 hours under GDPR).
  FastTrack Tip: Accountability is the core privacy principle - prove compliance, don't just claim it.

11. Data Rights Management and Technical Enforcement

Protects sensitive information through encryption, access controls, and usage restrictions, ensuring only authorized users can view, edit, or share data, even after it leaves the organization.

11.1 Information Rights Management (IRM)

Enforces encryption and usage policies on documents to control viewing, editing, and sharing rights.

- Control document use (view, print, forward, expiry).
- Embed policy in document metadata; enforce via client plug-ins.
- Combine with DLP and Cloud Access Security Broker to prevent leakage.

11.2 Data Loss Prevention (DLP)

Monitors and blocks unauthorized transfer or exposure of sensitive data across email, cloud, and endpoints.

- **At rest:** scan repositories and file shares.
- **In motion:** inspect email and network flows.
- **In use:** monitor clipboard, print, USB.
- Define patterns (credit cards, names, project codes).
- Integrate with labeling and policy engines.

Manager logic: IRM controls usage; DLP controls movement. Together – enforce classification.

12. Third-Party and Cloud Data Governance

Ensures vendors and cloud providers protect organizational data with equal security, privacy, and accountability standards.

12.1 Shared Responsibility Model

Defines which security duties belong to the customer and which to the cloud provider across IaaS, PaaS, and SaaS models.

Cloud Model	Customer Responsible For	Provider Responsible For
IaaS (Infrastructure as a Service)	Data, applications, OS, network controls (e.g., firewall rules)	Physical servers, storage, and network fabric
PaaS (Platform as a Service)	Data and custom applications	OS, middleware, runtime environment
SaaS (Software as a Service)	Data content and user access control	Application stack and infrastructure

FastTrack Tip: “Shared responsibility” = provider secures the cloud – you secure what’s in it. Data breaches = customer governance failure.

12.2 Contractual Safeguards

Defines security, privacy, and audit obligations in vendor agreements to ensure accountability and compliance. Contracts must formalize expectations and accountability.

- Include **security, privacy, and audit clauses** aligned to regulation.
- Require **right to assess** or **third-party audit reports** (SOC 2, ISO 27001).
- Define **incident notification timelines** (e.g., < 72 h for PII breach).
- Specify **data location**, **deletion verification**, and **return on termination**.
- Enforce **liability and insurance** coverage.
  FastTrack Tip: No audit rights + no breach clause = no real assurance.

12.3 Cloud Data Lifecycle

Applies classification, encryption, and deletion controls across all cloud stages to maintain ownership and compliance.

- **Classify before upload**; apply encryption and labeling policies.
- Use **BYOK (Bring Your Own Key)** or **HYOK (Hold Your Own Key)** for sensitive data to retain cryptographic ownership.
- **Verify deletion** via provider logs or destruction certificate.
- Continuously audit configurations using **Cloud Security Posture Management (CSPM)** or **Cloud Workload Protection Platforms (CWPP)**.
  FastTrack Tip: CSPM finds misconfigurations before attackers do - always enable it.

13. Monitoring, Auditing, and Continuous Improvement

Provides ongoing verification and enhancement of control effectiveness to sustain a mature and resilient security posture.

13.1 Continuous Monitoring

Delivers near real-time visibility into system activity and policy compliance through centralized telemetry and analytics

- Aggregate telemetry from **SIEM**, **DLP**, **CASB**, and **EDR/NDR**.
- Detect unauthorized access, data exfiltration, or privilege escalation.
- Correlate events using automated rules and thresholds.
- Retain logs per law (HIPAA 6 yrs, SOX 7 yrs).
- Preserve integrity via **Write-Once-Read-Many (WORM)** or cryptographic hashing.
- Visualize trends and drift with dashboards for management.
  FastTrack Tip: “Ongoing verification of control effectiveness” – Continuous Monitoring.

13.2 Auditing and Assessment

Independently verifies that implemented controls meet policies, standards, and compliance requirements. Formal, documented verification that controls exist and work as intended.

- Compare actual settings against policies (classification, retention, encryption).
- Validate configuration hardening and patch compliance.
- Review third-party attestations (SOC 2, ISO 27001, PCI DSS).
- Record evidence – finding – corrective action – closure.
- Management must review and accept residual risk.
  Scenario: “Audit finds unencrypted archives” – re-encrypt, update SOPs, document closure.
  FastTrack Tip: Audit = independent proof that security controls match policy.

13.3 Metrics and Governance Review

Transforms monitoring and audit data into actionable insights that guide executive decisions and drive ongoing improvement.

- **Quantitative:** patch compliance %, audit closure %, MTTD, MTTR.
- **Qualitative:** culture maturity, training impact, management visibility.
- Review quarterly and feed results into **Plan–Do–Check–Act (PDCA)** cycle or ISO 27001 Continuous Improvement.
  FastTrack Tip: Monitoring = detect; Auditing = prove; Improvement = mature.

14. Security Awareness and Data Culture

Develops user behavior and organizational habits that make security part of everyday actions rather than an afterthought.

14.1 Awareness Program Core Topics

- Data classification & handling.
- Clean desk / clear screen discipline.
- Social engineering and phishing defense.
- Incident reporting channels.
- Secure use of removable media and cloud apps.
- Safe mobile work and remote access practices.
  FastTrack Tip: “Employee finds lost USB” – correct answer = report immediately.

14.2 Effective Awareness Program

Training must be **targeted, measured, and ongoing**.

- **Role-based:** customize content for developers, HR, finance, admins.
- **Continuous refreshers:** micro-learning and phishing simulations.
- **Measure impact:** completion %, incident reduction, behavioral change.
- **Leadership support:** executives model expected behavior.
  FastTrack Tip: Culture change = training + metrics + management example.

14.3 Embedding Security in Daily Processes

Integrates protection and compliance checks directly into everyday workflows for consistent enforcement. Make security part of workflow, not a post-audit fix.

- Add classification and retention fields to document templates.
- Require security sign-off in change or procurement workflows.
- Automate retention and destruction rules in systems.
- Integrate dashboards for real-time policy compliance.
  FastTrack Tip: “How to ensure consistent data handling?” – Embed controls into workflow and automation.

15. Endpoint, Mobile, and User Device Security

Protects user-facing devices where most cyberattacks originate by enforcing secure configurations, monitoring, and lifecycle management.

15.1 Endpoint Lifecycle Management

Manages devices from procurement to disposal, ensuring each phase maintains accountability, security, and traceability.

Phase	CISSP Manager Action
Procurement	Approve devices that support security features (TPM, Secure Boot).
Provisioning	Deploy hardened images, enable full-disk encryption, register in MDM.
Operation	Patch, monitor, enforce policies (DLP, AV, EDR).
Decommission	Sanitize per NIST SP 800-88 and record proof of destruction.

Scenario: “Old laptop reassigned without wipe” – violation of sanitization policy.
FastTrack Tip: Every asset must have a defined lifecycle - unmanaged = untrusted.

15.2 Baseline Hardening

Applies standardized security configurations and eliminates unnecessary services to minimize vulnerabilities.

- Build from **CIS Benchmarks** or **DISA STIGs**.
- Remove default accounts; disable unused ports and services.
- Enforce **least functionality** - only what the job requires.
- Validate with automated compliance scans (**SCAP**, CIS-CAT).
  FastTrack Tip: Any deviation from the baseline requires formal **Change Advisory Board (CAB)** approval.

15.3 Patch and Vulnerability Management

Continuously identifies, prioritizes, and fixes software weaknesses to maintain system stability and reduce risk exposure.

- Discover all assets; rank by **CVSS score** + business criticality.
- Test – Deploy – Verify.
- Track patch compliance and mean time to patch (MTTP).
- Use **emergency CAB** approval for zero-day or critical flaws.
  Scenario: "Critical patch released; production risk moderate" – apply emergency patch with documentation.
  FastTrack Tip: Patching without testing = instability; testing without patching = exposure. Balance both.

16. Mobile Device Management (MDM / EMM)

Secures mobile devices through centralized control of enrollment, encryption, and remote-wipe policies for both corporate and BYOD environments.

16.1 Core Controls

- Enroll only after **Multi-Factor Authentication (MFA)**.
- Enforce encryption, remote wipe, passcode policies.
- Block rooted or jail-broken devices.
- Use **containerization** for **BYOD** separation.
- Require **Network Access Control (NAC)** before connection.
  FastTrack Tip: Lost device = Remote wipe + Incident report + Verification of success.

16.2 BYOD Governance

Balances personal privacy with organizational control through clear ownership policies and containerized corporate data.

- Require signed **user agreements** defining ownership and wipe rights.
- Restrict storage of sensitive data on personal devices.
- Apply **Mobile Application Management (MAM)** to corporate apps only.
  Scenario: "Employee refuses company wipe after resignation" – enforce contractual consent and revoke access immediately.
  FastTrack Tip: Privacy rights ≠ security waiver - clear policy defines both.

17. Endpoint Detection and Response (EDR) & Behavioral Control

Enhances endpoint security by detecting and automatically responding to suspicious or malicious behavior in real time.

17.1 EDR Capabilities

- Detect anomalies and lateral movement.
- Record process trees, memory snapshots, and command history.
- Isolate or quarantine infected hosts automatically.
- Integrate with **Security Orchestration, Automation & Response (SOAR)** for playbook execution.
  FastTrack Tip: EDR = detect + contain; integrate with SIEM for central visibility.

Domain 3 – Security Architecture & Engineering

Develops secure system designs using layered defenses, security models, and strong technical controls to preserve confidentiality, integrity, and availability. It bridges principles with practice-embedding protection into hardware, operating systems, networks, and applications from the start.

1. Core Concept and Lifecycle Integration

Security architecture = policy in motion. It embeds confidentiality, integrity, and availability (CIA) into each system phase.

Lifecycle Phase	Security Goal	Managerial Focus
Initiation / Requirements	Identify assets, classify data, set CIA priorities.	Approve security objectives before design.
Design / Architecture	Map trust boundaries, perform threat modeling, select controls.	Review least privilege, SoD, defense-in-depth.
Implementation / Development	Apply secure coding standards, version control, signed builds.	Verify secure SDLC, enforce code review.
Testing / Verification	Validate security functions via SAST, DAST, pen test.	Require independent testing & remediation.
Deployment / Transition	Harden baselines, enable logging, confirm patch status.	Authorize deployment after risk sign-off.
Operation / Maintenance	Continuous monitoring & change control.	Approve patch plans and audit cycles.
Retirement / Disposal	Decommission securely; sanitize media.	Verify data destruction and close ATO.

Tip “When should security be considered?” – During initiation and design (Shift Left).

2. Secure Design Principles (Managerial Filters)

Principle	Essence	Application / Example	Decision Logic
Least Privilege	Minimum rights necessary.	Admin can reset passwords but not approve payroll.	Reduces blast radius.
Need-to-Know	Access limited to role requirements.	HR cannot read finance records.	Supports confidentiality.
Separation of Duties	Divide critical tasks.	One creates payment, another approves.	Prevents fraud / abuse.
Defense in Depth	Multiple independent layers.	Firewall + IDS + EPP + training.	Avoid single failure points.
Fail-Safe vs Fail-Secure	Safe = protect people; Secure = protect data.	Fire door unlocks; vault stays locked.	Choose based on impact priority.
Secure Defaults	Deny-by-default.	Firewall blocks all until rules added.	Enforces explicit authorization.
Complete Mediation	Check every access each time.	API authenticates every call.	Stops session reuse.
Simplicity (Economy)	Less complex = more trustworthy.	Modular code easier to test.	Fewer bugs = smaller attack surface.
Open Design	Don’t hide design; hide keys.	Cryptographic algorithms public, keys secret.	Encourages review & assurance.

Least Common Mechanism	Avoid shared resources.	Unique API tokens per user.	Prevents cross-data leakage.
Privacy by Design	Embed privacy early.	Encrypt identifiers, minimize fields.	Reduces regulatory risk.
Zero Trust	“Never trust, always verify.”	MFA + device health checks.	Removes implicit internal trust.

When Principles Conflict:

- Prioritize human safety > legal compliance > continuity.
- Document deviations and risk acceptance.

3. Threat Modeling Essentials

Identify and prioritize what can go wrong *before* attackers exploit it. Threat modeling bridges business impact with technical exposure.

3.1 Core Process (Universal Steps)

Step	What You Do	Managerial Objective
1. Identify Assets	Determine what needs protection - data, systems, people, reputation.	Define *what truly matters* to the mission.
2. Diagram System	Visualize components, data flows, and trust boundaries (where data changes owners or privilege levels).	Expose attack surfaces early.
3. Identify Threats & Vulnerabilities	Apply frameworks (STRIDE, PASTA, DREAD) to each asset or data flow.	Ensure completeness and traceability.
4. Evaluate Risk	Score threats by likelihood × impact (quantitative or qualitative).	Focus on highest business risk.
5. Plan Mitigations	Map controls to design principles (least privilege, defense-in-depth, secure defaults).	Design out risk - don’t patch later.
6. Validate & Iterate	Revisit model after each design or environment change.	Continuous assurance across lifecycle.

FastTrack Principle: Threat modeling isn’t a one-time step - it’s a **living process** that matures with the system.

3.2 STRIDE Framework (Microsoft)

STRIDE is a mnemonic for six threat classes, each mapped to a security property (CIA + AAA). Apply STRIDE to every component and data flow in your system diagram.

Threat	Attacker Goal	Broken Property	Control Focus	Design Example
S – Spoofing Identity	Impersonate a user or system.	Authentication	Strong AuthN (MFA, certs, tokens).	Verify user & device identity before access.
T – Tampering with Data	Modify data or code in transit or storage.	Integrity	Hashing, digital signatures, input validation.	Signed updates, WORM storage.
R – Repudiation	Deny performing an action.	Accountability / Non-repudiation	Audit logs, digital signatures, time-stamps.	Immutable logs in SIEM.
I – Information Disclosure	Steal or expose sensitive data.	Confidentiality	Encryption (TLS, AES), access control, masking.	Secure API responses, data classification.

D – Denial of Service	Block or degrade availability.	Availability	Redundancy, rate limiting, WAF, resource quotas.	Auto-scaling, DoS protection.
E – Elevation of Privilege	Gain higher access than authorized.	Authorization	Least privilege, role separation, PAM, patching.	No root by default, privilege audit.

STRIDE in Practice: Apply one row at a time across each component - e.g., for the web API, how could spoofing occur? Then repeat for tampering, etc.

3.3 PASTA – Process for Attack Simulation & Threat Analysis

Purpose: Business-driven, seven-stage threat modeling methodology that links **technical threats to business impact**.

Stage	Focus
1. Define Objectives	Business mission and compliance drivers.
2. Define Technical Scope	Systems, users, data flows, interfaces.
3. Decompose Application	Break into modules and data flows.
4. Analyze Threats	Use STRIDE/DREAD logic.
5. Vulnerability Analysis	Identify existing weaknesses.
6. Attack Modeling	Simulate attack paths and likelihood.
7. Risk & Mitigation	Rank by business impact and propose controls.

Key Differentiator: Links *business impact – threat – vulnerability – control* in a traceable chain.

3.4 DREAD – Threat Scoring

Used for prioritization after STRIDE or PASTA has identified threats. Each factor rated 1–10 – average = risk score.

Factor	Meaning
Damage	Impact if exploited.
Reproducibility	Ease of repeating attack.
Exploitability	Effort or resources required.
Affected Users	Number of users impacted.
Discoverability	Likelihood of finding the flaw.

Decision: Focus mitigation on high-score threats first.

3.5 Attack Trees

Visual representation of attacker goals and sub-steps - each path to the root equals a possible exploit scenario. Useful for what-if reasoning and communicating attack logic to non-technical managers.

FastTrack Summary:
STRIDE = What can go wrong
PASTA = Why it matters to business
DREAD = How severe each threat is

Attack Trees = How it might happen

4. Access Control Fundamentals (IAAA)

Explains the four core functions, Identification, Authentication, Authorization, and Accountability - that govern how users are verified, granted access, and monitored.

Step	Definition	Example
Identification	Claim of identity.	Username or badge ID.
Authentication	Prove the claim.	Password, token, biometric.
Authorization	Decide what actions allowed.	Access to HR folder only.
Accountability	Record actions for audit.	SIEM logs of file access.

Triggers: “Validate digital certificate” – Authentication. “Log user actions” – Accountability.

5. Access Control Models – Decision Basis

Describes the main models that determine access decisions (DAC, MAC, RBAC, ABAC, RuBAC) based on ownership, role, attributes, or system rules.

Model	Decision Owner	Description	Common Use
DAC	Data owner	Grants permissions discretionarily.	File sharing / personal systems.
MAC	System enforces labels and clearances.	Mandatory classification model.	Military / Gov.
RBAC	Based on job role.	Roles map to permissions.	Enterprise IAM.
ABAC	Based on attributes (user, object, context).	Policy evaluates dynamic conditions.	Cloud / Zero Trust.
RuBAC	Rule-based, system-driven If/Then.	Time, IP, state conditions.	Firewalls, NAC.

