

Comprehensive Enterprise Security Checklist

Version: 3.0
Last Updated: July 2025
Classification: Public
Owner: Chief Information Security Officer (CISO)
Review Cycle: Quarterly
Next Review: October 2025

Table of Contents

- 1. [Executive Summary](#)
- 2. [Information Security Fundamentals](#)
- 3. [Application Security](#)
- 4. [Infrastructure Security](#)
- 5. [Cloud Security](#)
- 6. [Network Security](#)
- 7. [Data Protection & Privacy](#)
- 8. [Identity & Access Management](#)
- 9. [Incident Response & Management](#)
- 10. [Business Continuity & Disaster Recovery](#)
- 11. [Physical Security](#)
- 12. [Employee Security & Awareness](#)
- 13. [Third-Party & Supply Chain Security](#)
- 14. [Compliance & Regulatory Requirements](#)
- 15. [Security Architecture & Design](#)
- 16. [DevSecOps & Secure Development](#)
- 17. [AI/ML Security](#)
- 18. [Mobile Security](#)
- 19. [IoT & OT Security](#)
- 20. [Endpoint Security](#)
- 21. [Email Security](#)
- 22. [Web Security](#)
- 23. [Database Security](#)
- 24. [API Security](#)

- 25. [Container & Kubernetes Security](#)
- 26. [Vulnerability Management](#)
- 27. [Security Monitoring & SIEM](#)
- 28. [Forensics & Investigation](#)
- 29. [Security Metrics & KPIs](#)
- 30. [Security Tools & Technologies](#)

1. Executive Summary {#executive-summary}

This comprehensive security checklist serves as the definitive guide for implementing, maintaining, and auditing enterprise security controls across all domains. It encompasses technical, administrative, and physical security measures designed to protect organizational assets, data, and operations from evolving cyber threats.

Purpose and Scope

This checklist provides:

- **Comprehensive Coverage:** Over 2,500 security controls across 30 domains
- **Risk-Based Approach:** Prioritized controls based on threat landscape
- **Compliance Alignment:** Mapped to major frameworks (ISO 27001, NIST, SOC 2, etc.)
- **Actionable Guidance:** Clear implementation steps for each control
- **Measurable Outcomes:** KPIs and metrics for security effectiveness

How to Use This Checklist

1. **Initial Assessment:** Use as a baseline for security maturity evaluation
2. **Implementation Guide:** Follow detailed steps for control deployment
3. **Audit Tool:** Verify security posture against industry standards
4. **Continuous Improvement:** Regular reviews and updates based on threats

Risk Rating System

Each control is rated based on:

- **Critical (C):** Immediate implementation required
 - **High (H):** Implementation within 30 days
 - **Medium (M):** Implementation within 90 days
 - **Low (L):** Implementation within 180 days
-

2. Information Security Fundamentals {#information-security-fundamentals}

2.1 Information Security Policy Framework

Policy Development and Management

Critical Controls:

- ☐ [C] Establish comprehensive Information Security Policy
 - **Implementation:** Create policy covering all security domains
 - **Review Cycle:** Annual or upon significant changes
 - **Approval:** Board and executive level sign-off required
 - **Distribution:** All employees, contractors, third parties
- ☐ [C] Define Information Classification Policy
 - **Categories:** Public, Internal, Confidential, Restricted
 - **Handling Requirements:** Storage, transmission, disposal
 - **Labeling Standards:** Physical and digital assets
 - **Access Controls:** Based on classification level
- ☐ [H] Implement Acceptable Use Policy
 - **Coverage:** IT resources, internet, email, social media
 - **Restrictions:** Prohibited activities and content
 - **Monitoring:** User activity logging and review
 - **Consequences:** Violation penalties defined

High Priority Controls:

- ☐ [H] Security Awareness and Training Policy
 - **Frequency:** Initial onboarding plus annual refresh
 - **Content:** Current threats, policies, procedures
 - **Testing:** Phishing simulations, knowledge assessments
 - **Tracking:** Completion rates and effectiveness metrics
- ☐ [H] Data Retention and Disposal Policy
 - **Retention Schedules:** By data type and regulatory requirements
 - **Disposal Methods:** Secure deletion, shredding standards
 - **Certificate of Destruction:** For sensitive data
 - **Legal Hold Procedures:** Preservation requirements

Medium Priority Controls:

- ☐ [M] Remote Work Security Policy

- **Device Requirements:** Encryption, patching, antivirus
- **Network Security:** VPN usage, WiFi standards
- **Physical Security:** Clean desk, device storage
- **Data Handling:** Local storage restrictions
- ☐ **[M] Bring Your Own Device (BYOD) Policy**
 - **Allowed Devices:** Approved types and models
 - **Security Requirements:** MDM enrollment, compliance
 - **Data Separation:** Corporate vs. personal data
 - **Exit Procedures:** Data removal upon termination

2.2 Risk Management Framework

Risk Assessment and Treatment

Critical Controls:

- ☐ **[C] Conduct Annual Enterprise Risk Assessment**
 - **Methodology:** Quantitative and qualitative analysis
 - **Asset Inventory:** Complete catalog of information assets
 - **Threat Modeling:** Current and emerging threats
 - **Vulnerability Assessment:** Technical and process gaps
 - **Risk Register:** Documented risks with treatments
- ☐ **[C] Implement Risk Treatment Plans**
 - **Risk Acceptance:** Documented approval for retained risks
 - **Risk Mitigation:** Control implementation timelines
 - **Risk Transfer:** Insurance and contractual measures
 - **Risk Avoidance:** Process or technology changes

Implementation Guidelines:

1. Asset Identification and Valuation

- Hardware inventory with criticality ratings
- Software and application catalog
- Data classification and ownership
- Business process dependencies
- Third-party service inventory

2. Threat and Vulnerability Analysis

- External threat intelligence feeds

- Internal vulnerability scanning results
- Penetration testing findings
- Security incident history
- Industry-specific threats

3. Risk Calculation and Prioritization

Risk Score = (Threat Likelihood × Vulnerability) × Asset Value × Impact

- Likelihood Scale: 1-5 (Rare to Almost Certain)
- Impact Scale: 1-5 (Negligible to Catastrophic)
- Risk Matrix: 5×5 grid for visualization
- Treatment Priority: Based on risk score

2.3 Security Governance Structure

Organizational Security Roles

Critical Controls:

- ☐ **[C]** Appoint Chief Information Security Officer (CISO)
 - **Reporting Line:** Direct to CEO or Board
 - **Authority:** Policy enforcement and incident response
 - **Budget:** Dedicated security budget allocation
 - **Team Structure:** Adequate staffing for coverage
- ☐ **[C]** Establish Security Steering Committee
 - **Membership:** Executive stakeholders
 - **Meeting Frequency:** Monthly minimum
 - **Responsibilities:** Strategy, budget, risk decisions
 - **Documentation:** Minutes and action tracking

Role-Based Security Responsibilities:

Role	Primary Responsibilities	Accountability
CISO	Strategy, Policy, Compliance	Board/CEO
Security Architects	Design, Standards, Reviews	CISO
Security Engineers	Implementation, Operations	Security Manager
Security Analysts	Monitoring, Incident Response	SOC Manager
Compliance Officers	Audits, Regulatory Requirements	CISO/Legal
Risk Managers	Assessment, Treatment, Reporting	CISO/CRO

2.4 Security Metrics and Reporting

Key Performance Indicators (KPIs)

Critical Metrics:

- ☐ **[C]** Mean Time to Detect (MTTD)
 - **Target:** < 24 hours for critical incidents
 - **Measurement:** From breach to detection
 - **Improvement:** Enhance monitoring and analytics
- ☐ **[C]** Mean Time to Respond (MTTR)
 - **Target:** < 4 hours for critical incidents
 - **Measurement:** From detection to containment
 - **Improvement:** Automate response procedures
- ☐ **[H]** Security Training Completion Rate
 - **Target:** 95% within 30 days
 - **Measurement:** Employees completing required training
 - **Enforcement:** Access restrictions for non-compliance

Dashboard Requirements:

- Real-time security posture visualization
 - Trend analysis for key metrics
 - Comparative benchmarking data
 - Risk heat maps by business unit
 - Compliance status tracking
-

3. Application Security {#application-security}

3.1 Secure Software Development Lifecycle (SSDLC)

Development Security Requirements

Critical Controls:

- ☐ **[C]** Implement Security Requirements in SDLC
 - **Phase Integration:** Security at each development phase
 - **Requirements Gathering:** Security user stories
 - **Threat Modeling:** STRIDE/PASTA methodology
 - **Security Champions:** Embedded in dev teams
- ☐ **[C]** Secure Coding Standards

- **Language-Specific:** Guidelines for all used languages
- **OWASP Top 10:** Address current vulnerabilities
- **Code Examples:** Secure vs. insecure patterns
- **Tool Integration:** IDE security plugins

Secure Development Phases:

1. Planning Phase Security

- ☐ Security requirements documentation
- ☐ Risk assessment for new features
- ☐ Compliance requirements mapping
- ☐ Security budget allocation

2. Design Phase Security

- ☐ Architecture security review
- ☐ Threat modeling sessions
- ☐ Security design patterns selection
- ☐ Data flow diagram analysis

3. Development Phase Security

- ☐ Secure coding training completion
- ☐ Peer code review process
- ☐ Static code analysis (SAST)
- ☐ Dependency vulnerability checking

4. Testing Phase Security

- ☐ Dynamic security testing (DAST)
- ☐ Interactive security testing (IAST)
- ☐ Penetration testing
- ☐ Security test case execution

5. Deployment Phase Security

- ☐ Security configuration review
- ☐ Production hardening checklist
- ☐ Security monitoring setup
- ☐ Incident response plan update

3.2 Application Security Testing

Comprehensive Testing Program

Critical Controls:

- ☐ **[C]** Static Application Security Testing (SAST)
 - **Coverage:** 100% of custom code

- **Frequency:** Every code commit
 - **Tools:** Commercial and open source
 - **Remediation:** Critical findings before release
- ☐ **[C]** Dynamic Application Security Testing (DAST)
- **Coverage:** All external-facing applications
 - **Frequency:** Weekly for production
 - **Authentication:** Test authenticated functions
 - **API Testing:** REST, SOAP, GraphQL endpoints

Testing Methodology Matrix:

Test Type	When	Coverage	Tools	Success Criteria
SAST	Each commit	100% code	SonarQube, Checkmarx	Zero critical
DAST	Weekly	All apps	OWASP ZAP, Burp	Zero high findings
IAST	Runtime	Critical apps	Contrast, Seeker	Real-time alerts
SCA	Build time	All dependencies	Snyk, WhiteSource	No critical CVEs
Pen Test	Quarterly	High-risk apps	Internal/External	Passed assessment

3.3 API Security

API Protection Framework

Critical Controls:

- ☐ **[C]** API Authentication and Authorization
- **Standards:** OAuth 2.0, OpenID Connect
 - **Token Management:** Rotation, expiration
 - **Scope Definition:** Least privilege access
 - **Multi-factor:** For sensitive operations
- ☐ **[C]** API Rate Limiting and Throttling
- **Limits:** By user, IP, endpoint
 - **DDoS Protection:** Adaptive rate limiting
 - **Monitoring:** Unusual patterns detection
 - **Response:** Graduated blocking

API Security Checklist:

- ☐ Input validation on all parameters
- ☐ Output encoding for all responses
- ☐ Encryption in transit (TLS 1.3)

- ☐ Request/response signing
- ☐ API versioning strategy
- ☐ Deprecation procedures
- ☐ Security headers implementation
- ☐ CORS policy configuration
- ☐ API gateway deployment
- ☐ Centralized logging

3.4 Web Application Security

OWASP Top 10 Mitigation

Critical Controls for Each OWASP Risk:

1. Injection Prevention

- ☐ Parameterized queries mandatory
- ☐ Input validation whitelist approach
- ☐ Stored procedure usage
- ☐ ORM framework security features

2. Broken Authentication

- ☐ Multi-factor authentication
- ☐ Account lockout mechanisms
- ☐ Session management controls
- ☐ Password complexity requirements

3. Sensitive Data Exposure

- ☐ Encryption at rest and in transit
- ☐ Data classification implementation
- ☐ Key management procedures
- ☐ Secure data disposal

4. XML External Entities (XXE)

- ☐ XML parser hardening
- ☐ DTD processing disabled
- ☐ XML upload restrictions
- ☐ Input validation for XML

5. Broken Access Control

- ☐ Role-based access control (RBAC)
- ☐ Principle of least privilege
- ☐ Access control testing
- ☐ Privilege escalation prevention

6. Security Misconfiguration

- ☐ Hardening guidelines followed
- ☐ Default credentials changed
- ☐ Unnecessary features disabled
- ☐ Security headers configured

7. Cross-Site Scripting (XSS)

- ☐ Context-aware output encoding
- ☐ Content Security Policy (CSP)
- ☐ Input validation and sanitization
- ☐ Template engine security

8. Insecure Deserialization

- ☐ Deserialization restrictions
- ☐ Type checking implementation
- ☐ Integrity checks required
- ☐ Isolation of deserialization

9. Using Components with Known Vulnerabilities

- ☐ Software composition analysis
- ☐ Dependency update process
- ☐ Vulnerability monitoring
- ☐ License compliance checks

10. Insufficient Logging & Monitoring

- ☐ Comprehensive audit logging
- ☐ Log integrity protection
- ☐ Real-time alerting
- ☐ Log retention policies

4. Infrastructure Security {#infrastructure-security}

4.1 Server Security

Operating System Hardening

Critical Controls:

- ☐ **[C]** Implement OS Hardening Standards
 - **Baseline:** CIS Benchmarks compliance
 - **Automation:** Configuration management tools
 - **Validation:** Regular compliance scanning
 - **Documentation:** Exceptions and compensating controls
- ☐ **[C]** Patch Management Program

- **SLA:** Critical patches within 24 hours
- **Testing:** Patch validation environment
- **Scheduling:** Maintenance windows defined
- **Rollback:** Procedures documented and tested

Platform-Specific Hardening:

Windows Server Hardening Checklist:

- ☐ Remove unnecessary roles and features
- ☐ Configure Windows Firewall with Advanced Security
- ☐ Enable and configure BitLocker
- ☐ Implement AppLocker policies
- ☐ Configure audit policies
- ☐ Disable unnecessary services
- ☐ Configure User Account Control (UAC)
- ☐ Implement Local Security Policy
- ☐ Enable Windows Defender
- ☐ Configure automatic updates

Linux Server Hardening Checklist:

- ☐ Minimize installed packages
- ☐ Configure iptables/firewalld
- ☐ Enable SELinux/AppArmor
- ☐ Implement file integrity monitoring
- ☐ Configure auditd rules
- ☐ Disable unnecessary services
- ☐ Implement access controls (sudo)
- ☐ Configure syslog forwarding
- ☐ Enable automatic security updates
- ☐ Implement kernel hardening (sysctl)

4.2 Virtualization Security

Hypervisor Protection

Critical Controls:

- ☐ **[C]** Hypervisor Hardening
 - **Access Control:** Role-based administration
 - **Network Isolation:** Management network separation
 - **Resource Limits:** Prevent resource exhaustion

- **Monitoring:** Performance and security events
- ☐ **[C]** Virtual Machine Security
 - **Templates:** Hardened base images
 - **Sprawl Prevention:** Lifecycle management
 - **Snapshot Control:** Retention and access policies
 - **Migration Security:** Encrypted vMotion

VMware vSphere Security Checklist:

- ☐ Enable lockdown mode
- ☐ Configure host firewall rules
- ☐ Implement vCenter SSO policies
- ☐ Enable VM encryption
- ☐ Configure distributed switch security
- ☐ Implement resource pools
- ☐ Enable vSphere Trust Authority
- ☐ Configure syslog forwarding
- ☐ Implement backup encryption
- ☐ Regular security patching

4.3 Storage Security

Data Storage Protection

Critical Controls:

- ☐ **[C]** Storage Encryption Implementation
 - **At Rest:** Full disk encryption mandatory
 - **In Transit:** Encrypted protocols only
 - **Key Management:** HSM or key management service
 - **Performance:** Monitor encryption overhead
- ☐ **[C]** Storage Access Controls
 - **Authentication:** Multi-factor for admin access
 - **Authorization:** Role-based permissions
 - **Audit Logging:** All access tracked
 - **Data Loss Prevention:** Monitoring and alerts

SAN/NAS Security Requirements:

- ☐ Fabric/network isolation
- ☐ Zoning and LUN masking
- ☐ Management interface security

