AUDITREADY ENTERPRISE COMPLIANCE

Generated on Monday, September 15, 2025

EXECUTIVE SUMMARY

SELECTED FRAMEWORKS:

- ISO 27001:2022
- ISO 27002:2022
- CIS Controls IG3 v8.1

TOTAL CATEGORIES: 20 compliance domains analyzed

Coverage: Focused Analysis

UNIFIED COMPLIANCE REQUIREMENTS

Streamlined Framework Integration for Enterprise Compliance

This comprehensive compliance report presents unified requirements where multiple regulatory frameworks have been consolidated to simplify implementation across organizational departments.

Our unified approach enables:

- Streamlined compliance management across multiple standards simultaneously
- Reduced complexity through intelligently consolidated requirements
- Enhanced departmental coordination and consistent implementation
- Clear mapping between different regulatory frameworks and standards
- Simplified audit preparation with comprehensive requirement coverage

Each category on the following pages contains:

- Unified requirements combining all selected frameworks
- Clean, consolidated requirements text for efficient implementation

This approach reduces duplication and ensures comprehensive coverage while maintaining compliance with all selected standards.

CATEGORY 1 OF 20: GOVERNANCE & LEADERSHIP

CATEGORY	UNIFIED REQUIREMENTS
01. GOVERNANCE & LEADERSHIP	b) ORGANIZATIONAL STRUCTURE (ISMS Requirement: Define roles and responsibilities as part of your ISMS implementation): Establish roles, responsibilities, and reporting lines for ICT risk management with regular oversight and governance a) MANAGEMENT BODY ACCOUNTABILITY: Assign clear accountability for digital operational resilience to the management body with approved ICT strategy and risk appetite c) SCOPE AND APPLICABILITY: Determine and document DORA applicability across all relevant business activities and organizational entities d) PROPORTIONATE IMPLEMENTATION: Apply requirements proportionate to entity size, nature, scale, complexity, and risk profile while ensuring effectiveness e) REGULATORY COMPLIANCE: Maintain compliance with supervisory requirements, reporting obligations, and regulatory cooperation frameworks f) INFORMATION SHARING: Participate in vetted cyber threat information sharing arrangements with appropriate safeguards and governance

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 2 OF 20: RISK MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
02. RISK MANAGEMENT	a) ICT RISK MANAGEMENT FRAMEWORK: Implement comprehensive ICT risk management framework covering strategy, policies, assessment, and controls b) ICT SYSTEMS AND INFRASTRUCTURE: Maintain inventory and architecture of ICT assets, manage lifecycle, configuration, and capacity for operational resilience c) ASSET IDENTIFICATION AND CLASSIFICATION: Identify and classify assets and information, map critical functions to supporting technologies and dependencies d) DETECTION AND MONITORING: Deploy monitoring, logging, and alerting capabilities to identify anomalous activities and potential ICT incidents

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 3 OF 20: INVENTORY AND CONTROL OF SOFTWARE ASSETS

CATEGORY	UNIFIED REQUIREMENTS
03. INVENTORY AND CONTROL OF SOFTWARE ASSETS	a) SOFTWARE INVENTORY MANAGEMENT: Establish and maintain comprehensive inventory of ALL software assets including installed applications, versions, licenses, dependencies, and security patches. Use automated software discovery tools with agent-based and agentless scanning to capture operating systems, applications, browser plugins, and development tools. Update inventory within 24 hours of software changes and maintain 95% inventory accuracy. b) UNAUTHORIZED SOFTWARE CONTROL: Implement automated detection and removal of unauthorized software within 72 hours of discovery. Establish software allowlisting policies with defined business justification processes for new software requests. Deploy technical controls (application whitelisting, endpoint protection) to prevent unauthorized software installation. Document all software removal actions with business impact assessment. c) SOFTWARE LICENSING COMPLIANCE: Maintain comprehensive software licensing records including license types, quantities, expiration dates, and compliance status. Conduct monthly license reconciliation against installed software inventory. Establish automated alerting for license violations or approaching expiration (30-day notice). Maintain vendor relationships and license agreements with centralized license management. d) AUTOMATED SOFTWARE DISCOVERY: Deploy automated software inventory tools across all enterprise assets including workstations, servers, mobile devices, and cloud instances. Configure continuous scanning with real-time inventory updates, software change detection, and comprehensive coverage validation. Integrate discovery tools with CMDB and asset management systems for consolidated asset visibility. e) SOFTWARE ALLOWLISTING ENFORCEMENT: Implement technical controls to enforce software allowlisting including application control technologies, code signing verification, and hash-based allowlisting. Define software categories (approved, conditional, prohibited) with documented business justification. Establish change management processes for allowlist modifications with security review and approval workflows. f) SECURE SOFTWARE LIBRARIES: Maintain approved software library inventory including third-party components, open-source libraries, and development frameworks. Implement vulnerability scanning for software dependencies and components. Establish secure coding standards requiring use of approved libraries only. Monitor for library vulnerabilities and implement rapid patching for critical security issues. g) EXECUTABLE AND SCRIPT CONTROL: Control execution of scripts, macros, and executable content through technical controls and policy enforcement. Implement script execution policies restricting unauthorized PowerShell, batch files, and interpreted code execution. Deploy endpoint detection and response (EDR) solutions to monitor and control script activities. Maintain digital signing requirements for approved scripts. h) OPERATIONAL SOFTWARE CONTROL: Establish formal change management processes for software installation, modification, and removal on operational systems. Require security impact assessments for all software changes affecting production environments. Implement separation of duties between software requesters, approvers, and installers. Maintain rollback capabilities for all software deployments. i) SOFTWARE LIFECYCLE MANAGEMENT: Manage complete software lifecycle from procurement through disposal including vendor evaluation, security assessment, deployment, maintenance, and end-of-life planning. Establish software retirement procedures ensuring secure data removal and license compliance. Maintain software roadmaps with version control and upgrade planning. j) SOFTWARE SECURITY ASSESSMENT: Conduct security assessments of all software before deployment including vulnerability scanning, code review (for custom applications), and security configuration validation. Establish software security standards and acceptance criteria. Implement