Quick Recall: Owner – DAC System Label – MAC Job Role – RBAC Context – ABAC System Rule – RuBAC.

6. Formal Security Models (Assurance by Logic)

Defines mathematical and logical models that prove confidentiality, integrity, and separation of duties through structured control enforcement.

Model	Focus	What It Prevents	Real-World Analogy / Keyword
Bell–LaPadula	Confidentiality	Prevents information *leakage* from higher – lower classification.	No Read Up / No Write Down: No Leaks.
Biba	Integrity	Prevents untrusted data from *corrupting* trusted data.	No Write Up / No Read Down: No Corruption.
Clark–Wilson	Commercial Integrity + Accountability	Prevents *fraud* and enforces *well-formed transactions*.	Separation of Duties – No Fraud.
Brewer–Nash (Chinese Wall)	Conflict of Interest	Prevents a consultant from accessing competing clients’ data.	Dynamic controls – No Conflict.
Lattice-Based	Classifications + Categories	Prevents improper information flow between sensitivity *levels or compartments.*	Dominance relationship: Labels & Levels.

Non-Interference	Isolation / Covert Channels	Prevents high-level actions from influencing low-level observations.	Stop inference: No Leakage via Behavior.

7. Theoretical Access-Right Models

Covers conceptual frameworks showing how rights are assigned, transferred, and managed among users and system objects.

Model	Essence	CISSP Relevance
Access Control Matrix	Table mapping subjects (rows) to objects (columns) with permissions.	Conceptual basis for ACL & Capability List.
Take-Grant	Graph showing how rights transfer between subjects.	"Propagation of rights."
Graham–Denning	Defines 8 admin operations (create, delete, grant, revoke…).	Foundation of admin RBAC.
Harrison–Ruzzo–Ullman (HRU)	Extends take-grant; proves safety cannot be guaranteed globally.	Explains need for policy constraints.

Tip "Model representing who can access what and how rights propagate" – Access Control Matrix / Take-Grant.

8. System Security Modes (Shared Environments)

Outlines different operational modes that dictate how users with various clearances share systems securely under mandatory controls.

Mode	Access Condition	Requirements	Example
Dedicated	All users cleared & need-to-know for all data.	Highest uniform trust.	Air-gapped classified network.
System-High	Same clearance, different need-to-know.	MAC controls per object.	Shared research network.
Compartmented	Clearance + project authorization.	Need-to-know per compartment.	Nuclear vs Space projects.
Multilevel	Mixed clearances sharing system.	MAC + labeling + auditing.	MLS database.

Decision Rule: Same data – Dedicated Same clearance / different project – System-High or Compartmented Mixed levels – Multilevel (MAC).

9. Trusted Computing Concepts (Foundation of Assurance)

Explains the architectural components that enforce security policies, such as TCB, reference monitor, and security kernel.

Term	Definition	Key Properties / Purpose
Trusted Computing Base (TCB)	All hardware, software, firmware enforcing policy.	Smaller TCB = easier assurance. If TCB fails – system fails.
Reference Monitor	Abstract mechanism mediating subject ↔ object access.	Tamper-proof - Complete Mediation - Verifiable.
Security Kernel	Implementation of Reference Monitor in OS.	Always active - isolated - enforces policy calls.
Trusted Path / Channel	Secure user ↔ TCB communication.	Prevents credential interception (Ctrl-Alt-Del login).
Assurance	Confidence that security functions work correctly.	Verified by testing, certification (CC EAL, TCSEC).

10. Fail Modes & Trusted Recovery

Describes how systems should respond to failures-whether prioritizing safety, data protection, or availability-and recover securely to a trusted state.

Mode	Priority	Example	Managerial Use
Fail-Safe	Human safety.	Fire doors unlock during fire.	Life-critical systems.
Fail-Secure	Data protection.	Vault remains locked on power loss.	Confidential environments.
Fail-Open	Availability.	Router continues traffic if firewall fails.	Business continuity.
Trusted Recovery	Return to secure state after failure.	Restart with policy enforcement intact.	Required for high-assurance systems.

11. Evaluation & Assurance Frameworks

Defines structured standards and processes used to assess and validate the security assurance of systems and products.

11.1 Common Criteria (CC) - ISO/IEC 15408

A global standard for evaluating product security, assigning assurance levels (EAL 1–7) based on testing depth and design rigor.

Component	Description
PP (Protection Profile)	Generic set of requirements for a product class (e.g., firewalls).
ST (Security Target)	Vendor’s implementation claim for a specific product.
TOE (Target of Evaluation)	Actual product/system being evaluated.
EAL (Evaluation Assurance Level)	Assurance rating from EAL 1 (lowest) to EAL 7 (formally verified).

EAL	Level Description	Example
1	Functionally tested	Minimal assurance.
2	Structurally tested	Basic config control.
3	Methodically tested & checked	Commercial baseline.
4	Methodically designed, tested, and reviewed	Industry norm for most products.
5–7	Semi- to formally verified design	Used for high-risk or military systems.

FastTrack Recall: “EAL 4+” – Formally reviewed and tested for commercial/government use.
“EAL 7” – Formal design verification (highest assurance).

11.2 TCSEC (Trusted Computer System Evaluation Criteria) - “Orange Book”

A U.S. Department of Defense standard focused on confidentiality, categorizing systems from minimal to formally verified protection.

Class	Level	Description
D	Minimal Protection	Not evaluated.
C1	Discretionary Security Protection	User ID, DAC.
C2	Controlled Access Protection	DAC + individual accountability (unique IDs, auditing).
B1	Labeled Security Protection	MAC + data labels.
B2	Structured Protection	Formal design + TCB modularization.

B3	Security Domains	Trusted recovery + reference validation.
A1	Verified Design	Fully formal proof of correctness.

Mapping: C2 ≈ EAL 2–3 B1 ≈ EAL 4 A1 ≈ EAL 6–7.

11.3 ITSEC (Information Technology Security Evaluation Criteria)

A European framework that separates functionality and assurance levels, providing flexibility for evaluating integrity and availability in addition to confidentiality.

11.4 Certification vs Accreditation

Differentiates between the technical validation of security controls (certification) and managerial acceptance of system risk (accreditation).

Term	Meaning	Who Performs
Certification	Technical evaluation of controls and compliance with policy.	Security team or auditor.
Accreditation	Management approval of system risk (ATO).	Authorizing Official (AO).

Tip "Authority to Operate (ATO)" – Result of accreditation.

12. Security Control Mechanisms

Categories:

1. **Preventive** – stop incidents (e.g., firewalls, encryption, MFA).
2. **Detective** – identify events (IDS, logging, audits).
3. **Corrective** – fix after detection (patch, restore, re-image).
4. **Deterrent** – discourage actions (policy, banners, guards).
5. **Compensating** – alternate control when primary isn't possible.
6. **Recovery** – restore operations (backups, redundancy).

FastTrack Recall:
"Policy statement displayed before login" – Deterrent.
"Logging system activity" – Detective.
"Firewall" – Preventive.

13. Cryptographic Foundations (Architecture Context)

Introduces the principles, algorithms, and mechanisms that protect data confidentiality, integrity, authentication, and non-repudiation within system design.

13.1 Core Types

Type	Key Use	Examples	Notes
Symmetric Encryption	Single shared key	AES, DES, 3DES, ChaCha20	Fast, but key distribution problem.
Asymmetric Encryption	Public/private key pair	RSA, ECC, Diffie-Hellman	Solves distribution, slower.
Hash Functions	One-way data fingerprint	SHA-2, SHA-3	Integrity check.
HMAC	Hash + secret key	API signatures, integrity + authentication.	Protects against tampering.
Digital Signature	Private key encrypts hash	RSA/ECC with SHA	Non-repudiation + integrity.

PKI	Framework of trust using digital certificates	X.509, CA, OCSP	Supports SSL/TLS, email signing.

13.2 Cryptographic Lifecycle

1. Generate and store keys securely (KMS, HSM).
2. Distribute via secure channels.
3. Rotate and revoke periodically.
4. Destroy keys safely after use.

FastTrack Recall:

- Bulk data encryption – Symmetric.
- Authentication/signature – Asymmetric.
- Verification – Hash.
- Integrity + Auth – HMAC.
- Trust management – PKI.

14. Architecture Resilience & System Reliability

Ensures systems remain available, fault-tolerant, and recoverable during failures through redundancy, replication, and resilience testing.

Concept	Purpose	Example
Redundancy / High Availability	Eliminate single failure points.	N+1 servers, RAID, clustering.
Fault Tolerance	Continue operation under failure.	Dual power supplies, hot standby.
Failover Systems	Automatic switch to backup.	Load-balanced firewalls.
Data Integrity	Prevent corruption, ensure ACID.	Checksums, journaling.
Data Replication	Synchronize copies for continuity.	Geo-redundant storage.
Resilience Testing	Validate continuity under stress.	DR simulation, chaos testing.

FastTrack Recall: “System continues running with partial failure” – Fault Tolerance.

15. Secure Architecture Concepts

Applies layered design, isolation, and modern deployment models (virtualization, containers, Zero Trust) to minimize attack surfaces and enforce control boundaries.

Concept	Purpose	Example
Layered Architecture	Compartmentalize system into tiers.	Presentation / Application / Data layers.
Segregation of Environments	Separate dev, test, prod.	Prevent unauthorized code deployment.
Virtualization Security	Hypervisor isolation and control.	Type 1 hypervisor = more secure.
Container Security	Enforce image integrity & namespace isolation.	Docker signing, minimal base image.
Microservices Security	Each service least-privileged & isolated.	Use API gateway, mutual TLS.
Serverless / Cloud Function	Ephemeral and event-driven.	Enforce identity-based access (ABAC).
Zero Trust Architecture (ZTA)	Continuous verification & minimal implicit trust.	MFA, device posture checks, context rules.

FastTrack Recall: “Users authenticated repeatedly inside the network” – Zero Trust.

16. Memory, Process & Hardware Security

Protects system integrity and confidentiality through hardware-based trust, process isolation, and secure boot mechanisms.

Mechanism	Purpose	Example
Memory Protection	Prevent process interference.	Paging, segmentation, ASLR, DEP.
Ring Protection Model	Defines privilege levels.	Ring 0 (kernel) – Ring 3 (user).
Trusted Platform Module (TPM)	Hardware root of trust for keys.	BitLocker encryption.
Secure Boot / UEFI	Validate OS before load.	BIOS integrity verified by signature.
Hardware Security Module (HSM)	Physical cryptographic processor.	Key generation, signing.
Process Isolation	Prevent process-to-process data leakage.	Sandbox / container.

FastTrack Recall: "Enforces least privilege at CPU level" – Ring protection. "Verifies OS integrity at startup" – Secure Boot.

17. Security Evaluation, Testing & Assurance

Validates that security features work correctly and can be proven reliable through testing, reviews, and formal verification.

Term	Purpose	Method
Functional Testing	Verify features perform securely.	Test cases / unit tests.
Penetration Testing	Simulate attack to validate defenses.	Ethical hacking phases.
Vulnerability Scanning	Automated detection of known flaws.	CVE-based tools.
Formal Verification	Mathematical proof of correctness.	TCSEC A1 / CC EAL 7.
Code Review	Human verification of logic.	Manual or assisted.
Configuration Audit	Check compliance with baseline.	CIS Benchmark comparison.

FastTrack Recall: Functional = Does it work? Assurance = Can we prove it's correct?

18. Security Models in Operation & Evaluation Context

Explains operational concepts like trusted paths, domains, and covert channels that ensure controlled and verified data flow.

Concept	Role	Example
Security Domain	Logical or physical boundary under one policy.	Network zone, business unit.
Trusted Path	Secure communication channel to TCB.	Login prompt protected by OS.
Covert Channel	Unauthorized communication path.	Timing or storage channels.
Side Channel Attack	Exploit physical behavior.	Power or timing analysis.
Information Flow Model	Regulates data movement between domains.	Prevent low – high trust leaks.

FastTrack Call: "Unauthorized communication between processes bypassing policy" – Covert Channel.

19. Final Recall Summary

Concept	Memory Anchor
Security by Design	Integrate from day one (“Shift Left”).
TCB Failure	Total trust failure.
Reference Monitor	Always check, never bypass.
Bell-LaPadula	Stop leaks (Confidentiality).
Biba	Stop corruption (Integrity).
Clark-Wilson	Stop fraud (Commercial Integrity).
Brewer-Nash	Stop conflict (Dynamic Separation).
Access Control Matrix	Foundation for ACLs.
CC / TCSEC	Assurance hierarchy.
Zero Trust	Verify continuously.
Trusted Recovery	Resume safely after crash.
Fail-Safe / Fail-Secure	People first, data next.
Architecture Verification	“Prove, not assume.”

Domain 4 – Communication and Network Security

Protects data in transit through secure network design, segmentation, and encryption-ensuring confidentiality, integrity, and availability across wired, wireless, and cloud communication channels.

1. Core Network Concepts

Communication directions

- **Simplex:** One-way only (e.g., keyboard – computer).
- **Half-duplex:** Two-way but not simultaneous (e.g., walkie-talkies, legacy hubs).
- **Full-duplex:** Two-way simultaneously (modern switches/fiber); eliminates collisions.

Signaling and multiplexing

- **Baseband:** One signal per medium (Ethernet).
- **Broadband:** Multiple signals via distinct frequencies (cable television, Data Over Cable Service Interface Specification-DOCSIS).
- **Quality of Service (QoS):** Traffic classification, queuing, and shaping for latency-sensitive flows (voice/video).

Switching methods

- **Circuit switching:** Dedicated end-to-end path (Public Switched Telephone Network-PSTN / Integrated Services Digital Network-ISDN); stable latency, low efficiency.
- **Packet switching:** Per-packet routing (Internet Protocol-IP); scalable and efficient.

Network scopes

Personal Area Network (PAN) – Local Area Network (LAN) – Metropolitan Area Network (MAN) – Wide Area Network (WAN) – Global Area Network (GAN).

Virtual Private Network (VPN): Encrypted tunnel across untrusted networks (remote access or site-to-site).

2. Open Systems Interconnection (OSI) Model - Seven Layers

Defines the seven-layer framework for how data moves through a network, helping identify where each protocol operates and where specific attacks may occur.

L#	Layer	Primary functions	Typical protocols	Typical risks
7	Application	User-facing services	Hypertext Transfer Protocol/Secure (HTTP/HTTPS), File Transfer Protocol (FTP), Simple Mail Transfer Protocol (SMTP), Simple Network Management Protocol (SNMP)	Injection, application Denial of Service
6	Presentation	Transform/encode/ encrypt	Transport Layer Security (TLS), American Standard Code for Information Interchange (ASCII), Joint Photographic Experts Group (JPEG)	Weak ciphers, improper encoding
5	Session	Establish/manage/ terminate sessions	Network Basic Input/Output System (NetBIOS), Remote Procedure Call (RPC)	Session hijacking
4	Transport	End-to-end delivery, ports	Transmission Control Protocol (TCP), User Datagram Protocol (UDP)	SYN floods, scanning
3	Network	Routing, logical addressing	Internet Protocol (IP), Internet Control Message Protocol (ICMP), IP Security (IPsec)	Spoofing, amplification
2	Data Link	Framing, Media Access Control	Ethernet, Point-to-Point Protocol (PPP), Address Resolution Protocol (ARP)	ARP poisoning, MAC flooding
1	Physical	Signaling, media, connectors	Cables, Network Interface Cards (NICs), hubs	Wiretapping, electromagnetic interference

Protocol Data Unit (PDU) map: Application–Session = **Data** – Transport = **Segments** – Network = **Packets** – Data Link = **Frames** – Physical = **Bits**

Quick anchors: cryptographic sessions (TLS) operate at **Layer 6/7**; routing is **Layer 3**; Media Access Control addressing is **Layer 2**.

3. Transmission Control Protocol / Internet Protocol (TCP/IP) Model

Describes the four practical layers of Internet communication and how core protocols like TCP, UDP, and IP enable reliable or fast data transfer.

TCP/IP layer	Maps to OSI	Purpose	Examples
Application	5–7	Application services	HTTP/HTTPS, Domain Name System (DNS), SMTP
Transport	4	Ports, reliability	TCP, UDP
Internet	3	Routing across networks	IP, ICMP, Internet Group Management Protocol (IGMP)
Link	1–2	Local delivery on media	Ethernet, Wi-Fi, ARP

TCP: Connection-oriented, ordered, reliable (web, email, file transfer). **UDP:** Connectionless, minimal overhead (streaming, voice, DNS).

3.1 Common ports

Lists well-known network ports, their associated protocols, and corresponding security concerns critical for firewall and exam scenarios.

