UNIT-IV: Audit Control

Detailed Lecture Notes — Infrastructure, Operating Systems, & Operational Security Controls

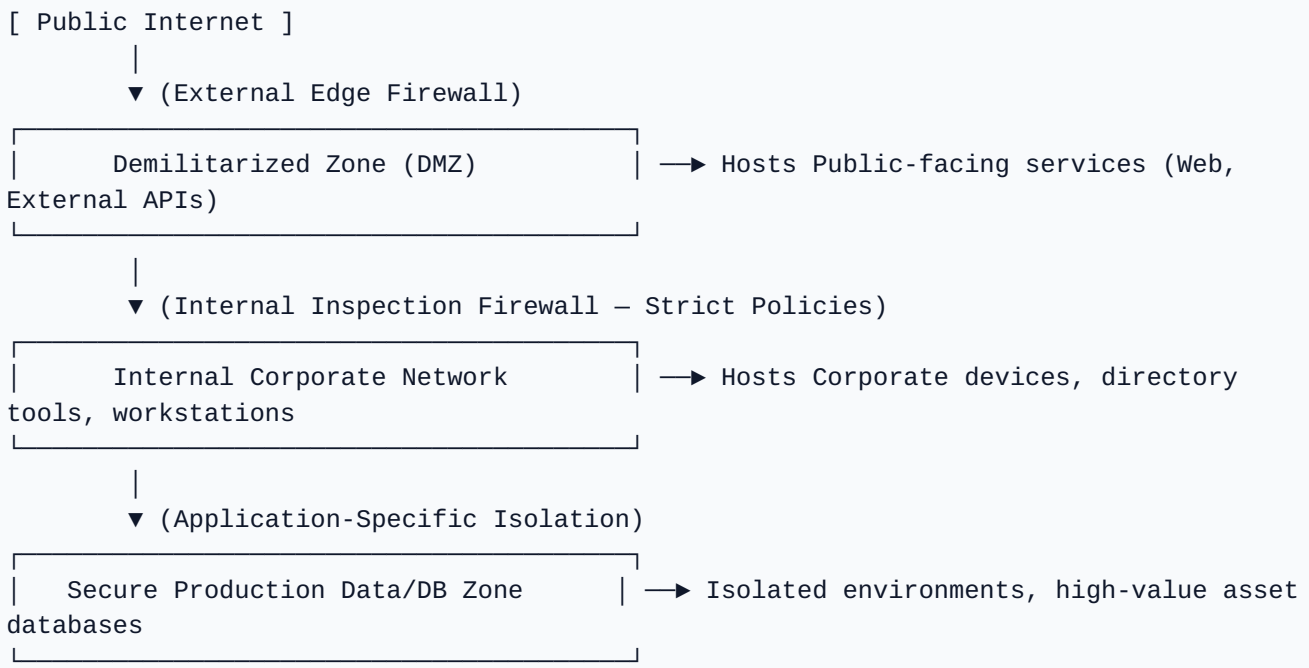
1. Network Security and Control

Networks serve as the structural communication pathways for modern enterprise IT. Auditing network security requires evaluating controls across multiple layers of the Open Systems Interconnection (OSI) reference model to guarantee the confidentiality, integrity, and availability (the **CIA Triad**) of data both in transit and at rest.

A. Network Architecture and Perimeter Security

An IS auditor must evaluate how an organization segments its network topology to establish clear defensive boundaries. Proper segmentation prevents unauthorized **lateral movement**, which is an adversarial technique where an attacker compromises a low-risk edge system and leverages it to traverse deeper into internal systems.

FIGURE 1.1: MULTI-TIER NETWORK SEGMENTATION & BOUNDARY ENFORCEMENT



1. Demilitarized Zone (DMZ) Architecture

The DMZ is a physical or logical subnetwork designed to isolate an organization's public-facing interfaces from the untrusted public internet. By positioning public services (such as web, mail, or application proxy servers) within this perimeter buffer zone, the organization ensures that a compromise of a public-facing system does not grant direct access to the internal corporate directory or database layers.