CATEGORY	UNIFIED REQUIREMENTS
	continuous monitoring for software security posture and emerging threats. k) CLOUD SOFTWARE GOVERNANCE: Extend software asset management to cloud-based software including Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS) components. Monitor cloud software usage, licensing, and security configurations. Establish cloud software approval processes and shadow IT detection capabilities. l) SOFTWARE COMPLIANCE REPORTING: Generate comprehensive software compliance reports including inventory status, licensing compliance, security posture, and policy violations. Provide executive dashboards with key metrics, trends, and compliance indicators. Maintain audit trails for all software management activities and ensure regulatory compliance documentation.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 4 OF 20: INVENTORY AND CONTROL OF HARDWARE ASSETS

CATEGORY	UNIFIED REQUIREMENTS
04. INVENTORY AND CONTROL OF HARDWARE ASSETS	a) COMPREHENSIVE HARDWARE INVENTORY: Establish and maintain detailed inventory of ALL hardware assets including computers, servers, network devices, mobile devices, IoT devices, and peripheral equipment. Document hardware specifications, locations, ownership, criticality, and security classification. Use automated discovery tools with network scanning, agent-based detection, and manual verification to achieve 98% inventory accuracy with weekly updates. b) UNAUTHORIZED HARDWARE DETECTION: Implement automated detection of unauthorized hardware connections within 4 hours using network access control (NAC), endpoint detection, and physical security monitoring. Establish immediate quarantine procedures for unauthorized devices with automated network isolation. Document all unauthorized hardware incidents with investigation and remediation procedures. Deploy network monitoring tools to detect rogue devices and unauthorized connections. c) AUTOMATED ASSET DISCOVERY: Deploy comprehensive automated asset discovery tools including network scanners, DHCP monitoring, wireless access point detection, and endpoint agents. Configure continuous scanning across all network segments, VLANs, and remote locations. Integrate discovery tools with Configuration Management Database (CMDB) and asset management systems. Implement discovery tool monitoring with 24/7 coverage and real-time alerting for new device detection. d) NETWORK ACCESS CONTROL: Implement technical controls to prevent unauthorized hardware connections including 802.1X authentication, NAC solutions, port security, and wireless access controls. Configure automatic device quarantine for non-compliant or unknown devices. Establish device onboarding procedures with security validation and compliance verification. Deploy certificate-based device authentication where possible. e) ASSET LIFECYCLE MANAGEMENT: Manage complete hardware lifecycle from procurement through secure disposal including acquisition approval, deployment, maintenance, upgrades, and retirement. Establish asset tracking with unique identifiers, barcodes, or RFID tags. Implement asset transfer procedures with security validation and documentation updates. Maintain asset warranty and support contract tracking with automated renewal notifications. f) HARDWARE CLASSIFICATION AND LABELING: Implement comprehensive asset classification based on criticality, sensitivity, and business function including public, internal, confidential, and restricted classifications. Apply physical labels and digital tags to all assets. Establish handling procedures for each classification level including storage, transport, and access requirements. Maintain classification review and update procedures with annual validation. g) ASSET OWNERSHIP AND RESPONSIBILITY: Assign and document asset ownership for every hardware device including asset custodian, technical owner, and business owner responsibilities. Establish clear accountability for asset security, maintenance, and compliance. Implement asset transfer procedures with ownership updates and security validation. Maintain asset responsibility matrices with contact information and escalation procedures. h) CONTINUOUS INVENTORY AUDITING: Conduct regular physical inventory audits using barcode scanning, RFID systems, and visual verification with quarterly full audits and monthly spot checks. Implement automated inventory reconciliation with discovery tools and manual verification. Establish discrepancy investigation procedures with root cause analysis and corrective actions. Maintain audit trails with photographic evidence and location verification. i) MOBILE AND PORTABLE DEVICE CONTROL: Implement enhanced controls for mobile devices including laptops, tablets, smartphones, and USB storage devices with mobile device management (MDM), encryption requirements, and remote wipe capabilities. Establish device check-out/check-in procedures with security validation. Deploy asset tracking for portable devices using GPS or asset management software with location monitoring.

CATEGORY	UNIFIED REQUIREMENTS
	j) IoT AND EMBEDDED DEVICE MANAGEMENT: Extend asset management to Internet of Things (IoT) devices, embedded systems, and specialized equipment including industrial controls, security cameras, and building automation systems. Implement network segmentation for IoT devices with dedicated VLANs and security monitoring. Establish firmware update procedures and security configuration management for embedded devices. k) CLOUD AND VIRTUAL ASSET TRACKING: Manage cloud-based infrastructure and virtual assets including virtual machines, containers, cloud storage, and Platform-as-a-Service resources. Implement cloud asset discovery and inventory tools with cost tracking and security configuration monitoring. Establish cloud asset lifecycle management with automated provisioning and deprovisioning procedures. l) ASSET SECURITY AND COMPLIANCE: Implement security controls for all hardware assets including encryption requirements, access controls, monitoring capabilities, and compliance validation. Establish asset security baselines with configuration standards and security monitoring. Conduct regular security assessments of critical assets with vulnerability scanning and compliance checking. Maintain asset security documentation for audit and regulatory compliance.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 5 OF 20: IDENTITY & ACCESS MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
05. IDENTITY & ACCESS MANAGEMENT	a) ACCOUNT INVENTORY & LIFECYCLE: Establish and maintain comprehensive inventory of all accounts (user, administrative, service, shared) with complete lifecycle management from provisioning to deprovisioning including automated processes for joiners, movers, and leavers b) UNIQUE AUTHENTICATION: Implement unique passwords/credentials for all enterprise assets and accounts, eliminate default credentials, enforce password complexity requirements, and implement secure password storage and transmission c) ACCOUNT MANAGEMENT: Disable or delete dormant accounts after maximum 45 days of inactivity, regularly review account status, implement automated account monitoring, and maintain account ownership records d) PRIVILEGED ACCESS CONTROLS: Restrict administrator privileges to dedicated administrator accounts, implement privileged access management (PAM) solutions, control utility program usage, and monitor privileged activities e) MULTI-FACTOR AUTHENTICATION: Require MFA for all externally-exposed applications, remote network access, administrative access, and sensitive system access with support for multiple authentication factors and continuous authentication where appropriate f) ACCESS PROVISIONING: Establish formal access granting processes with proper authorization workflows, role-based access control (RBAC), principle of least privilege, and regular access reviews and certifications g) ACCESS REVOCATION: Implement automated access revocation processes for terminated employees, role changes, and expired access, with immediate revocation capabilities for emergency situations h) CENTRALIZED IDENTITY MANAGEMENT: Deploy centralized account management through directory services or identity providers with single sign-on (SSO) capabilities, identity federation, and centralized policy enforcement i) ROLE-BASED ACCESS CONTROL: Define and maintain comprehensive RBAC with documented access rights, role definitions, segregation of duties, and regular role reviews and updates j) AUTHENTICATION INFORMATION SECURITY: Secure allocation, distribution, storage, and management of authentication information with proper encryption, secure transmission, and credential recovery procedures k) ACCESS RIGHTS MANAGEMENT: Provision, review, modify, and remove access rights based on business requirements with formal approval processes and regular access certifications l) REMOTE ACCESS SECURITY: Implement specific security measures for remote working including VPN controls, device management, secure remote access protocols, and monitoring of remote activities m) PHYSICAL AND LOGICAL ACCESS INTEGRATION: Coordinate physical and logical access controls with unified access policies, visitor management, and area access restrictions