Port(s)	Protocol / Service	Description / Function	Security Notes / Tips
20 / 21	FTP (File Transfer Protocol)	Transfers files between client and server (20 = data, 21 = control).	Unencrypted. Use SFTP (22) or FTPS (990) for secure transfers.
22	SSH (Secure Shell)	Secure remote login, tunneling, SCP/SFTP.	Replaces Telnet/FTP; encrypted at Layer 7. Common in admin access scenarios.
23	Telnet	Legacy remote terminal access.	Unencrypted - subject to sniffing. Replaced by SSH (22).
25 / 587	SMTP (Simple Mail Transfer Protocol)	Sends outgoing email messages between servers.	Secure versions use STARTTLS or port 465. Often blocked externally to prevent spam.
53	DNS (Domain Name System)	Resolves hostnames to IP addresses (UDP for queries, TCP for zone transfers).	Attack vector: DNS poisoning, amplification. Secure via DNSSEC.
67 / 68	DHCP (Dynamic Host Configuration Protocol)	Auto-assigns IPs, subnet mask, gateway.	UDP-based; can be spoofed (Rogue DHCP attacks).
69	TFTP (Trivial File Transfer Protocol)	Simple file transfer, no authentication.	Common in PXE boot or network device configs. Highly insecure - often blocked by firewalls.
80 / 8080	HTTP (Web)	Unencrypted web traffic. 8080 = alternate port.	Vulnerable to sniffing, MITM. Use HTTPS (443) instead.
110	POP3 (Post Office Protocol v3)	Downloads email from mail server to client.	Unencrypted; use POP3S (995).
123	NTP (Network Time Protocol)	Synchronizes system clocks over network.	UDP; used in time-based authentication. Beware amplification DDoS.

Port(s)	Protocol / Service	Description / Function	Security Notes / Tips
143	IMAP (Internet Message Access Protocol)	Accesses email directly on server.	Use IMAPS (993) for TLS. More modern than POP3.
161 / 162	SNMP (Simple Network Management Protocol)	Device monitoring (161 = queries, 162 = traps).	Use SNMPv3 for encryption/authentication. Older v1/v2 are plaintext.
443	HTTPS (HTTP Secure)	Encrypted web traffic using TLS/SSL.	Core for secure websites, APIs. Tip: Port 443 = encrypted HTTP.
514	Syslog	Sends event/log messages to centralized log server.	Typically UDP. Use TCP 6514 for secure syslog over TLS.
3389	RDP (Remote Desktop Protocol)	Remote graphical desktop (Windows).	Encrypted, but targeted by brute force / credential attacks. Restrict access.

4. Media Access Control (MAC) Addresses - Layer 2 Identity

Defines unique hardware identifiers used for local network communication and switching operations at the data link layer.

- **EUI-48 (48-bit):** 24-bit Organizationally Unique Identifier (OUI) + 24-bit device ID.
- **EUI-64 (64-bit):** Common with Internet Protocol version 6 (IPv6) mechanisms.
- Burned into NIC but spoofable; used for local switching, not routed.

5. IP Addressing - Layer 3

Internet Protocol version 4 (IPv4)

- 32-bit dotted-decimal (e.g., 192.168.1.10).
- Private ranges: 10.0.0.0/8 · 172.16.0.0–172.31.0.0/12 · 192.168.0.0/16.
- Loopback 127.0.0.1; link-local Automatic Private IP Addressing 169.254.0.0/16; broadcast 255.255.255.255.

Internet Protocol version 6 (IPv6)

- 128-bit hexadecimal (e.g., 2001:db8::1).
- Zero compression with "::" once; link-local **fe80::/10** on every interface.
- Supports unicast, multicast, anycast (no broadcast).

Traffic scopes: unicast (one-to-one), multicast (one-to-group), broadcast (IPv4 local subnet only).

6. Address Authorities and Allocation

- Internet Assigned Numbers Authority (IANA) – Regional Internet Registries (ARIN, Réseaux IP Européens-RIPE, Asia-Pacific Network Information Centre-APNIC, Latin America and Caribbean Network Information Centre-LACNIC, African Network Information Centre-AFRINIC).
- **Classless Inter-Domain Routing (CIDR):** route summarization and efficient allocation; fewer prefix bits = larger networks (e.g., /24 = 255.255.255.0).

Network Address Translation (NAT)

- **Static NAT:** one-to-one mapping.
- **Dynamic NAT:** pool of public addresses.
- **Port Address Translation (PAT):** many-to-one with port multiplexing ("NAT overload").

7. Essential Network Protocols

Summarizes foundational communication protocols (ARP, ICMP, DNS, DHCP, SNMP) with their purposes and secure configuration practices.

Protocol	Purpose	Secure usage note
Address Resolution Protocol (ARP)	Internet Protocol v4 (IPv4) IP–MAC mapping	Protect with Dynamic ARP Inspection (DAI); pair with DHCP snooping
Internet Control Message Protocol (ICMP)	Diagnostics (ping/traceroute)	Rate-limit; monitor for reconnaissance
Domain Name System (DNS)	Name resolution	Use DNS Security Extensions (DNSSEC) for integrity
Dynamic Host Configuration Protocol (DHCP)	Automatic addressing	Block rogues with DHCP snooping
Simple Network Management Protocol (SNMP)	Telemetry/management	Prefer SNMP version 3 (authentication + encryption)
HTTP/HTTPS	Web transport	Prefer HTTPS with TLS 1.2/1.3

8. Media and Topologies

Copper (twisted pair): Unshielded Twisted Pair (UTP) is cost-effective but EMI-susceptible; Shielded Twisted Pair (STP) resists EMI. Category 5e ≈ 1 Gbps; Category 6/6A ≈ 10 Gbps (short runs).

Coaxial: Better EMI resistance; legacy broadband and Closed-Circuit Television (CCTV).

Fiber: Single-mode (long-haul, laser) and multi-mode (short-range); immune to EMI; supports Wavelength Division Multiplexing (WDM); harder to tap but still requires pathway security.

Topologies:

- **Star:** Each node ↔ switch; modern default; simple isolation.
- **Mesh:** Redundant and resilient; higher cost/complexity.
- **Bus/Ring:** Legacy; single faults can disrupt many nodes.
- **Tree:** Hierarchical enterprise design.

Propagation and emanations: control attenuation/dispersion, EMI/RFI; consider TEMPEST/emanation shielding in high-sensitivity environments.

9. Operational Decision Anchors

- Replace plaintext management and data paths with **TLS/SSH/IPsec** equivalents.
- Apply **Quality of Service (QoS)** where predictability matters (voice/video).
- Use **CIDR** consistently for addressing, summarization, and access control clarity.
- Map issues to layers quickly: Layer 3 = routing, Layer 2 = switching/MAC, Layer 6/7 = TLS/application.

10. Fast Recall Table

Requirement	Preferred choice
Ordered, reliable delivery	Transmission Control Protocol (TCP)
Low-overhead transport	User Datagram Protocol (UDP)
Encryption at the application/session layer	Transport Layer Security (TLS)
Network-layer Virtual Private Network	IP Security (IPsec)

Secure telemetry/management	Simple Network Management Protocol version 3 (SNMPv3)
Integrity for name resolution	Domain Name System Security Extensions (DNSSEC)
Efficient IPv4 allocation/routing	Classless Inter-Domain Routing (CIDR) + Network Address Translation/Port Address Translation (NAT/PAT)
EMI immunity and tap resistance	Fiber optic cabling

11. Local Area Networks (LAN) and Ethernet Basics

Covers Ethernet architecture, duplex modes, and collision handling as the foundation for modern switched LANs.

Ethernet frame structure
Header – Destination Media Access Control (MAC) + Source MAC + Type
Payload – Data (46–1500 bytes)
Trailer – Frame Check Sequence (FCS) for error detection

Duplex modes

- **Half-duplex:** One direction at a time; used in legacy hubs.
- **Full-duplex:** Simultaneous send and receive; standard in switched networks.

Collision handling

- Legacy: Carrier Sense Multiple Access with Collision Detection (CSMA/CD).
- Modern: Eliminated by switches-each port forms its own collision domain.

Design anchors
Modern LANs use **switched full-duplex Ethernet** in **star topology**, providing isolation and scalability.

11.1 Network Planes and Switching Logic

Explains the separation of data, control, and management planes in switches and routers, emphasizing secure management isolation.

Control, data, and management planes

- **Data plane:** Moves packets at line speed (user traffic).
- **Control plane:** Maintains routing and switching intelligence (OSPF, Border Gateway Protocol-BGP, Spanning Tree).
- **Management plane:** Administrative access (SSH, HTTPS, Simple Network Management Protocol-SNMP).

Switching behaviors

- **Store-and-forward:** Reads entire frame and validates checksum; higher latency, best integrity.
- **Cut-through:** Forwards after reading destination MAC; minimal latency, higher corruption risk.

Protection principle
Always isolate the **management plane**-dedicated network, access control list (ACL), and Virtual Private Network (VPN) protection.

12. Switch Operations and Security Controls

Switches operate at **OSI Layer 2 (Data Link)**, learning MAC addresses and forwarding frames only where needed.

Key hardening actions

1. Disable unused ports.
2. Enable **Port Security**-limit permitted MAC addresses per port.
3. Enforce **IEEE 802.1X** authentication (RADIUS backend).
4. Disable unused trunking or auto-negotiation (802.1Q).

5. Enable **Dynamic ARP Inspection (DAI)** to prevent spoofing.
6. Enable **DHCP Snooping** to block rogue DHCP servers.
7. Enable **Bridge Protocol Data Unit (BPDU) Guard** to protect Spanning Tree Protocol (STP) roots.
8. Keep firmware updated and forward logs to the Security Information and Event Management (SIEM) system.

Performance metrics

- Bandwidth (capacity)
- Throughput (real data rate)
- Latency (delay)
- Jitter (variance in delay)
- Signal-to-Noise Ratio (SNR) for wireless/optical quality

Traffic directions

- **North–South:** Between clients and data centers or Internet.
- **East–West:** Lateral movement inside the data center or cloud.

Network protection note

Micro-segmentation or east–west firewalls are recommended to contain lateral movement within internal environments.

13. Routers and Routing Security

Routers operate at **OSI Layer 3 (Network)** to forward packets between networks based on IP addresses. They separate broadcast domains and define network boundaries.

Core functions

- Path selection and routing tables.
- Address translation (Network Address Translation-NAT).
- Policy enforcement through ACLs.

Router hardening checklist

- Disable unused interfaces and management services.
- Replace Telnet/HTTP management with SSH/HTTPS.
- Filter spoofed and private addresses on public-facing interfaces.
- Authenticate routing protocols:
    - Open Shortest Path First (OSPF) with Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) authentication.
    - Border Gateway Protocol (BGP) with Time To Live (TTL) security and Route Origin Authorization (ROA).
- Apply ingress and egress ACLs to limit exposure.
- Maintain configuration backups and apply formal change control.

Key design logic

Routers segment traffic domains and enforce security policy between zones; they are the first line of policy enforcement in perimeter or multi-site architectures.

14. Firewalls - Architecture and Types

A firewall enforces network policy at trust boundaries, deciding which traffic is permitted or denied. It’s the most critical preventive control for network security.

Firewall categories

Firewall Type	OSI Layer	Function / Description	Example Features
Packet-Filtering Firewall	3 – Network Layer	Inspects IP headers (source/destination IP, protocol, port). Stateless - no session tracking.	Access Control Lists (ACLs), simple router-based filtering.

Firewall Type	OSI Layer	Function / Description	Example Features
Stateful Inspection Firewall	3 & 4 – Network & Transport Layers	Tracks active sessions and allows only packets matching a known connection state.	Connection tables, dynamic packet filtering, TCP handshake validation.
Circuit-Level Gateway	5 – Session Layer	Monitors TCP handshakes and session initiation; doesn't inspect packet contents.	SOCKS proxy, session validation.
Application-Level Firewall (Proxy Firewall)	7 – Application Layer	Inspects full application data (HTTP, SMTP, DNS). Can enforce user- or content-based rules.	Web proxy, content filtering, malware scanning.
Next-Generation Firewall (NGFW)	3–7 (Multi-layer)	Combines stateful inspection with deep packet inspection (DPI), intrusion prevention (IPS), and application awareness.	App control, user ID mapping, SSL inspection, threat intelligence integration.
Network Address Translation (NAT) Firewall	3 – Network Layer	Hides internal IPs by translating private ↔ public addresses. Often integrated with stateful inspection.	Basic home/edge firewall functionality.
Web Application Firewall (WAF)	7 – Application Layer	Specifically protects web apps by inspecting HTTP/HTTPS traffic for malicious patterns (XSS, SQLi, etc.).	OWASP Top 10 protections, reverse proxy or inline mode.
Cloud / API Gateway Firewall	7 – Application Layer	Protects APIs and microservices; enforces rate limits, authentication, JSON schema validation.	AWS WAF, Azure Front Door, API Gateway policies.

Deployment models

- **Network-perimeter firewall:** Between Internet and internal or demilitarized zone (DMZ).
- **Internal segmentation firewall:** Between sensitive internal networks.
- **Host-based firewall:** Local protection on endpoints and servers.
- **Cloud or virtual firewall:** Security groups or policies in software-defined networks.

Configuration principles

- Default deny inbound and outbound traffic unless explicitly allowed.
- Apply least privilege on rule sets and review regularly.
- Log and audit all policy changes.
- Place firewalls to separate trust zones (Internet ↔ DMZ ↔ internal).

Operational guidance

- Simplify rules using address objects, zones, and named groups.
- Regularly recertify rules and remove obsolete entries.
- Conduct controlled rule-set reviews to align with business changes.

15. Intrusion Detection and Prevention Systems (IDS / IPS)

Detects and prevents malicious network or host activity that bypasses firewalls by analyzing traffic patterns and behaviors.

15.1 Detection Methods

- **Signature-based:** Matches traffic to known attack signatures. – Fast, reliable, but blind to new threats.

- **Anomaly-based:** Flags deviations from normal baselines. – Detects zero-day activity; may cause false alerts.
- **Heuristic / Behavioral:** Identifies suspicious or malicious **actions** rather than specific code. – Detects unknown or polymorphic attacks.

15.2 Deployment Models

- **Network-based (NIDS / NIPS):** Monitors traffic at choke points to detect network attacks.
- **Host-based (HIDS / HIPS):** Protects individual systems by inspecting local files and logs.
- **Inline (IPS):** Actively blocks or drops malicious packets in real time.
- **Passive (IDS):** Detects and alerts without intervening in traffic flow.

15.3 Integration Guidance

- Send IDS/IPS alerts to **SIEM** for correlation and triage.
- Build **escalation playbooks** for containment and investigation.
- Tune thresholds to reduce noise and false positives.
- Regularly update **signatures / baselines** for accuracy.

16. Network Segmentation and Virtual Local Area Networks (VLANs)

Divides a network into smaller zones to improve performance, contain attacks, and enforce least-privilege access.

16.1 Core Principles

- Each VLAN = separate **broadcast domain**.
- Inter-VLAN traffic passes through a **Layer 3** device (router / firewall).
- Reduces **lateral movement** and limits attack spread.

16.2 Trunking (IEEE 802.1Q)

Allows multiple VLANs to share one physical link between switches using VLAN ID tagging.

16.3 VLAN Security Measures

- Disable **auto-trunk negotiation (DTP)** on user ports.
- Limit each port to a specific VLAN.
- Prune unused VLANs from trunks.
- Use a **dedicated management VLAN** for admin traffic.
- Prevent **VLAN hopping** by manual trunk configuration.

16.4 Demilitarized Zone (DMZ)

Hosts **public-facing servers** (web, mail, DNS) in an isolated segment between Internet and internal network – limits exposure if breached.

16.5 Segmentation Layers

- **Physical:** Separate hardware / cabling.
- **Logical:** VLANs, VRF, subnets.
- **Micro-segmentation:** Per-workload isolation in virtualized or SDN environments.

Management Takeaway: Tighter segmentation = smaller **blast radius** during compromise.

17. Network Access Control (NAC) and IEEE 802.1X

Controls which devices and users can access the network, verifying both identity and system health before granting or maintaining connectivity.

17.2 Core Workflow

1. Device connects to switch / AP.
2. **802.1X** sends authentication to **RADIUS**.
3. **NAC** checks posture (AV, patch, encryption).
4. Device placed in compliant / quarantine VLAN accordingly.

Supplicant – Authenticator – Authentication Server (RADIUS) chain.

17.3 Access Enforcement Models

- **Pre-admission:** Validate before granting access.
- **Post-admission:** Monitor compliance after connection.

17.4 Integration Points

Works with **MDM**, **EDR**, and **PKI** for identity- and health-based policy enforcement.