2. Firewall Governance & Configuration Controls

Firewalls serve as the primary policy enforcement points for network traffic routing. Auditors assess firewall configurations against precise technical criteria:

- **The Implicit Deny Posture:** The firewall control table must be built so that all data packets are blocked by default. Only communication explicit by IP addresses, protocols, and communication ports is permitted. The absolute final entry within the configuration lookup matrix must be a catch-all `Deny Any/Any` statement.
- **Stateful Inspection vs. Next-Generation Firewalls (NGFW):** Traditional stateful firewalls validate connections purely via structural layer headers (Source IP, Destination IP, Protocol, Port). Modern compliance audits require Next-Generation Firewalls (NGFWs), which execute **Deep Packet Inspection (DPI)** up to the Application Layer (Layer 7). This allows the firewall to identify and strip malicious payloads or scripts hidden inside standard traffic flows (e.g., within legitimate HTTPS traffic on port 443).
- **Rule-Base Optimization & Cleanup:** Over time, production firewall rules accumulate obsolete, duplicate, or overly permissive configurations. Auditors inspect the rule tables to flag legacy configurations that widen the network's attack surface.

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

- **IDS (Intrusion Detection System):**** A passive monitoring mechanism that processes mirrored copies of network traffic via port monitoring or physical TAP components. It scans for patterns that match known attack signatures or structural anomalies and issues immediate alerts to security operations teams.
- **IPS (Intrusion Prevention System):**** An active inline security appliance placed directly in the communication path. Upon discovering an exploit pattern or signature match, it drops the malicious packets immediately, neutralizing the threat before it interacts with target infrastructure.
- **Auditor Evaluation Focus:** Auditors review log files to check signature update frequencies and tune false-positive rates to confirm that the platform is actively maintained rather than ignored due to alert fatigue.

B. Encryption and Data in Transit

Data moving across untrusted or public networks must be programmatically shielded against eavesdropping (packet sniffing) and unauthorized mid-flight alteration (man-in-the-middle exploits).

1. Virtual Private Networks (VPNs)

VPN architectures construct secure, encrypted tunnels across public communication backbones, primarily to facilitate remote work paths or bridge remote corporate facilities.

- **Protocols:** Modern secure deployments rely on **IPsec** (Internet Protocol Security) working at the Network Layer (Layer 3) or **SSL/TLS** working at the Transport Layer (Layer 4).
- **Auditor Checkpoint:** Auditors evaluate configurations to ensure deprecated, insecure protocols—such as PPTP (Point-to-Point Tunneling Protocol) or native L2TP lacking IPsec cryptographic encapsulation—are disabled globally.

2. Transport Layer Security (TLS) Engineering

TLS acts as the industry standard for securing web applications and browser-based transactional data exchanges (HTTPS).

- **Cipher Suite Verification:** Auditors run automated scanners against exposed web listeners to confirm that they enforce strong cryptographic ciphers (such as AES-256-GCM or ChaCha20-Poly1305) and employ ephemeral key exchanges (such as ECDHE) to guarantee **Perfect Forward Secrecy (PFS)**.
- **Protocol Deprecation:** Auditors ensure that obsolete versions of the standard—specifically SSL v2.0, SSL v3.0, TLS 1.0, and TLS 1.1—have been disabled at the host system layer, leaving only TLS 1.2 and TLS 1.3 active.

C. Network Audit Checklist and Evidence Artifacts

Evidence Artifact Required	Audit Testing Procedure	Target Risk Mitigation
Firewall Configuration Tables	Programmatically check configuration rules for any active rows containing source or destination parameters set to `ANY`.	Prevents unauthorized network entry and access control bypasses.
Network Architecture Diagrams	Cross-reference logical system layouts against active routing tables to verify production databases are isolated from public corporate Wi-Fi or testing zones.	Prevents unauthorized lateral movement across infrastructure security zones.
Internal & External Vulnerability Logs	Analyze historical monthly vulnerability reports to ensure core routing, switching, and load balancing hardware are updated.	Identifies unpatched firmware flaws or active default SNMP community strings.