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 6 OF 20: DATA PROTECTION

CATEGORY	UNIFIED REQUIREMENTS
06. DATA PROTECTION	a) DATA CLASSIFICATION: Establish comprehensive data classification scheme with categories, handling requirements, and protection levels based on sensitivity, regulatory requirements, and business value b) CRYPTOGRAPHIC CONTROLS: Implement appropriate cryptographic controls including encryption at rest, in transit, and in processing with key management, algorithm selection, and secure implementation c) DATA LOSS PREVENTION: Deploy data loss prevention (DLP) solutions with monitoring, detection, and prevention of unauthorized data access, transmission, and storage across all channels d) DATA HANDLING PROCEDURES: Establish secure data handling procedures covering data collection, processing, storage, transmission, sharing, and disposal throughout the data lifecycle e) PRIVACY BY DESIGN: Implement privacy by design principles with data minimization, purpose limitation, consent management, and privacy impact assessments for all data processing activities f) GDPR COMPLIANCE: Ensure full GDPR compliance including lawful basis determination, data subject rights, consent mechanisms, breach notification, and data protection impact assessments g) DATA SUBJECT RIGHTS: Implement comprehensive data subject rights management including access, rectification, erasure, portability, and objection rights with automated response capabilities h) CROSS-BORDER DATA TRANSFERS: Manage international data transfers with appropriate safeguards, adequacy decisions, standard contractual clauses, and binding corporate rules i) DATA BREACH MANAGEMENT: Establish data breach response procedures including detection, assessment, notification, and remediation with regulatory reporting and stakeholder communication j) DATA RETENTION AND DISPOSAL: Implement data retention policies and secure disposal procedures with automated retention management and certified data destruction processes k) THIRD-PARTY DATA PROCESSING: Manage third-party data processing relationships with data processing agreements, due diligence, monitoring, and compliance verification l) DATA PROTECTION TRAINING: Provide comprehensive data protection training for all personnel with role-specific guidance, GDPR awareness, and privacy-conscious culture development m) TECHNICAL AND ORGANIZATIONAL MEASURES: Implement comprehensive technical and organizational measures (TOMs) ensuring appropriate security level relative to risk with regular assessment and updates

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 7 OF 20: SECURE CONFIGURATION OF HARDWARE AND SOFTWARE

CATEGORY	UNIFIED REQUIREMENTS
07. SECURE CONFIGURATION OF HARDWARE AND SOFTWARE	a) SECURE CONFIGURATION PROCESS: Establish and maintain documented secure configuration process for all enterprise assets including configuration standards, baselines, and hardening guidelines b) NETWORK INFRASTRUCTURE CONFIGURATION: Implement secure configuration process for network infrastructure with network device hardening, secure protocols, and configuration management c) AUTOMATIC SESSION SECURITY: Configure automatic session locking on all enterprise assets with appropriate timeout settings, screen savers, and session termination controls d) FIREWALL IMPLEMENTATION: Implement and manage firewalls on servers and end-user devices with rule sets, monitoring, logging, and regular configuration reviews e) MOBILE DEVICE SECURITY: Enforce automatic device lockout and remote wipe capability on portable end-user devices with mobile device management (MDM) solutions f) CONFIGURATION BASELINES: Establish and maintain secure configuration baselines for operating systems, applications, and network devices with regular baseline updates and compliance monitoring g) CONFIGURATION CHANGE MANAGEMENT: Implement formal change management for configuration modifications with approval processes, testing, and rollback procedures h) CLOUD SECURITY CONFIGURATION: Implement comprehensive security controls for cloud services including data encryption, access management, and cloud provider security assessments i) SYSTEM HARDENING: Apply system hardening measures including unnecessary service removal, port closure, default account management, and security feature enablement j) CONFIGURATION MONITORING: Continuously monitor configuration drift and unauthorized changes with automated detection, alerting, and remediation capabilities k) VULNERABILITY REMEDIATION IN CONFIGURATION: Address configuration-related vulnerabilities through systematic review, testing, and implementation of security patches and updates l) SECURE DEPLOYMENT: Implement secure deployment processes for new systems and applications with security validation, testing, and approval before production use

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 8 OF 20: VULNERABILITY MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
08. VULNERABILITY MANAGEMENT	a) VULNERABILITY MANAGEMENT PROCESS: Establish and maintain documented vulnerability management process covering identification, assessment, prioritization, remediation, and verification of vulnerabilities across all enterprise assets b) VULNERABILITY SCANNING: Perform automated vulnerability scans of internal and externally-exposed enterprise assets on at least quarterly basis (or more frequently) using SCAP-compliant vulnerability scanners with comprehensive coverage c) THREAT INTELLIGENCE: Collect, analyze, and integrate threat intelligence information to identify emerging threats, vulnerabilities, and attack patterns relevant to the organization d) PATCH MANAGEMENT PROCESS: Establish and maintain systematic remediation and patching process with defined baselines, testing procedures, and rollback capabilities for enterprise assets e) AUTOMATED OS PATCH MANAGEMENT: Implement automated operating system patch management for all enterprise assets with appropriate testing, scheduling, and deployment controls f) AUTOMATED APPLICATION PATCH MANAGEMENT: Implement automated application patch management for all enterprise software with version control, testing, and deployment procedures g) VULNERABILITY REMEDIATION: Remediate detected vulnerabilities through systematic processes and tooling on monthly or more frequent basis with risk-based prioritization and tracking h) VULNERABILITY ASSESSMENT: Conduct systematic vulnerability assessments including technical vulnerability identification, impact analysis, and risk assessment of information systems i) EXTERNAL VULNERABILITY SCANNING: Perform regular automated vulnerability scans of externally-exposed assets using qualified scanning services or tools with public-facing coverage j) VULNERABILITY REPORTING: Maintain comprehensive vulnerability reporting including status tracking, metrics, and management reporting on vulnerability posture and remediation progress k) EMERGENCY PATCHING: Establish emergency patching procedures for critical vulnerabilities with expedited testing, approval, and deployment processes l) VULNERABILITY VERIFICATION: Implement verification procedures to confirm successful remediation and validate that vulnerabilities have been properly addressed