- ☐ Firmware update procedures
- ☐ Replication encryption
- ☐ Snapshot access controls
- ☐ Performance monitoring
- ☐ Capacity planning security
- ☐ Deduplication security
- ☐ Backup integration security

4.4 Database Security

Database Protection Framework

Critical Controls:

- ☐ **[C]** Database Access Control
 - **Authentication:** Strong authentication methods
 - **Authorization:** Principle of least privilege
 - **Segregation:** Development/production separation
 - **Service Accounts:** Unique per application
- ☐ **[C]** Database Encryption
 - **Transparent Encryption:** TDE implementation
 - **Column Encryption:** Sensitive data fields
 - **Connection Encryption:** SSL/TLS required
 - **Key Rotation:** Regular key updates

Database Security Checklist by Platform:

Oracle Database Security:

- ☐ Enable Oracle Database Vault
- ☐ Implement Transparent Data Encryption
- ☐ Configure Oracle Audit Vault
- ☐ Enable Oracle Label Security
- ☐ Implement Virtual Private Database
- ☐ Configure network encryption
- ☐ Enable unified auditing
- ☐ Implement data redaction
- ☐ Configure privilege analysis
- ☐ Regular security patching

Microsoft SQL Server Security:

- ☐ Enable Transparent Data Encryption

- ☐ Configure Always Encrypted
- ☐ Implement Row-Level Security
- ☐ Enable SQL Server Audit
- ☐ Configure Dynamic Data Masking
- ☐ Implement backup encryption
- ☐ Enable SSL/TLS connections
- ☐ Configure firewall rules
- ☐ Implement separation of duties
- ☐ Regular security updates

PostgreSQL Security:

- ☐ Enable SSL/TLS connections
 - ☐ Configure pg_hba.conf properly
 - ☐ Implement Row Level Security
 - ☐ Enable logging and auditing
 - ☐ Configure connection limits
 - ☐ Implement backup encryption
 - ☐ Use SCRAM authentication
 - ☐ Configure role-based access
 - ☐ Enable data checksums
 - ☐ Regular security patches
-

5. Cloud Security {#cloud-security}

5.1 Cloud Security Architecture

Multi-Cloud Security Strategy

Critical Controls:

- ☐ **[C]** Cloud Security Architecture Design
 - **Reference Architecture:** Define standard patterns
 - **Security Zones:** Network segmentation approach
 - **Identity Federation:** Centralized authentication
 - **Data Residency:** Compliance with regulations
- ☐ **[C]** Cloud Service Provider Assessment
 - **Security Certifications:** SOC 2, ISO 27001
 - **Compliance Coverage:** Industry-specific requirements
 - **SLA Review:** Security and availability terms
 - **Incident Response:** Provider procedures

Cloud Security Shared Responsibility Model:

Layer	IaaS	PaaS	SaaS
Data	Customer	Customer	Customer
Applications	Customer	Customer	Provider
Runtime	Customer	Provider	Provider
Middleware	Customer	Provider	Provider
OS	Customer	Provider	Provider
Virtualization	Provider	Provider	Provider
Servers	Provider	Provider	Provider
Storage	Provider	Provider	Provider
Networking	Provider	Provider	Provider

5.2 AWS Security

AWS Security Best Practices

Critical Controls:

- ☐ **[C]** AWS Identity and Access Management (IAM)
 - **MFA Enforcement:** All human users
 - **Service Accounts:** Unique per application
 - **Policy Management:** Least privilege principle
 - **Access Keys:** Regular rotation required
- ☐ **[C]** AWS Network Security
 - **VPC Design:** Segmented architecture
 - **Security Groups:** Restrictive rules
 - **NACLs:** Additional layer of control
 - **PrivateLink:** For service connectivity

AWS Security Checklist:

Account Security:

- ☐ Enable AWS Organizations
- ☐ Implement Service Control Policies
- ☐ Configure AWS CloudTrail
- ☐ Enable AWS Config
- ☐ Implement AWS GuardDuty
- ☐ Configure AWS Security Hub
- ☐ Enable AWS Access Analyzer

- ☐ Implement AWS SSO
- ☐ Configure billing alerts
- ☐ Enable MFA on root account

Compute Security:

- ☐ Use AWS Systems Manager
- ☐ Implement EC2 Instance Connect
- ☐ Configure AWS Inspector
- ☐ Enable EBS encryption by default
- ☐ Implement AWS Secrets Manager
- ☐ Use Parameter Store for config
- ☐ Configure CloudWatch logging
- ☐ Implement backup strategies
- ☐ Use AWS Backup service
- ☐ Configure lifecycle policies

Network Security:

- ☐ Implement AWS WAF
- ☐ Configure AWS Shield
- ☐ Use AWS Network Firewall
- ☐ Implement VPC Flow Logs
- ☐ Configure Route 53 Resolver
- ☐ Use AWS Direct Connect
- ☐ Implement Transit Gateway
- ☐ Configure VPC endpoints
- ☐ Enable DNS query logging
- ☐ Implement network segmentation

5.3 Azure Security

Azure Security Implementation

Critical Controls:

- ☐ **[C]** Azure Active Directory Security
 - **Conditional Access:** Risk-based policies
 - **Privileged Identity Management:** Just-in-time access
 - **Identity Protection:** Risk detection and remediation
 - **B2B/B2C Security:** External identity management
- ☐ **[C]** Azure Network Security
 - **Network Security Groups:** Micro-segmentation

- **Azure Firewall:** Centralized protection
- **DDoS Protection:** Standard tier minimum
- **Private Endpoints:** Service connectivity

Azure Security Checklist:

Identity and Access:

- ☐ Enable Azure AD MFA
- ☐ Configure Conditional Access
- ☐ Implement PIM
- ☐ Enable Identity Protection
- ☐ Configure RBAC
- ☐ Implement JIT VM access
- ☐ Enable Azure AD logs
- ☐ Configure access reviews
- ☐ Implement B2B security
- ☐ Enable password protection

Infrastructure Security:

- ☐ Enable Azure Security Center
- ☐ Configure Azure Sentinel
- ☐ Implement Azure Policy
- ☐ Enable Update Management
- ☐ Configure Key Vault
- ☐ Implement disk encryption
- ☐ Enable backup encryption
- ☐ Configure NSG flow logs
- ☐ Implement Azure Firewall
- ☐ Enable DDoS protection

5.4 Google Cloud Platform (GCP) Security

GCP Security Framework

Critical Controls:

- ☐ **[C]** GCP Identity and Access Management
 - **Organization Policies:** Centralized controls
 - **Service Accounts:** Workload identity
 - **Binary Authorization:** Container security
 - **VPC Service Controls:** API security perimeter

- ☐ **[C]** GCP Data Protection
 - **Cloud KMS:** Key management service
 - **Cloud DLP:** Data loss prevention
 - **Cloud HSM:** Hardware security modules
 - **Secret Manager:** Credential management

GCP Security Checklist:

Account and Access:

- ☐ Configure organization policies
 - ☐ Implement resource hierarchy
 - ☐ Enable Cloud IAM conditions
 - ☐ Configure Workload Identity
 - ☐ Implement VPC Service Controls
 - ☐ Enable Access Transparency
 - ☐ Configure Cloud Audit Logs
 - ☐ Implement Access Context Manager
 - ☐ Enable Security Command Center
 - ☐ Configure Cloud Asset Inventory
-

6. Network Security {#network-security}

6.1 Network Architecture Security

Defense in Depth Network Design

Critical Controls:

- ☐ **[C]** Network Segmentation Implementation
 - **Zone Architecture:** DMZ, internal, restricted
 - **Micro-segmentation:** Application-level isolation
 - **VLAN Design:** Logical separation by function
 - **Air Gap Networks:** Critical infrastructure isolation
- ☐ **[C]** Network Access Control (NAC)
 - **802.1X Implementation:** Certificate-based authentication
 - **Guest Network:** Isolated access for visitors
 - **BYOD Segmentation:** Separate device networks
 - **Posture Assessment:** Health checks before access

Network Security Zones:

Internet

|

[External Firewall]

|

DMZ Zone

|-- Web Servers

|-- Email Gateway

|-- Reverse Proxy

|

[Internal Firewall]

|

Internal Zone

|-- Application Servers

|-- Database Servers

|-- File Servers

|

[Core Firewall]

|

Restricted Zone

|-- Domain Controllers

|-- PKI Infrastructure

|-- Backup Systems

6.2 Firewall Management

Enterprise Firewall Strategy

Critical Controls:

- ☐ **[C]** Firewall Rule Management
 - **Rule Review:** Quarterly audit minimum
 - **Change Control:** Approval process required
 - **Least Privilege:** Minimal required access
 - **Documentation:** Business justification required
- ☐ **[C]** Next-Generation Firewall Features
 - **IPS/IDS:** Intrusion prevention enabled
 - **Application Control:** Layer 7 filtering
 - **URL Filtering:** Category-based blocking
 - **SSL Inspection:** Decrypt and inspect

Firewall Configuration Standards:

Perimeter Firewall Rules:

- ☐ Default deny all inbound
- ☐ Explicit allow rules only
- ☐ Source IP restrictions
- ☐ Service/port limitations
- ☐ Time-based rules where applicable
- ☐ Geo-blocking implementation
- ☐ Anti-spoofing rules
- ☐ Rate limiting configuration
- ☐ Logging all connections
- ☐ Regular rule cleanup

Internal Firewall Rules:

- ☐ Segment by security zones
- ☐ Restrict lateral movement
- ☐ Application-specific rules
- ☐ Database access control
- ☐ Management network isolation
- ☐ Service account restrictions
- ☐ Backup network separation
- ☐ Development/production isolation
- ☐ Jump host requirements
- ☐ Privileged access paths

6.3 Network Monitoring and Detection

Network Threat Detection

Critical Controls:

- ☐ **[C]** Network Traffic Analysis
 - **Full Packet Capture:** 30-day retention minimum
 - **NetFlow Analysis:** Behavioral monitoring
 - **DNS Monitoring:** Query analysis and blocking
 - **SSL/TLS Inspection:** Encrypted traffic visibility
- ☐ **[C]** Intrusion Detection/Prevention
 - **Signature Updates:** Daily minimum
 - **Custom Rules:** Organization-specific threats
 - **Tuning Process:** False positive reduction
 - **Correlation Rules:** Multi-event detection

Network Monitoring Architecture:

Component	Function	Data Retention	Alert Priority
IDS/IPS	Threat detection	90 days	High/Critical
NetFlow	Traffic analysis	180 days	Medium/High
Packet Capture	Forensics	30 days	On-demand
DNS Logs	Query monitoring	365 days	Medium/High
Firewall Logs	Access tracking	365 days	All levels
Web Proxy	Content filtering	90 days	Medium/High

6.4 Wireless Security

Enterprise WiFi Security

Critical Controls:

- ☐ **[C]** Wireless Authentication and Encryption
 - **WPA3 Enterprise:** Minimum standard
 - **802.1X/EAP:** Certificate-based authentication
 - **RADIUS Integration:** Centralized authentication
 - **Guest Isolation:** Separate VLAN required
- ☐ **[C]** Wireless Intrusion Detection
 - **Rogue AP Detection:** Continuous monitoring
 - **Evil Twin Detection:** SSID monitoring
 - **Client Monitoring:** Unauthorized devices
 - **Spectrum Analysis:** Interference detection

Wireless Security Checklist:

Infrastructure Security:

- ☐ Hidden SSID for corporate network
- ☐ Strong pre-shared keys (if used)
- ☐ MAC address filtering (defense in depth)
- ☐ Disable WPS
- ☐ Regular firmware updates
- ☐ Physical security of APs
- ☐ Power level optimization
- ☐ Channel optimization
- ☐ Band steering configuration
- ☐ Load balancing setup

Client Security:

- ☐ Certificate deployment
 - ☐ Supplicant configuration
 - ☐ Profile deployment (GPO/MDM)
 - ☐ BYOD onboarding portal
 - ☐ Network access control
 - ☐ Posture assessment
 - ☐ Remediation network
 - ☐ Client isolation
 - ☐ Time-based access
 - ☐ Location-based controls
-

7. Data Protection & Privacy {#data-protection-privacy}

7.1 Data Classification and Handling

Enterprise Data Governance

Critical Controls:

- ☐ **[C]** Data Classification Framework
 - **Classification Levels:** Public, Internal, Confidential, Restricted
 - **Automated Classification:** DLP integration
 - **Manual Classification:** User training and tools
 - **Metadata Tagging:** Searchable attributes
- ☐ **[C]** Data Handling Procedures
 - **Storage Requirements:** By classification level
 - **Transmission Standards:** Encryption requirements
 - **Access Controls:** Role-based permissions
 - **Retention Policies:** Legal and business requirements

Data Classification Matrix:

Classification	Description	Storage	Transmission	Access	Examples
Restricted	Severe impact if disclosed	Encrypted, HSM	Encrypted, secured channel	Need-to-know only	PII, PHI, PCI
Confidential	Significant impact	Encrypted	Encrypted	Authorized users	Financial, IP
Internal	Limited impact	Access controlled	Internal only	Employees	Policies, procedures
Public	No impact	Standard	Any method	Anyone	Marketing materials

7.2 Data Loss Prevention (DLP)

Comprehensive DLP Program

Critical Controls:

- ☐ **[C]** DLP Policy Implementation
 - **Content Inspection:** Deep packet inspection
 - **Context Analysis:** User, location, time
 - **Channel Coverage:** Email, web, endpoint
 - **Response Actions:** Block, alert, encrypt
- ☐ **[C]** DLP Rule Development
 - **Regulatory Rules:** PCI, HIPAA, GDPR
 - **Custom Rules:** Organization-specific data
 - **Testing Process:** Validate before enforcement
 - **Tuning Cycle:** Monthly refinement minimum

DLP Implementation Checklist:

Discovery Phase:

- ☐ Data inventory creation
- ☐ Sensitive data identification
- ☐ Data flow mapping
- ☐ Risk assessment
- ☐ Policy development
- ☐ Stakeholder approval

Deployment Phase:

- ☐ Endpoint agent rollout
- ☐ Network DLP configuration
- ☐ Email gateway integration
- ☐ Cloud app integration
- ☐ Discovery scanning
- ☐ Policy activation

Operational Phase:

- ☐ Incident response procedures
- ☐ False positive handling
- ☐ Policy refinement
- ☐ User awareness training

- ☐ Metrics tracking
- ☐ Executive reporting

7.3 Encryption Management

Enterprise Encryption Strategy

Critical Controls:

- ☐ **[C]** Encryption Standards Definition
 - **Algorithm Requirements:** AES-256 minimum
 - **Key Length Standards:** 2048-bit RSA minimum
 - **Protocol Standards:** TLS 1.3 preferred
 - **Certificate Management:** Centralized PKI
- ☐ **[C]** Key Management System
 - **Key Generation:** Hardware security modules
 - **Key Storage:** Segregated and encrypted
 - **Key Rotation:** Automated schedules
 - **Key Recovery:** Documented procedures

Encryption Requirements by Data State:

Data at Rest Encryption:

- ☐ Full disk encryption (FDE)
- ☐ Database encryption (TDE)
- ☐ File-level encryption
- ☐ Backup encryption
- ☐ Archive encryption
- ☐ Removable media encryption
- ☐ Cloud storage encryption
- ☐ Mobile device encryption
- ☐ Application data encryption
- ☐ Email encryption

Data in Transit Encryption:

- ☐ TLS/SSL for web traffic
- ☐ VPN for remote access
- ☐ Email transport encryption
- ☐ File transfer encryption
- ☐ Database connection encryption
- ☐ API communication encryption

- ☐ Backup replication encryption
- ☐ Inter-site link encryption
- ☐ Wireless encryption
- ☐ Voice/video encryption

7.4 Privacy Compliance

Privacy Regulatory Framework

Critical Controls:

- ☐ **[C]** Privacy Impact Assessments
 - **New Projects:** Mandatory assessment
 - **Data Collection:** Minimization principle
 - **Purpose Limitation:** Defined use cases
 - **Consent Management:** Opt-in mechanisms
- ☐ **[C]** Data Subject Rights Management
 - **Access Requests:** 30-day response SLA
 - **Deletion Rights:** Right to be forgotten
 - **Portability:** Standard format export
 - **Correction Rights:** Update procedures

GDPR Compliance Checklist:

Organizational Measures:

- ☐ Data Protection Officer appointment
- ☐ Privacy by design implementation
- ☐ Data protection impact assessments
- ☐ Records of processing activities
- ☐ Lawful basis documentation
- ☐ Consent management platform
- ☐ Data breach procedures
- ☐ Third-party agreements
- ☐ Cross-border transfer mechanisms
- ☐ Employee training program