17.5 Best Practices

- Require **MFA** for privileged users.
- Maintain **continuous posture checks** for Zero Trust.
- Use **quarantine VLANs** for remediation of risky endpoints.

17.6 Zero Trust Extension

NAC enforces Zero Trust by verifying **user + device identity every session**, not just at login.

18. Secure Device Management and Network Monitoring

Protects network infrastructure through isolated management, logging, and secure administration practices.

18.1 Out-of-Band (OOB) Management

Provides a **separate admin network** for configuration and recovery, ensuring management access even if production is down.

18.2 System Logging and Telemetry

Collects and centralizes **system and network logs** for visibility, correlation, and forensics.

- Use **Syslog UDP 514 / TCP 6514 (TLS)** to forward data to SIEM.
- Protect logs with **integrity, time sync, and retention** controls.

18.3 Simple Network Management Protocol (SNMP)

Monitors and manages network devices.

- Use **SNMPv3** (auth + encryption).
- Disable **v1/v2c**, restrict community strings / source IPs.

18.4 Time Synchronization (NTP)

Keeps all devices on **accurate coordinated time**, vital for forensics, Kerberos, and digital signatures.

- Use **NTP UDP 123** with authentication.

18.5 Administrative Controls

Defines how administrators securely manage network devices.

- Restrict management to **secure subnets / bastion hosts**.

- Use **SSH (22)** and **HTTPS (443)** - never Telnet (23) or HTTP (80).
- Enforce **RBAC** and **JIT privilege elevation**.
- Record and audit all admin sessions.

Operational Note: OOB networks and secure management paths protect the **control plane** from user traffic and limit damage from compromise.

19. Local Area Network (LAN) Threats and Countermeasures

Protects Layer 2 switching environments from spoofing, flooding, and unauthorized access.

19.1 Common LAN Threats

Threat	Description	Primary Control
ARP spoofing	Fakes MAC-IP bindings to intercept or redirect traffic.	Dynamic ARP Inspection (DAI) + Port Security
Rogue DHCP	Issues malicious IP configurations to clients.	DHCP Snooping
MAC flooding	Overloads switch CAM table – broadcasts traffic.	Port Security + Storm Control
STP manipulation	Attacker becomes root bridge and redirects paths.	BPDU Guard + Root Guard
Unauthorized port access	Device plugged into open switch port.	Disable unused ports + Port Security
VLAN hopping	Exploits trunk misconfiguration to reach other VLANs.	Disable auto-trunking + prune VLANs

19.2 Operational Best Practices

- Audit Layer 2 configurations regularly.
- Keep switch/router firmware updated.
- Maintain **VLAN maps** and trunk documentation in CMDB.
- Automate compliance checks via configuration tools.

A secure switching fabric enforces device identity, limits compromise scope, and ensures predictable traffic paths.

20. Wide Area Network (WAN) Architecture and Technologies

Connects multiple LANs across geographic distances using carrier or public infrastructure for reliable, secure connectivity.

20.1 Common WAN Technologies

Technology	Description	Security Consideration
Leased Line (T1/E1/T3)	Dedicated point-to-point circuit with fixed bandwidth.	Physically isolated; still encrypt sensitive data.
Circuit-switched (PSTN / ISDN)	Temporary dedicated path per session.	Legacy; weak or no encryption.
Packet-switched (Frame Relay, MPLS, Internet)	Shared infrastructure; packets routed dynamically.	Add IPsec / TLS for confidentiality.
MPLS	Label-based forwarding with QoS and logical separation.	Not encrypted by default – add IPsec / TLS.

Technology	Description	Security Consideration
SD-WAN	Centralized overlay using broadband, fiber, or 4G/5G.	Usually has built-in encryption + policy control.

20.2 Design Anchors

- Encrypt data across untrusted networks.
- Use **dual providers** for high availability.
- Validate routing updates and SLAs.

21. WAN Security and Partner Connectivity

Secures communication across carrier links and partner networks.

21.1 WAN Security Principles

- Encrypt untrusted links with **IPsec / TLS**.
- Authenticate peers via **certificates / PSKs**.
- Apply **ingress/egress ACLs**.
- Monitor latency, routing changes, and loss for tampering.
- Disable legacy protocols (**Telnet, SNMP v1/v2**).

21.2 Third-Party or Partner Connections

- **Extranet VPN:** Limit reachable services.
- **Carrier links:** Request diverse paths / redundant circuits.
- **Contractual controls:** SLAs must include encryption + incident reporting.
- **Isolation:** Use **VRF** or distinct zones per tenant.

Example: Partner access restricted to one application via **Extranet VPN** with tight ACLs.

22. Wireless Local Area Networks (WLANs)

Provides short-range wireless connectivity using IEEE 802.11 standards.

22.1 Radio Frequency Fundamentals

Band	Range	Throughput	Interference Risk
2.4 GHz	Long	Moderate	High
5 GHz	Medium	High	Moderate
6 GHz (Wi-Fi 6E)	Short	Very High	Low

22.2 Key IEEE 802.11 Standards

Standard	Feature	Max Speed
802.11n	MIMO	600 Mbps
802.11ac	Beamforming, 5 GHz	6 Gbps
802.11ax (Wi-Fi 6)	OFDMA, efficiency	9.6 Gbps
802.11be (Wi-Fi 7)	Multi-link, ultra-high throughput	> 30 Gbps

22.3 Core Terminology

- **Access Point (AP):** Bridges wireless to wired LAN.
- **SSID/BSSID/ESS:** Identify and group WLANs.
- Use **non-overlapping channels**; hiding SSID adds no real security.

23. Wireless Encryption and Authentication

Ensures confidentiality and identity verification in WLAN communication.

23.1 Encryption Standards

Standard	Algorithm	Security Status
WEP	RC4	Obsolete
WPA	TKIP	Legacy / Weak
WPA2	AES-CCMP	Baseline
WPA3	AES-GCMP + SAE	Modern / Recommended

23.2 Enterprise Mode (802.1X + EAP)

- Centralized auth via **RADIUS**.
- **EAP-TLS** (cert-based) = strongest.
- **PMF (802.11w)** protects management frames.

23.3 Security Alignment

- Use **WPA3-Enterprise + EAP-TLS** for corporate WLANs.
- Enable **PMF**; disable **WEP/TKIP**.

24. Wireless Threats and Mitigation

Addresses attacks unique to Wi-Fi and Bluetooth networks.

24.1 Common Wireless Threats

Threat	Description	Control
Rogue AP	Unauthorized access point bridging internal LAN.	WIDS/WIPS + Port Security
Evil Twin	Fake SSID to steal credentials.	EAP-TLS + User Awareness
Deauth attack	Forces clients to reconnect via attacker.	PMF (802.11w)
Packet sniffing	Captures plaintext frames.	VPN / HTTPS
War driving	Mapping open networks.	Auth + Monitoring
Bluetooth exploits	Unauthorized pairing / data theft.	Disable discoverability + patches

24.2 Operational Hygiene

- Scan for rogue APs periodically.
- Log AP associations centrally.
- Segment **guest vs corporate** WLANs.
- Use separate admin credentials.

25. Cellular and Mobile Network Security

Secures mobile communications and manages endpoint risks across 2G–5G.

25.1 Technology Evolution

- **2G (GSM):** Weak A5/1 encryption; easily intercepted.
- **3G (UMTS):** Adds mutual authentication.
- **4G (LTE):** IP-based with AES-128 encryption.
- **5G:** Stronger crypto, network slicing, ultra-low latency.

25.2 Common Mobile Risks

Lost/stolen devices, untrusted apps, unsafe Wi-Fi, fake base stations (**IMSI catchers**).

25.3 Defensive Controls

Area	Recommended Action
Device Management	Use MDM/MAM for patching + remote wipe.
Access Control	Enforce MFA or certificate-based login (EAP-TLS).
Encryption	Require full-disk + VPN encryption.
Segregation	Separate work / personal data (containerization).
Connectivity	Prefer cellular / trusted VPN over public Wi-Fi.

26. Wireless Management and Operational Controls

Maintains administrative integrity, visibility, and compliance in WLAN deployments.

26.1 Administrative Separation

- Use a **dedicated management SSID** isolated from users.
- Protect controller traffic with **TLS / IPsec**.
- Require **strong credentials, MFA, audit logs**.

26.2 Hardware and Physical Controls

- Lock and label all **Access Points**.
- Restrict console access.
- Conduct **RF site surveys** and detect rogues periodically.

26.3 Logging and Visibility

- Centralize **RADIUS / WLAN** logs.
- Correlate wireless events in **SIEM**.
- Retain logs per **policy / compliance**.

27. Internet of Things (IoT) and Emerging Wireless Risks

IoT device exposure

- Minimal security, default credentials, and poor patch support.
- Use dedicated VLANs or networks to isolate IoT traffic.
- Require signed firmware and secure boot to prevent tampering.

Mesh and edge devices

- Authenticate nodes mutually in wireless mesh environments.

- Apply encryption on backhaul links.
- Audit firmware integrity and communication patterns.

5G slicing

- Separate virtual network segments with different policies for performance and isolation.
- Maintain visibility using flow logs and identity-based policies.

Management insight
IoT security depends on restricting trust, minimizing privileges, and applying lifecycle governance similar to other endpoints.

28. Cloud and Virtual Private Cloud (VPC) Segmentation

Implements logical isolation and traffic control in cloud environments using subnets, ACLs, and identity-based policies.

28.1 VPC Structure

- **Public Subnets:** Expose web or load-balancing tiers with restricted Internet access.
- **Private Subnets:** Host apps/databases with no direct Internet route.
- **Security Groups:** Stateful instance-level allow lists (Layer 4–7).
- **Network ACLs (NACLs):** Stateless subnet filters controlling ingress/egress.
- **Transit Gateway:** Connects multiple VPCs or hybrid sites.
- **Private Link / Service Endpoints:** Provide private access to cloud services without public IPs.

28.2 Best Practices

- Use security groups for **fine-grained least-privilege** control.
- Separate **production, staging, and development** VPCs.
- Enable and review **VPC Flow Logs** in the SIEM.
- Enforce **identity-based policies (IAM)**.
- Apply **WAF + DDoS** protection at the perimeter.

FastTrack Tip: Security Groups = stateful; NACLs = stateless. Keep cloud segmentation aligned with Zero Trust principles.

29. Internet Protocol Security (IPsec)

Secures IP traffic at OSI Layer 3 by providing encryption, integrity, and peer authentication.

29.1 Core Components

- **Authentication Header (AH):** Integrity + authentication only (no encryption).
- **Encapsulating Security Payload (ESP):** Encryption + integrity + authentication.
- **Internet Key Exchange (IKE):** Negotiates Security Associations (SAs).
- **Perfect Forward Secrecy (PFS):** Generates unique session keys per exchange.

29.2 Modes

- **Transport Mode:** Encrypts payload only; host-to-host.
- **Tunnel Mode:** Encrypts entire packet; gateway-to-gateway (VPN use).

29.3 Ports and Protocols

- **AH:** IP 51 | **ESP:** IP 50
- **IKE:** UDP 500 | **NAT-Traversal:** UDP 4500

29.4 Configuration Highlights

- Use **tunnel mode** for inter-site VPNs.
- Enable **PFS + SHA-2** integrity.
- Store keys in **HSM** or secure key modules.

FastTrack Tip: ESP = encryption + auth; AH = auth only. Each IPsec tunnel = two one-way Security Associations.

30. Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Encrypts application-layer communications (OSI Layers 6–7) to secure web, email, and API traffic.

30.1 Best Practices

- Use **TLS 1.2 or 1.3** only.
- Disable **SSL**, **TLS 1.0**, **TLS 1.1**.
- Prefer **ECDHE + AES-GCM** ciphers for forward secrecy.
- Validate **X.509 certificates** from trusted CAs.

30.2 Common Secure Ports

- **HTTPS 443 • SMTPS 465 • IMAPS 993 • POP3S 995**

30.3 TLS 1.3 Advantages

- One-round-trip handshake (faster).
- Removes legacy ciphers.
- PFS enabled by default.

30.4 Managerial Responsibilities

- Maintain full **certificate lifecycle** (issuance – renewal – revocation).
- Audit TLS configs on servers and load balancers.
- Ensure **secure cipher order** and strong defaults.

FastTrack Tip: TLS 1.3 = speed + strong crypto + PFS. Terminate TLS only at trusted points; re-encrypt to backend if data is sensitive.

31. Secure Shell (SSH)

Provides encrypted remote terminal and file-transfer access, replacing plaintext protocols like Telnet and FTP.

31.1 Key Features

- Runs over **TCP 22**.
- Supports **key-based authentication** and secure tunneling.
- Enables **SCP** and **SFTP** for file transfer.

31.2 Hardening Practices

- Disable password and root logins.
- Restrict source IPs/subnets via ACLs.
- Rotate SSH keys periodically.
- Enable **session logging + command auditing**.
- Use **bastion hosts** for administrative jump access.

FastTrack Tip: All management access should use SSH or equivalent secure channels. Key-based auth > passwords for resilience and auditability.

32. Secure Protocol Equivalents

Function	Insecure protocol	Secure alternative
Web	HTTP	HTTPS (TLS)
Remote access	Telnet	SSH
File transfer	FTP	SFTP or FTPS
Email send	SMTP	SMTPS
Email receive	POP3 / IMAP	POP3S / IMAPS
Directory access	Lightweight Directory Access Protocol (LDAP)	LDAP Secure (LDAPS)
Network management	SNMPv1/v2	SNMPv3
Voice/Video	Session Initiation Protocol (SIP) / Real-Time Transport Protocol (RTP)	SIP Secure (SIPS) / Secure Real-Time Transport Protocol (SRTP)
Time synchronization	NTP	Authenticated NTP
Domain Name System (DNS)	Standard DNS	DNS over HTTPS (DoH) / DNS over TLS (DoT)

Core principle: Always replace plaintext management or application protocols with their encrypted counterparts.

33. Software-Defined Networking (SDN) and Network Function Virtualization (NFV)

Enables centralized, programmable control of networks and virtualized network services for agility and automation.

35.1 Concepts

- **Software-Defined Networking (SDN):** Separates control plane from data plane; a central controller enforces policy through APIs.
- **Network Function Virtualization (NFV):** Virtualizes appliances (firewalls, load balancers, IDS/IPS) to improve scalability and automation.

35.2 Security Implications

- Isolate and harden **SDN controller networks**.
- Use **mutual TLS** between controller ↔ devices.
- Apply **Role-Based Access Control (RBAC)** for administrators.
- Maintain configuration integrity via **GitOps / Infrastructure as Code** pipelines.

35.3 Advantages

- Rapid, policy-driven deployment.
- Consistent segmentation across hybrid clouds.
- Simplified integration with **Zero Trust** and automation frameworks.

FastTrack Tip: Protect the SDN controller as a critical asset; it dictates enterprise-wide network behavior.

34. Secure Email, Voice, and Collaboration

Protects enterprise communication channels (email, VoIP, video, and chat) against interception and impersonation.

35.1 Email Security

- Enable **STARTTLS** for transport encryption.

- **End-to-end options:**
  • **S/MIME:** Uses X.509 certificates.
  • **PGP:** User-managed key pairs.
- **Anti-spoofing chain:** SPF – DKIM – DMARC (validates sender authenticity).

35.2 Voice and Video

- **SIP:** Use TLS for signaling (**SIPS**, TCP 5061).
- **RTP:** Encrypt with **SRTP** for media streams.
- Separate **voice VLANs** with QoS and monitoring.

35.3 Operational Integrity

- Monitor **Call Detail Records (CDRs)**.
- Restrict admin access to **PBX systems**.
- Enforce strong auth for conferencing platforms (Teams, Zoom, etc.).

FastTrack Tip: Layer encryption + auth (SPF/DKIM/DMARC for email, TLS/SRTP for voice) to prevent both eavesdropping and spoofing.

36. Network Resilience and High Availability

Ensures continuous service during hardware failure, network outage, or cyberattack.

36.1 Core Concepts

- **Redundancy:** Duplicate links/devices (firewalls, routers, switches).
- **Failover:** Automatic switch to standby.
- **Load Balancing:** Distributes traffic for performance and fault tolerance.
- **Clustering:** Multiple servers operate as one logical unit.
- **Geographic Diversity:** Separate sites reduce regional risk.

36.2 Metrics

- **MTBF (Mean Time Between Failures)** = average uptime.
- **MTTR (Mean Time to Repair)** = average recovery duration.
- **Availability = MTBF / (MTBF + MTTR).**

36.3 Design Actions

- Eliminate single points of failure.
- Use dual ISPs and redundant paths.
- Combine **LACP** + dynamic routing for auto-recovery.

FastTrack Tip:
Aim for “Five Nines” (99.999%) availability by combining redundancy + monitoring + tested failover.

37. Power, Environment, and Physical Continuity

Preserves infrastructure availability through electrical resilience and environmental safeguards.