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 9 OF 20: PHYSICAL & ENVIRONMENTAL SECURITY CONTROLS

CATEGORY	UNIFIED REQUIREMENTS
09. PHYSICAL & ENVIRONMENTAL SECURITY CONTROLS	a) PHYSICAL ACCESS CONTROL: Implement comprehensive physical access controls including perimeter security, facility access restrictions, visitor management, and area-based access controls b) SECURE AREAS AND ZONES: Establish and maintain secure areas with appropriate physical protection including restricted zones, data center security, and equipment protection areas c) EQUIPMENT PROTECTION: Protect equipment from physical and environmental threats including power protection, climate control, fire suppression, and equipment security measures d) ENVIRONMENTAL MONITORING: Implement environmental monitoring and control systems for temperature, humidity, water detection, and other environmental factors affecting information systems f) EQUIPMENT MAINTENANCE: Establish secure equipment maintenance procedures including authorized service provider access, maintenance logging, and equipment sanitization g) SECURE DISPOSAL: Implement secure disposal or reuse procedures for equipment and media containing sensitive information with data destruction and verification processes h) OFF-SITE EQUIPMENT SECURITY: Protect off-site equipment and remote working environments with appropriate physical security measures and monitoring capabilities i) CABLING SECURITY: Secure power and telecommunications cabling to protect against interception, interference, and damage with proper cable management and protection j) DELIVERY AND LOADING AREAS: Control delivery and loading areas to prevent unauthorized access to facilities and ensure secure handling of equipment and materials k) PHYSICAL SECURITY MONITORING: Implement physical security monitoring systems including surveillance, intrusion detection, and access logging with 24/7 monitoring capabilities l) EMERGENCY PROCEDURES: Establish emergency response procedures for physical security incidents including evacuation plans, emergency contacts, and business continuity measures

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 10 OF 20: NETWORK INFRASTRUCTURE MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
10. NETWORK INFRASTRUCTURE MANAGEMENT	a) NETWORK INFRASTRUCTURE MAINTENANCE: Ensure all network infrastructure components are kept up-to-date with current firmware, software patches, and security updates with documented maintenance schedules b) SECURE NETWORK ARCHITECTURE: Establish and maintain secure network architecture with network segmentation, defense-in-depth principles, and documented security zones and boundaries c) SECURE NETWORK MANAGEMENT: Implement secure management of network infrastructure using encrypted protocols, secure administrative access, and protected management interfaces d) NETWORK DOCUMENTATION: Establish and maintain comprehensive network architecture diagrams, topology documentation, and configuration records with regular updates and change tracking e) CENTRALIZED NETWORK AAA: Implement centralized network authentication, authorization, and auditing (AAA) systems for all network device access with comprehensive logging and monitoring f) SECURE COMMUNICATION PROTOCOLS: Use secure network management and communication protocols including 802.1X, WPA2/WPA3, encrypted management protocols, and secure wireless configurations g) VPN AND REMOTE ACCESS: Ensure remote devices utilize VPN connections and connect to enterprise AAA systems with strong encryption and access controls h) DEDICATED ADMINISTRATIVE RESOURCES: Establish and maintain dedicated computing resources for administrative work, either physically or logically separated from general user systems i) OT/IT NETWORK ISOLATION: Implement appropriate isolation between operational technology (OT) and information technology (IT) networks while maintaining necessary operational connectivity j) INDUSTRIAL CONTROL SYSTEM SECURITY: Secure industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems with appropriate access controls and monitoring k) DNS AND INTERNET INFRASTRUCTURE SECURITY: Implement comprehensive security measures for DNS services, internet exchange points, and other internet infrastructure components under organizational control l) NETWORK CHANGE MANAGEMENT: Implement formal change management procedures for network infrastructure modifications with testing, approval, and rollback capabilities m) NETWORK CAPACITY MANAGEMENT: Monitor and manage network capacity, performance, and availability with proactive capacity planning and performance optimization

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 11 OF 20: SECURE SOFTWARE DEVELOPMENT

CATEGORY	UNIFIED REQUIREMENTS
11. SECURE SOFTWARE DEVELOPMENT	a) SECURE DEVELOPMENT LIFECYCLE INTEGRATION: Establish comprehensive secure SDLC processes integrated into all development methodologies (Waterfall, Agile, DevOps) with security requirements definition, threat modeling, secure design reviews, and security acceptance criteria. Implement security gates at each SDLC phase with mandatory security sign-off before progression. Train development teams on secure coding practices with annual security training and competency validation. b) SECURE CODING STANDARDS AND PRACTICES: Implement comprehensive secure coding standards covering input validation, output encoding, authentication, authorization, error handling, logging, and cryptographic implementation. Establish coding guidelines for each programming language and framework used. Deploy secure coding training programs with hands-on exercises and regular security code review training. Maintain secure code libraries and approved security functions. c) SECURITY CODE REVIEW PROCESSES: Conduct mandatory security-focused code reviews for all code changes using both automated static analysis and manual review processes. Establish security review criteria with specific focus on OWASP Top 10, common vulnerabilities, and business logic flaws. Train developers on security review techniques and maintain security-focused code review checklists. Implement peer review requirements with security champion involvement. d) AUTOMATED SECURITY TESTING INTEGRATION: Implement comprehensive application security testing including Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), Interactive Application Security Testing (IAST), and Software Composition Analysis (SCA) integrated into CI/CD pipelines. Configure automated security testing to run on every code commit with build failure for critical security issues. Maintain security testing tool management with regular signature updates. e) SECURE DEPLOYMENT AND CONFIGURATION: Establish secure deployment processes including environment hardening, secure configuration management, secrets management, and deployment validation testing. Implement infrastructure-as-code with security configuration templates and automated compliance checking. Deploy container security scanning for containerized applications and implement secure orchestration platforms. Maintain deployment security checklists and validation procedures. f) DEPENDENCY AND THIRD-PARTY SECURITY: Implement comprehensive third-party component security management including Software Bill of Materials (SBOM) generation, vulnerability scanning of dependencies, license compliance checking, and supply chain security validation. Establish approved component libraries with regular security assessments. Deploy automated dependency update processes with security patch prioritization. Maintain vendor security assessment procedures for commercial components. g) PENETRATION TESTING AND SECURITY VALIDATION: Conduct comprehensive application penetration testing by qualified security professionals including black-box, white-box, and gray-box testing methodologies. Perform security validation testing throughout the development lifecycle with threat-based testing scenarios. Implement red team exercises for critical applications with comprehensive attack simulation. Maintain penetration testing schedules based on application risk and criticality. h) APPLICATION SECURITY MONITORING: Implement runtime application security monitoring including application performance monitoring (APM) with security instrumentation, runtime application self-protection (RASP), and Web Application Firewalls (WAF) with custom rule development. Deploy security logging and monitoring for application security events with SIEM integration. Establish application security incident response procedures with automated threat detection. i) SECURITY REQUIREMENTS AND THREAT MODELING: Establish comprehensive security