2. Internet Banking Risks and Control

Internet banking services present a unique challenge by exposing a financial institution's core backend ledger systems directly to the public web. This architecture amplifies standard banking risks and introduces sophisticated cyber threat vectors that require automated, multi-tiered defense mechanisms.

A. Core Vulnerabilities and Threat Vectors

1. Phishing & Reverse-Proxy Social Engineering

Attackers deploy look-alike domains, typosquatting (e.g., `bnaokofamerica.com`), and cloned authentication interfaces to trick customers into surrendering credentials. Modern attack setups use reverse-proxy tools to capture active authentication cookies in real-time, allowing them to bypass traditional multi-factor authentication checkpoints.

2. Credential Stuffing & Automated Brute-Force Attacks

Attackers use automated botnets to rapidly test large credential pairs obtained from third-party data breaches. Because many users reuse passwords across different platforms, these automated stuffing attacks allow adversaries to compromise customer accounts without needing to breach the bank's core infrastructure directly.

3. Man-in-the-Middle (MitM) & Session Hijacking

Adversaries intercept the active data stream between a customer's browser or mobile device and the banking web server. This typically occurs over compromised public Wi-Fi access points or via malicious browser extensions on the client machine. Once authenticated, the attacker steals the active session cookie to take control of the account.

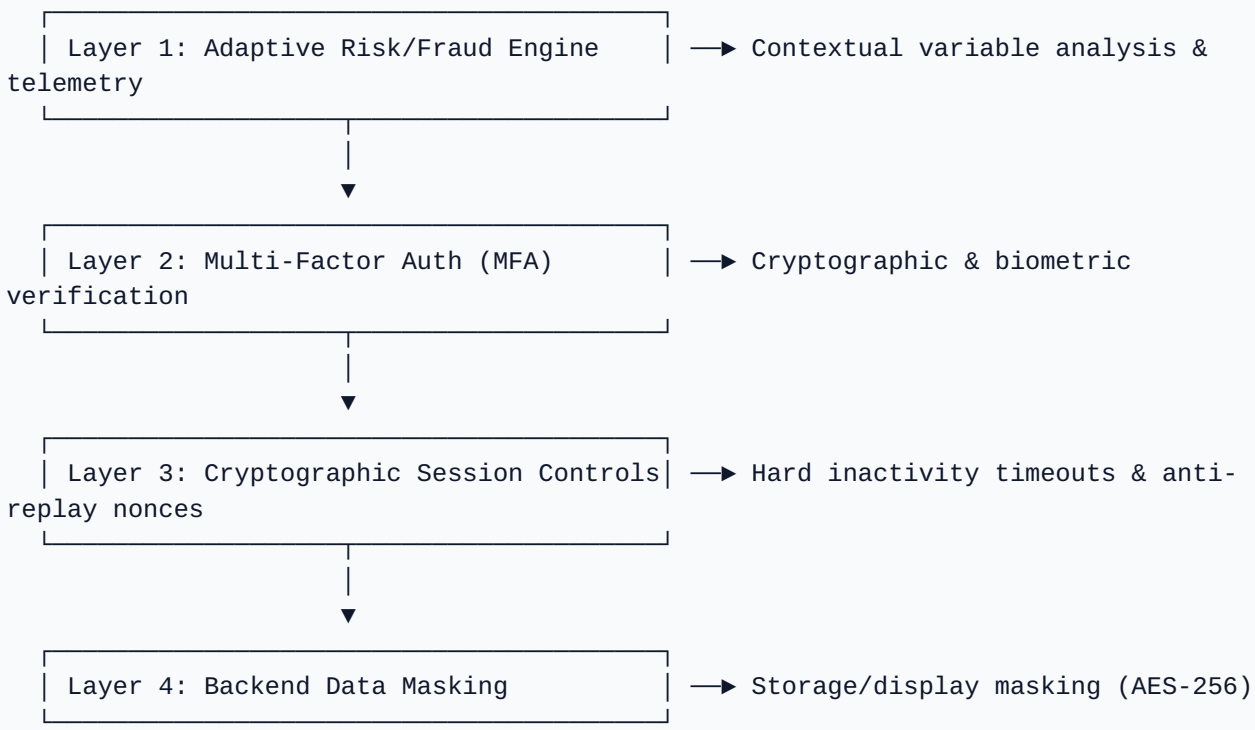
4. API Security Exploits (OWASP API Top 10)