Technical Measures:

- ☐ Data minimization controls
- ☐ Purpose limitation enforcement
- ☐ Storage limitation automation
- ☐ Accuracy maintenance procedures

- ☐ Confidentiality controls
- ☐ Integrity protections
- ☐ Availability guarantees
- ☐ Resilience mechanisms
- ☐ Pseudonymization implementation
- ☐ Anonymization capabilities

8. Identity & Access Management {#identity-access-management}

8.1 Identity Governance

Enterprise Identity Framework

Critical Controls:

- ☐ [C] Identity Lifecycle Management
 - **Provisioning:** Automated workflows
 - **Modifications:** Approval processes
 - **De-provisioning:** Immediate termination
 - **Recertification:** Quarterly reviews
- ☐ [C] Privileged Access Management (PAM)
 - **Discovery:** All privileged accounts identified
 - **Vaulting:** Centralized credential storage
 - **Rotation:** Automated password changes
 - **Monitoring:** All privileged activity logged

Identity Governance Processes:

Process	Frequency	Stakeholders	Automation Level	Compliance Requirement
Access Reviews	Quarterly	Managers, Owners	80%	SOX, ISO 27001
Privilege Analysis	Monthly	Security, IT	100%	PCI-DSS, HIPAA
Orphan Account Cleanup	Weekly	IAM Team	100%	All frameworks
Role Mining	Annually	Business, IT	60%	Efficiency goal
Segregation of Duties	Continuous	Compliance	90%	SOX, Basel III

8.2 Authentication Systems

Multi-Factor Authentication Strategy

Critical Controls:

- ☐ [C] MFA Implementation Requirements

- **Coverage:** 100% of remote access
 - **Admin Access:** Mandatory for all
 - **High-Value Apps:** Risk-based enforcement
 - **Methods:** Multiple factors available
- ☐ **[C] Authentication Standards**
- **Password Policy:** Complexity and length
 - **Account Lockout:** Brute force protection
 - **Session Management:** Timeout controls
 - **Token Security:** Encrypted storage

MFA Implementation Matrix:

User Type	Required Factors	Acceptable Methods	Re-authentication
Standard Users	2	SMS, App, Email	8 hours
Remote Users	2	App, Hardware token	4 hours
Administrators	2+	Hardware token, Biometric	2 hours
Privileged Service	2+	Certificate, Hardware	Per action
Third Party	2	App, Hardware token	4 hours

8.3 Authorization Management

Role-Based Access Control (RBAC)

Critical Controls:

- ☐ **[C] Role Definition and Management**
- **Role Catalog:** Comprehensive inventory
 - **Permission Mapping:** Least privilege
 - **Approval Workflow:** Multi-level
 - **Conflict Detection:** SOD validation
- ☐ **[C] Attribute-Based Access Control (ABAC)**
- **Attribute Definition:** User, resource, environment
 - **Policy Engine:** Centralized decisions
 - **Context Awareness:** Dynamic permissions
 - **Audit Trail:** Decision logging

Access Control Implementation:

Role Engineering Process:

1. Business Function Analysis

- ☐ Department structure mapping
- ☐ Job function identification
- ☐ Task analysis completion
- ☐ Access requirements gathering

2. Technical Role Design

- ☐ Permission grouping
- ☐ Inheritance hierarchy
- ☐ Conflict resolution
- ☐ Exception handling

3. Implementation Planning

- ☐ Migration strategy
- ☐ Testing procedures
- ☐ Rollback plans
- ☐ Training materials

4. Operational Management

- ☐ Request workflows
- ☐ Approval chains
- ☐ Review cycles
- ☐ Metrics tracking

8.4 Single Sign-On (SSO)

Enterprise SSO Architecture

Critical Controls:

- ☐ **[C]** SSO Platform Requirements
 - **Protocol Support:** SAML 2.0, OAuth, OIDC
 - **High Availability:** 99.9% uptime SLA
 - **Scalability:** Growth accommodation
 - **Integration:** Legacy app support
- ☐ **[C]** Federation Management
 - **Trust Relationships:** Documented agreements
 - **Certificate Management:** Automated renewal
 - **Metadata Exchange:** Secure channels
 - **Monitoring:** Transaction tracking

SSO Security Checklist:

Infrastructure Security:

- ☐ Redundant authentication servers
- ☐ Load balancing configuration
- ☐ SSL/TLS certificate management
- ☐ Session encryption
- ☐ Token signing certificates
- ☐ Clock synchronization
- ☐ Backup authentication methods
- ☐ Disaster recovery procedures
- ☐ Performance monitoring
- ☐ Capacity planning

Application Integration:

- ☐ SAML assertion validation
 - ☐ OAuth scope definition
 - ☐ OpenID Connect claims
 - ☐ Session timeout sync
 - ☐ Logout propagation
 - ☐ Error handling
 - ☐ Attribute mapping
 - ☐ Authorization callbacks
 - ☐ Deep linking support
 - ☐ Mobile app integration
-

9. Incident Response & Management {#incident-response-management}

9.1 Incident Response Planning

Comprehensive IR Program

Critical Controls:

- ☐ **[C]** Incident Response Plan Development
 - **Scope Definition:** All security incidents
 - **Team Structure:** Roles and responsibilities
 - **Communication Plan:** Internal and external
 - **Legal Considerations:** Evidence preservation
- ☐ **[C]** Incident Classification System
 - **Severity Levels:** P1-P4 definitions
 - **Impact Assessment:** Business-based
 - **Escalation Triggers:** Automated alerts

- **SLA Requirements:** Response times

Incident Severity Classification:

Priority	Description	Response Time	Escalation	Examples
P1 - Critical	Business critical impact	15 minutes	Immediate to CISO	Ransomware, data breach
P2 - High	Significant impact	1 hour	Within 2 hours	System compromise
P3 - Medium	Moderate impact	4 hours	Within 8 hours	Malware infection
P4 - Low	Minimal impact	24 hours	Next business day	Policy violation

9.2 Incident Response Procedures

Structured Response Methodology

Critical Response Phases:

1. Preparation Phase

- ☐ IR plan documentation
- ☐ Team training completion
- ☐ Tool deployment
- ☐ Contact lists updated
- ☐ Playbook development
- ☐ Tabletop exercises
- ☐ Legal counsel engagement
- ☐ PR team coordination
- ☐ Insurance notification procedures
- ☐ Evidence handling training

2. Detection & Analysis Phase

- ☐ Alert validation
- ☐ Indicator collection
- ☐ Timeline construction
- ☐ Scope determination
- ☐ Impact assessment
- ☐ Attribution analysis
- ☐ Evidence preservation
- ☐ Initial containment
- ☐ Stakeholder notification
- ☐ Documentation start

3. Containment Phase

- ☐ Short-term containment

- ☐ System isolation
- ☐ Network segmentation
- ☐ Account disabling
- ☐ Evidence collection
- ☐ Backup verification
- ☐ Long-term containment
- ☐ System rebuilding
- ☐ Patch deployment
- ☐ Configuration hardening

4. Eradication Phase

- ☐ Malware removal
- ☐ Vulnerability patching
- ☐ System hardening
- ☐ Account resets
- ☐ Network cleaning
- ☐ Registry cleaning
- ☐ Log analysis
- ☐ IOC hunting
- ☐ Persistence checks
- ☐ Verification testing

5. Recovery Phase

- ☐ System restoration
- ☐ Service validation
- ☐ Monitoring enhancement
- ☐ User communication
- ☐ Normal operations
- ☐ Performance validation
- ☐ Security validation
- ☐ Business verification
- ☐ Stakeholder updates
- ☐ Insurance claims

6. Lessons Learned Phase

- ☐ Incident review meeting
- ☐ Timeline analysis
- ☐ Response effectiveness
- ☐ Process improvements
- ☐ Tool enhancements

- ☐ Training needs
- ☐ Plan updates
- ☐ Metrics collection
- ☐ Report generation
- ☐ Action items tracking

9.3 Digital Forensics

Forensic Readiness Program

Critical Controls:

- ☐ **[C]** Forensic Capability Development
 - **Tools:** Licensed forensic software
 - **Training:** Certified investigators
 - **Procedures:** Chain of custody
 - **Storage:** Evidence management system
- ☐ **[C]** Evidence Collection Procedures
 - **Live Response:** Memory acquisition
 - **Disk Imaging:** Bit-for-bit copies
 - **Network Captures:** Full packet data
 - **Log Aggregation:** Centralized storage

Digital Forensics Checklist:

Evidence Collection:

- ☐ Volatile data capture
- ☐ Memory dump acquisition
- ☐ Running process list
- ☐ Network connections
- ☐ System information
- ☐ Registry capture
- ☐ Disk imaging
- ☐ File system timeline
- ☐ Log file collection
- ☐ Email preservation

Analysis Procedures:

- ☐ Hash verification
- ☐ Timeline creation
- ☐ Artifact analysis

- ☐ Malware analysis
- ☐ Network reconstruction
- ☐ Data recovery
- ☐ Keyword searching
- ☐ Pattern analysis
- ☐ Correlation analysis
- ☐ Report generation

9.4 Threat Intelligence

Threat Intelligence Program

Critical Controls:

- ☐ **[C]** Intelligence Collection Strategy
 - **Internal Sources:** Logs, alerts, incidents
 - **External Sources:** Feeds, sharing groups
 - **Commercial Sources:** Vendor intelligence
 - **Open Source:** OSINT collection
- ☐ **[C]** Intelligence Processing
 - **Normalization:** Standard formats
 - **Enrichment:** Context addition
 - **Correlation:** Pattern identification
 - **Distribution:** Automated sharing

Threat Intelligence Lifecycle:

Phase	Activities	Tools	Outputs
Planning	Requirements, priorities	Frameworks	Intelligence requirements
Collection	Gather raw data	Feeds, crawlers	Raw intelligence
Processing	Parse, normalize	STIX/TAXII	Structured data
Analysis	Correlate, contextualize	SIEM, TIP	Actionable intelligence
Dissemination	Share, alert	API, email	Alerts, reports
Feedback	Measure effectiveness	Metrics	Improvements

10. Business Continuity & Disaster Recovery {#business-continuity-disaster-recovery}

10.1 Business Continuity Planning

Enterprise Continuity Framework

Critical Controls:

- ☐ [C] Business Impact Analysis (BIA)
 - **Process Identification:** Critical business functions
 - **Dependency Mapping:** System interdependencies
 - **RTO/RPO Definition:** Recovery objectives
 - **Resource Requirements:** People, technology, facilities
- ☐ [C] Continuity Strategy Development
 - **Risk Scenarios:** Threat-based planning
 - **Recovery Strategies:** Multiple options
 - **Resource Allocation:** Budget and personnel
 - **Third-Party Dependencies:** Vendor continuity

BIA Components:

Business Function	Criticality	RTO	RPO	Dependencies	Recovery Strategy
Payment Processing	Critical	1 hr	15 min	Database, Network	Hot standby
Email Services	High	4 hrs	1 hr	Exchange, AD	Warm standby
File Sharing	Medium	8 hrs	4 hrs	Storage, Network	Cold standby
HR Systems	Low	24 hrs	24 hrs	Database, Apps	Backup restore

10.2 Disaster Recovery Planning

DR Strategy Implementation

Critical Controls:

- ☐ [C] DR Site Requirements
 - **Geographic Separation:** 100+ miles minimum
 - **Infrastructure Capacity:** 100% production capability
 - **Network Connectivity:** Redundant links
 - **Security Equivalence:** Same controls as primary
- ☐ [C] Data Replication Strategy
 - **Synchronous Replication:** Critical data
 - **Asynchronous Replication:** Standard data
 - **Backup Strategy:** Offline copies
 - **Testing Frequency:** Monthly minimum

DR Implementation Checklist:

Infrastructure Preparation:

- ☐ Site selection and contracting
- ☐ Power and cooling capacity
- ☐ Network connectivity setup
- ☐ Hardware procurement
- ☐ Software licensing
- ☐ Security controls implementation
- ☐ Access control systems
- ☐ Environmental monitoring
- ☐ Communication systems
- ☐ Documentation repository

Data Protection:

- ☐ Replication technology selection
- ☐ Bandwidth requirements
- ☐ Replication monitoring
- ☐ Backup automation
- ☐ Offsite storage contracts
- ☐ Media rotation schedules
- ☐ Encryption implementation
- ☐ Integrity verification
- ☐ Recovery testing
- ☐ Documentation updates

10.3 Crisis Management

Crisis Response Framework

Critical Controls:

- ☐ **[C] Crisis Management Team**
 - **Leadership Structure:** Clear chain of command
 - **Communication Protocols:** Internal and external
 - **Decision Authority:** Predefined limits
 - **Resource Authority:** Emergency spending
- ☐ **[C] Communication Planning**
 - **Stakeholder Matrix:** Contact information
 - **Message Templates:** Pre-approved content
 - **Media Relations:** Spokesperson designation
 - **Customer Communication:** Multiple channels

Crisis Communication Plan:

Internal Communications:

- ☐ Employee notification system
- ☐ Management escalation tree
- ☐ Department liaison network
- ☐ Status update frequency
- ☐ Information repositories
- ☐ Rumor control procedures
- ☐ Morale management
- ☐ Family notification procedures
- ☐ Union communications
- ☐ Board reporting

External Communications:

- ☐ Customer notification procedures
- ☐ Vendor communication plans
- ☐ Regulatory notifications
- ☐ Media response strategy
- ☐ Social media monitoring
- ☐ Website updates
- ☐ Call center scripts
- ☐ Partner notifications
- ☐ Investor relations
- ☐ Community outreach

10.4 Testing and Maintenance

BC/DR Testing Program

Critical Controls:

- ☐ **[C]** Testing Schedule and Scope
 - **Tabletop Exercises:** Quarterly
 - **Functional Tests:** Semi-annually
 - **Full DR Tests:** Annually
 - **Component Tests:** Monthly
- ☐ **[C]** Test Documentation
 - **Test Plans:** Detailed procedures
 - **Success Criteria:** Measurable objectives
 - **Results Documentation:** Findings and gaps
 - **Improvement Plans:** Corrective actions

Testing Methodology:

Test Type	Frequency	Duration	Participants	Success Criteria
Tabletop	Quarterly	4 hours	Management	Process validation
Walkthrough	Semi-annual	8 hours	Key staff	Procedure clarity
Functional	Semi-annual	24 hours	IT teams	System recovery
Full Scale	Annual	48 hours	All teams	RTO/RPO achievement

11. Physical Security {#physical-security}

11.1 Facility Security

Physical Access Control Systems

Critical Controls:

- ☐ [C] Access Control Infrastructure
 - **Card Reader Systems:** Multi-factor capability
 - **Biometric Controls:** High-security areas
 - **Visitor Management:** Registration and escorts
 - **Access Logs:** 90-day retention minimum
- ☐ [C] Perimeter Security
 - **Fencing:** Anti-climb design
 - **Lighting:** Motion-activated supplements
 - **CCTV Coverage:** No blind spots
 - **Intrusion Detection:** Multiple technologies

Facility Security Zones:

Zone	Access Requirements	Controls	Monitoring
Public	Visitor badge	Reception, cameras	Real-time
General Office	Employee badge	Card readers	Motion detection
Secure Areas	Badge + PIN	Biometrics, mantrap	24/7 surveillance
Data Center	Badge + Biometric	Multiple factors	Continuous

11.2 Data Center Security

Data Center Protection Standards

Critical Controls:

- ☐ [C] Environmental Controls

- **Temperature Monitoring:** Automated alerts
- **Humidity Control:** 40-60% range
- **Water Detection:** Under-floor sensors
- **Fire Suppression:** Gas-based systems
- ☐ **[C] Power Infrastructure**
 - **UPS Systems:** N+1 redundancy
 - **Generator Backup:** 72-hour fuel supply
 - **Power Distribution:** Dual feeds
 - **Surge Protection:** Building-wide

Data Center Security Checklist:

Physical Access:

- ☐ Biometric authentication required
- ☐ Man-trap entry systems
- ☐ Security guard presence
- ☐ Cabinet/cage locking
- ☐ Work authorization verification
- ☐ Tool inventory control
- ☐ Two-person integrity
- ☐ Escort requirements
- ☐ Time-limited access
- ☐ Video surveillance

Environmental Protection:

- ☐ HVAC redundancy (N+1)
- ☐ Temperature monitoring
- ☐ Humidity monitoring
- ☐ Water leak detection
- ☐ Smoke detection (VESDA)
- ☐ Fire suppression (FM-200)
- ☐ Emergency power off (EPO)
- ☐ Static control measures
- ☐ Rodent/pest control
- ☐ Vibration monitoring