CATEGORY	UNIFIED REQUIREMENTS
	requirements gathering processes including business security requirements, technical security controls, and compliance requirement integration. Conduct threat modeling exercises using structured methodologies (STRIDE, PASTA, LINDDUN) with threat landscape analysis and attack vector identification. Maintain security requirement traceability throughout the development lifecycle. j) SECURE ARCHITECTURE AND DESIGN: Implement secure architecture design processes including security architecture reviews, design pattern security validation, and architectural threat assessment. Establish security architecture principles including defense-in-depth, least privilege, fail-safe defaults, and complete mediation. Deploy reference security architectures for common application patterns with security control integration guidance. k) SECURITY TESTING AND QUALITY ASSURANCE: Establish comprehensive security testing programs including unit security testing, integration security testing, and system security testing with automated and manual testing procedures. Implement security test case development with negative testing scenarios and boundary condition validation. Deploy security testing frameworks with test data management and security test environment controls. l) CONTINUOUS SECURITY IMPROVEMENT: Implement continuous security improvement processes including security metrics collection, vulnerability trend analysis, security debt management, and security practice maturity assessment. Establish security champion programs with developer security training and mentoring. Deploy security feedback loops with post-incident security enhancement and lessons learned integration.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 12 OF 20: NETWORK MONITORING & DEFENSE

CATEGORY	UNIFIED REQUIREMENTS
12. NETWORK MONITORING & DEFENSE	a) NETWORK SEGMENTATION AND SECURE ARCHITECTURE: Implement comprehensive network segmentation with micro-segmentation capabilities, zero-trust network architecture principles, and software-defined perimeter (SDP) technologies. Deploy network access control (NAC) with device authentication, VLAN assignment, and policy enforcement. Establish security zones including DMZ, internal networks, management networks, and guest networks with strict inter-zone communication controls and monitoring. b) FIREWALL AND SECURITY CONTROL MANAGEMENT: Deploy and maintain next-generation firewalls (NGFW) with application awareness, intrusion prevention, URL filtering, and advanced threat protection capabilities. Implement firewall rule management with least-privilege principles, regular rule reviews (quarterly), and automated rule optimization. Deploy web application firewalls (WAF) for web-based applications with custom rule development and OWASP Top 10 protection. c) SECURE REMOTE ACCESS AND VPN: Establish comprehensive secure remote access solutions including zero-trust VPN, multi-factor authentication, device compliance checking, and session monitoring capabilities. Deploy secure remote desktop solutions with jump servers, privileged access management (PAM), and session recording. Implement remote access policy enforcement with user behavior analytics and anomaly detection. d) WIRELESS NETWORK SECURITY CONTROLS: Implement enterprise-grade wireless security with WPA3 encryption, certificate-based authentication, rogue access point detection, and wireless intrusion prevention systems (WIPS). Deploy wireless network segmentation with guest network isolation, BYOD management, and device classification. Establish wireless security monitoring with RF analysis and threat detection capabilities. e) NETWORK DOCUMENTATION AND CONFIGURATION MANAGEMENT: Maintain comprehensive network documentation including topology diagrams, IP address management (IPAM), configuration baselines, and change management procedures. Implement network configuration management with automated backups, version control, and compliance monitoring. Deploy network discovery tools with asset inventory integration and configuration drift detection. f) NETWORK ACCESS CONTROL AND AUTHENTICATION: Deploy comprehensive network access control (NAC) solutions with 802.1X authentication, device profiling, policy enforcement, and quarantine capabilities. Implement network authentication integration with Active Directory, RADIUS, and certificate-based authentication. Establish device onboarding procedures with security validation and compliance checking. g) ADVANCED NETWORK MONITORING AND ANALYSIS: Deploy comprehensive network monitoring tools including network traffic analysis (NTA), flow monitoring, packet capture capabilities, and bandwidth monitoring with performance and security analytics. Implement network behavior analysis with machine learning and artificial intelligence for anomaly detection. Deploy network forensics capabilities with full packet capture and analysis tools. h) INTRUSION DETECTION AND PREVENTION SYSTEMS: Implement comprehensive network-based intrusion detection and prevention systems (NIDS/NIPS) with signature-based and behavioral analysis capabilities, threat intelligence integration, and automated response capabilities. Deploy host-based intrusion detection systems (HIDS) with file integrity monitoring, log analysis, and system behavior monitoring. Configure IDPS with custom rules and tuning for organization-specific threats. i) NETWORK TRAFFIC ANALYSIS AND LOGGING: Establish comprehensive network traffic analysis including flow analysis, deep packet inspection (DPI), encrypted traffic analysis, and metadata extraction with centralized logging and long-term retention (minimum 90 days). Implement network traffic baseline establishment with anomaly detection and trend analysis. Deploy network traffic correlation with security event analysis and incident response integration.