Modern mobile and web banking applications rely heavily on APIs (Application Programming Interfaces). Attackers intercept application traffic to uncover flaws like **Broken Object Level Authorization (BOLA)**. For example, an attacker logs into their own account, intercepts the outbound API call, and modifies the account identification string from their own to a victim's (e.g., changing `account_id=20045` to `account_id=20046`) to verify if the backend server improperly discloses the victim's account data.

B. Security Control Frameworks for Internet Banking

To mitigate these public-facing vectors, banks implement an integrated **Defense-in-Depth** model across their web infrastructure.

FIGURE 2.1: LAYERED DEFENSE-IN-DEPTH MODEL FOR INTERNET BANKING



1. Advanced Multi-Factor Authentication (MFA) Architecture

Banks enforce multi-factor verification across all public digital interfaces, requiring users to supply credentials across distinct validation factors:

- **Something You Know:** Standard secret variables like passwords, PINs, or alphanumeric challenge phrases.
- **Something You Have:** Physical assets including hardware tokens, cryptographic smart cards, or authenticator applications.
- **Something You Are:** Unique anatomical biomarkers such as fingerprint data, facial geometry, or iris scans.
- *Auditor Evaluation Note:* Traditional SMS-based One-Time Passwords (OTPs) are increasingly flagged as high-risk due to **SIM-swapping** attacks and network interception. Auditors check if banks are transitioning toward secure alternatives, such as Time-Based One-Time Passwords (TOTP), FIDO2/WebAuthn cryptographic keys, or encrypted push notifications.

2. Adaptive and Behavioral Fraud Detection Engines

Advanced security layers evaluate contextual variables during the authentication phase to detect anomalies:

- **Geographic Velocity Anomalies:** Flagging logins if an authentication event occurs from London and a subsequent request initiates from Tokyo 20 minutes later (an impossible travel speed).
- **Device Fingerprinting Telemetry:** Verifying system indicators, including browser type, installed font packs, active operating system versions, MAC addresses, and default language profiles.
- **Behavioral Biometrics:** Profiling interaction mechanics, including typing speed, mouse pointer movement fluidity, and touchscreen compression metrics. If an automated bot or a third-party attacker takes over an account, their behavior deviates from the user's historical baseline, triggering step-up authentication or an account lock.

3. Strict Session Management Controls

- **Inactivity Timeouts:** Active web sessions must terminate automatically after a brief period of user inactivity (typically 5 to 10 minutes) to mitigate risks associated with unattended client devices.
- **Post-Login ID Regeneration:** Session identifiers must provide high entropy and change immediately upon user authentication to neutralize session fixation threats.
- **Anti-Replay / Nonce Controls:** Transaction pipelines must embed single-use cryptographic nonces to prevent adversaries from capturing a valid fund transfer request and replaying it to duplicate the transaction.

4. Server-Side Data Masking and Storage Controls

- **Display Masking:** Sensitive data fields must be masked on screen (e.g., primary credit card account numbers must display as `XXXX-XXXX-XXXX-4321`).
- **Backend Isolation:** Sensitive authentication data, such as card CVVs or plain-text PIN codes, must never be stored in backend files following transaction completion. Databases protect data at rest using high-grade encryption standards like AES-256.

3. Operating System (OS) Risks and Control

The operating system represents the foundational software layer that coordinates hardware resources and hosts system applications. A compromise at the operating system level undermines security controls implemented at higher application layers.

A. Critical OS Security Risks

1. Unpatched Kernel Flaws & Local Privilege Escalation (LPE)

Operating system kernels may contain structural code vulnerabilities. Attackers exploit these flaws via Local Privilege Escalation attacks, which allow an account with restricted, low-privilege system access to bypass security boundaries and gain full root, SYSTEM, or kernel-level administrative authority.