11.3 Workplace Security

Office Security Standards

Critical Controls:

- ☐ **[C]** Clean Desk Policy
 - **Requirements:** Lock sensitive materials
 - **Enforcement:** Regular inspections
 - **Screen Locks:** Automatic activation
 - **Disposal:** Secure shredding bins
- ☐ **[C]** Asset Protection
 - **Device Cables:** Laptop locks required
 - **Asset Tracking:** Inventory systems
 - **Removal Authorization:** Approval process
 - **Loss Reporting:** Immediate notification

Office Security Implementation:

Access Control Measures:

- ☐ Badge-activated elevators
- ☐ Floor access restrictions
- ☐ Conference room security
- ☐ Print room controls
- ☐ Server room locks
- ☐ Supply room security
- ☐ Mail room procedures
- ☐ Loading dock controls
- ☐ Parking access
- ☐ After-hours procedures

Asset Security:

- ☐ Equipment inventory
- ☐ Cable lock deployment
- ☐ Portable device encryption
- ☐ Asset tagging system
- ☐ Check-out procedures
- ☐ Visitor device policy
- ☐ Personal device restrictions
- ☐ Media handling procedures
- ☐ Secure disposal bins
- ☐ Lost device procedures

11.4 Security Monitoring

Physical Security Operations Center

Critical Controls:

- ☐ **[C]** 24/7 Monitoring Capability
 - **Staffing:** Trained security personnel
 - **Procedures:** Documented responses
 - **Communication:** Direct law enforcement
 - **Integration:** Cyber-physical correlation
- ☐ **[C]** Surveillance Systems
 - **Camera Coverage:** 100% critical areas
 - **Recording Duration:** 90-day retention
 - **Quality Standards:** Identification capability
 - **Privacy Compliance:** Notice postings

Security Monitoring Components:

Technology Stack:

- ☐ Video management system (VMS)
 - ☐ Access control integration
 - ☐ Intrusion detection integration
 - ☐ Visitor management integration
 - ☐ Incident management system
 - ☐ Mass notification system
 - ☐ Duress alarm system
 - ☐ Environmental monitoring
 - ☐ Analytics platform
 - ☐ Mobile patrol tracking
-

12. Employee Security & Awareness {#employee-security-awareness}

12.1 Security Awareness Training

Comprehensive Training Program

Critical Controls:

- ☐ **[C]** Mandatory Security Training
 - **New Hire Training:** Within first week
 - **Annual Refresher:** All employees
 - **Role-Based Training:** Specialized content

- **Compliance Tracking:** 95% completion required
- ☐ **[C]** Phishing Awareness Program
 - **Simulations:** Monthly testing
 - **Reporting Mechanism:** One-click reporting
 - **Metrics Tracking:** Click rates, reporting rates
 - **Remedial Training:** Automatic assignment

Training Curriculum Matrix:

Audience	Topics	Frequency	Duration	Testing Required
All Employees	Security basics, phishing	Annual	60 min	Yes
IT Staff	Technical security	Quarterly	4 hours	Yes
Developers	Secure coding	Bi-annual	8 hours	Yes
Executives	Risk, compliance	Annual	2 hours	No
Contractors	Policy, access	Initial	30 min	Yes

12.2 Personnel Security

Background Verification Program

Critical Controls:

- ☐ **[C]** Pre-Employment Screening
 - **Criminal Background:** 7-year history
 - **Employment Verification:** Previous employers
 - **Education Verification:** Claimed degrees
 - **Reference Checks:** Professional references
- ☐ **[C]** Ongoing Monitoring
 - **Annual Rechecks:** High-risk positions
 - **Financial Monitoring:** Positions with access
 - **Security Clearance:** Where required
 - **Behavioral Indicators:** Insider threat program

Screening Requirements by Role:

Position Type	Criminal Check	Credit Check	Drug Test	Reference Check	Clearance
Standard Employee	Yes	No	No	Yes	No
Financial Role	Yes	Yes	Yes	Yes	No
IT Administrator	Yes	Yes	Yes	Yes	Possible
Executive	Yes	Yes	Optional	Yes	Possible
Contractor	Yes	No	No	Yes	No

12.3 Security Culture Development

Building Security Awareness Culture

Critical Controls:

- ☐ **[C]** Security Champion Program
 - **Selection Criteria:** Volunteer advocates
 - **Training Program:** Advanced security topics
 - **Recognition System:** Rewards and visibility
 - **Responsibilities:** Department liaison
- ☐ **[C]** Communication Strategy
 - **Regular Updates:** Security newsletters
 - **Awareness Campaigns:** Monthly themes
 - **Success Stories:** Positive reinforcement
 - **Incident Lessons:** Anonymous case studies

Security Culture Initiatives:

Engagement Activities:

- ☐ Security awareness month
- ☐ Lunch and learn sessions
- ☐ Security escape rooms
- ☐ Capture the flag events
- ☐ Bug bounty program
- ☐ Security suggestion box
- ☐ Peer recognition program
- ☐ Department competitions
- ☐ Executive participation
- ☐ Family cybersecurity day

12.4 Insider Threat Program

Insider Risk Management

Critical Controls:

- ☐ [C] Behavioral Monitoring Program
 - **Indicators:** Technical and behavioral
 - **Detection Tools:** UBA/UEBA deployment
 - **Investigation Process:** Fair and consistent
 - **Privacy Balance:** Legal compliance
- ☐ [C] Risk Indicators
 - **Technical Indicators:** Unusual access patterns
 - **Behavioral Indicators:** Concerning behaviors
 - **Life Events:** Financial stress, termination
 - **Correlation Analysis:** Multiple indicators

Insider Threat Detection Matrix:

Indicator Category	Examples	Detection Method	Response
Technical	Large downloads, after-hours access	SIEM, DLP	Investigation
Behavioral	Disgruntlement, policy violations	Manager reports	HR intervention
Financial	Bankruptcy, gambling	Background checks	Counseling
Access	Privilege accumulation	Access reviews	Adjustment

13. Third-Party & Supply Chain Security {#third-party-supply-chain-security}

13.1 Vendor Risk Management

Third-Party Risk Assessment Program

Critical Controls:

- ☐ [C] Vendor Risk Assessment Process
 - **Initial Assessment:** Before contracting
 - **Risk Categorization:** Critical/High/Medium/Low
 - **Due Diligence:** Based on risk level
 - **Contract Requirements:** Security addendum
- ☐ [C] Ongoing Vendor Monitoring
 - **Annual Assessments:** Risk-based frequency
 - **Performance Metrics:** SLA compliance
 - **Incident Tracking:** Vendor-caused events
 - **Financial Health:** Viability monitoring

Vendor Risk Categories:

Category	Criteria	Assessment Depth	Monitoring Frequency
Critical	Access to sensitive data	Full assessment	Quarterly
High	Business critical service	Detailed review	Semi-annual
Medium	Moderate impact	Standard review	Annual
Low	Minimal access/impact	Basic review	Bi-annual

13.2 Supply Chain Security

Software Supply Chain Protection

Critical Controls:

- ☐ [C] Software Composition Analysis
 - **Dependency Scanning:** All applications
 - **License Compliance:** Automated checking
 - **Vulnerability Detection:** Known CVEs
 - **Update Management:** Patch coordination
- ☐ [C] Code Integrity Verification
 - **Code Signing:** Vendor verification
 - **Hash Verification:** Download integrity
 - **Repository Security:** Access controls
 - **Build Pipeline:** Security integration

Supply Chain Security Checklist:

Software Acquisition:

- ☐ Vendor security assessment
- ☐ License verification
- ☐ Source code review rights
- ☐ Vulnerability disclosure SLA
- ☐ Update/patch commitments
- ☐ End-of-life planning
- ☐ Escrow agreements
- ☐ Compliance certifications
- ☐ Insurance requirements
- ☐ Breach notification terms

Hardware Acquisition:

- ☐ Vendor facility audits

- ☐ Component sourcing verification
- ☐ Tamper-evident packaging
- ☐ Firmware verification
- ☐ Hardware attestation
- ☐ Secure delivery requirements
- ☐ Asset tracking integration
- ☐ Disposal/return procedures
- ☐ Warranty terms
- ☐ Support agreements

13.3 Cloud Service Provider Management

Cloud Vendor Governance

Critical Controls:

- ☐ **[C]** Cloud Security Assessment
 - **Certifications:** SOC 2, ISO 27001
 - **Compliance:** Industry requirements
 - **Architecture Review:** Security controls
 - **Data Sovereignty:** Location controls
- ☐ **[C]** Contractual Protections
 - **SLA Requirements:** Availability, security
 - **Audit Rights:** Assessment capabilities
 - **Breach Notification:** Timeframe requirements
 - **Data Portability:** Exit planning

Cloud Provider Evaluation Matrix:

Evaluation Area	Requirements	Verification Method	Weight
Security Certifications	SOC 2 Type II, ISO 27001	Certificate review	25%
Compliance Coverage	HIPAA, PCI, GDPR	Attestation review	20%
Technical Controls	Encryption, access control	Architecture review	20%
Operational Maturity	Incident response, BCM	Process review	15%
Financial Stability	Revenue, customers	Financial analysis	10%
Contract Terms	SLA, liability	Legal review	10%

13.4 Partner Security Requirements

Business Partner Security Standards

Critical Controls:

- ☐ **[C]** Partner Connection Security
 - **Network Segregation:** Dedicated segments
 - **Authentication:** Federated identity
 - **Encryption:** Data in transit
 - **Monitoring:** Activity logging
- ☐ **[C]** Data Sharing Agreements
 - **Classification:** Permitted data types
 - **Usage Restrictions:** Purpose limitation
 - **Retention Limits:** Defined periods
 - **Deletion Requirements:** Verified destruction

Partner Integration Security:

Technical Requirements:

- ☐ Dedicated VPN connections
 - ☐ API security standards
 - ☐ Certificate-based authentication
 - ☐ Encrypted data transfer
 - ☐ Activity monitoring
 - ☐ Rate limiting
 - ☐ Input validation
 - ☐ Error handling
 - ☐ Audit logging
 - ☐ Incident response coordination
-

14. Compliance & Regulatory Requirements {#compliance-regulatory-requirements}

14.1 Regulatory Compliance Framework

Multi-Regulation Compliance Strategy

Critical Controls:

- ☐ **[C]** Compliance Mapping
 - **Requirement Inventory:** All applicable regulations
 - **Control Mapping:** Common controls framework
 - **Gap Analysis:** Missing controls
 - **Implementation Plan:** Prioritized roadmap
- ☐ **[C]** Compliance Monitoring

- **Automated Testing:** Continuous compliance
- **Evidence Collection:** Audit preparation
- **Exception Management:** Risk acceptance
- **Reporting Dashboard:** Executive visibility

Major Regulatory Requirements:

Regulation	Scope	Key Requirements	Audit Frequency
GDPR	EU data protection	Privacy by design, data rights	Annual
HIPAA	Healthcare data	Encryption, access controls	Annual
PCI-DSS	Payment cards	Network security, encryption	Annual
SOX	Financial reporting	Internal controls, segregation	Annual
CCPA	California privacy	Consumer rights, data inventory	Annual

14.2 Industry-Specific Compliance

Sector Compliance Requirements

Financial Services Compliance:

- ☐ **[C]** Basel III Requirements
 - **Operational Risk:** Control framework
 - **Cyber Resilience:** Recovery capabilities
 - **Third-Party Risk:** Vendor management
 - **Data Governance:** Quality controls
- ☐ **[C]** SWIFT Security Controls
 - **Environment Protection:** Network security
 - **Know Your Customer:** Identity verification
 - **Access Control:** Privileged management
 - **Detect and Respond:** Monitoring capabilities

Healthcare Compliance:

- ☐ **[C]** HIPAA Security Rule
 - **Administrative Safeguards:** Policies, training
 - **Physical Safeguards:** Facility security
 - **Technical Safeguards:** Access, encryption
 - **Breach Notification:** 60-day requirement
- ☐ **[C]** FDA Cybersecurity Guidelines
 - **Medical Device Security:** Design controls

- **Software Validation:** Testing requirements
- **Post-Market Surveillance:** Ongoing monitoring
- **Vulnerability Disclosure:** Coordinated process

14.3 Privacy Regulations

Global Privacy Compliance

Critical Controls:

- ☐ **[C]** Privacy Program Implementation
 - **Privacy Officer:** Designated role
 - **Privacy Notices:** Transparent communication
 - **Consent Management:** Opt-in/opt-out
 - **Rights Management:** Subject requests
- ☐ **[C]** Cross-Border Data Transfers
 - **Transfer Mechanisms:** SCCs, adequacy
 - **Data Localization:** Country requirements
 - **Transfer Agreements:** Legal frameworks
 - **Risk Assessments:** Transfer impact

Privacy Compliance Checklist:

GDPR Compliance:

- ☐ Lawful basis documentation
- ☐ Privacy impact assessments
- ☐ Data protection by design
- ☐ Data minimization controls
- ☐ Purpose limitation enforcement
- ☐ Storage limitation automation
- ☐ Data subject rights portal
- ☐ Breach notification procedures
- ☐ DPO appointment (if required)
- ☐ Representative designation

CCPA Compliance:

- ☐ Consumer rights portal
- ☐ Opt-out mechanisms
- ☐ Data inventory maintenance
- ☐ Vendor agreement updates
- ☐ Employee training

- ☐ Privacy policy updates
- ☐ Metrics tracking
- ☐ Annual reporting
- ☐ Non-discrimination policies
- ☐ Financial incentive disclosures

14.4 Audit Management

Internal and External Audit Programs

Critical Controls:

- ☐ **[C]** Audit Program Structure
 - **Risk-Based Planning:** Annual audit plan
 - **Independence:** Reporting structure
 - **Competence:** Qualified auditors
 - **Coverage:** All critical areas
- ☐ **[C]** Audit Finding Management
 - **Tracking System:** Centralized repository
 - **Remediation Plans:** Time-bound actions
 - **Verification:** Closure validation
 - **Trend Analysis:** Systemic issues

Audit Preparation Checklist:

Pre-Audit Activities:

- ☐ Scope confirmation
- ☐ Evidence gathering
- ☐ Document organization
- ☐ System access setup
- ☐ Team briefing
- ☐ Logistics planning
- ☐ Communication plan
- ☐ Issue log review
- ☐ Control testing
- ☐ Management preparation

During Audit:

- ☐ Daily status meetings
- ☐ Evidence provision
- ☐ Query responses

- ☐ Issue tracking
 - ☐ Scope management
 - ☐ Escalation process
 - ☐ Documentation
 - ☐ Team coordination
 - ☐ Finding discussion
 - ☐ Remediation planning
-

15. Security Architecture & Design {#security-architecture-design}

15.1 Enterprise Security Architecture

Security Architecture Framework

Critical Controls:

- ☐ **[C]** Architecture Principles
 - **Defense in Depth:** Multiple control layers
 - **Least Privilege:** Minimal access rights
 - **Segregation:** Duty and system separation
 - **Resilience:** Failure tolerance
- ☐ **[C]** Reference Architecture
 - **Standard Patterns:** Approved designs
 - **Security Patterns:** Common controls
 - **Integration Standards:** Connectivity rules
 - **Technology Standards:** Approved products

Security Architecture Layers:

Layer	Components	Security Controls	Standards
Presentation	Web, mobile apps	WAF, authentication	OWASP
Application	Business logic	Input validation, encryption	Secure coding
Integration	APIs, middleware	API gateway, certificates	OAuth, mTLS
Data	Databases, storage	Encryption, access control	PCI, HIPAA
Infrastructure	Servers, network	Hardening, segmentation	CIS, NIST

15.2 Zero Trust Architecture

Zero Trust Implementation

Critical Controls:

- ☐ **[C] Identity-Centric Security**
 - **Continuous Verification:** Every transaction
 - **Risk-Based Access:** Context awareness
 - **Micro-Segmentation:** Granular controls
 - **Encryption Everywhere:** Default protection
- ☐ **[C] Policy Decision Points**
 - **Centralized Engine:** Policy evaluation
 - **Distributed Enforcement:** Multiple points
 - **Real-Time Decisions:** Dynamic access
 - **Audit Everything:** Complete visibility

Zero Trust Components:

Core Technologies:

- ☐ Identity provider (IdP)
- ☐ Multi-factor authentication
- ☐ Device trust platform
- ☐ Policy engine
- ☐ Micro-segmentation platform
- ☐ Software-defined perimeter
- ☐ CASB deployment
- ☐ Endpoint detection
- ☐ Network analytics
- ☐ Encryption gateway