CATEGORY	UNIFIED REQUIREMENTS
	j) NETWORK-BASED MALWARE DETECTION: Deploy network-based malware detection capabilities including sandbox analysis, reputation-based filtering, command-and-control (C2) communication detection, and data exfiltration prevention. Implement DNS filtering and monitoring with malicious domain blocking and DNS tunneling detection. Deploy network-based threat intelligence with indicator of compromise (IoC) integration and automated blocking. k) NETWORK SECURITY MONITORING AND SOC INTEGRATION: Establish comprehensive network security monitoring with Security Operations Center (SOC) integration, 24/7 monitoring capabilities, and incident response coordination. Implement network security event correlation with SIEM integration, automated alerting, and escalation procedures. Deploy threat hunting capabilities with proactive threat detection and investigation procedures. l) NETWORK FORENSICS AND INCIDENT RESPONSE: Develop comprehensive network forensics capabilities including packet capture analysis, network timeline reconstruction, and evidence preservation procedures with legal admissibility requirements. Implement network incident response procedures with network isolation, traffic analysis, and attack vector identification. Deploy network-based indicators of compromise (IoC) with automated detection and response capabilities. m) THREAT INTELLIGENCE AND NETWORK SECURITY: Integrate comprehensive threat intelligence feeds with network security tools including threat intelligence platforms (TIP), automated indicator sharing, and contextual threat analysis. Implement threat intelligence-driven security with proactive defense measures and predictive analytics. Deploy threat intelligence correlation with network monitoring and incident response integration. n) NETWORK SECURITY EVENT CORRELATION: Establish advanced security event correlation capabilities with machine learning and artificial intelligence for pattern recognition, anomaly detection, and automated threat detection across multiple network security tools and data sources. Implement correlation rule development with custom logic and business-specific threat scenarios. Deploy automated response capabilities with security orchestration and automated response (SOAR) integration. o) NETWORK SECURITY ASSESSMENT AND VALIDATION: Conduct regular network security assessments including penetration testing, vulnerability scanning, configuration reviews, and security architecture validation with external and internal testing capabilities. Implement continuous network security validation with automated testing tools and manual verification procedures. Deploy network security metrics with key performance indicators (KPIs) and security posture measurement.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 13 OF 20: SUPPLIER & THIRD-PARTY RISK MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
13. SUPPLIER & THIRD-PARTY RISK MANAGEMENT	a) THIRD-PARTY RISK INTEGRATION: Integrate ICT third-party risk into overall risk management framework with comprehensive governance b) SERVICE PROVIDER REGISTER: Maintain register of ICT services using standard templates with detailed provider information c) CONCENTRATION RISK ASSESSMENT: Assess entity-level concentration risk and implement mitigations to avoid undue concentration d) CONTRACTUAL PROVISIONS: Include key contractual clauses addressing service levels, security, audit rights, and termination procedures e) CRITICAL PROVIDER OVERSIGHT: Monitor and engage with oversight framework for critical ICT third-party service providers f) CONTINUITY AND EXIT PLANNING: Manage continuity planning and exit strategies including data portability and service transition

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 14 OF 20: SECURITY AWARENESS & SKILLS TRAINING

CATEGORY	UNIFIED REQUIREMENTS
14. SECURITY AWARENESS & SKILLS TRAINING	a) SECURITY AWARENESS PROGRAM: Establish and maintain comprehensive security awareness program with regular training schedules, content updates, and effectiveness measurement across all organizational levels b) SOCIAL ENGINEERING TRAINING: Train all workforce members to recognize and respond to social engineering attacks including phishing, pretexting, tailgating, and other manipulation techniques c) AUTHENTICATION BEST PRACTICES: Provide comprehensive training on authentication best practices including password management, multi-factor authentication, secure credential handling, and account security d) DATA HANDLING TRAINING: Train workforce members on data handling best practices including data classification, data protection, secure data transmission, and data lifecycle management e) UNINTENTIONAL DATA EXPOSURE PREVENTION: Educate users on causes and prevention of unintentional data exposure including data loss prevention, secure file sharing, and privacy protection measures f) SECURITY INCIDENT RECOGNITION: Train workforce members on recognizing and reporting security incidents with clear procedures, escalation paths, and incident classification guidelines g) SECURITY UPDATE AWARENESS: Train workforce on identifying and reporting missing security updates on enterprise assets with proper procedures for security maintenance and vulnerability reporting h) SECURE NETWORK USAGE: Educate workforce on dangers of connecting to and transmitting enterprise data over insecure networks with guidance on secure connectivity and data protection i) ROLE-SPECIFIC SECURITY TRAINING: Conduct specialized security awareness and skills training tailored to specific roles, responsibilities, and risk profiles within the organization j) CYBER HYGIENE PRACTICES: Implement basic cyber hygiene practices and cybersecurity training covering fundamental security behaviors, digital safety, and security-conscious culture development k) TRAINING EFFECTIVENESS MEASUREMENT: Establish metrics and assessment methods to measure training effectiveness, knowledge retention, and behavioral change through testing and simulation l) CONTINUOUS SECURITY EDUCATION: Provide ongoing security education and awareness activities including newsletters, briefings, alerts, and refresher training to maintain security consciousness m) SPECIALIZED PERSONNEL TRAINING: Ensure personnel with elevated access or security responsibilities receive appropriate specialized information security education and skills development

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 15 OF 20: BUSINESS CONTINUITY & DISASTER RECOVERY MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
15. BUSINESS CONTINUITY & DISASTER RECOVERY MANAGEMENT	a) BACKUP AND RECOVERY PROCEDURES: Define, operate, and verify backup, restoration, and recovery methods for systems and data b) INCIDENT RESPONSE PLANS: Establish ICT incident response and recovery plans with roles, procedures, and escalation paths c) BUSINESS CONTINUITY PLANNING: Maintain business continuity plans that support timely restoration and continuity objectives d) LEARNING AND IMPROVEMENT: Conduct post-incident reviews, integrate lessons learned, and provide mandatory awareness training

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 16 OF 20: INCIDENT RESPONSE MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
16. INCIDENT RESPONSE MANAGEMENT	a) INCIDENT MANAGEMENT PROCESS: Operate end-to-end ICT incident management from detection to closure with documentation and analysis b) INCIDENT CLASSIFICATION: Classify ICT incidents and cyber threats using consistent criteria and materiality thresholds c) INCIDENT REPORTING: Report major ICT incidents to competent authorities using prescribed formats and timelines d) COMMUNICATION PROCESSES: Establish internal and external crisis communication to inform stakeholders during disruptions e) HARMONIZED REPORTING: Use standardized content and templates for incident notifications and reports f) SUPERVISORY FEEDBACK: Review and implement supervisory feedback on reported incidents and required improvements