2. Insecure Directory Permissions & Weak Access Control Lists (ACLs)

Improperly configured file system permissions can allow standard users or unauthorized local processes to read, modify, or overwrite critical system configuration files. These files include system binaries, local environment variables, system logs, or cryptographic password hashes (such as `/etc/shadow` in Linux environments or the SAM registry database in Windows environments).

3. Proliferation of Non-Essential Services & Default Port Configurations

Operating systems are often deployed out-of-the-box with various default services, pre-installed testing utilities, and guest account profiles active. Leaving unneeded services running (such as print spoolers, unencrypted Telnet servers, legacy FTP daemons, or remote registry services) expands the system's attack surface by providing more potential entry points for attackers.

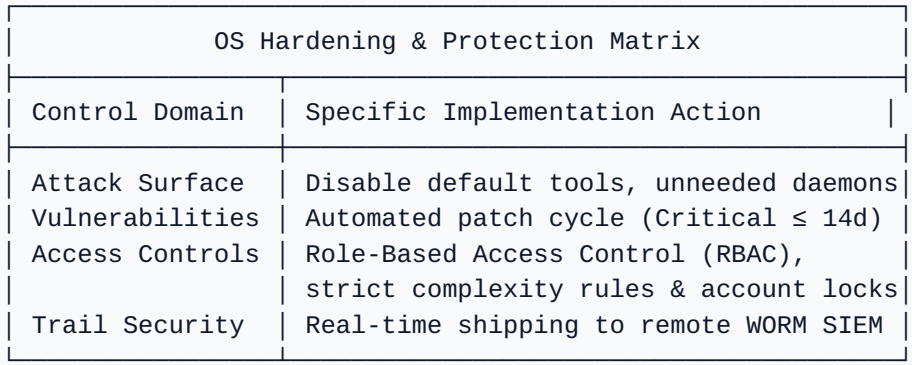
4. Vulnerable Audit Trail Architectures & Log Tampering

If security logs are stored locally without strict access controls, any user who gains administrative access can modify or clear those files. This allows a rogue insider or external attacker to delete evidence of their activities, leaving the organization without a reliable audit trail for forensic investigations.

B. Key OS Control Implementations

Auditors evaluate system configurations against standardized security baselines, such as the **Center for Internet Security (CIS) Benchmarks** or the Defense Information Systems Agency (DISA) STIGs.

FIGURE 3.1: OPERATING SYSTEM SECURITY & HARDENING ARCHITECTURE



1. Rigorous OS Hardening Procedures

OS hardening involves systematically reconfiguring default system deployments to eliminate known security liabilities:

- Disabling all non-essential background processes and application servers.
- Uninstalling default compilers, system tools, and testing utilities from production environments.
- Disabling interactive root or administrative log-ins, requiring administrators to log in using standard accounts first and elevate privileges via auditable commands like `sudo` or `RunAs`.
- Closing unused logical communication ports at the local host level via built-in firewalls (e.g., `iptables` or Windows Defender Firewall).

2. Enterprise Patch Management Lifecycle

Organizations must maintain a structured, documented framework to discover, evaluate, test, and deploy security updates across their entire server farm.

- **Staging Deployments:** Security updates must be deployed and validated within controlled staging environments first to ensure system stability before rolling them out to production assets.
- **Velocity Metrics:** Auditors review patch deployment history logs to measure the elapsed time between a critical flaw's release and its actual remediation. For critical, highly exploitable flaws (***CVSS*** ***≥ 9.0***), patches must be successfully applied within a mandatory operational window (e.g., 7 to 14 days).

3. Identity & Access Management (IAM) and Account Governance

- **Complexity and Lockout Rules:** Operating systems must enforce specific password complexity rules (e.g., minimum 14 characters, blending uppercase, lowercase, numbers, and special characters). Account lockout policies must be enabled to counter automated brute-force attempts (e.g., locking an account for 30 minutes after 5 consecutive failed authentication attempts).
- **Role-Based Access Control (RBAC):** Access permissions are tied directly to specific job functions rather than individual users. Administrators are assigned precise roles (e.g., Backup Operator, Log Viewer, System Configurator) to enforce the principle of least privilege.