15.3 Secure Design Patterns

Application Security Patterns

Critical Design Patterns:

Authentication Patterns:

- ☐ **[C] Centralized Authentication**
 - **SSO Integration:** Enterprise identity
 - **Token Management:** Secure storage
 - **Session Handling:** Timeout controls
 - **Password Policies:** Complexity rules

Authorization Patterns:

- ☐ **[C] Role-Based Access**

- **Permission Model:** Hierarchical roles
- **Dynamic Authorization:** Attribute-based
- **Delegation Model:** Temporary access
- **Audit Trail:** All decisions logged

Data Protection Patterns:

- ☐ **[C]** Encryption Patterns
- **Field-Level:** Sensitive data
 - **Transport:** TLS everywhere
 - **Storage:** At-rest encryption
 - **Key Management:** Centralized HSM

15.4 Security Services Design

Shared Security Services

Critical Controls:

- ☐ **[C]** Security Service Catalog
- **Authentication Service:** Enterprise SSO
 - **Authorization Service:** Policy management
 - **Encryption Service:** Key management
 - **Logging Service:** Centralized SIEM
- ☐ **[C]** Service Level Agreements
- **Availability:** 99.9% minimum
 - **Performance:** Response times
 - **Support:** 24/7 coverage
 - **Maintenance:** Change windows

Security Service Architecture:

Service	Function	SLA	Integration Method
Authentication	Identity verification	99.99%	SAML, OAuth
Authorization	Access decisions	99.95%	REST API
Encryption	Key management	99.99%	SDK, API
Logging	Event collection	99.9%	Syslog, API
Monitoring	Security events	99.9%	SNMP, API

16. DevSecOps & Secure Development {#devsecops-secure-development}

16.1 DevSecOps Implementation

Security Integration in CI/CD

Critical Controls:

- ☐ [C] Pipeline Security Integration
 - **Code Scanning:** Every commit
 - **Dependency Checking:** Build time
 - **Container Scanning:** Before deployment
 - **Compliance Checking:** Policy as code
- ☐ [C] Automated Security Testing
 - **SAST Integration:** IDE and pipeline
 - **DAST Automation:** Post-deployment
 - **License Scanning:** Compliance check
 - **Secrets Detection:** Credential scanning

DevSecOps Pipeline Stages:

Stage	Security Activities	Tools	Gates
Commit	Pre-commit hooks, secrets scan	Git hooks	Block secrets
Build	SAST, dependency check	SonarQube, OWASP	Quality gates
Test	Security unit tests, DAST	Selenium, ZAP	Coverage requirements
Package	Container scan, sign	Twistlock, Notary	Vulnerability threshold
Deploy	Config validation, RBAC	OPA, Kubernetes	Policy compliance
Monitor	Runtime protection, alerts	Falco, Prometheus	Anomaly detection

16.2 Infrastructure as Code Security

IaC Security Standards

Critical Controls:

- ☐ [C] IaC Security Scanning
 - **Template Scanning:** Pre-deployment
 - **Policy Enforcement:** Compliance rules
 - **Drift Detection:** Configuration changes
 - **Version Control:** Git integration
- ☐ [C] Secure IaC Patterns
 - **Least Privilege:** Minimal permissions
 - **Encryption Default:** Always enabled

- **Network Security:** Restrictive rules
- **Logging Enabled:** Audit trail

IaC Security Checklist:

Terraform Security:

- ☐ Remote state encryption
- ☐ State file access control
- ☐ Variable encryption
- ☐ Module security review
- ☐ Provider version pinning
- ☐ Security group validation
- ☐ IAM policy scanning
- ☐ Compliance validation
- ☐ Cost impact analysis
- ☐ Approval workflow

CloudFormation Security:

- ☐ Template validation
- ☐ Parameter encryption
- ☐ Stack policy enforcement
- ☐ Drift detection enabled
- ☐ Change set review
- ☐ IAM role boundaries
- ☐ Resource tagging
- ☐ Deletion protection
- ☐ Stack termination protection
- ☐ Audit logging

16.3 Container Security

Container and Kubernetes Security

Critical Controls:

- ☐ **[C]** Container Image Security
 - **Base Image:** Minimal, hardened
 - **Vulnerability Scanning:** Build and runtime
 - **Image Signing:** Cryptographic verification
 - **Registry Security:** Access controls
- ☐ **[C]** Kubernetes Security

- **RBAC Configuration:** Least privilege
- **Network Policies:** Micro-segmentation
- **Pod Security:** Security contexts
- **Secrets Management:** External vault

Container Security Implementation:

Image Security:

- ☐ Distroless base images
- ☐ Multi-stage builds
- ☐ Non-root containers
- ☐ Read-only filesystems
- ☐ Security scanning
- ☐ CVE threshold enforcement
- ☐ Image signing
- ☐ Registry scanning
- ☐ Admission control
- ☐ Runtime protection

Kubernetes Hardening:

- ☐ API server security
- ☐ etcd encryption
- ☐ Node security
- ☐ Network policies
- ☐ Pod security policies
- ☐ RBAC configuration
- ☐ Service mesh security
- ☐ Ingress protection
- ☐ Secrets encryption
- ☐ Audit logging

16.4 Secure Coding Practices

Developer Security Training

Critical Controls:

- ☐ **[C] Secure Coding Standards**
 - **Language-Specific:** All used languages
 - **Framework Security:** Best practices
 - **Common Vulnerabilities:** OWASP Top 10

- **Code Review:** Security focus
- ☐ **[C]** Developer Security Tools
 - **IDE Plugins:** Real-time scanning
 - **Pre-Commit Hooks:** Local scanning
 - **Security Libraries:** Approved components
 - **Testing Tools:** Security-focused

Secure Coding Guidelines:

Input Validation:

- ☐ Whitelist validation
- ☐ Length restrictions
- ☐ Type checking
- ☐ Format validation
- ☐ Range checking
- ☐ Canonicalization
- ☐ Encoding validation
- ☐ Business logic validation
- ☐ Error handling
- ☐ Logging suspicious input

Output Encoding:

- ☐ HTML encoding
- ☐ JavaScript encoding
- ☐ URL encoding
- ☐ CSS encoding
- ☐ SQL encoding
- ☐ LDAP encoding
- ☐ XML encoding
- ☐ Command encoding
- ☐ File path encoding
- ☐ Context-aware encoding

17. AI/ML Security {#ai-ml-security}

17.1 AI/ML Security Framework

Machine Learning Security Architecture

Critical Controls:

- ☐ [C] Model Security Lifecycle
 - **Training Data:** Poisoning prevention
 - **Model Development:** Secure environment
 - **Model Deployment:** Integrity verification
 - **Model Monitoring:** Drift detection
- ☐ [C] AI Ethics and Governance
 - **Bias Detection:** Fairness metrics
 - **Explainability:** Decision transparency
 - **Privacy Preservation:** Data minimization
 - **Accountability:** Audit trails

ML Security Threats:

Threat Type	Description	Mitigation	Detection Method
Data Poisoning	Malicious training data	Data validation	Statistical analysis
Model Inversion	Extract training data	Differential privacy	Access monitoring
Adversarial Examples	Malicious inputs	Input validation	Anomaly detection
Model Theft	Steal model logic	Access control	Query monitoring

17.2 AI Model Protection

Securing ML Models

Critical Controls:

- ☐ [C] Model Access Control
 - **Authentication:** API security
 - **Authorization:** Usage limits
 - **Rate Limiting:** Prevent extraction
 - **Monitoring:** Unusual patterns
- ☐ [C] Model Integrity
 - **Version Control:** Model tracking
 - **Cryptographic Signing:** Authenticity
 - **Deployment Verification:** Checksum
 - **Rollback Capability:** Previous versions

Model Security Checklist:

Development Security:

- ☐ Secure training environment

- ☐ Data source validation
- ☐ Feature engineering review
- ☐ Model architecture review
- ☐ Hyperparameter security
- ☐ Experiment tracking
- ☐ Code security scanning
- ☐ Dependency management
- ☐ Access logging
- ☐ Version control

Deployment Security:

- ☐ Model encryption
- ☐ Secure model serving
- ☐ API authentication
- ☐ Input validation
- ☐ Output filtering
- ☐ Performance monitoring
- ☐ Security monitoring
- ☐ Update procedures
- ☐ Rollback plans
- ☐ Incident response

17.3 Data Security for AI

Training Data Protection

Critical Controls:

- ☐ **[C]** Data Privacy Controls
 - **Anonymization:** PII removal
 - **Pseudonymization:** Reversible masking
 - **Aggregation:** Statistical privacy
 - **Synthetic Data:** Privacy-preserving
- ☐ **[C]** Federated Learning Security
 - **Distributed Training:** Data locality
 - **Secure Aggregation:** Encrypted updates
 - **Privacy Guarantees:** Differential privacy
 - **Model Validation:** Poisoning detection

AI Data Security Matrix:

Data Type	Privacy Risk	Protection Method	Validation
Personal Data	High	Anonymization	Re-identification test
Behavioral Data	Medium	Aggregation	K-anonymity check
Transactional	High	Tokenization	Format preservation
Biometric	Critical	Encryption	Access audit

17.4 AI Security Operations

Monitoring AI Systems

Critical Controls:

- ☐ **[C]** AI Security Monitoring
 - **Performance Metrics:** Accuracy tracking
 - **Fairness Metrics:** Bias detection
 - **Security Metrics:** Attack detection
 - **Drift Detection:** Model degradation
- ☐ **[C]** Incident Response for AI
 - **Attack Detection:** Adversarial inputs
 - **Response Procedures:** Model updates
 - **Recovery Plans:** Rollback procedures
 - **Investigation:** Root cause analysis

AI Security Operations:

Monitoring Requirements:

- ☐ Model performance tracking
- ☐ Input distribution monitoring
- ☐ Output distribution analysis
- ☐ Prediction confidence tracking
- ☐ Feature importance changes
- ☐ Data drift detection
- ☐ Concept drift detection
- ☐ Adversarial detection
- ☐ Resource usage monitoring
- ☐ API usage analytics

18. Mobile Security {#mobile-security}

18.1 Mobile Device Management

Enterprise Mobility Strategy

Critical Controls:

- ☐ [C] MDM Platform Implementation
 - **Device Enrollment:** Automated process
 - **Policy Enforcement:** Compliance checking
 - **App Management:** Whitelist/blacklist
 - **Data Protection:** Container isolation
- ☐ [C] Mobile Security Policies
 - **Device Requirements:** OS versions, patches
 - **Authentication:** Biometric + PIN
 - **Encryption:** Device and app level
 - **Network Security:** VPN requirements

MDM Configuration Standards:

Policy Area	iOS Requirements	Android Requirements	Enforcement
OS Version	Latest - 1	Latest - 1	Block non-compliant
Passcode	6+ digits	6+ digits	Wipe after 10 fails
Encryption	Mandatory	Mandatory	Automatic
Jailbreak	Prohibited	Root prohibited	Immediate wipe
Apps	Managed only	Managed only	Containerized

18.2 Mobile Application Security

Secure Mobile Development

Critical Controls:

- ☐ [C] Mobile App Security Testing
 - **Static Analysis:** Source code review
 - **Dynamic Analysis:** Runtime testing
 - **Binary Protection:** Anti-tampering
 - **API Security:** Certificate pinning
- ☐ [C] App Distribution Security
 - **Code Signing:** Developer certificates
 - **App Wrapping:** Additional protection
 - **Store Compliance:** Platform requirements
 - **Update Mechanism:** Secure delivery

Mobile App Security Checklist:

iOS Security:

- ☐ Keychain usage for secrets
- ☐ Certificate pinning
- ☐ Jailbreak detection
- ☐ Anti-debugging measures
- ☐ Secure data storage
- ☐ Biometric authentication
- ☐ App Transport Security
- ☐ Code obfuscation
- ☐ Binary packing
- ☐ Runtime protection

Android Security:

- ☐ ProGuard/R8 obfuscation
- ☐ Certificate pinning
- ☐ Root detection
- ☐ Anti-tampering
- ☐ Secure SharedPreferences
- ☐ Biometric API usage
- ☐ Network Security Config
- ☐ SafetyNet attestation
- ☐ App bundles signing
- ☐ Play Integrity API

18.3 BYOD Security

Bring Your Own Device Program

Critical Controls:

- ☐ **[C]** BYOD Policy Framework
 - **Acceptable Use:** Clear boundaries
 - **Security Requirements:** Minimum standards
 - **Privacy Balance:** Personal vs. corporate
 - **Support Model:** Self-service focus
- ☐ **[C]** Technical Controls
 - **App Containerization:** Data isolation
 - **Selective Wipe:** Corporate data only
 - **DLP Controls:** Prevent data leakage

- **Network Access:** Conditional access

BYOD Implementation Plan:

Enrollment Process:

- ☐ User agreement acceptance
- ☐ Device compatibility check
- ☐ MDM agent installation
- ☐ Certificate deployment
- ☐ Policy configuration
- ☐ App deployment
- ☐ Training completion
- ☐ Compliance verification
- ☐ Support contact info
- ☐ Incident procedures

18.4 Mobile Threat Defense

Advanced Mobile Protection

Critical Controls:

- ☐ **[C]** Mobile Threat Detection
 - **App Analysis:** Behavioral monitoring
 - **Network Threats:** Man-in-middle detection
 - **Device Threats:** OS vulnerability detection
 - **Phishing Protection:** URL checking
- ☐ **[C]** Response Automation
 - **Threat Isolation:** Automatic quarantine
 - **User Notification:** Risk communication
 - **Remediation:** Guided resolution
 - **Reporting:** Centralized visibility

Mobile Security Monitoring:

Threat Category	Detection Method	Response Action	User Impact
Malicious Apps	Behavior analysis	App removal	Minimal
Network Attacks	Traffic inspection	VPN activation	Transparent
OS Vulnerabilities	Version checking	Update prompt	User action
Phishing	URL reputation	Block access	Protection

19. IoT & OT Security {#iot-ot-security}

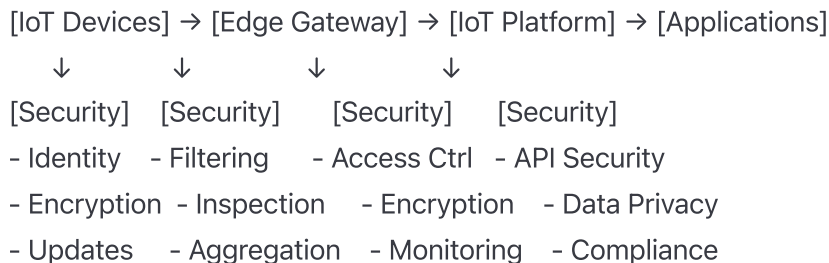
19.1 IoT Security Framework

Internet of Things Protection

Critical Controls:

- ☐ **[C]** IoT Device Management
 - **Asset Inventory:** All connected devices
 - **Firmware Management:** Update procedures
 - **Authentication:** Strong device identity
 - **Network Segmentation:** IoT VLANs
- ☐ **[C]** IoT Data Security
 - **Encryption:** End-to-end protection
 - **Data Minimization:** Collect necessary only
 - **Local Processing:** Edge computing
 - **Secure Storage:** Encrypted at rest

IoT Security Architecture:



19.2 OT Security

Operational Technology Protection

Critical Controls:

- ☐ **[C]** OT Network Segmentation
 - **Air Gap Options:** Critical systems
 - **DMZ Implementation:** IT/OT boundary
 - **Conduit Model:** Controlled data flow
 - **Purdue Model:** Level segregation
- ☐ **[C]** Industrial Control Security
 - **SCADA Protection:** Access control
 - **PLC Security:** Firmware validation

- **HMI Hardening:** Operator stations
- **Historian Security:** Data protection

OT Security Zones:

Purdue Level	Systems	Security Focus	Network Controls
Level 0	Physical process	Physical security	Isolated
Level 1	Basic control	Device hardening	Local only
Level 2	Area supervision	Access control	Segmented
Level 3	Site operations	Application security	DMZ boundary
Level 4-5	Enterprise	IT security	Full controls

19.3 IoT/OT Risk Management

Converged Risk Assessment

Critical Controls:

- ☐ **[C]** Safety and Security Integration
 - **Risk Correlation:** Safety impact
 - **Failure Analysis:** Cascading effects
 - **Recovery Priority:** Life safety first
 - **Testing Constraints:** Production limits
- ☐ **[C]** Supply Chain Security
 - **Component Verification:** Authenticity
 - **Vendor Assessment:** Security practices
 - **Update Verification:** Signed firmware
 - **EOL Planning:** Replacement strategy