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 17 OF 20: MALWARE DEFENSES

CATEGORY	UNIFIED REQUIREMENTS
17. MALWARE DEFENSES	a) COMPREHENSIVE ANTI-MALWARE DEPLOYMENT: Deploy and maintain enterprise-grade anti-malware software on ALL enterprise assets including workstations, servers, mobile devices, and email systems with centrally managed solutions providing real-time protection, behavioral analysis, and machine learning detection capabilities. Implement endpoint detection and response (EDR) solutions with advanced threat hunting capabilities. Configure anti-malware with heuristic analysis, sandboxing, and zero-day protection mechanisms. b) AUTOMATED SIGNATURE AND DEFINITION UPDATES: Configure anti-malware software for automatic signature updates with multiple daily update cycles (minimum every 4 hours) and emergency update capabilities for critical threats. Implement update verification procedures ensuring successful deployment across all endpoints with automated rollback capabilities for problematic updates. Deploy threat intelligence feeds and community-based threat information sharing to enhance detection capabilities. c) REAL-TIME PROTECTION AND MONITORING: Enable comprehensive real-time scanning and monitoring including file system monitoring, network traffic analysis, email attachment scanning, web download inspection, and USB/removable media scanning with immediate threat quarantine and user notification. Deploy behavioral analysis engines to detect unknown malware and advanced persistent threats (APTs) with machine learning and artificial intelligence capabilities. d) MALWARE INCIDENT RESPONSE PROCEDURES: Establish comprehensive malware incident response procedures including immediate isolation protocols, forensic evidence preservation, malware analysis procedures, and system restoration processes with detailed incident documentation and reporting requirements. Implement automated incident response workflows with security orchestration and automated response (SOAR) capabilities. Deploy incident classification with severity-based response procedures. e) EMAIL AND WEB MALWARE FILTERING: Implement advanced email security gateways with multi-layer malware filtering including attachment scanning, URL reputation checking, sandboxing analysis, and phishing protection with real-time threat intelligence integration. Deploy web security solutions with URL filtering, download protection, and browser isolation capabilities. Configure DNS filtering to block malicious domains and command-and-control communications. f) COMPREHENSIVE SYSTEM SCANNING: Conduct regular comprehensive malware scans including full system scans (weekly), quick scans (daily), and on-demand scanning capabilities with scheduled scanning during off-hours and scan result monitoring. Implement memory scanning, rootkit detection, and boot sector analysis with custom scanning policies based on system criticality and threat landscape. Deploy network-based malware scanning for encrypted traffic analysis. g) USER TRAINING AND AWARENESS: Provide comprehensive malware awareness training covering malware identification, social engineering tactics, safe computing practices, and incident reporting procedures with role-specific training and simulated phishing exercises. Implement security awareness measurement with user behavior analytics and training effectiveness assessment. Deploy just-in-time training triggered by risky user behavior or security events. h) CENTRALIZED MALWARE MANAGEMENT: Maintain centralized management of all anti-malware solutions with unified policy management, centralized reporting and analytics, and coordinated threat response capabilities across all enterprise assets. Implement malware dashboard with real-time threat status, infection statistics, and trend analysis. Deploy automated policy enforcement with compliance monitoring and remediation workflows. i) ADVANCED THREAT PROTECTION: Deploy advanced threat protection capabilities including threat intelligence integration, advanced persistent threat (APT) detection, fileless malware detection, and supply chain attack protection with behavioral analysis and anomaly detection. Implement threat hunting capabilities with proactive threat detection and investigation procedures. Deploy deception technologies and honeypots for early threat detection.

CATEGORY	UNIFIED REQUIREMENTS
	j) MOBILE DEVICE MALWARE PROTECTION: Extend malware protection to mobile devices with mobile device management (MDM) integration, mobile application management (MAM), and mobile threat defense (MTD) solutions covering iOS and Android platforms. Implement mobile-specific threat detection including malicious app detection, network-based attacks, and device compromise indicators. Deploy secure mobile app distribution with app whitelisting and malware scanning. k) CLOUD AND VIRTUAL ENVIRONMENT PROTECTION: Implement malware protection for cloud environments and virtualized infrastructure including virtual machine (VM) scanning, container security, and cloud-native security solutions with API-based protection and serverless security. Deploy cloud workload protection platforms (CWPP) with runtime protection and compliance monitoring. Implement cloud-specific threat detection for cloud-native attacks and misconfigurations. l) MALWARE ANALYSIS AND INTELLIGENCE: Establish malware analysis capabilities including static and dynamic analysis, reverse engineering procedures, and threat intelligence development with internal analysis capabilities or external service integration. Deploy malware sandboxing and analysis platforms with automated analysis workflows and threat intelligence sharing. Implement indicators of compromise (IoC) management with threat hunting integration and attribution analysis.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 18 OF 20: EMAIL & WEB BROWSER PROTECTIONS