4. Centralized, Remote Audit Logging Structures

Local operating system event logs must record security-relevant events, including successful and failed login attempts, privilege escalations, account creations, configuration changes, and file integrity violations. To protect these logs from tampering, local operating systems must use real-time log-shipping agents to stream event data to a centralized, remote SIEM platform stored on write-once, read-many (WORM) storage architecture.

4. Operational Control Overview

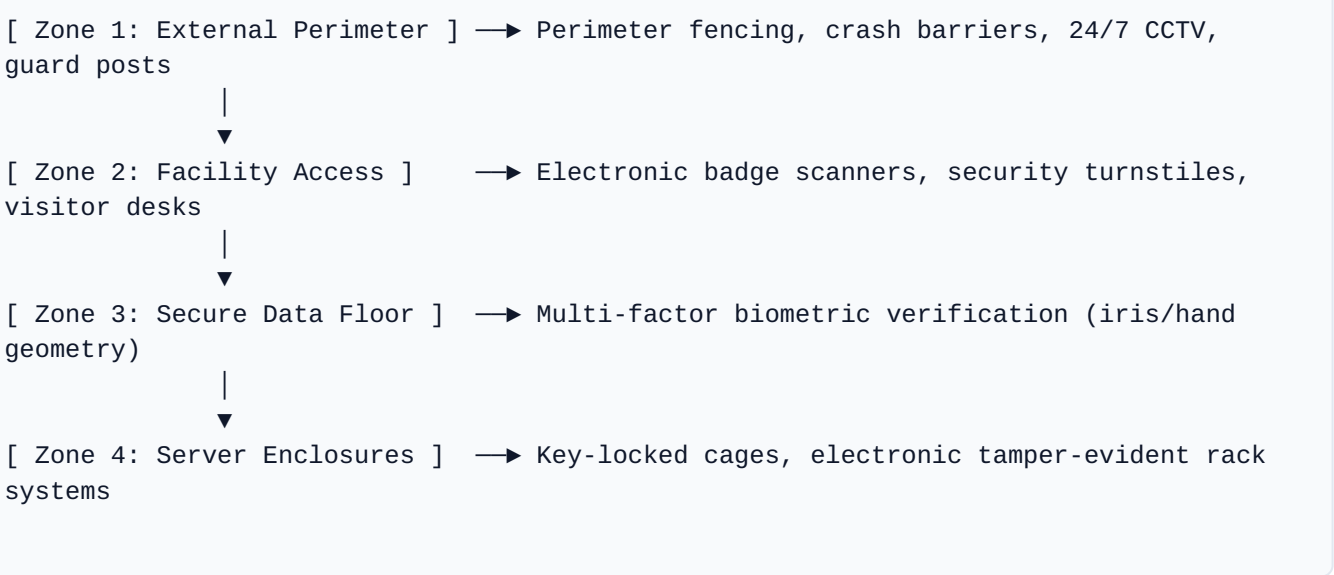
Operational controls encompass the day-to-day administrative, physical, and human resource processes designed to safeguard an organization's IT assets, manage operational risk, and ensure business continuity.

A. Data Center Physical and Environmental Security

Technical logical security controls can be undermined if an attacker gains physical access to hardware infrastructure, enabling them to bypass software restrictions, steal physical hard drives, or disrupt operations.

1. Concentric Physical Security Zones

FIGURE 4.1: TIERED SECURITY PERIMETERS IN ENTERPRISE DATA CENTERS



2. Advanced Environmental Infrastructure Controls

- **Climate Regulation:** Automated HVAC (Heating, Ventilation, and Air Conditioning) systems must maintain stable temperature and humidity levels inside server rooms to prevent equipment overheating or electrostatic damage.
- **Fire Detection and Suppression:** Facilities utilize automated aspirating smoke detection systems (such as VESDA) for early fire detection. Rather than traditional water sprinklers, which destroy computing hardware, data centers deploy clean-agent gaseous suppression systems (such as FM-200, Novec 1230, or Inergen) to extinguish fires by removing heat or oxygen without damaging electrical equipment.