37.1 Power Controls

- **UPS** for short-term backup.
- **Generators** for long outages.
- Dual power feeds + redundant PSUs.
- **Surge suppression** and power conditioning.

37.2 Environmental Controls

- Maintain temperature/humidity per **ASHRAE** standards.
- Fire suppression:
  - Wet pipe – office areas.
  - Pre-action – server rooms.
  - Gas systems (FM-200, CO_2) – electronics.

37.3 Cabling and Documentation

- Separate power / data conduits.
- Label and document routes for quick repair.

37.4 Maintenance

- Test failover systems regularly.
- Track hardware lifecycle and warranty per **RTO/RPO** targets.

FastTrack Tip: Power redundancy + environmental controls protect the physical layer of availability in the CIA triad.

38. Business Continuity Integration

Links network design and resilience objectives to organizational BCP/DRP strategy.

38.1 Alignment Metrics

- **RPO (Recovery Point Objective):** Maximum acceptable data loss.
- **RTO (Recovery Time Objective):** Target restoration time.
- **MTD (Maximum Tolerable Downtime):** Absolute limit of disruption.
- **WRT (Work Recovery Time):** Time to full business operations.

38.2 Recovery Sites

Site Type	Recovery Time	Cost	Description
Hot Site	Immediate	High	Fully equipped and synchronized
Warm Site	Hours	Moderate	Partial systems; some restoration needed
Cold Site	Days	Low	Power and space only; no systems

Domain 5 – Identity & Access Management (IAM)

Ensures the right individuals and devices access the right resources at the right time-using identification, authentication, authorization, and accountability to enforce least privilege, prevent misuse, and maintain traceability across systems.

1. What IAM Is and Why It Matters

Controls *who* or *what* can access *which* resource, *when*, and *how*-enforcing confidentiality, integrity, and accountability.

- **IAM = Policies + Processes + Technology**
  - **People:** Users, approvers, admins, auditors
  - **Process:** Onboard – change – offboard – review
  - **Technology:** Directory / IdP, SSO, MFA, PAM, NAC, logging / SIEM
    FastTrack Tip: IAM turns governance intent into operational control-the real engine of least privilege.

2. The I-A-A-A Sequence (Identify – Authenticate – Authorize – Account)

Always follow this order.

1. **Identification:** Claim an identity (username / badge).
2. **Authentication:** Prove it (password, token, biometric).
3. **Authorization:** Grant only required rights.
4. **Accountability:** Log and time-sync all actions.
   FastTrack Tip: Authorization follows authentication; accountability depends on tamper-proof, synchronized logs.

3. Physical and Logical Access

Both layers apply IAM principles.

- **Physical:** Badges, PIN pads, biometrics, guards, mantraps, visitor logs, anti-passback.
- **Logical:** Passwords, tokens, MFA, RBAC/ABAC, 802.1X NAC, session timeouts, re-auth for sensitive tasks.
  FastTrack Tip: Revoke physical badges and logical accounts simultaneously at termination.

4. Foundational Principles

- **Least Privilege / Need-to-Know** – access only as required.
- **Separation of Duties / Dual Control** – divide high-risk actions.
- **Implicit Deny** – deny by default.
- **Job Rotation / Mandatory Vacation** – detect fraud and ensure continuity.
  FastTrack Tip: These four principles anchor all IAM policies and audits.

5. Authentication – Factors, Passwordless, Biometrics

Validates identity before granting access.

- **Factors:** Something you know (password), have (token), are (biometric), where (geolocation), do (behavior).
- **MFA:** Two different factors required; two passwords ≠ MFA.
- **Passwordless:** FIDO2 / WebAuthn smart keys; private key never leaves device.
- **Biometrics:** Measure FAR, FRR, CER; add liveness detection; hash templates.
  Assurance Levels (NIST SP 800-63): IAL (identity proofing) · AAL (authenticator strength) · FAL

(federation assertion).
FastTrack Tip: FIDO2 is phishing-resistant; lower CER = better biometric accuracy.

6. Before the Account Exists – Proof, Bind, Issue

Establishes identity and credentials prior to use.

1. **Registration / Proofing:** Verify identity from authoritative source.
2. **Binding:** Link verified identity to credential.
3. **Issuance / Activation:** Deliver securely; require first-use setup.
   Credential Lifecycle: Activate – Maintain – Renew – Revoke.
   FastTrack Tip: Provisioning must be auditable and revocable throughout the account lifecycle.

7. Device and Service Identities (Non-Human)

Extends IAM to machines and applications.

- **Device Identity:** PKI certificates, TPM attestation, NAC compliance checks.
- **Service Identity:** Short-lived tokens, mTLS, vault-stored secrets with automatic rotation.
- **Frameworks:** SPIFFE/SPIRE standardize workload identities.
  FastTrack Tip: Every machine identity must be unique, monitored, and revocable like a user account.

8. Authorization Models

Define how access decisions are made.

Model	Concept	Use Case / Strength
DAC	Owner grants rights	Flexible but higher spill risk
MAC	System-enforced labels	Classified / government
RBAC	Roles map to permissions	Simplifies audits; prevents privilege creep
ABAC	Attributes (user, resource, context)	Context-aware; Zero Trust ready
Rule-Based	If/Then logic (time, IP)	Firewalls / NAC
Risk-Adaptive	Real-time risk evaluation	Step-up MFA or deny access

FastTrack Tip: RBAC = static roles; ABAC = context; Risk-Adaptive = dynamic real-time policy.

9. Decision and Enforcement Architecture

Defines how policies are created, evaluated, and enforced.

- **PDP:** Policy Decision Point – evaluates requests.
- **PEP:** Policy Enforcement Point – enforces allow/deny.
- **PIP:** Policy Information Point – provides attributes.
- **PAP:** Policy Administration Point – where admins define policy.
- **Standard:** XACML for machine-readable ABAC rules.
  FastTrack Tip: PDP is the brain; PEP is the gatekeeper-together they implement policy as code.

10. Sessions and Tokens (Post-Login)

Maintains security after authentication through session and token controls.

- **Session Management:** Idle + absolute timeouts; re-auth for sensitive actions; single logout.
- **Token Hygiene:** Cookies (HttpOnly, Secure, SameSite); OTP short-life; JWT signed + short TTL; Bearer tokens rotate frequently.

- **Defenses:** Nonces/timestamps (anti-replay); token rotation (anti-fixation); avoid token exposure to scripts.
  FastTrack Tip: Treat tokens as temporary keys-protect them in transit and expire them quickly.

11. Federated Identity and Single Sign-On (SSO)

Enables seamless, trusted access across systems and organizations by extending authentication beyond one domain.

- **Federated Identity:** Establishes trust between independent domains (e.g., corporate login to AWS) so one Identity Provider (IdP) authenticates users for multiple external services.
- **Single Sign-On (SSO):** Allows users to authenticate once and access multiple systems within the same domain without re-entering credentials.
- **Protocols:** SAML 2.0 (enterprise federation), OpenID Connect (OIDC) on OAuth 2.0, OAuth 2.0 (API authorization), Kerberos (ticket-based internal SSO), RADIUS/TACACS+ (network AAA; TACACS+ encrypts entire payload).
- **SSO Practices:** MFA at IdP, sign and encrypt assertions, ensure IdP high availability and central logging.

FastTrack Tip: SSO improves usability within a domain; federation extends that trust across domains-protect the IdP as the single point of authentication truth.

12. Privileged Access Management (PAM) and Just-In-Time (JIT)

Reduces constant administrative exposure and enforces accountability for privileged operations.

- **Vault & Rotation:** Securely stores administrator and service passwords; rotates them automatically to prevent reuse.
- **Session Control:** Provides brokered logins, approval workflows, and full keystroke or screen recording of admin sessions.
- **Just-In-Time (JIT) Elevation:** Grants administrator rights only for a specific task or time window, then auto-revokes.
- **Dual Control:** Requires two separate approvals for high-impact operations.
- **Operational Practices:** Unique credentials per system, monitored “break-glass” emergency accounts, and regular review of privileged roles.
  FastTrack Tip: PAM + JIT replaces always-on admin accounts with time-bound, auditable, least-privilege access.

13. Adaptive / Risk-Based Access and Continuous Trust

Access decisions adapt dynamically to the user’s context and behavior.

- **Context Signals:** Device posture (encryption / antivirus / patch status), geolocation, IP reputation, access time, and behavioral patterns.
- **Responses:**
  - *Low risk* – allow normally.
  - *Medium risk* – require Multi-Factor Authentication (MFA).
  - *High risk* – deny or quarantine.
- **CARTA – Continuous Adaptive Risk and Trust Assessment:** Continuously re-scores trust *during* a session; can revoke tokens, force re-authentication, or switch user to read-only mode when anomalies appear.
  FastTrack Tip: Adaptive access ensures security remains proportional to real-time risk, not static assumptions.

14. Zero Trust Architecture (ZTA)

Built on the principle *“Never trust, always verify.”*

- **Core Tenets (NIST SP 800-207):** Verify explicitly, enforce least privilege, assume breach, micro-segment networks, and monitor continuously.

- **Building Blocks:**
  - Hardened Identity Provider (IdP) with MFA.
  - Device validation through Network Access Control (NAC) and Endpoint Detection and Response (EDR).
  - Policy Decision Point (PDP) and Policy Enforcement Point (PEP) to evaluate and enforce access in real time.
  - Software-Defined Perimeter (SDP) to hide internal services from public exposure.
  - Telemetry feeds and analytics to recalculate trust continuously.
    FastTrack Tip: Zero Trust is a strategy-identity, device, and session are verified every time, from anywhere.

15. Identity-as-a-Service (IDaaS), Hybrid Identity, and Cloud Workloads

Extends IAM controls to cloud and hybrid environments.

- **Identity-as-a-Service (IDaaS):** Cloud-hosted IAM providing Single Sign-On (SSO), MFA, user lifecycle automation, federation, and reporting.
- **Hybrid Identity:** Synchronizes on-premises directories such as Microsoft Active Directory with cloud IdPs; enables conditional access policies (device compliance, location, risk).
- **Cloud Workload Identity:** Uses short-lived tokens or roles, Mutual Transport Layer Security (mTLS), and secrets managed in vaults or Key Management Service (KMS); avoids hard-coded credentials.
  FastTrack Tip: Cloud identity should be short-lived, scoped narrowly, and managed centrally through policy-not stored in code.

16. Session, Token, and API Security in Practice

Protects what happens *after* login-session integrity, token safety, and secure API communication.

- **Web Sessions:** Cookies must be flagged HttpOnly (prevent JavaScript access), Secure (HTTPS only), and SameSite (prevent cross-site theft); use short idle and absolute timeouts; re-authenticate for sensitive actions.
- **JSON Web Token (JWT):** Compact, signed (JWS) and optionally encrypted (JWE) token carrying identity claims; validate issuer, audience, and expiration; rotate when privilege changes.
- **APIs:** Use OAuth 2.0 for delegated authorization and OpenID Connect (OIDC) for authentication; always require Transport Layer Security (TLS), narrow token scopes, and Proof Key for Code Exchange (PKCE) to prevent interception.
  FastTrack Tip: Treat tokens like digital cash-issue for one purpose, keep lifespan short, transmit only over TLS.

17. Monitoring, Detection, and Automated Response (ITDR)

Integrates IAM with threat analytics and automated containment.

- **Identity Threat Detection and Response (ITDR):** Consolidates identity events to detect account compromise or misuse.
- **Security Information and Event Management (SIEM):** Aggregates and correlates logs such as login attempts, token use, privilege changes, or anomalous access (“impossible travel”).
- **User and Entity Behavior Analytics (UEBA):** Learns normal user / device / service behavior through statistical baselines or machine learning, flagging deviations.
- **Security Orchestration, Automation, and Response (SOAR):** Executes pre-approved automated playbooks-revokes tokens, forces password resets, disables accounts, and opens incidents in ticketing systems.
- **Prerequisites:** Network Time Protocol (NTP) for time sync, immutable Write-Once-Read-Many (WORM) log storage, and separation of duties for auditing.
  FastTrack Tip: Combine SIEM + UEBA + SOAR = detect identity abuse early and automate containment before escalation.

18. Governance and Reviews (IGA)

Identity Governance and Administration (IGA) links people, policy, and process to ensure proper access at all times.

- **Functions:** Establish authoritative source (e.g., HR database), automate Joiner-Mover-Leaver lifecycle, perform role mining to detect privilege creep, run quarterly access recertifications, and enforce Separation of Duties (SoD).
- **Goal:** Real-time deprovisioning and zero orphaned accounts.
  FastTrack Tip: IGA proves compliance by showing *who has access to what and why*-and that it's reviewed regularly.

19. Metrics and Maturity (Measure Effectiveness)

Quantifies how well IAM processes perform and improve.

- **Key Performance Indicators (KPIs):**
  - Mean time to provision < 1 hour; deprovision < 15 minutes.
  - MFA coverage ≥ 90% users / 100% admins.
  - Orphaned accounts = 0.
  - Privilege creep trending down after each quarterly review.
  - Access review completion ≥ 95% on time.
- **Maturity Path:** *Ad hoc – Defined – Managed – Measured – Optimized* (ZTA + automation feedback loop).
  FastTrack Tip: Mature IAM is quantified IAM-metrics validate efficiency, control strength, and audit readiness.

20. Standards and Frameworks (Map to Authorities)

Aligns IAM controls with internationally recognized standards.

- **NIST Special Publication 800-63 – Digital Identity Guidelines:**
  - *Identity Assurance Level (IAL):* Strength of identity proofing.
  - *Authenticator Assurance Level (AAL):* Strength of authentication method (password vs MFA vs FIDO2).
  - *Federation Assurance Level (FAL):* Strength of federation assertions and protection mechanisms.
- **NIST SP 800-53:** Access Control family (AC-2 Account Management, AC-5 Separation of Duties, AC-6 Least Privilege).
- **ISO/IEC 27001 & 27002:** Access control policies, user registration, and privilege management.
- **FIDO2 / WebAuthn:** Passwordless and phishing-resistant authentication standards.
- **NIST SP 800-207:** Zero Trust Architecture principles.
- **CIS Controls v8:** Practical baseline for account and privilege management.
  FastTrack Tip: Map IAM processes to these frameworks to ensure audit alignment and cross-industry credibility.

21. Practical Roadmap (Baseline – Adaptive IAM)

Step-by-step journey toward mature identity security.

1. **Foundation:** Form IAM governance committee, define policies, centralize directory and authoritative sources.
2. **Authentication:** Roll out MFA (start with admins), plan passwordless migration (FIDO2/WebAuthn).
3. **Authorization:** Adopt Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC); enforce Separation of Duties.
4. **Privileged Access:** Deploy PAM with vaulting, recording, and Just-In-Time elevation.
5. **Federation & SaaS:** Integrate applications via SAML or OpenID Connect; automate provisioning using System for Cross-Domain Identity Management (SCIM).
6. **Operate & Improve:** Integrate with SIEM/UEBA/SOAR (ITDR); measure KPIs; perform role mining and recertification; review Zero Trust posture annually.

FastTrack Tip: Build IAM maturity gradually-governance first, then authentication, authorization, privilege, and continuous feedback.

22. Common Threats and Counter-Controls

Threat	Primary Controls / Countermeasures
Credential stuffing	Multi-Factor Authentication, breached-password blocking, login throttling
Phishing / MFA fatigue	Number-matching push verification, FIDO2/WebAuthn
Privilege escalation / misuse	Privileged Access Management, Separation of Duties, approval workflow
Session hijack / replay	TLS everywhere, short-lived tokens, nonces and timestamps, token binding
Pass-the-Hash / Kerberos ticket abuse	Disable legacy NTLM, shorten ticket lifetimes, Endpoint Detection and Response
Third-party exposure	Federation with conditional access, time-bound roles, least-privilege scopes

FastTrack Tip: Link threats – controls mentally; CISSP scenarios often test this cause-and-mitigation mapping.

Domain 6 – Security Assessment and Testing

Verifies that security controls are effective and performing as intended through audits, vulnerability scans, penetration tests, and continuous monitoring-turning measurement into assurance and improvement.

1. Purpose and Scope

Security Assessment and Testing ensures that implemented controls - **technical, administrative, and physical** - actually work and continue to protect the organization over time. **Key objectives**

- Verify control effectiveness (“are they doing what we expect?”)
- Detect weaknesses before attackers or auditors do
- Confirm compliance with policy, standards, and regulations
- Provide measurable assurance for management decision-making

2. Four Core Activities and How They Differ

Activity	Core Purpose	Typical Performer	Focus Example
Assessment	Identify control or process gaps.	Internal risk or compliance team	Gap analysis vs NIST 800-53 or ISO 27001
Audit	Independent, formal verification of compliance.	Certified internal/external auditors	PCI DSS audit, SOC 2 Type II report
Testing	Actively measure control effectiveness.	Security engineers, QA, red team	Vulnerability scan, code review
Monitoring	Continuous detection of events/anomalies.	SOC or operations team	SIEM, EDR, log analysis

Verification vs Validation

- **Verification:** Was it built right? – meets the spec/design.
- **Validation:** Was it the right thing to build? – meets business need.