IoT/OT Risk Matrix:

Risk Category	IoT Impact	OT Impact	Mitigation Priority
Device Compromise	Data breach	Safety risk	Critical
Network Attack	Service loss	Production stop	High
Firmware Vulnerability	Privacy risk	Equipment damage	High
Supply Chain	Backdoor risk	Counterfeit parts	Medium

19.4 Emerging Technology Security

5G and Edge Computing Security

Critical Controls:

- ☐ **[C]** 5G Security Implementation
 - **Network Slicing:** Isolation controls
 - **Edge Security:** Distributed protection
 - **API Security:** Service exposure
 - **Identity Management:** Device and user
- ☐ **[C]** Edge Computing Protection
 - **Edge Node Security:** Hardening standards
 - **Data Sovereignty:** Location controls
 - **Workload Protection:** Container security
 - **Orchestration Security:** Management plane

Edge Security Architecture:

Security Layers:

- ☐ Physical security at edge
 - ☐ Boot security/secure boot
 - ☐ OS and firmware hardening
 - ☐ Application sandboxing
 - ☐ Network micro-segmentation
 - ☐ Data encryption at rest
 - ☐ Secure communication channels
 - ☐ Local security monitoring
 - ☐ Centralized log aggregation
 - ☐ Automated threat response
-

20. Endpoint Security {#endpoint-security}

20.1 Endpoint Protection Platform

Comprehensive Endpoint Defense

Critical Controls:

- ☐ **[C]** Next-Gen Antivirus (NGAV)
 - **Behavioral Analysis:** AI/ML detection
 - **Exploit Prevention:** Memory protection
 - **Ransomware Protection:** Behavior blocking
 - **Cloud Intelligence:** Real-time updates
- ☐ **[C]** Endpoint Detection & Response (EDR)
 - **Continuous Monitoring:** All endpoints

- **Threat Hunting:** Proactive search
- **Forensic Capabilities:** Investigation tools
- **Automated Response:** Isolation, remediation

Endpoint Security Stack:

Layer	Technology	Function	Coverage Target
Prevention	NGAV	Block known/unknown threats	99%+
Detection	EDR	Identify advanced threats	95%+
Response	Automation	Isolate and remediate	<10 min
Recovery	Backup	Restore from ransomware	100%

20.2 Endpoint Configuration Management

Endpoint Hardening Standards

Critical Controls:

- ☐ **[C]** Operating System Hardening
 - **Baseline Configuration:** CIS benchmarks
 - **Security Updates:** Automated deployment
 - **Feature Restrictions:** Least functionality
 - **Local Policies:** Enforced settings
- ☐ **[C]** Application Control
 - **Whitelisting:** Approved applications
 - **Publisher Rules:** Signed software
 - **Path Rules:** Execution restrictions
 - **Hash Rules:** Known good files

Windows 10/11 Hardening:

Security Features:

- ☐ BitLocker encryption enabled
- ☐ Windows Defender enabled
- ☐ Firewall configured
- ☐ AppLocker/WDAC implemented
- ☐ Credential Guard enabled
- ☐ Device Guard configured
- ☐ UEFI Secure Boot
- ☐ TPM 2.0 utilized
- ☐ Attack Surface Reduction

- ☐ Controlled folder access

macOS Hardening:

- ☐ FileVault encryption
- ☐ Gatekeeper enabled
- ☐ XProtect updated
- ☐ System Integrity Protection
- ☐ Firmware password set
- ☐ Firewall enabled
- ☐ Secure boot configured
- ☐ T2 security chip features
- ☐ Privacy controls configured
- ☐ MDM profile enforcement

20.3 Privileged Access Workstations

PAW Implementation

Critical Controls:

- ☐ **[C]** PAW Architecture
 - **Dedicated Hardware:** Admin-only devices
 - **Network Isolation:** Restricted access
 - **Enhanced Monitoring:** All activities
 - **Restricted Software:** Minimal tools
- ☐ **[C]** PAW Security Controls
 - **Hardware Security:** TPM required
 - **Boot Security:** Measured boot
 - **Application Control:** Strict whitelist
 - **Network Restrictions:** Outbound limits

PAW Deployment Checklist:

Hardware Requirements:

- ☐ Business-class devices only
- ☐ TPM 2.0 chip present
- ☐ Secure boot capable
- ☐ Dedicated to admin tasks
- ☐ Asset tagged and tracked
- ☐ Physical security cable
- ☐ Biometric authentication

- ☐ Hardware inventory recorded
- ☐ Warranty coverage active
- ☐ Disposal procedures defined

20.4 Remote Endpoint Security

Work From Anywhere Security

Critical Controls:

- ☐ **[C]** Remote Access Security
 - **VPN Requirements:** Always-on policy
 - **Device Compliance:** Health checks
 - **Split Tunneling:** Prohibited
 - **MFA Enforcement:** All connections
- ☐ **[C]** Home Network Guidance
 - **Router Security:** Configuration guide
 - **WiFi Protection:** WPA3 standards
 - **Network Segmentation:** Work devices
 - **DNS Protection:** Secure resolvers

Remote Worker Security Kit:

Technical Controls:

- ☐ Encrypted laptop/device
- ☐ VPN client configured
- ☐ EDR agent installed
- ☐ Patch automation enabled
- ☐ DLP agent active
- ☐ Cloud backup configured
- ☐ Password manager provided
- ☐ MFA tokens issued
- ☐ Secure browser configured
- ☐ Privacy screen provided

21. Email Security {#email-security}

21.1 Email Gateway Security

Advanced Email Protection

Critical Controls:

- ☐ **[C] Email Security Gateway (ESG)**
 - **Spam Filtering:** 99%+ effectiveness
 - **Malware Detection:** Sandboxing capability
 - **Phishing Protection:** URL rewriting
 - **Data Loss Prevention:** Content inspection
- ☐ **[C] Email Authentication**
 - **SPF Implementation:** Sender verification
 - **DKIM Signing:** Message integrity
 - **DMARC Policy:** Enforcement mode
 - **BIMI Display:** Brand indicators

Email Security Architecture:

Internet → [MX Records] → [Email Gateway] → [Internal Server] → [Mailboxes]

↓

[Security Checks]

- Reputation filtering
- Anti-spam scanning
- Anti-malware analysis
- URL sandboxing
- Attachment analysis
- DLP inspection
- Encryption gateway

21.2 Anti-Phishing Measures

Phishing Defense Strategy

Critical Controls:

- ☐ **[C] Technical Anti-Phishing**
 - **Link Analysis:** Real-time checking
 - **Attachment Sandboxing:** Zero-day protection
 - **Impersonation Detection:** Display name tricks
 - **Computer Vision:** Image-based phishing
- ☐ **[C] User Reporting Integration**
 - **Report Button:** One-click reporting
 - **Automated Analysis:** Reported messages
 - **Threat Sharing:** Community protection
 - **User Feedback:** Report outcomes

Phishing Protection Layers:

Protection Layer	Technology	Effectiveness	User Impact
Gateway filtering	ML/AI analysis	95%+	Transparent
URL rewriting	Time-of-click	90%+	Slight delay
User warnings	Banner display	70%+	Awareness
Sandbox analysis	Behavioral	85%+	Delivery delay

21.3 Email Encryption

Message Protection Standards

Critical Controls:

- ☐ [C] Encryption Implementation
 - **TLS Enforcement:** Opportunistic + forced
 - **S/MIME Support:** Certificate management
 - **Portal Encryption:** Web-based delivery
 - **Rights Management:** IRM/RMS integration
- ☐ [C] Key Management
 - **Certificate Lifecycle:** Automated renewal
 - **Key Escrow:** Recovery procedures
 - **User Provisioning:** Self-service portal
 - **Partner Integration:** B2B encryption

Email Encryption Decision Matrix:

Scenario	Method	Key Management	User Experience
Internal email	Automatic TLS	Transparent	Seamless
Sensitive internal	S/MIME/RMS	Managed	Transparent
External partners	TLS forced	Negotiated	Seamless
Sensitive external	Portal/S/MIME	Self-service	Additional steps

21.4 Email Archiving and Retention

Compliance and e-Discovery

Critical Controls:

- ☐ [C] Email Archiving System
 - **Automatic Capture:** All messages
 - **Immutable Storage:** Tamper-proof

- **Search Capabilities:** e-Discovery ready
- **Retention Policies:** Automated enforcement
- ☐ **[C] Legal Hold Management**
 - **Hold Implementation:** Preserve in place
 - **Scope Management:** User and date ranges
 - **Chain of Custody:** Audit trail
 - **Export Capabilities:** Standard formats

Retention Policy Framework:

Email Type	Retention Period	Legal Hold Override	Deletion Method
General business	3 years	Yes	Automated
Financial	7 years	Yes	Automated
Legal matters	Indefinite	N/A	Manual review
Transactional	90 days	Yes	Automated

22. Web Security {#web-security}

22.1 Web Application Firewall

WAF Implementation Strategy

Critical Controls:

- ☐ **[C] WAF Deployment Architecture**
 - **Coverage:** All web applications
 - **Mode:** Block mode for production
 - **Rule Sets:** OWASP Core Rule Set
 - **Custom Rules:** Application-specific
- ☐ **[C] WAF Management**
 - **Rule Tuning:** False positive reduction
 - **Learning Mode:** New app onboarding
 - **Performance Impact:** <10ms latency
 - **High Availability:** Active-active setup

WAF Configuration Standards:

Protection Profiles:

- ☐ SQL injection prevention
- ☐ Cross-site scripting (XSS)

- ☐ Directory traversal blocking
- ☐ Command injection prevention
- ☐ XML/JSON attack protection
- ☐ File upload restrictions
- ☐ Rate limiting rules
- ☐ Geographic restrictions
- ☐ Bot management
- ☐ DDoS protection

22.2 Web Browser Security

Enterprise Browser Management

Critical Controls:

- ☐ **[C]** Browser Configuration Management
 - **Group Policy:** Centralized settings
 - **Extension Control:** Whitelist approach
 - **Update Management:** Automated patches
 - **Security Features:** Enabled by default
- ☐ **[C]** Browser Isolation
 - **Remote Browsing:** High-risk sites
 - **Container Tabs:** Site isolation
 - **Sandbox Enforcement:** Process isolation
 - **Download Protection:** Scanning integration

Browser Security Checklist:

Chrome Enterprise:

- ☐ Automatic updates enabled
- ☐ Extension whitelist only
- ☐ Safe Browsing enabled
- ☐ Password manager integration
- ☐ Certificate pinning
- ☐ Legacy plugin blocking
- ☐ Download scanning
- ☐ Incognito mode controls
- ☐ Cloud management enrolled
- ☐ Telemetry configured

22.3 Content Delivery Security

CDN and Web Performance Security

Critical Controls:

- ☐ [C] CDN Security Configuration
 - **Origin Protection:** IP whitelisting
 - **SSL/TLS:** End-to-end encryption
 - **Access Control:** Token authentication
 - **DDoS Protection:** Always-on mitigation
- ☐ [C] Content Security
 - **Integrity Checking:** SRI implementation
 - **Cache Poisoning:** Prevention controls
 - **Header Security:** Security headers
 - **CORS Policy:** Restrictive configuration

Web Security Headers:

Header	Purpose	Recommended Value
Strict-Transport-Security	Force HTTPS	max-age=31536000; includeSubDomains
Content-Security-Policy	XSS prevention	default-src 'self'; script-src 'self'
X-Frame-Options	Clickjacking	SAMEORIGIN
X-Content-Type-Options	MIME sniffing	nosniff
Referrer-Policy	Privacy	strict-origin-when-cross-origin

22.4 API Gateway Security

API Management and Protection

Critical Controls:

- ☐ [C] API Gateway Architecture
 - **Centralized Entry:** Single point
 - **Authentication:** OAuth/JWT
 - **Rate Limiting:** Per client/API
 - **Monitoring:** All transactions
- ☐ [C] API Security Policies
 - **Input Validation:** Schema enforcement
 - **Output Filtering:** Data minimization
 - **Version Control:** Deprecation process
 - **Documentation:** OpenAPI specs

API Security Implementation:

Gateway Features:

- ☐ OAuth 2.0/OIDC support
 - ☐ API key management
 - ☐ JWT validation
 - ☐ Rate limiting/throttling
 - ☐ Request/response transformation
 - ☐ Schema validation
 - ☐ Error handling standardization
 - ☐ Logging and analytics
 - ☐ Circuit breaker pattern
 - ☐ Service mesh integration
-

23. Database Security {#database-security}

23.1 Database Access Control

Comprehensive Database Security

Critical Controls:

- ☐ [C] Database Authentication
 - **Strong Authentication:** No default passwords
 - **Service Accounts:** Unique per application
 - **Password Policies:** Complexity enforced
 - **Certificate Auth:** For high-security
- ☐ [C] Database Authorization
 - **Least Privilege:** Minimal grants
 - **Role Separation:** DBA vs. users
 - **Schema Permissions:** Object-level
 - **Row-Level Security:** Data filtering

Database User Management:

User Type	Permissions	Authentication	Audit Level
Application Service	CRUD on app schema	Certificate	All queries
Read-Only Reporting	SELECT only	AD integrated	Connections
DBA	Full admin	MFA required	Everything
Developer	Dev environment only	AD + approval	Schema changes

23.2 Database Encryption

Data Protection Implementation

Critical Controls:

- ☐ **[C]** Encryption at Rest
 - **Transparent Encryption:** TDE enabled
 - **Column Encryption:** Sensitive fields
 - **Backup Encryption:** All backups
 - **Key Management:** HSM integration
- ☐ **[C]** Encryption in Transit
 - **SSL/TLS:** Forced connections
 - **Certificate Validation:** Mutual TLS
 - **Version Requirements:** TLS 1.2+
 - **Cipher Suites:** Strong only

Encryption Implementation Guide:

Data Classification-Based Encryption:

- ☐ PII columns: Always encrypted
- ☐ Financial data: Column encryption
- ☐ General data: TDE protection
- ☐ Audit logs: Immutable + encrypted
- ☐ Backups: AES-256 minimum
- ☐ Archives: Encrypted + signed
- ☐ Temp data: Encrypted swap
- ☐ Memory: Encrypted pages
- ☐ Replication: SSL required
- ☐ Log shipping: Encrypted channel

23.3 Database Activity Monitoring

Real-Time Database Protection

Critical Controls:

- ☐ **[C]** DAM Implementation
 - **Full SQL Capture:** All queries
 - **Privileged Monitoring:** DBA activities
 - **Anomaly Detection:** Behavioral analysis
 - **Real-Time Alerts:** Critical events

- ☐ [C] Audit Configuration
- **Native Auditing:** Supplementary logs
 - **Performance Impact:** <5% overhead
 - **Storage Management:** Compression/rotation
 - **Tamper Protection:** Separate storage

Database Monitoring Rules:

Activity Type	Alert Priority	Response Time	Action
Schema changes	Critical	Immediate	Block + alert
Mass data export	High	5 minutes	Alert + review
After-hours access	Medium	15 minutes	Log + alert
Failed logins	Low	Hourly summary	Track patterns

23.4 Database Security Hardening

Platform-Specific Hardening

Critical Controls:

- ☐ [C] Configuration Hardening
- **Unnecessary Features:** Disabled
 - **Sample Data:** Removed
 - **Network Protocols:** Minimal enabled
 - **File Permissions:** Restricted
- ☐ [C] Patch Management
- **Critical Patches:** Within 30 days
 - **Security Updates:** Quarterly minimum
 - **Version Currency:** N-1 maximum
 - **Testing Process:** Non-prod first

Database Hardening Checklist:

Universal Controls:

- ☐ Change default ports
- ☐ Disable unnecessary services
- ☐ Remove sample databases
- ☐ Configure audit logging
- ☐ Enable connection encryption
- ☐ Implement backup encryption
- ☐ Set resource limits

- ☐ Configure error handling
- ☐ Disable remote administration
- ☐ Implement connection limits