3. Power Redundancy Systems

To protect against primary utility grid failures, data centers implement multi-tiered power backup architectures:

- **Uninterruptible Power Supplies (UPS):** Large battery banks that provide immediate power to server racks during an outage, maintaining system stability while backup generators initialize. They also act as power conditioners to neutralize voltage spikes or sags.
- **Secondary Diesel Generators:** On-site generators configured to start automatically within seconds of a utility outage. Organizations maintain service contracts with local fuel vendors to guarantee continuous fuel replenishment during extended disruptions.

B. IT Operational Practices and Human Resource Management

1. Formal Change Management Governance

Uncontrolled, unreviewed modifications to production environments are a frequent cause of both security vulnerabilities and unexpected system downtime. Organizations use a structured workflow to govern changes:

RFC Request ──► ***Impact & Security Analysis*** ──► ***Staging Test*** ──► ***CAB Approval*** ──► ***Production Release*** ──► ***Post-Review***

- **Change Advisory Board (CAB):** A cross-functional committee composed of IT managers, security analysts, and business owners that reviews proposed changes for technical stability and business impact before authorizing deployment.
- **Rollback Planning:** Every approved change package must contain a documented, tested rollback plan to restore systems to their last known stable configuration if the production deployment fails.

2. Human Resource Operational Controls

- **Mandatory Consecutive Vacation Policy:** Organizations require employees holding high-privilege technical or financial roles (e.g., database administrators, core system engineers, or treasury operators) to take a minimum of two consecutive weeks of vacation annually. During this vacation window, the employee's active system permissions are completely revoked. This control is designed to detect internal fraud, as long-running malicious schemes often require the continuous presence of the perpetrator to avoid detection.
- **Structured Job Rotation:** Periodically rotating personnel between different technical roles reduces the opportunity for collusion, prevents single points of failure, and helps uncover operational irregularities or hidden control bypasses.

5. Comprehensive Unit-IV Evaluation Matrix for Auditors

Before completing an audit engagement, the lead IS auditor uses this standardized matrix to ensure all technical controls have been systematically tested and verified against acceptable evidence criteria:

Domain Area	Evaluated Control Dimension	Primary Audit Testing Procedure	Acceptable Audit Evidence Artifacts
Network Security	Perimeter Separation	Perform configuration reviews of external and internal firewall tables; verify the presence of a catch-all `Deny All/Any` default rule.	Active firewall configuration tables, network architecture diagrams, rule optimization reports.
Network Security	Data in Transit Protection	Use network scanning utilities to assess exposed web servers and verify the use of strong cipher suites and modern TLS versions.	TLS cipher scan logs, VPN configuration templates, SSL certificate validation data.
Internet Banking	Authentication Controls	Inspect system configuration profiles to confirm multi-factor authentication requirements and evaluate fraud detection triggers.	IAM identity rules, adaptive engine log outputs, authentication workflow schematics.
Internet Banking	Session Integrity	Test web application behaviors to confirm automatic session termination and verify post-login session ID changes.	App source code snippets, HTTP interception logs, timeout configuration parameters.
Operating Systems	Attack Surface Reduction	Run automated security scanners across a sample of production servers to check for unneeded active background services.	Active process lists, host firewall rule configurations, CIS benchmark assessment logs.
Operating Systems	Patch Compliance	Review patch deployment history logs to measure the elapsed time between a critical flaw's release and its actual remediation.	Automated patch management dashboard metrics, staging environment test sign-offs.
Operational Control	Physical & Site Security	Physically tour the data center facility to inspect access points, verify biometric logging, and review environment maintenance history.	Automated biometric badge log exports, fire suppression service logs, generator load test records.
Operational Control	Administrative Governance	Review a sample of historical change tickets to verify staging tests and Change Advisory Board (CAB) approvals.	Signed change authorization forms, CAB meeting minutes, user access revocation records for mandatory vacations.