3. Security Assessments

Evaluates how current practices align with intended design and policy across people, process, and technology.
Common types:

1. **Self-Assessment** – internal checklist for awareness.
2. **Third-Party Assessment** – external review without regulatory power.
3. **Risk Assessment** – quantifies likelihood × impact to rank priorities.
4. **Gap Analysis** – measures current posture vs target framework (ISO 27001, NIST CSF).
5. **Control Review** – validates that controls exist and function correctly.
   Methods: policy and configuration review, interviews, observation, automated scans.
   Deliverable: *Security Assessment Report (SAR)* summarizing findings, root cause, impact, recommendations, and residual risk.
   FastTrack Tip: Assessments show *where you are vs where you should be*-they guide remediation and budget planning before formal audits.

4. Security Audits

Formal, independent evaluations comparing actual controls with standards, laws, or internal policies.
Key characteristics: independent, evidence-based, scoped, repeatable, traceable.

Lifecycle: planning – fieldwork – analysis – reporting – follow-up.
Types: internal, external, operational, compliance, and technical audits.

Effectiveness testing:

- *Design effectiveness* – is the control appropriate?
- *Operating effectiveness* – is it applied consistently?
  FastTrack Tip: *formal, independent, documented*, it's an **audit**-otherwise it's an **assessment**.

5. Audit Logs and Accountability

Logs provide the factual record supporting detection, forensics, and compliance.

Why they matter: detect anomalies, prove non-repudiation, support investigations, and demonstrate due diligence.

Best practices:

- Centralize in a Security Information and Event Management (SIEM) platform.
- Synchronize time via Network Time Protocol (NTP).
- Protect integrity with hashing or Write-Once-Read-Many (WORM) storage.
- Restrict access to authorized personnel.
- Retain per policy or regulation (e.g., PCI DSS ≥ 1 year).
- Review alerts daily for critical systems, weekly for others.
  FastTrack Tip: Logs equal accountability only when protected from tampering and reviewed regularly.

6. Auditing in Cloud and Hybrid Environments

Validates security controls under the shared-responsibility model between provider and customer.
Responsibility split: provider = datacenter / hardware / hypervisor; customer = data / identity / config / monitoring.
Challenges: limited visibility below virtualization, short-lived assets (containers, serverless), evidence must be API-driven.

Audit strategy:

1. Define ownership of each control (provider vs customer).
2. Enable provider logs – AWS CloudTrail, Azure Monitor, GCP Audit Logs.
3. Use Cloud Security Posture Management (CSPM) tools.
4. Review encryption-key management (KMS / HSM).
5. Collect attestations – SOC 2, ISO 27017 / 27018.
6. Correlate hybrid logs in SIEM / SOAR for unified view.
7. Verify IAM hygiene – MFA, least privilege, conditional access.
   FastTrack Tip: In cloud audits think *shared responsibility + provider telemetry + CSPM + API evidence*.

7. Vulnerability Scanning (Baseline Testing)

Automated detection of known weaknesses using Common Vulnerabilities and Exposures (CVE) data and Common Vulnerability Scoring System (CVSS) metrics.

Process flow:

1. Define asset scope.
2. Run scans (prefer authenticated).
3. Analyze results / remove false positives.
4. Prioritize by exposure + exploitability + asset value.
5. Remediate – re-scan – verify closure.
6. Track Mean Time to Remediate (MTTR).
   Types:

- *Unauthenticated:* external view, quick, low risk.
- *Authenticated:* deeper, accurate with credentials.
- *Internal:* inside the perimeter.

- *External:* internet-facing targets.
  FastTrack Tip: Scanning finds vulnerabilities; **penetration testing** safely exploits them to prove business impact.

8. Continuous Monitoring

Ongoing analysis of security events for real-time visibility and assurance.

Examples:

- SIEM correlation rules linking events across systems.
- Endpoint / Network Detection and Response (EDR / NDR) anomaly analytics.
- Dashboards tracking compliance, patch, and vulnerability status.
  Key metrics: Mean Time to Detect (MTTD), Mean Time to Respond (MTTR), and Incident Recurrence Rate.
  FastTrack Tip: Continuous monitoring transforms periodic testing into real-time assurance-the backbone of adaptive and Zero Trust security.

9. Application and Software Security Testing

Validates that software itself-not just infrastructure-is secure across the Software Development Life Cycle (SDLC).

Static Application Security Testing (SAST)

- Analyzes source code or binaries *without* execution.
- Detects hard-coded credentials, injection flaws, and input-validation errors.
- Performed early in development (“shift-left”).

Dynamic Application Security Testing (DAST)

- Executes the running application to probe for runtime flaws (cross-site scripting, logic bypass, broken authentication).
- Reveals vulnerabilities attackers can actually exploit.

Interactive Application Security Testing (IAST)

- Combines SAST + DAST; sensors instrument the running code.
- Provides runtime context and fewer false positives.

Runtime Application Self-Protection (RASP)

- Monitors and blocks attacks from *within* the production runtime environment.

Fuzz Testing

- Sends malformed or random input to discover crashes, logic failures, and memory corruption-especially useful for parsers and IoT devices.

Manual Code Review

- Human review for logic errors, insecure design, or misuse of crypto APIs-issues automated tools miss.

FastTrack Tip: SAST – before run; DAST – while running; RASP – in production. Fuzzing tests resilience; code review tests reasoning.

10. Configuration and Network Testing

Ensures infrastructure follows hardened baselines and network boundaries behave as intended.

Configuration Compliance

- Compare system settings to hardening guides (Center for Internet Security [CIS] Benchmarks, Defense Information Systems Agency [DISA] Security Technical Implementation Guides [STIGs], NIST SP 800-53A).
- Tools: Security Content Automation Protocol (SCAP) / OpenSCAP, Chef InSpec, Ansible Audit.
- Review enabled services, permissions, password policies, and logging configurations.

Network Security Testing

- **Port Scanning:** Identify open services.
- **Banner Grabbing:** Discover software name & version.

- **Firewall / Access Control List (ACL) Review:** Verify least-privilege rules and directionality.
- **Routing Validation:** Confirm proper segmentation and path control.
- **Wireless Checks:** Detect rogue access points; verify WPA3 and IEEE 802.1X (EAP-TLS) security.

FastTrack Tip: Misconfiguration is the #1 breach cause-baseline reviews turn configuration drift into measurable, fixable risk.

11. Social Engineering and Physical Testing

Validates human and facility defenses-the weakest link in most attacks.

Social-Engineering Techniques

- **Phishing:** Fraudulent email.
- **Smishing / Vishing:** SMS or voice fraud.
- **Pretexting:** Impersonation using authority or fabricated story.
- **Baiting:** Leaving infected USB drives or enticing media.
- **Tailgating:** Following an authorized person into secure areas.

Rules of Engagement (RoE)

1. Obtain written senior-management authorization.
2. Define scope, timing, and contact points.
3. Halt immediately if safety or legal issues arise.

Physical Testing

- Verify locks, door controls, CCTV coverage, alarms, badge expiration, mantraps.
- Test anti-passback, visitor escort, and emergency response procedures.

FastTrack Tip: Human testing requires legal scope and clear RoE-unauthorized simulation = criminal intrusion, not assessment.

12. Penetration Testing

Demonstrates what vulnerabilities can be exploited and the resulting business impact.

Phases

1. Planning & Scoping – Define systems, legal approval, and Rules of Engagement.
2. Reconnaissance – Gather open-source (OSINT) information (WHOIS, social data).
3. Scanning & Enumeration – Identify services and weaknesses.
4. Exploitation – Controlled proof of impact (screenshots, data access).
5. Post-Exploitation – Privilege escalation, lateral movement (within scope).
6. Reporting – Translate technical findings into business risk and recommendations.
7. Remediation & Re-test – Verify fixes and lessons learned.

Test Depths

- **Black Box:** No knowledge (outsider view).
- **Gray Box:** Partial knowledge (user view).
- **White Box:** Full knowledge (developer view).
- **Red Team:** Stealth attack simulation.
- **Blue Team:** Detection and defense.
- **Purple Team:** Red + Blue collaboration for joint improvement.

Legal Essentials: Written authorization, defined stop conditions, and no destructive actions or privacy breaches.
Distinctions: Vulnerability scan = find; Pen test = prove; Red team = emulate adversary; Purple team = improve both sides.

FastTrack Tip: Pen testing shows impact and validates detection and response - always authorized, measured, and documented.

13. Business Continuity and Incident-Response Testing

Confirms that continuity and response plans actually work before a real disaster.

Business Continuity Plan (BCP) / Disaster Recovery Plan (DRP) Testing Levels (low – high risk)

1. **Checklist / Read-Through:** Document review only.
2. **Tabletop:** Discussion walk-through, no systems touched.
3. **Simulation / Functional:** Limited live exercise of specific functions.
4. **Parallel:** Recovery site runs alongside production.
5. **Full Interruption:** Production stopped for complete failover test.

Incident-Response Testing

- Exercises all phases: Preparation – Detection – Containment – Eradication – Recovery – Lessons Learned.
- Validates communication flow, escalation paths, and technical steps.

FastTrack Tip: Tabletop = low risk coordination check; Functional = hands-on validation of process and technology.

14. Test Data Management and Ethics

Security testing must never risk real sensitive data or breach confidentiality.

Best Practices

- Use synthetic or anonymized datasets.
- Mask Personally Identifiable Information (PII) and Protected Health Information (PHI).
- Secure test environments and outputs as production-grade.
- Destroy test data securely after completion.
- Disclose discovered vulnerabilities responsibly to vendors or owners.

FastTrack Tip: Testing with live data is a policy and compliance violation - use anonymized inputs and controlled outputs only.

15. Vulnerability Management Lifecycle

A continuous improvement loop-not a one-time scan-linking discovery to verification and reporting.

Phase	Key Actions
1. Discovery	Inventory all assets and tie them to the Configuration Management Database (CMDB).
2. Scanning	Run authenticated internal and external vulnerability scans.
3. Analysis	Validate and de-duplicate results; correlate with threat intelligence and exploit availability.
4. Prioritization	Rank by Common Vulnerability Scoring System (CVSS) score + business impact.
5. Remediation	Patch, reconfigure, or apply compensating controls.
6. Verification	Re-scan to confirm closure and update ticketing.
7. Reporting	Track Mean Time to Remediate (MTTR) and trend lines.
8. Continuous Monitoring	Feed results into Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) for visibility.

Supporting Concepts CVSS 0–10 = severity baseline; exploitability + asset criticality = true risk; formally document exceptions and accepted risk.

FastTrack Tip: Vulnerability management = discover – assess – fix – verify – repeat-closed-loop assurance, not a project.

6. Reporting and Communication

Transforms technical findings into business risk and accountable actions.
Report Structure Executive summary (plain language) – Scope & methodology – Findings with severity + evidence – Recommendations and priorities – Re-test plan with owners.

Level	CVSS	Example	Action
Critical	9 – 10	Remote code execution	Patch immediately
High	7 – 8.9	Authentication bypass	Fix ASAP
Medium	4 – 6.9	Misconfiguration	Schedule patch
Low	< 4	Informational	Monitor only

Effective Communication Tailor to audience (executives = impact; engineers = detail). Use visuals (MTTR, open vs closed issues). Context matters more than raw counts.

FastTrack Tip: Good reports translate findings into business risk language-what could happen, how bad, and who owns the fix.

17. Metrics and Continuous Validation

Uses measurable indicators to prove control effectiveness and drive accountability.

Quantitative Metrics (Numerical Indicators)

Measure *how quickly and effectively* security operations perform.

Metric	Meaning	Why It Matters
Mean Time to Detect (MTTD)	Average time between the start of an incident and its discovery.	Shorter MTTD = faster visibility into attacks.
Mean Time to Remediate (MTTR)	Average time from detection to full fix or closure.	Lower MTTR = quicker containment and reduced risk exposure.
Patch Compliance Rate	Percentage of systems patched within Service Level Agreement (SLA).	Shows how well patch management meets policy timelines.
Scan Coverage	Percentage of known assets included in regular vulnerability scans.	Gaps indicate “shadow IT” or unmonitored systems.
False Positive Rate	Percentage of reported issues that aren’t real.	High rate wastes analyst time; goal is <10%.
Vulnerability Recurrence Rate	How often previously fixed vulnerabilities reappear.	Reveals weak change control or regression in configuration management.

Qualitative Metrics (Process and Culture Indicators)

Measure *how mature and sustainable* the security program is.

Metric	Meaning / Focus	Why It Matters
Systems Meeting Baseline	% of systems configured per approved security baseline.	Reflects control consistency and policy adherence.
Repeat Audit Findings Trend	Whether known weaknesses keep reappearing in audits.	Declining trend proves lasting remediation.

Metric	Meaning / Focus	Why It Matters
User Security Awareness	Observed improvement from phishing tests or awareness training.	Indicates reduced human risk and improved security culture.

Continuous Monitoring & Automation

Transforms security testing into an ongoing assurance process where data, alerts, and fixes flow automatically.

Component	What It Does	Key Outcome
Security Information and Event Management (SIEM)	Centralizes and correlates logs from all systems (firewalls, servers, cloud, endpoints).	Detects suspicious patterns and policy violations in real time.
Security Orchestration, Automation, and Response (SOAR)	Automates standard response playbooks (disable account, block IP, re-scan system).	Reduces human response time and increases consistency.
Endpoint Detection and Response (EDR)	Monitors endpoint activities (processes, registry, memory) for abnormal behavior.	Stops lateral movement and insider threats early.
Network Detection and Response (NDR)	Analyzes network traffic for anomalies or command-and-control indicators.	Reveals attacks that bypass endpoint or perimeter controls.
Automated Re-scan and Ticketing	After a patch, system automatically re-scans, updates the dashboard, and closes tickets once verified.	Ensures closed-loop remediation with minimal manual effort.

Continuous Authorization (CA)

Used in programs like Federal Risk and Authorization Management Program (FedRAMP) and NIST Risk Management Framework (RMF) - it means continuously validating controls to maintain an active Authority to Operate (ATO).

Instead of a one-time audit, CA confirms security posture *every day* through telemetry and evidence.

FastTrack Tip: Continuous monitoring turns snapshots into motion pictures-**SIEM detects, SOAR reacts, EDR/NDR observe, and Continuous Authorization proves compliance in real time.**

18. Validation, Re-Testing, and Improvement

Confirms remediation and feeds lessons back into the security program.

Steps: Review fix – Re-test – Confirm closure – Update risk register – Document exceptions.

Regression Testing: Ensure patches or configuration changes did not break other controls or functions.

Independent Validation: Performed when required by compliance (e.g., Qualified Security Assessor for Payment Card Industry Data Security Standard – PCI DSS).

Threat Correlation: Map vulnerabilities to known exploits using Cybersecurity and Infrastructure Security Agency Known Exploited Vulnerabilities (CISA KEV) and MITRE ATT&CK framework to prioritize remediation.

Maturity Path: 1 Reactive – 2 Periodic – 3 Proactive – 4 Adaptive – 5 Optimized (DevSecOps + automation integration).

FastTrack Tip: Validation closes the loop-re-test to prove fixes and adapt processes to new threats.

19. Integration Across Domains

Testing links every CISSP domain into one assurance framework.

Related Domain	Integration Example
Governance (D1)	Audits verify policy compliance and risk ownership.
Architecture (D3)	Testing validates design assumptions and control implementation.
Network (D4)	Scanning and pen tests confirm segmentation and defense-in-depth.
Operations (D7)	Monitoring feeds Incident Response (IR) metrics and service continuity data.
Software Development (D8)	SAST / DAST integrate into Secure SDLC and DevSecOps pipelines.

FastTrack Tip: Testing is the bridge between policy and proof-it verifies that every domain's controls actually work together.

Domain 7 – Security Operations

Maintains and safeguards daily security functions through monitoring, incident response, forensics, and continuity planning-ensuring systems remain protected, available, and recoverable under all conditions.

1. Operations Security Principles

Operations security bridges policy and technology, ensuring systems remain **secure, stable, and predictable**.
Core principles:

- **Least Privilege & Need-to-Know:** Only required access, no more.
- **Separation of Duties & Dual Control:** Split critical tasks to prevent fraud.
- **Job Rotation & Mandatory Vacation:** Detect hidden issues and ensure continuity.
- **Operational Assurance:** Periodically verify that controls still work (access reviews, patch reports, drift detection).
- **Change Governance:** All modifications are planned, approved, reversible, and documented.
- **Documentation & Accountability:** Every operational task must be reproducible and auditable.