24. API Security {#api-security}

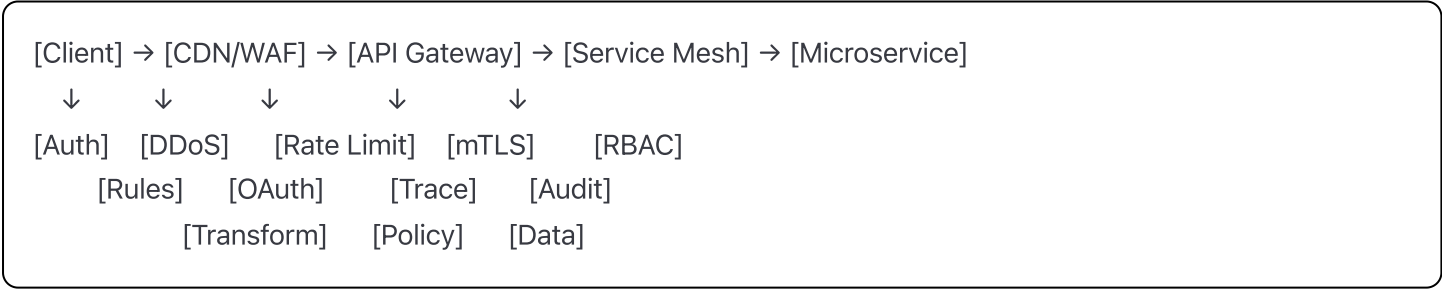
24.1 API Security Architecture

Comprehensive API Protection

Critical Controls:

- ☐ **[C]** API Gateway Implementation
 - **Centralized Management:** All APIs
 - **Security Policies:** Standardized
 - **Version Control:** Lifecycle management
 - **Developer Portal:** Self-service
- ☐ **[C]** API Authentication
 - **OAuth 2.0:** Standard implementation
 - **API Keys:** Backup method
 - **Mutual TLS:** High-security APIs
 - **JWT Tokens:** Stateless auth

API Security Layers:



24.2 API Threat Protection

OWASP API Security Top 10

Critical Controls by Threat:

1. Broken Object Level Authorization

- ☐ Implement object-level checks
- ☐ Validate user permissions
- ☐ Use UUIDs not sequences
- ☐ Test authorization thoroughly

2. Broken User Authentication

- ☐ Strong authentication required
- ☐ Implement account logout
- ☐ Use secure password reset
- ☐ Enable MFA where possible

3. Excessive Data Exposure

- ☐ Implement data filtering
- ☐ Remove sensitive fields
- ☐ Use response schemas
- ☐ Minimize data returned

4. Lack of Resources & Rate Limiting

- ☐ Implement rate limiting
- ☐ Set pagination limits
- ☐ Configure timeouts
- ☐ Monitor resource usage

5. Broken Function Level Authorization

- ☐ Check function permissions
- ☐ Separate admin functions
- ☐ Validate all endpoints
- ☐ Use deny by default

24.3 API Development Security

Secure API Development Lifecycle

Critical Controls:

- ☐ **[C]** API Design Security
 - **Threat Modeling:** Pre-development
 - **Security Requirements:** Documented
 - **Schema Definition:** OpenAPI/Swagger
 - **Error Handling:** Secure responses
- ☐ **[C]** API Testing Security
 - **Security Testing:** DAST/SAST
 - **Fuzzing:** Input validation
 - **Authorization Testing:** All endpoints
 - **Performance Testing:** DoS prevention

API Security Checklist:

Design Phase:

- ☐ Define security requirements
- ☐ Create threat model
- ☐ Design authentication flow
- ☐ Plan authorization model
- ☐ Define data schemas
- ☐ Plan rate limiting
- ☐ Design error responses
- ☐ Create API documentation
- ☐ Define versioning strategy
- ☐ Plan deprecation process

24.4 API Monitoring and Analytics

API Security Operations

Critical Controls:

- ☐ [C] API Monitoring Platform
 - **Traffic Analysis:** All API calls
 - **Performance Metrics:** Latency, errors
 - **Security Events:** Attack detection
 - **Business Metrics:** Usage patterns
- ☐ [C] API Threat Detection
 - **Anomaly Detection:** ML-based
 - **Pattern Recognition:** Attack signatures
 - **Behavioral Analysis:** User patterns
 - **Integration:** SIEM correlation

API Monitoring Dashboard:

Metric	Threshold	Alert Level	Response
Error rate	>5%	High	Investigate
Latency	>1000ms	Medium	Review
Auth failures	>10/min	High	Block IP
Rate limit hits	>100/hr	Low	Monitor

25. Container & Kubernetes Security {#container-kubernetes-security}

25.1 Container Security Fundamentals

Container Lifecycle Security

Critical Controls:

- ☐ **[C]** Secure Container Images
 - **Base Image:** Minimal, verified source
 - **Vulnerability Scanning:** Build-time checks
 - **Image Signing:** Cryptographic verification
 - **Registry Security:** Access controls
- ☐ **[C]** Runtime Protection
 - **Container Isolation:** Namespace separation
 - **Resource Limits:** CPU/memory caps
 - **Capability Dropping:** Least privilege
 - **Read-Only Root:** Immutable filesystem

Container Security Checklist:

Image Security:

- ☐ Use official base images
- ☐ Scan for vulnerabilities
- ☐ Remove unnecessary packages
- ☐ Don't run as root
- ☐ Use multi-stage builds
- ☐ Sign container images
- ☐ Implement SBOM
- ☐ Version pinning
- ☐ Secret management
- ☐ Health checks defined

25.2 Kubernetes Security

K8s Cluster Hardening

Critical Controls:

- ☐ **[C]** Cluster Configuration
 - **RBAC Enabled:** Default deny
 - **Network Policies:** Micro-segmentation
 - **Pod Security:** Admission control
 - **Secrets Management:** External vault

- ☐ **[C]** Control Plane Security
 - **API Server:** Authentication required
 - **etcd Encryption:** Data at rest
 - **Audit Logging:** All API calls
 - **Component Security:** TLS everywhere

Kubernetes Security Layers:

Layer	Security Controls	Implementation
Cluster	RBAC, admission control	Native K8s
Network	Policies, service mesh	Calico/Istio
Container	Scanning, runtime	Falco/Twistlock
Data	Encryption, secrets	Vault/Sealed Secrets

25.3 Service Mesh Security

Microservices Security Architecture

Critical Controls:

- ☐ **[C]** Service Mesh Implementation
 - **mTLS:** Automatic encryption
 - **Service Identity:** SPIFFE/SPIRE
 - **Policy Enforcement:** Fine-grained
 - **Observability:** Full visibility
- ☐ **[C]** Zero Trust Networking
 - **Service Authorization:** Every request
 - **Identity Verification:** Workload identity
 - **Encryption:** All traffic
 - **Policy as Code:** Version controlled

Service Mesh Security Features:

Istio Security Configuration:

- ☐ Automatic mTLS enabled
- ☐ Strict RBAC policies
- ☐ Service-level authorization
- ☐ JWT authentication
- ☐ Rate limiting configured
- ☐ Circuit breakers set
- ☐ Egress controls

- ☐ Ingress gateway security
- ☐ Telemetry collection
- ☐ Policy enforcement

25.4 Container Registry Security

Registry Protection Strategy

Critical Controls:

- ☐ **[C]** Registry Access Control
 - **Authentication:** No anonymous push
 - **Authorization:** Project isolation
 - **Audit Logging:** All activities
 - **Vulnerability Scanning:** Automatic
- ☐ **[C]** Image Lifecycle Management
 - **Retention Policies:** Age/vulnerability based
 - **Immutable Tags:** Production images
 - **Replication:** Multi-region backup
 - **Compliance Scanning:** License/security

Registry Security Implementation:

Harbor/DTR Configuration:

- ☐ LDAP/OIDC integration
 - ☐ Role-based access control
 - ☐ Vulnerability scanning enabled
 - ☐ Image signing enforced
 - ☐ Replication policies
 - ☐ Garbage collection scheduled
 - ☐ Audit logging configured
 - ☐ Quota management
 - ☐ Webhook notifications
 - ☐ High availability setup
-

26. Vulnerability Management {#vulnerability-management}

26.1 Vulnerability Assessment Program

Comprehensive Vulnerability Discovery

Critical Controls:

- ☐ [C] Vulnerability Scanning Strategy
 - **Coverage:** 100% of assets
 - **Frequency:** Risk-based scheduling
 - **Authenticated Scans:** Deep inspection
 - **Compliance Scanning:** Regulatory checks
- ☐ [C] Asset Discovery
 - **Automated Discovery:** Continuous
 - **Cloud Resources:** API integration
 - **Shadow IT:** Unauthorized systems
 - **Attribution:** Owner identification

Scanning Schedule Matrix:

Asset Type	Scan Frequency	Scan Type	Maintenance Window
External facing	Daily	Full	Automated
Internal servers	Weekly	Authenticated	Weekend
Workstations	Monthly	Agent-based	Non-business
Cloud resources	Continuous	API-based	N/A
Network devices	Weekly	SNMP/SSH	Maintenance

26.2 Vulnerability Prioritization

Risk-Based Remediation

Critical Controls:

- ☐ [C] CVSS Scoring Enhancement
 - **Environmental Score:** Asset criticality
 - **Temporal Score:** Exploit availability
 - **Threat Intelligence:** Active exploitation
 - **Business Context:** Impact assessment
- ☐ [C] Remediation SLAs
 - **Critical (CVSS 9-10):** 24 hours
 - **High (CVSS 7-8.9):** 7 days
 - **Medium (CVSS 4-6.9):** 30 days
 - **Low (CVSS 0-3.9):** 90 days

Vulnerability Prioritization Framework:

$$\text{Risk Score} = \text{CVSS Base} \times \text{Asset Criticality} \times \text{Exploit Probability} \times \text{Exposure Factor}$$

Where:

- Asset Criticality: 1-5 (Business impact)
- Exploit Probability: 0-1 (Threat intel)
- Exposure Factor: 0-1 (Accessibility)

26.3 Patch Management

Enterprise Patch Management Program

Critical Controls:

- ☐ **[C]** Patch Management Process
- **Patch Testing:** Pre-production validation
 - **Deployment Groups:** Phased rollout
 - **Rollback Plans:** Documented procedures
 - **Success Validation:** Post-patch verification
- ☐ **[C]** Emergency Patching
- **Zero-Day Response:** 24-hour deployment
 - **Out-of-Band Updates:** Process defined
 - **Communication Plan:** Stakeholder alerts
 - **Exception Process:** Risk acceptance

Patch Deployment Phases:

Phase	Environment	Timeline	Success Criteria
1. Test	Lab systems	Day 1-2	Functional validation
2. Pilot	IT systems	Day 3-5	No critical issues
3. Staged	10% production	Day 6-8	<1% failure rate
4. Full	All systems	Day 9-30	95% compliance

26.4 Vulnerability Metrics and Reporting

Vulnerability Management KPIs

Critical Controls:

- ☐ **[C]** Metrics Collection
- **Mean Time to Detect:** Vulnerability age
 - **Mean Time to Remediate:** Patch velocity
 - **Coverage Percentage:** Scanned assets

- **Compliance Rate:** SLA adherence
- ☐ **[C]** Executive Reporting
 - **Risk Trending:** Month-over-month
 - **Top Vulnerabilities:** Business impact
 - **Remediation Progress:** Burndown charts
 - **Benchmark Comparison:** Industry metrics

Vulnerability Dashboard Elements:

Real-Time Metrics:

- ☐ Total vulnerabilities by severity
 - ☐ Aging analysis (0-30-60-90 days)
 - ☐ Top 10 vulnerable systems
 - ☐ Patch compliance percentage
 - ☐ MTTR by severity level
 - ☐ Scanner coverage map
 - ☐ Exception tracking
 - ☐ Remediation velocity
 - ☐ Risk score trending
 - ☐ SLA compliance status
-

27. Security Monitoring & SIEM {#security-monitoring-siem}

27.1 SIEM Architecture

Enterprise SIEM Implementation

Critical Controls:

- ☐ **[C]** SIEM Platform Design
 - **Log Collection:** Universal coverage
 - **Storage Capacity:** 365-day retention
 - **Processing Power:** Peak load handling
 - **High Availability:** No single point of failure
- ☐ **[C]** Data Source Integration
 - **Critical Systems:** 100% coverage
 - **Network Devices:** Flow and logs
 - **Security Tools:** All platforms
 - **Cloud Services:** API integration

SIEM Data Sources Priority:

Priority	Source Type	Retention	Use Cases
Critical	AD, Firewall, IDS	365 days	Auth, threats
High	Servers, Apps	180 days	Compromise
Medium	Workstations	90 days	Investigations
Low	IoT, Printers	30 days	Compliance

27.2 Detection Engineering

Advanced Threat Detection

Critical Controls:

- ☐ **[C]** Detection Rule Development
 - **MITRE ATT&CK:** Mapped coverage
 - **Custom Rules:** Environment-specific
 - **ML Models:** Behavioral baselines
 - **Threat Intel:** IOC integration
- ☐ **[C]** Alert Tuning Process
 - **False Positive Rate:** <5% target
 - **True Positive Validation:** Weekly review
 - **Rule Optimization:** Performance tuning
 - **Coverage Assessment:** Gap analysis

Detection Rule Categories:

Authentication Anomalies:

- ☐ Impossible travel detection
- ☐ Brute force attempts
- ☐ Pass-the-hash indicators
- ☐ Service account anomalies
- ☐ Privileged escalation
- ☐ Failed login patterns
- ☐ Account lockout tracking
- ☐ Password spray detection
- ☐ Golden ticket detection
- ☐ Kerberoasting attempts

27.3 Security Orchestration

SOAR Implementation

Critical Controls:

- ☐ [C] Automated Response Playbooks
 - **Tier 1 Automation:** 80% of alerts
 - **Enrichment:** Context gathering
 - **Containment:** Automatic isolation
 - **Evidence Collection:** Forensic data
- ☐ [C] Integration Framework
 - **API Connectivity:** All security tools
 - **Bi-directional:** Read/write capability
 - **Error Handling:** Graceful failures
 - **Audit Trail:** All actions logged

SOAR Playbook Examples:

Alert Type	Automated Actions	Human Decision Point
Malware detected	Isolate, scan, collect	Reimage decision
Phishing reported	Analyze, block, purge	User notification
Brute force	Block IP, alert user	Account reset
Data exfiltration	Kill process, isolate	Investigation

27.4 Threat Hunting

Proactive Threat Discovery

Critical Controls:

- ☐ [C] Threat Hunting Program
 - **Dedicated Team:** Skilled analysts
 - **Hypothesis-Driven:** Structured approach
 - **Tool Access:** Full visibility
 - **Time Allocation:** 40% proactive
- ☐ [C] Hunting Methodology
 - **Intelligence-Led:** Threat actor TTPs
 - **Analytics-Driven:** Statistical anomalies
 - **Situational:** Environmental changes
 - **Campaign-Based:** Focused operations

Threat Hunting Playbook:

Hunt Planning:

- ☐ Define hypothesis
 - ☐ Identify data sources
 - ☐ Develop analytics
 - ☐ Set success criteria
 - ☐ Allocate resources
 - ☐ Create timeline
 - ☐ Document methodology
 - ☐ Prepare tools
 - ☐ Brief stakeholders
 - ☐ Establish communications
-

28. Forensics & Investigation {#forensics-investigation}

28.1 Digital Forensics Capability

Forensic Readiness Program

Critical Controls:

- ☐ **[C] Forensic Infrastructure**
 - **Lab Environment:** Isolated network
 - **Storage Capacity:** Evidence retention
 - **Processing Power:** Analysis capability
 - **Tool Licensing:** Commercial tools
- ☐ **[C] Evidence Management**
 - **Chain of Custody:** Documented process
 - **Storage Security:** Encrypted, controlled
 - **Integrity Verification:** Hash validation
 - **Legal Compliance:** Admissibility focus

Forensic Lab Requirements:

Component	Specification	Purpose
Workstations	High-spec, dedicated	Analysis
Storage	100TB+, RAID, encrypted	Evidence
Network	Isolated, monitored	Security
Tools	EnCase, FTK, X-Ways	Investigation
Write blockers	Hardware/software	Integrity

28.2 Incident Investigation

Investigation Methodology

Critical Controls:

- ☐ **[C]** Investigation Process
 - **Initial Assessment:** Scope determination
 - **Evidence Collection:** Comprehensive gathering
 - **Analysis Phase:** Systematic examination
 - **Reporting:** Findings documentation
- ☐ **[C]** Evidence Sources
 - **Volatile Data:** Memory, processes
 - **Non-Volatile:** Disk, logs
 - **Network:** Captures, flows
 - **External:** Third-party data

Investigation Checklist:

Data Collection Priority:

1. Volatile Evidence

- ☐ RAM contents
- ☐ Running processes
- ☐ Network connections
- ☐ Open files/handles
- ☐ System information

2. System Evidence

- ☐ System logs
- ☐ Application logs
- ☐ Registry/configuration
- ☐ User artifacts
- ☐ Temporary files

3. Storage Evidence

- ☐ File system timeline
- ☐ Deleted files recovery
- ☐ Slack space analysis
- ☐ Volume shadow copies
- ☐ Hibernation files

28.3 Malware Analysis

Malware Investigation Framework

Critical Controls:

- ☐ [C] Malware Analysis Lab
 - **Isolated Environment:** No production access
 - **Analysis Tools:** Static and dynamic
 - **Sandbox Systems:** Automated analysis
 - **Reverse Engineering:** Disassembly tools
- ☐ [C] Analysis Procedures
 - **Safe Handling:** Containment protocols
 - **Static Analysis:** Code examination
 - **Dynamic Analysis:** Behavior monitoring
 - **Reporting Format:** Standardized IOCs

Malware Analysis Workflow:

Phase	Activities	Tools	Output
Triage	Hash check, AV scan	VirusTotal	Initial classification
Static	Strings, PE analysis	IDA Pro, PEiD	Code structure
Dynamic	Sandbox execution	Cuckoo, Any.run	Behavior profile
Deep	Reverse engineering	x64dbg, Ghidra	Full analysis

28.4 Legal and Compliance

Legal Framework for Investigations

Critical Controls:

- ☐ [C] Legal Procedures
 - **Legal Counsel:** On-call availability
 - **Law Enforcement:** Cooperation protocols
 - **Evidence Standards:** Court admissibility
 - **Privacy Compliance:** Legal boundaries
- ☐ [C] Reporting Requirements
 - **Regulatory Notices:** Breach timelines
 - **Law Enforcement:** When required
 - **Executive Reporting:** Board-level
 - **External Disclosure:** PR coordination

Legal Considerations Checklist:

Pre-Investigation:

- ☐ Legal authority verified
- ☐ Privacy impact assessed
- ☐ Counsel consulted
- ☐ Scope documented
- ☐ Permissions obtained

During Investigation:

- ☐ Chain of custody maintained
- ☐ Actions documented
- ☐ Privacy protected
- ☐ Privilege preserved
- ☐ Compliance maintained

Post-Investigation:

- ☐ Report reviewed by legal
 - ☐ Retention requirements met
 - ☐ Disclosure obligations fulfilled
 - ☐ Lessons learned documented
 - ☐ Evidence properly stored
-

29. Security Metrics & KPIs {#security-metrics-kpis}

29.1 Security Metrics Framework

Comprehensive Measurement Program

Critical Controls:

- ☐ **[C] Metrics Definition**
 - **Strategic Metrics:** Board-level KPIs
 - **Operational Metrics:** Daily operations
 - **Tactical Metrics:** Project success
 - **Compliance Metrics:** Regulatory requirements
- ☐ **[C] Data Collection Architecture**
 - **Automated Collection:** Real-time feeds
 - **Manual Inputs:** Qualitative data
 - **Integration Points:** All security tools
 - **Data Quality:** Validation rules

Security Metrics Hierarchy:

Level	Audience	Metrics Type	Reporting Frequency
Strategic	Board	Risk, compliance	Quarterly
Executive	C-Suite	Program effectiveness	Monthly
Management	Directors	Operational efficiency	Weekly
Operational	Teams	Technical performance	Daily

29.2 Key Performance Indicators

Essential Security KPIs

Strategic KPIs:

- ☐ [C] Risk Reduction
 - **Risk Score Trend:** Downward trajectory
 - **Critical Risks:** Zero tolerance
 - **Risk Appetite:** Within boundaries
 - **Control Effectiveness:** >90%
- ☐ [C] Security Investment ROI
 - **Incident Cost Avoidance:** Calculated savings
 - **Efficiency Gains:** Automation metrics
 - **Risk Transfer:** Insurance optimization
 - **Program Maturity:** Year-over-year

Operational KPIs Matrix:

KPI Category	Metric	Target	Measurement
Vulnerability Management	MTTR Critical Vulns	<24 hrs	Automated
Incident Response	MTTD/MTTR	<1hr/<4hrs	SIEM
Patch Compliance	Coverage %	>95%	Scanner
Training Completion	Employee %	>95%	LMS
Phishing Resilience	Click Rate	<5%	Simulation

29.3 Security Dashboards and Reporting

Executive Dashboard Design

Critical Controls:

- ☐ [C] Dashboard Architecture
 - **Real-Time Data:** Live feeds where applicable
 - **Historical Trending:** 13-month rolling
 - **Drill-Down Capability:** Detail access

- **Mobile Responsive:** Executive access
- ☐ **[C]** Visualization Standards
 - **Color Coding:** Red/yellow/green
 - **Chart Types:** Appropriate selection
 - **Data Density:** Executive appropriate
 - **Refresh Rates:** Based on data type

Dashboard Components:

Executive Security Dashboard:

- ☐ Overall security posture score
- ☐ Critical incident status
- ☐ Compliance status by framework
- ☐ Vulnerability exposure trend
- ☐ Security project status
- ☐ Budget vs. spend
- ☐ Key risk indicators
- ☐ Threat intelligence summary
- ☐ Third-party risk status
- ☐ Security awareness metrics

29.4 Continuous Improvement

Security Program Optimization

Critical Controls:

- ☐ **[C]** Performance Analysis
 - **Trend Identification:** Statistical analysis
 - **Root Cause Analysis:** Systemic issues
 - **Benchmark Comparison:** Industry metrics
 - **Improvement Planning:** Action items
- ☐ **[C]** Maturity Assessment
 - **Annual Assessment:** Third-party review
 - **Capability Mapping:** CMMI model
 - **Gap Analysis:** Target vs. current
 - **Roadmap Development:** 3-year plan

Improvement Framework:

Assessment Area	Current State	Target State	Timeline	Investment
Process Maturity	Defined (3)	Managed (4)	18 months	\$500K
Tool Integration	Partial	Full	12 months	\$300K
Automation Level	40%	75%	24 months	\$750K
Staff Skills	Intermediate	Advanced	12 months	\$200K

30. Security Tools & Technologies {#security-tools-technologies}

30.1 Security Tool Portfolio

Enterprise Security Stack

Critical Controls:

- ☐ [C] Tool Selection Criteria
 - **Integration Capability:** API availability
 - **Scalability:** Growth accommodation
 - **Support Model:** 24/7 availability
 - **Total Cost:** TCO analysis
- ☐ [C] Tool Lifecycle Management
 - **Evaluation Process:** POC requirements
 - **Implementation:** Phased approach
 - **Optimization:** Continuous tuning
 - **Retirement:** Sunset planning

Core Security Technology Stack:

Category	Primary Tool	Backup/Secondary	Integration Points
SIEM	Splunk	QRadar	All security tools
EDR	CrowdStrike	Carbon Black	SIEM, SOAR
Vulnerability	Qualys	Tenable	CMDB, Ticketing
Network	Palo Alto	Fortinet	SIEM, NAC
Email	Proofpoint	Mimecast	SIEM, SOAR

30.2 Security Automation

Automation and Orchestration Platform

Critical Controls:

- ☐ [C] SOAR Implementation
 - **Use Case Selection:** High-volume alerts

- **Playbook Development:** Standardized response
- **Integration Breadth:** All key tools
- **Success Metrics:** Time savings
- ☐ **[C] Automation Governance**
 - **Change Control:** Playbook updates
 - **Testing Requirements:** Non-prod first
 - **Approval Process:** Risk-based
 - **Audit Trail:** All actions

Automation Priority Matrix:

Process	Volume	Complexity	Automation Potential	Priority
Phishing response	High	Low	90%	Critical
User provisioning	High	Medium	80%	High
Vulnerability scanning	Medium	Low	95%	High
Incident triage	High	High	60%	Medium
Threat hunting	Low	High	30%	Low

30.3 Emerging Technologies

Next-Generation Security Technologies

Critical Controls:

- ☐ **[C] Technology Evaluation**
 - **Proof of Concept:** Before purchase
 - **Risk Assessment:** New tech risks
 - **Pilot Program:** Limited deployment
 - **Success Criteria:** Measurable outcomes
- ☐ **[C] Innovation Pipeline**
 - **Technology Radar:** Tracking emerging tech
 - **Vendor Briefings:** Regular sessions
 - **Industry Research:** Analyst reports
 - **Peer Networks:** Experience sharing

Emerging Technology Roadmap:

Near-Term (0-12 months):

- ☐ XDR platform evaluation
- ☐ CASB deployment expansion

- ☐ Zero Trust network access
- ☐ Cloud security posture management
- ☐ Attack surface management

Medium-Term (12-24 months):

- ☐ AI-powered threat detection
- ☐ Quantum-safe cryptography planning
- ☐ Automated penetration testing
- ☐ Deception technology
- ☐ Security data lakes

Long-Term (24-36 months):

- ☐ Quantum computing readiness
- ☐ Advanced AI defense
- ☐ Autonomous response systems
- ☐ Predictive risk modeling
- ☐ Blockchain security applications

30.4 Tool Integration and Optimization

Security Platform Integration

Critical Controls:

- ☐ **[C]** Integration Architecture
 - **API Standards:** RESTful preferred
 - **Data Formats:** JSON/XML normalization
 - **Authentication:** OAuth/API keys
 - **Error Handling:** Graceful degradation
- ☐ **[C]** Performance Optimization
 - **Resource Monitoring:** CPU/memory/storage
 - **Query Optimization:** Database tuning
 - **Caching Strategy:** Improved response
 - **Load Balancing:** High availability

Integration Checklist:

Technical Integration:

- ☐ API documentation review
- ☐ Authentication setup
- ☐ Data mapping completed

- ☐ Error handling implemented
 - ☐ Logging configured
 - ☐ Performance baseline
 - ☐ Failover testing
 - ☐ Monitoring alerts
 - ☐ Documentation updated
 - ☐ Team training completed
-

Appendices

Appendix A: Compliance Mapping

Framework Cross-Reference

This section maps the security controls in this checklist to major compliance frameworks:

ISO 27001 Mapping:

- A.5: Information Security Policies → Section 2.1
- A.6: Organization of Information Security → Section 2.3
- A.7: Human Resource Security → Section 12
- A.8: Asset Management → Section 2.2
- A.9: Access Control → Section 8
- A.10: Cryptography → Section 7.3
- A.11: Physical Security → Section 11
- A.12: Operations Security → Sections 3-6
- A.13: Communications Security → Section 6
- A.14: System Development → Section 16
- A.15: Supplier Relationships → Section 13
- A.16: Incident Management → Section 9
- A.17: Business Continuity → Section 10
- A.18: Compliance → Section 14

NIST Cybersecurity Framework Mapping:

- Identify (ID) → Sections 2, 13, 26
- Protect (PR) → Sections 3-8, 11-12, 15-25
- Detect (DE) → Sections 9, 27, 28
- Respond (RS) → Sections 9, 10

- Recover (RC) → Sections 10, 28

Appendix B: Quick Reference Guides

Critical Security Checklist - Executive Summary

Daily Security Tasks:

- ☐ Review security dashboard
- ☐ Check critical alerts
- ☐ Verify backup completion
- ☐ Review access requests
- ☐ Monitor threat intelligence

Weekly Security Tasks:

- ☐ Vulnerability scan review
- ☐ Patch status check
- ☐ Security metrics review
- ☐ Incident post-mortems
- ☐ Team status meeting

Monthly Security Tasks:

- ☐ Security awareness metrics
- ☐ Compliance status review
- ☐ Third-party risk review
- ☐ Security project status
- ☐ Budget review

Quarterly Security Tasks:

- ☐ Risk assessment update
- ☐ Policy review cycle
- ☐ Tabletop exercise
- ☐ Vendor assessments
- ☐ Security training

Annual Security Tasks:

- ☐ Security audit
- ☐ Penetration testing
- ☐ Disaster recovery test
- ☐ Policy approval
- ☐ Strategy review

Appendix C: Security Contact Information

Emergency Response Contacts

Internal Contacts:

- Security Operations Center: [24/7 Hotline]
- CISO: [Contact Information]
- Incident Response Lead: [Contact Information]
- Legal Counsel: [Contact Information]
- Public Relations: [Contact Information]

External Contacts:

- Law Enforcement: [Local FBI Cyber Division]
- Incident Response Retainer: [Vendor Contact]
- Cyber Insurance: [Policy Number and Contact]
- Critical Vendors: [Support Contacts]
- Industry ISAC: [Sector-Specific Contact]

Appendix D: Incident Response Quick Cards

Ransomware Response Card

Immediate Actions (First 15 minutes):

- ☐ Isolate affected systems
- ☐ Notify Security Operations Center
- ☐ Activate incident response team
- ☐ Begin evidence preservation
- ☐ Document all actions taken

Secondary Actions (First hour):

- ☐ Assess scope of encryption
- ☐ Check backup availability
- ☐ Notify executive management
- ☐ Engage legal counsel
- ☐ Contact cyber insurance

Do NOT:

- Power off systems (preserves encryption keys in memory)
- Pay ransom without legal/executive approval

- Communicate with attackers without law enforcement guidance
- Delete any files or logs
- Attempt recovery without forensic imaging

Appendix E: Security Tools Command Reference

Common Security Commands

Network Reconnaissance:

```
bash

# Port scanning
nmap -sS -sV -O target_ip

# DNS enumeration
dig @dns_server domain.com ANY

# Network trace
tcpdump -i eth0 -w capture.pcap
```

System Investigation:

```
bash

# Process listing with network connections
netstat -antp (Linux)
netstat -anob (Windows)

# File integrity checking
find /path -type f -exec md5sum {} \;

# Log analysis
grep -i "failed password" /var/log/auth.log
```

Incident Response:

```
bash
```

```
# Memory dump (Linux)
```

```
dd if=/dev/mem of=memory.dump
```

```
# Live system data collection
```

```
date; hostname; whoami; netstat -an; ps aux
```

```
# Isolate system
```

```
iptables -A INPUT -j DROP
```

```
iptables -A OUTPUT -j DROP
```

Appendix F: Security Resources

Continuing Education and References

Industry Resources:

- SANS Internet Storm Center: <https://isc.sans.edu>
- NIST Cybersecurity Framework: <https://www.nist.gov/cyberframework>
- OWASP: <https://owasp.org>
- CIS Controls: <https://www.cisecurity.org>
- MITRE ATT&CK: <https://attack.mitre.org>

Threat Intelligence:

- US-CERT: <https://www.us-cert.gov>
- Industry ISACs: [Sector-specific]
- Vendor security advisories
- Security research blogs
- Threat intelligence platforms

Training and Certification:

- CISSP - Certified Information Systems Security Professional
- CCSP - Certified Cloud Security Professional
- CEH - Certified Ethical Hacker
- GCIH - GIAC Certified Incident Handler
- OSCP - Offensive Security Certified Professional

Implementation Guide

Getting Started with This Checklist

Phase 1: Assessment (Months 1-2)

1. Review entire checklist
2. Identify applicable sections
3. Perform gap analysis
4. Prioritize critical gaps
5. Develop remediation timeline

Phase 2: Quick Wins (Months 2-3)

1. Implement critical controls
2. Address compliance gaps
3. Deploy missing tools
4. Update documentation
5. Begin training program

Phase 3: Systematic Implementation (Months 4-12)

1. Follow prioritized roadmap
2. Implement controls by domain
3. Validate effectiveness
4. Document procedures
5. Train staff

Phase 4: Optimization (Ongoing)

1. Regular assessments
2. Continuous improvement
3. Automation opportunities
4. Metrics refinement
5. Program maturity

Success Factors

Key Success Factors:

- Executive sponsorship and support
- Adequate budget allocation
- Skilled security team
- Organizational buy-in

- Continuous improvement mindset

Common Pitfalls to Avoid:

- Trying to implement everything at once
 - Focusing on tools over processes
 - Neglecting the human element
 - Insufficient documentation
 - Lack of testing and validation
-

Conclusion

This comprehensive security checklist represents industry best practices across all major security domains. Organizations should:

1. **Customize** - Adapt controls to your specific environment
2. **Prioritize** - Focus on highest risks first
3. **Measure** - Track progress with metrics
4. **Iterate** - Continuously improve security posture
5. **Validate** - Regular testing and assessment

Remember: Security is not a destination but a journey. This checklist provides the roadmap, but success requires ongoing commitment, resources, and vigilance.

Document Maintenance:

- Review quarterly for updates
- Annual comprehensive revision
- Incorporate lessons learned
- Update for new threats
- Align with regulation changes

For questions or suggestions regarding this checklist, contact the Chief Information Security Officer.

END OF SECURITY CHECKLIST

Total Controls: 2,500+

Domains Covered: 30

Estimated Implementation Time: 18-24 months

Estimated Full Compliance: 85-95% achievable