FastTrack Tip: Operations assurance = proof that protection *still works* - not just that it was once deployed.

2. Security Operations Center (SOC)

The SOC is the **command hub** of detection and response. It collects telemetry, triages alerts, investigates anomalies, and coordinates containment.

SOC Tier	Focus	Key Activities
Tier 1 (Analyst)	Initial triage	Review alerts, dismiss false positives
Tier 2 (Investigator)	Deep analysis	Correlate events, escalate incidents
Tier 3 (Hunter / Engineer)	Proactive defense	Threat hunting, rule tuning, automation

Integration points: SIEM for correlation, SOAR for automation, UEBA for behavior baselining, and EDR for endpoint telemetry.

FastTrack Tip: SOC = “see everything, respond fast.” 24×7 visibility and defined escalation paths turn data into action.

2.1 SOC Processes and Escalation

- Use a central ticketing system (e.g., ServiceNow, JIRA SM) to record every alert, investigation, and escalation.
- Shift-hand-off logs ensure continuity between analysts - no missed alerts.
- Maintain escalation tiers and on-call contact lists for 24×7 coverage.
- Use standardized incident categories (e.g., phishing, malware, insider, data leak) for reporting metrics.
  FastTrack Tip: SOC efficiency = visibility + handoff + documentation - what isn’t ticketed didn’t happen.

3 Incident Response (IR) Governance

Incident Response (IR) provides a **structured approach** to detect, contain, eradicate, and recover from security events - while preserving evidence and maintaining business continuity.

IR Phases

1. **Preparation:** Define roles, playbooks, tools, contacts.
2. **Detection & Analysis:** Identify and confirm real incidents.
3. **Containment:** Isolate affected systems; prevent spread.
4. **Eradication:** Remove root cause - malware, misconfig, credentials.
5. **Recovery:** Restore systems, validate, monitor.

6. **Lessons Learned:** Review, document, and strengthen defenses.

IR Governance Integration

- **BCP/DR Link:** IR limits impact; DR restores systems; BCP ensures business survives.
- **Legal & PR Alignment:** Notify counsel, regulators, and media through predefined channels.
- **Documentation:** Maintain timeline and decision log for every action.

FastTrack Tip: When a scenario says “contain first or preserve evidence?” - do both safely – *preserve first*, then contain.

4. Digital Forensics and Evidence Handling

Digital forensics identifies **what happened, when, how, and by whom** - and presents evidence that withstands legal scrutiny.

Core Principles

- Never alter the original; analyze verified copies.
- Maintain an unbroken **chain of custody** (signed, dated).
- Use cryptographic hashes (e.g., SHA-256) before and after imaging.
- Document every action, tool, version, and handler.

Order of Volatility (Most to Least)

1. CPU cache/registers
2. Memory (RAM)
3. Running processes & network connections
4. Temporary files / swap
5. Disk data & firmware
6. Cloud logs
7. Backups & archives

Evidence Sources

Source	Artifacts	Key Insights
Endpoints/Servers	Logs, registry, temp files	User & malware activity
Network Devices	Firewall, router, DNS logs	Lateral movement, exfil
Cloud Platforms	Control-plane logs	Admin/API actions
Mobile/IoT	App data, GPS, sensors	Behavior & location
Third Parties	SaaS/MSSP logs	Shared-responsibility evidence

FastTrack Tip: Cloud forensics = identity & API trails, not packet captures.

Evidence Storage and Preservation

- Store collected evidence in tamper-evident bags or sealed evidence lockers with controlled access.
- Label each item with case ID, handler name, date/time, and unique hash.
- Digital evidence copies should be encrypted and stored in a write-protected repository or digital vault.
  FastTrack Tip: Proper storage keeps evidence admissible even years later - chain of custody must remain intact.

5. Logging and Continuous Monitoring

Collects and protects logs so you can detect issues, trace actions, and prove compliance.

Core Objectives:

- Attribute every action to an authenticated identity.
- Detect anomalies early.
- Reconstruct events precisely.
- Prove compliance and due diligence.

Reliable Logging Practices

- Synchronize time (NTP) across all systems.
- Centralize logs in a SIEM.
- Protect integrity via hashing or WORM storage.
- Restrict access and log view activity.
- Retain logs for the legal or policy period.

Monitoring Technologies

System	Function	Trait
IDS	Detects malicious activity	Passive
IPS	Detects + blocks	Inline
SIEM	Correlates logs and alerts	Central analytics
SOAR	Automates response	Playbook-driven
UEBA	Detects behavior anomalies	ML baselines
DLP	Prevents data leaks	Monitors data flows

FastTrack Tip: IDS detects – IPS prevents – SIEM correlates – SOAR responds.

6. Effective Detection and Threat Hunting

Proactively searches for hidden threats and tunes rules to reduce attacker dwell time.

Detection Practices:

- Establish behavior baselines.
- Correlate weak signals into strong alerts.
- Validate threat-intel feeds before automation.
- Perform proactive threat hunting to discover silent attacks.
- Refine rules and playbooks after each incident.

FastTrack Tip: Every incident is a lesson - refine rules, reduce dwell time, and improve resilience.

7. Configuration, Patch, and Change Management

Keeps systems standardized, patched, and changed only with approval and records.

7.1 Configuration Management

Defines a hardened baseline and fixes any drift from it.

- **Baseline:** CIS Benchmarks / DISA STIG = reference for compliance.
- **Drift:** Any deviation from baseline – investigate and restore.
- **Tools:** Ansible, Chef, Puppet, OpenSCAP automate enforcement.
- **CMDB:** Records every configuration item (CI), owner, and change history.
  FastTrack Tip: Unknown or drifting systems = untrusted systems – restore or isolate immediately.

7.2 Patch and Vulnerability Management

Eliminates known weaknesses before attackers exploit them.

1. Identify assets.
2. Detect vulnerabilities (scanner, vendor alert).
3. Rate risk (CVSS + business impact).
4. Test in staging.
5. Deploy under change control.
6. Verify closure.
   Metrics: patch-compliance %, mean time to patch (MTTP).
   FastTrack Tip: Untested patch = new vulnerability - always stage first, then deploy.

7.3 Change Management

All operational changes must be approved, scheduled, and reversible.

Workflow: **Request – Review – Approve – Schedule – Implement – Verify – Document.**

Use a **Change Advisory Board (CAB)** for evaluation.
Emergency changes – allowed only for urgent security fixes; log and review afterward.

FastTrack Tip: No surprise changes. Unauthorized change = incident + audit violation.

7.4 How They Work Together

- Configuration – what's approved.
- Patch/Vulnerability – what's secure.
- Change – how it evolves.
  FastTrack Tip: Together = secure, predictable, and recoverable operations.

8. Core Operational Controls

Ensures people, privileges, and resources remain accountable and safe.

8.1 Least Privilege and Need-to-Know

Provide only required access - nothing extra. Enforce Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and quarterly reviews.

FastTrack Tip: Least privilege shrinks blast radius; need-to-know preserves confidentiality.

8.2 Separation of Duties & Dual Control

Divide critical tasks (e.g., initiate vs approve payments).
Dual control = two people must act together (e.g., cryptographic key access).
FastTrack Tip: Prevents fraud and accidental catastrophes.

8.3 Job Rotation & Mandatory Vacation

Rotating staff and forcing time off exposes hidden malpractice or dependence.
Common in finance and IT operations.

FastTrack Tip: No break in routine = no oversight - rotation reveals risk.

8.4 Privileged Account Management (PAM)

Admins have great power - apply tight control.

- Store credentials in vaults.
- Require MFA + session recording.
- Use Just-In-Time (JIT) access that auto-revokes.

- Ban shared administrator accounts.
  FastTrack Tip: PAM = vault + rotate + record + expire - trace every admin action.

8.5 Media & Resource Protection

Safeguard storage devices and backups. Label and encrypt media, keep custody logs, and destroy retired media securely (degauss / crypto-wipe / shred).

FastTrack Tip: Protect media – protect data – prove compliance.

9. Operational Documentation and Accountability

Uses SOPs, runbooks, and playbooks so work is consistent and auditable.

Document	Purpose
Standard Operating Procedure (SOP)	Step-by-step how-to for routine tasks
Runbook	Technical sequence for specific operations
Playbook	Predefined incident response workflow
Log / Report	Who did what and when (proof of control)

FastTrack Tip: “If it’s not documented, it didn’t happen.” Auditors need paper trails, not memories.

10. Monitoring for Compliance and Performance

Assures operations stay effective and aligned with policy and Service Level Agreements (SLAs).

10.1 Key Metrics

- **MTTD (Mean Time to Detect):** Speed of finding issues.
- **MTTR (Mean Time to Respond/Recover):** Efficiency of resolution.
- **MTBF (Mean Time Between Failures):** Reliability measure.
- **Patch Compliance %** and **Incident Closure Rate.**
- **False-Positive Rate / System Uptime %.**
  FastTrack Tip: Metrics prove resilience - trend them over time to show improvement.

10.2 Reporting and Review

Executives see impact; analysts see detail. Tie each metric to a policy goal or SLA.
Report trends (monthly/quarterly) to show progress and risk reduction.

FastTrack Tip: Numbers mean nothing without context - link every metric to a business objective.

11 Business Continuity and Disaster Recovery (BCP/DR)

Ensures critical business processes survive disruptions and IT services restore within tolerable limits.

11.1 Key Concepts

- **BCP (Business Continuity Plan):** Keeps operations running during disaster.
- **DRP (Disaster Recovery Plan):** Restores IT systems and data.
- **COOP (Continuity of Operations):** Minimum essential function mode.
  FastTrack Tip: BCP = keep running; DRP = restore IT; COOP = survive at reduced level.

11.2 Business Impact Analysis (BIA)

Identifies critical processes, dependencies, and maximum downtime.

Metric	Definition	Purpose
MTD (Maximum Tolerable Downtime)	Longest acceptable outage	Defines business limit
RTO (Recovery Time Objective)	Target restore time	Determines site type
RPO (Recovery Point Objective)	Max data loss (in time)	Determines backup frequency

Formula: **MTD ≥ RTO + WRT (Work Recovery Time).**
FastTrack Tip: BIA sets priority - what to save first and how fast.

11.3 BCP Lifecycle

1. Management approval and policy.
2. BIA and risk assessment.
3. Develop continuity / recovery strategies.
4. Document plans and contacts.
5. Implement and train teams.
6. Test and maintain regularly.
   FastTrack Tip: “First step in BCP?” – Get executive support and policy approval.

11.4 Recovery Sites

Chooses hot, warm, cold, active-active, or cloud sites based on RTO/RPO and budget.

Type	Description	RTO	Cost
Hot	Fully equipped, live data	Hours	$$$
Warm	Ready hardware, partial data	4–24 h	$$
Cold	Power only, no systems	Days	$
Active-Active	Both sites live simultaneously	Near 0	$$$$
Cloud DR	On-demand failover	Variable	Pay-as-used

FastTrack Tip: Tight RTO/RPO – hot or active-active; low budget – warm or cold.

12 Backup, Redundancy, and Fault Tolerance

Backups and redundancy ensure that when-not if-failure occurs, data and services remain recoverable.

12.1 Backup and Data Protection

Uses full/incremental/differential/snapshots with encryption and regular restore tests.

Type	What It Saves	Restore Need	Notes
Full	Everything	Only last full	Slow backup, fast restore
Incremental	Since last backup	Full + all incrementals	Fast backup, slow restore
Differential	Since last full	Full + last differential	Balanced approach
Snapshot	Point-in-time	Independent	Quick rollback before change

Rules: 3-2-1 (3 copies, 2 media, 1 off-site); encrypt backups in transit and at rest; store keys separately (HSM / KMS); test restores regularly.

FastTrack Tip: RAID is not a backup-RAID survives hardware failure; backups recover lost data.

12.2 Redundancy and High Availability

Adds spare components and paths to remove single points of failure.

Prevent single points of failure.

- **System:** Dual PSU, fans, servers.
- **Network:** Dual switches / ISPs.
- **Data:** RAID or replication.

RAID Summary: 0 = speed only | 1 = mirror | 5 = 1 disk parity | 6 = 2 disk parity | 10 = mirror + stripe (best mix).

FastTrack Tip: True high availability = redundancy + monitoring + tested failover.

12.3 Personnel Continuity

Technology fails - people must continue. Cross-train staff, define alternates, enable secure remote work (VPN + MFA), and delegate authority by role, not name.

FastTrack Tip: No single human point of failure should exist in operations.

12.4 Testing and Updating BC/DR Plans

Exercises plans regularly and improves them after every test.

Test Type	Description	Risk / Cost	Realism
Checklist / Read-through	Verify documentation completeness	Low	Low
Tabletop / Walkthrough	Discuss scenarios only	Low – Medium	Moderate
Simulation / Functional	Limited live execution	Medium	High
Parallel Test	Recovery site runs with production	Medium – High	Very high
Full Interruption	Complete failover	Highest	Maximum

FastTrack Tip: Best balance = Parallel test (realistic without outage); update plans after every test or organizational change.

13. Incident Response (IR) and Forensics Integration

Structured response limits damage, preserves evidence, and improves future resilience.

13.1 Incident Response Lifecycle

1. **Preparation:** Define policy, roles, playbooks, contacts.
2. **Detection & Analysis:** Validate alerts, determine scope and impact.
3. **Containment:** Isolate affected systems, block attacker access.
4. **Eradication:** Remove malware, bad accounts, or config changes.
5. **Recovery:** Restore operations and monitor for re-infection.
6. **Lessons Learned:** Update controls, documentation, and training.

FastTrack Tip: Always preserve evidence before cleanup - no proof = no case.

13.2 Roles and Responsibilities

Defines who coordinates, who investigates, who communicates, and who advises legally.

Role	Function
IR Manager	Coordinates response activities

Role	Function
Technical Analysts	Investigate systems and alerts
Forensic Team	Capture and analyze evidence
Communications / PR	Manage internal and public messaging
Legal / HR	Handle compliance and employee issues

FastTrack Tip: Contain before eradicate - act fast but methodically.

13.3 Digital Forensics Essentials

Proves what happened and by whom - legally admissible.

- Don’t touch original media; work on bit-for-bit copies.
- Maintain chain of custody (log every transfer).
- Hash before and after analysis (SHA-256).
- Record tool versions and time zones.
- Capture volatile data first (memory – disk – cloud logs).
  FastTrack Tip: Forensic integrity = hash + custody + documentation.

14. Monitoring, Detection, and Threat Intelligence

Combines real-time visibility, alert correlation, automated response, and attacker intelligence to detect, analyze, and counter security threats before they escalate into major incidents.

14.1 Core Monitoring Tools

System	Full Name	Function	Key Trait
IDS	Intrusion Detection System	Detects attacks	Passive
IPS	Intrusion Prevention System	Blocks attacks	Inline
SIEM	Security Information and Event Management	Aggregates + correlates logs	Central analytics
SOAR	Security Orchestration, Automation and Response	Automates response playbooks	Fast and consistent
UEBA	User and Entity Behavior Analytics	Detects anomalous behavior	Machine-learning baselines
DLP	Data Loss Prevention	Monitors / blocks data exfiltration	Outbound control

FastTrack Tip: IDS detects; IPS prevents; SIEM correlates; SOAR automates; UEBA learns; DLP protects data.

14.2 Monitoring Layers

1. **Network:** firewall, DNS, VPN logs - detect scans / exfiltration.
2. **Host / Endpoint:** EDR monitors processes and registry.
3. **Application:** trace auth, errors, transactions.
4. **Cloud:** CloudTrail / Azure Monitor / GCP Audit Logs - watch API calls.
5. **User & Identity:** login failures, privilege changes, off-hour logins.
   FastTrack Tip: Cloud forensics relies on immutable control-plane logs, not packet captures.

14.3 Threat Intelligence (TI)

Provides context on attacker tactics and indicators.

- **Strategic:** big-picture trends (for executives).
- **Tactical:** methods and MITRE ATT&CK mappings.
- **Operational:** active campaign intel.

- **Technical:** indicators (IPs, hashes, domains).
  Sources: ISACs, CERTs, vendors, internal feeds.
  Integrate with SIEM/SOAR for auto-blocking and alert enrichment.
  FastTrack Tip: Intelligence + automation = contextual defense at machine speed.

14.4 Automation / SOAR

Automates routine incident response steps.

Examples: auto-isolate host, disable compromised account, create ticket, notify analyst.
Benefits: speed, consistency, and reduced human error.

FastTrack Tip: Keyword “reduce workload + faster response” – SOAR.

15. Physical and Environmental Security

Protects facilities, equipment, and supporting infrastructure from unauthorized access, power loss, fire, and environmental hazards to ensure continuous and safe system operations.

15.1 Physical Layers

1. **Perimeter:** fences, lighting, guards, CCTV.
2. **Building:** mantraps, badge check, reception screening.
3. **Internal:** locked server rooms, escort policy.
4. **Asset:** tamper seals, locks, camera coverage.
   FastTrack Tip: Two-factor physical entry (badge + biometric) stops tailgating.

15.2 Environmental Controls

Threat	Control	Example
Power loss	UPS, generators	UPS = short term; generator = long term
Fire	Detectors, gas suppression	FM-200, inert gas
Heat / Humidity	HVAC	Redundant cooling
Water / Leak	Raised floors, sensors	Avoid sprinklers above racks
Dust / Air	Filters, positive pressure	Protects hardware

15.3 Media Handling

Label by classification, encrypt, log custody, and transport in tamper-evident containers.

Sanitization: Clear = overwrite; Purge = degauss/crypto-erase; Destroy = shred/melt.
FastTrack Tip: For “Top Secret” media – destroy physically.

16. Auditing, Metrics, and Continuous Improvement

16.1 Audit Lifecycle

1. Plan scope and criteria.
2. Collect evidence (logs, configs, interviews).
3. Analyze findings vs policy.
4. Report risks and recommendations.
5. Verify remediation and closure.
   FastTrack Tip: Audit = independent verification of trust - evidence must be repeatable.

16.2 Operational Metric Mapping

Metric	Indicates	Control Validated
MTTD (Mean Time to Detect)	Detection speed	SIEM / SOC efficiency
MTTR (Mean Time to Recover)	Recovery agility	IR / BCP process
Patch Compliance %	Hygiene and proactivity	Configuration & Change Mgmt
Incident Closure Rate	Response throughput	IR team capacity
False Positive Rate	Alert tuning accuracy	SIEM / UEBA rules
SLA Uptime %	Reliability	High availability controls

FastTrack Tip: Metrics only matter if they validate a control - link each number to a policy objective.

Domain 8 – Software Development Security

Integrates security into every phase of the software development lifecycle-ensuring applications are designed, coded, tested, and deployed to resist vulnerabilities and protect data from inception to retirement.

2) Secure SDLC - what to do at each phase

Add security tasks to plan, design, code, test, deploy, operate, and retire to catch issues early.

Plan / Initiate

- List data types and laws that apply (PII, HIPAA, PCI).
- Note risks early. Write security goals in the project charter.

Requirements

- Write **business** and **security** needs together.
- Add misuse cases (“what if a user tries X?”).
- Make acceptance tests measurable (e.g., “log who/when for all changes”).

Design / Architecture

- Draw the system and **trust boundaries**.
- Run a quick **threat model** (what can go wrong, where, how to stop it).
- Pick known-safe patterns (sandbox, reference monitor). Decide crypto & key storage.
- Hold a **design review** before coding starts.

Implement / Build

- Follow OWASP/CERT rules. Do **peer review** on all changes.
- Run **SAST** (code scan) and **SCA** (library scan) on each commit.
- Keep secrets in a **vault**, not in code.
- Use **signed commits** and protected branches.

Test / Verify

- Run **DAST/IAST**, fuzzing, and negative tests.
- Fix issues before release freeze.

Deploy / Release

- Ship **signed artifacts** only. Use hardened images.
- Go through **change control** and have a **rollback** plan.
- Verify TLS, permissions, and logging are on.

Operate / Maintain

- Patch on schedule. Rotate keys/certs.
- Send logs to SIEM. Scan regularly after releases.

Retire / Dispose

- Wipe data per **NIST 800-88** (clear/purge/destroy).
- Revoke tokens/certs. Archive docs for audit.

Why “shift left”: finding bugs in design/coding is cheap; in production it is costly.

3) Development styles - how security fits

Tailor security gates and tests to Waterfall, Agile, DevOps, and other methods.

- **Waterfall**: fixed phases. Add **security gates** at each phase (good for regulated work).
- **Spiral**: each loop = design + **risk** review. Do a mini threat model per loop.
- **Agile/Scrum**: add **security stories**; “definition of done” includes SAST + review; name a **security champion**.
- **XP**: TDD and pair programming; build **security unit tests**.
- **DevOps/DevSecOps**: CI/CD runs **SAST/SCA/IaC/DAST automatically**; require signed artifacts.
- **SAFe**: many Agile teams; central security rules and metrics.

4) Who does what

- **Data Owner**: classifies data, approves access, sets retention.

- **System/Service Owner**: makes sure controls run in production.
- **Security Architect/Engineer**: standards, secure design, threat models.
- **Developers / QA**: follow standards, write tests, fix findings.
- **Ops/Platform**: hardening, patching, monitoring, backups.
- **Audit/Compliance**: independent checks and evidence.

Keep artifacts: threat models, scan reports, code reviews, change tickets, release signatures, logs.

5) Change & Config (stability and proof)

Controls changes and keeps configs baseline-aligned, versioned, and auditable.

Change management steps

1. Request (reason, risk, test, rollback).
2. Review/approve.
3. Test in **staging**.
4. Controlled deploy.
5. Post-review and update records.
   Emergency changes: allow, but **retro-approve** and document.

Configuration management

- Set **baselines** for OS/DB/app. Version-control configs.
- Track in **CMDB**. Detect and fix **drift**.
- Prove prod matches the approved baseline.

6) Secure coding

- **Validate input** (length/type/range; allow-lists; schemas).
- **Encode output** (stop XSS; use CSP).
- **Strong authN/authZ** (central service; check every request).
- **Safe errors** (generic to users; detail to logs).
- **Encrypt** data (TLS 1.3, AES-256; keys in HSM/KMS).
- **No secrets in code** (use a vault).
- **Least privilege** for apps and DB users.
- **Deny by default**; allow explicitly.
- **Log safely** (no secrets; time-synced; integrity protected).
- **Update components** (automated SCA).

Common flaws – fixes

- Buffer overflow – bounds checks + ASLR/DEP + canaries.
- Injection (SQL/command) – **parameterized queries** + validation.
- Broken sessions – rotate IDs on login; secure cookies; short token life.
- Insecure deserialization – type checks; signed objects.
- Logic/authorization bugs – peer reviews; negative tests; threat model.

7) SCM & repository hygiene (proof of who/what/when)

Uses version control, signed commits, reviews, and scans to protect code history.

- Everything in **version control**; identify author/time/reason.
- **Signed commits**, protected main branch, **two-person** reviews.
- Auto-run scans before merge; keep **build manifests** (hashes, tool versions).
- Repo access: **SSO + MFA**, RBAC, audit logs, secret-scanning.

8) Languages & runtimes (risk snapshot)

- **C/C++**: memory errors – need bounds checks, compiler hardening, fuzzing.

- **Java/C#/Go/Python/Rust**: safer memory; still need strong authZ and logic checks.
- Managed runtimes risks: **insecure deserialization**, **SSRF**, **reflection abuse** – sign objects, egress allow-lists, restrict reflection, sandbox.

9) Third-party & supply chain (start here)

- Risks: known CVEs, bad licenses, fake packages.
- Controls: **SCA**, **version pinning/lockfiles**, **private registries**, **SBOM**, license policy, continuous vuln alerts.

10) Application Security Testing - when and why

Security testing checks whether software resists attacks and meets policy.

Test	When	What it finds	Key idea
SAST (Static)	Before running the code	Insecure coding (SQLi, XSS, unsafe APIs)	Scan source or binaries early - cheap fix
DAST (Dynamic)	Against running app	Runtime issues - bad validation, auth flaws	Simulates real attack
IAST (Interactive)	During test run	Combines code + runtime view	Accurate, needs agent
SCA (Composition)	Build or runtime	Vulnerable libraries/dependencies	Supply chain control
Fuzzing	Build/test	Crashes, overflow, rare logic bugs	Sends random inputs
RASP	Production	Detects/block attacks in live app	Runtime self-protection

Best flow: SAST + SCA (during coding) – DAST/IAST (before release) – RASP/WAF (in production). **Logic**

examples:

- Detect vulnerable library – **SCA**
- Find SQL injection – **DAST**
- Catch flaws early – **SAST**

11) Build, CI/CD, and Toolchain Security

Locks down build systems, signs artifacts, and enforces policy-as-code in pipelines.

Build System Best Practices

- Use **isolated, patched build servers**.
- Run each build in a clean temporary (ephemeral) environment.
- Limit privileges and network access.
- Store **signing keys** in a Hardware Security Module (HSM).
- Generate **build provenance** (who built, when, what sources, which tools).
- Sign every build artifact; verify signatures before deployment.
- Use **policy-as-code** gates - fail builds that skip tests or scans.

CI/CD Pipeline Security

1. **Isolated runners** – each job starts clean.
2. **Short-lived credentials** – auto-expire tokens.
3. **Secrets vaults** – no plain-text keys in scripts.
4. **Auto checks** – fail build on failed scan/test.
5. **Artifact signing + verification** before deploy.
6. **Immutable logs** for every step.
7. **No manual deploys** - pipeline automation only.
8. **Alert** on abnormal or unsigned builds.

Infrastructure as Code (IaC)

- Define servers/networks as code – version-controlled.
- Scan templates for misconfigurations (open ports, public buckets).
- Enforce **policy-as-code** to block unsafe deployments.
- Keep full version history for traceability.

Scenario: "Fast, frequent, yet secure releases" – Automate SAST, SCA, IaC scans, and signing in CI/CD.

12) Developer Workstation and IDE Security

Developer systems are part of the attack surface.

Common Risks

- Malicious plugins or extensions.
- Secrets or passwords in local files.
- Shared or reused credentials.
- Unencrypted drives, missing endpoint protection.

Controls

- Install only verified plugins.
- Use secure vaults, not local `.env` files.
- Enforce full disk encryption and Endpoint Detection & Response (EDR).
- Patch automatically; remove admin rights.
- Use MFA + VPN for internal access.
- Block production data in debugging sessions.
- Run code scan plugins directly in the IDE for instant feedback.

Rule: Treat developer laptops like production servers - compromise = full source code leak.

13) Runtime Environments - Containers, Orchestration, Serverless

Hardens images, enforces RBAC and network policies, and limits function privileges.

Container Security

- Build from **minimal base images**.
- Run as **non-root**, use read-only filesystems.
- Scan images before & after deployment.
- Use namespaces / control groups for isolation.
- No privileged containers unless absolutely required.

Kubernetes / Orchestration

- Apply **Role-Based Access Control (RBAC)** per namespace.
- **Deny-all network policy** by default.
- Use **admission controllers** to enforce image signing & scanning.
- Store secrets securely, not in environment vars.
- Patch master and node components regularly.

Serverless

- **Least privilege** per function.
- Sanitize all event inputs.
- Auto-rotate credentials.
- Set **timeout/concurrency limits** to contain denial-of-service.
- Keep test and prod separate.

Scenario cues:

- Block unsigned containers – Admission controller policy.
- Reduce blast radius – Least privilege + timeout limits.

14) API Security

Authenticates with OAuth/OIDC, validates input, encrypts transport, and rate limits.
APIs = main attack front door.

Area	Best Practices
AuthN	Use OAuth 2.0 / OpenID Connect; short-lived JWT tokens
AuthZ	Check permission and token scope on every call
Input Validation	Use strict JSON/XML schemas
Transport	Enforce TLS 1.2+ or mutual TLS (mTLS)
Rate Limit	Throttle brute force or DoS
Data Minimization	Return only needed fields; mask PII
Logging	Log every API call with request IDs
Gateway	Central control point for auth and throttling

REST – OAuth 2.0, JWT, TLS. **SOAP** – WS-Security, XML signatures & encryption
Exam logic:

- Partner API – OAuth + mTLS
- Brute-force prevention – Rate limit + lockout
- Internal system-to-system – mTLS

15) Risk and Assurance in Software Projects

Identifies, ranks, and treats software risks, then monitors as the system evolves.

Software Risk Steps

1. **Identify assets** - source code, build systems, data, credentials.
2. **Identify threats** - insider abuse, vulnerable libraries, API misuse, data leaks.
3. **Find weaknesses** - bad validation, weak crypto, config errors.
4. **Evaluate** - estimate likelihood and impact (CVSS or DREAD).
5. **Decide treatment** - avoid, mitigate, transfer, or accept.
6. **Monitor** - verify controls after updates or new releases.

Strategy	Meaning	Example
Avoid	Remove the risk completely	Drop risky feature
Mitigate	Add controls to reduce risk	Validate inputs, patch flaws
Transfer	Pass risk via contract/insurance	Vendor SLA or cyber insurance
Accept	Approve residual risk	Low-severity bug logged and accepted

16) Auditing, Evidence, and Continuous Improvement

Prove the SDLC followed policy and controls worked.

Key Audit Checks

- Secure-coding, change, and testing steps documented.
- Review configuration baselines and signed approvals.
- Confirm separation of duties (developer ≠ approver ≠ deployer).

- Verify SAST/DAST/SCA ran and issues were fixed.
- Maintain a **traceability matrix** (requirement – test – evidence – sign-off).

Change and Code Integrity

- Use **digital signatures** and timestamps for all commits.
- Keep records showing who changed what, when, and why.
- Validate build hashes match approved source.

Logging and Monitoring

- Log **who, what, when, where, why** for each event.
- Sync time (NTP).
- Protect logs using WORM or hashes.
- Forward to **Security Information and Event Management (SIEM)**.
- Alert on key events (failed logins, privilege changes).
- Redact sensitive data before storing.

Good rule: If it's not logged or signed, it cannot be trusted or audited.

17) Third-Party and Outsourced Software

Vet vendors and contractors; set security SLAs, audit rights, and code controls.

Commercial Off-the-Shelf (COTS)

- Check vendor reputation, update cycle, and certifications (SOC 2, ISO 27001).
- Review patch policy and incident process.
- Require encryption compliance and **right-to-audit** clause.

Open-Source Software (OSS)

- Use only from trusted repositories.
- Keep a **Software Bill of Materials (SBOM)**.
- Scan with **SCA** for known CVEs and license risks.
- Replace abandoned projects.

Outsourced Development

- Sign **Non-Disclosure Agreements (NDAs)** and define IP ownership.
- Do background checks and code reviews.
- Enforce controlled, monitored environments (no local copies).
- Use **source-code escrow** for continuity if vendor fails.
- Define security Service Level Agreements (SLAs).

Cloud & Managed Services

- Understand the **shared responsibility model** (you vs. provider).
- Verify provider certifications (ISO 27017, SOC 2, CSA STAR).
- Require encryption at rest and in transit.
- Confirm tenant isolation and incident reporting time limits.

Model	Who Patches What
SaaS	Provider handles OS & app updates
PaaS	Provider OS, customer app
IaaS	Customer OS & app

18) Secure Coding Standards and Reference Frameworks

Follows OWASP, SEI CERT, ISO 27034, and NIST guides for consistent defenses.

Standard	Focus
OWASP Secure Coding Practices	Common web coding defenses
SEI CERT	Language-specific coding rules
ISO/IEC 27034	Application Security Management lifecycle
NIST SP 800-64	Integrating security into SDLC

19) Artificial Intelligence (AI) and Machine Learning (ML) Security

Protects training data and models from poisoning, evasion, leakage, and bias.

- **ML** learns from data; **DL** (Deep Learning) uses layered networks.
- **AI risk = data integrity risk** - poisoned training – wrong results.

Threat	Description	Defense
Data poisoning	Fake data during training	Validate and checksum datasets
Model evasion	Crafted input fools model	Normalize input; adversarial tests
Model inversion	Extracting hidden data	Rate-limit queries; differential privacy
Bias	Skewed or unfair outputs	Diverse datasets; bias audits
Lack of transparency	Unexplainable decisions	Use Explainable AI (XAI); log reasoning

20) Software-Defined and Automated Security

Applies policy-as-code and IaC checks for continuous, automated compliance.

- Express controls as **code** (policy-as-code).
- Auto-deploy firewall rules, IAM policies, and config compliance.
- Integrate with Infrastructure as Code and CI/CD.
- Tools: **Open Policy Agent (OPA)**, **AWS Config**, **Terraform Sentinel**.
- Benefits: faster updates, fewer manual errors, continuous compliance.

21) Governance, Documentation, and Metrics

Maintains policies, traceability, and metrics to show the SDLC is secure and controlled.

Documents to keep:

- Secure SDLC policy and procedures.
- Crypto/key-management policy.
- Third-party software usage policy.
- Privacy-by-Design guideline.
- Traceability matrix (requirements – code – test – sign-off).
- Risk register and audit reports.

Continuous improvement:

- Feed lessons from incidents and audits back into design and training.
- Re-evaluate maturity (SAMM/CMM).
- Track metrics: vulnerability fix rate, Mean Time to Remediate (MTTR), and test coverage.

END

License and Usage Terms

This publication, **“FastTrack CISSP Reference,”** is provided free of charge for **educational and non-commercial use**. You may copy, share, or distribute it **with full credit to the author**.

Author Website: www.jobyer.me
Company Website: www.bytium.com