CATEGORY	UNIFIED REQUIREMENTS
18. EMAIL & WEB BROWSER PROTECTIONS	a) SUPPORTED WEB BROWSER AND EMAIL CLIENT MANAGEMENT: Deploy and maintain only fully supported, up-to-date web browsers and email clients with automated patch management, version control, and end-of-life tracking. Establish browser and email client standards with approved software lists, configuration baselines, and security hardening guidelines. Implement centralized software deployment with automatic updates enabled and security configuration enforcement. Remove unsupported software within 30 days of end-of-support notifications. b) DNS FILTERING AND SECURITY SERVICES: Implement comprehensive DNS filtering services for all enterprise assets including malicious domain blocking, command-and-control (C2) communication prevention, DNS over HTTPS (DoH) protection, and DNS tunneling detection. Deploy DNS security services with threat intelligence integration, real-time reputation checking, and category-based filtering with policy enforcement. Configure DNS logging and monitoring with anomaly detection and incident response integration. c) NETWORK-BASED URL FILTERING: Deploy and maintain comprehensive network-based URL filtering policies covering malicious sites, inappropriate content, and business-use restrictions with real-time URL reputation checking and category-based filtering. Implement SSL inspection capabilities for encrypted web traffic with certificate validation and privacy protection. Configure bypass procedures for legitimate business needs with approval workflows and monitoring controls. d) EMAIL SECURITY GATEWAY PROTECTION: Deploy comprehensive email security gateways with multi-layer protection including anti-spam filtering, anti-malware scanning, advanced threat protection, attachment sandboxing, and URL rewriting for link protection. Implement email authentication protocols (SPF, DKIM, DMARC) with policy enforcement and monitoring. Deploy email encryption capabilities with key management and secure message delivery systems. e) WEB APPLICATION FIREWALL DEPLOYMENT: Implement Web Application Firewalls (WAF) for all web-based applications with application-specific rule sets, OWASP Top 10 protection, DDoS mitigation capabilities, and API security protection. Configure WAF with automated rule updates, threat intelligence integration, and custom rule development for application-specific threats. Deploy WAF monitoring with attack detection, incident response, and security analytics integration. f) SECURE EMAIL COMMUNICATIONS: Configure comprehensive email encryption and digital signatures including end-to-end encryption for sensitive communications, S/MIME or PGP implementation, certificate management, and secure key distribution. Implement email data loss prevention (DLP) with content inspection, policy enforcement, and automated classification. Deploy email archiving and retention systems with legal hold capabilities and compliance monitoring. g) WEB AND EMAIL SECURITY TRAINING: Provide comprehensive user training on safe web browsing and email handling practices including phishing recognition, social engineering awareness, safe link clicking procedures, and secure file handling with regular training updates and effectiveness measurement. Implement simulated phishing exercises with user behavior tracking and targeted training. Deploy security awareness messaging and real-time coaching systems. h) TRAFFIC MONITORING AND THREAT DETECTION: Deploy comprehensive monitoring of web and email traffic for security threats including behavioral analysis, anomaly detection, advanced persistent threat (APT) detection, and data exfiltration prevention. Implement Security Information and Event Management (SIEM) integration with correlation rules and automated alerting. Deploy threat hunting capabilities with proactive threat detection and investigation procedures. i) BROWSER SECURITY HARDENING: Implement comprehensive browser security hardening including security policy enforcement, extension management, download protection, and cookie security with centralized browser configuration management. Deploy browser isolation technologies for high-risk web browsing with virtualized browsing environments. Configure browser security settings including script blocking, plugin management, and certificate validation with user override controls where appropriate.

CATEGORY	UNIFIED REQUIREMENTS
	j) EMAIL FLOW SECURITY AND AUTHENTICATION: Implement comprehensive email flow security including mail transfer agent (MTA) hardening, transport layer security (TLS) enforcement, and email authentication verification with sender policy framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) policies. Deploy email security monitoring with message flow analysis, authentication failure tracking, and spoofing detection. k) ADVANCED WEB THREAT PROTECTION: Deploy advanced web threat protection capabilities including zero-day exploit protection, drive-by download prevention, malvertising protection, and browser exploit mitigation with real-time threat intelligence integration. Implement web reputation services with dynamic risk assessment and automated blocking of malicious sites. Deploy sandboxing technologies for suspicious web content analysis and threat investigation. l) CLOUD EMAIL AND WEB SECURITY: Extend email and web security controls to cloud-based services including cloud email security (Office 365, G Suite), cloud web security, and Software-as-a-Service (SaaS) application protection with API-based security integration. Implement cloud access security broker (CASB) solutions with data protection, threat protection, and compliance monitoring. Deploy cloud-native security services with centralized policy management and unified threat protection.

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

CATEGORY 19 OF 20: PENETRATION TESTING

CATEGORY	UNIFIED REQUIREMENTS
19. PENETRATION TESTING	a) TESTING PROGRAMME: Maintain risk-based testing programme covering people, processes, and technology with suitable independence b) ICT SYSTEM TESTING: Perform regular testing including vulnerability assessments, configuration reviews, and scenario testing c) THREAT-LED PENETRATION TESTING: Conduct TLPT on live production environments for critical functions at least every three years d) QUALIFIED TESTERS: Engage qualified, independent testers under clear rules of engagement protecting operations and data

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

- Comprehensive policy documentation
- Documented security procedures
- Adequate resource allocation
- Staff training and awareness
- Management approval processes

ADVANCED CONTROLS

- Continuous monitoring systems
- Regular security reviews
- Integrated business processes
- Performance metrics & KPIs
- Automated control validation

IMPLEMENTATION TRACKING

- Systematic implementation monitoring
- Complete requirement coverage
- Regular gap analysis
- Documented corrective actions
- Continuous improvement tracking

IMPLEMENTATION GUIDE

- Phase over 6-12 months
- Start with foundational controls
- Build monitoring capabilities
- Implement automation gradually
- Measure and demonstrate value

CATEGORY 20 OF 20: AUDIT LOG MANAGEMENT

CATEGORY	UNIFIED REQUIREMENTS
20. AUDIT LOG MANAGEMENT	a) AUDIT LOG COLLECTION: Implement comprehensive audit log collection and management for all systems, applications, networks, and security devices with centralized logging infrastructure b) LOG MONITORING AND ANALYSIS: Establish continuous monitoring and analysis of audit logs with automated correlation, alerting, and anomaly detection capabilities c) LOG RETENTION AND ARCHIVAL: Implement appropriate log retention policies and secure archival procedures meeting regulatory requirements and business needs with long-term storage management d) LOG INTEGRITY PROTECTION: Ensure audit log integrity through cryptographic protection, access controls, and tamper-evident storage with digital signatures and hash verification e) CENTRALIZED LOG MANAGEMENT: Deploy centralized log management systems with log aggregation, normalization, and correlation across all enterprise assets and security tools f) SECURITY EVENT CORRELATION: Implement security event correlation and SIEM capabilities to identify security incidents, threats, and compliance violations through log analysis g) LOG ACCESS CONTROLS: Establish strict access controls for audit logs with role-based permissions, privileged access monitoring, and audit trail for log access activities h) COMPLIANCE REPORTING: Generate compliance reports and audit trails from log data to support regulatory requirements, internal audits, and security assessments i) LOG BACKUP AND RECOVERY: Implement secure backup and recovery procedures for audit logs with disaster recovery capabilities and business continuity planning j) REAL-TIME ALERTING: Configure real-time alerting for critical security events, policy violations, and suspicious activities detected in audit logs k) LOG STANDARDIZATION: Establish log format standardization and normalization procedures to ensure consistent log data across different systems and applications l) PERFORMANCE OPTIMIZATION: Optimize log management performance with efficient storage, indexing, search capabilities, and resource management for large-scale log processing

IMPLEMENTATION SCORECARD

OPERATIONAL EXCELLENCE INDICATORS

Track these metrics to demonstrate audit readiness

FOUNDATIONAL CONTROLS

Comprehensive policy documentation

Documented security procedures

Adequate resource allocation

Staff training and awareness

Management approval processes

ADVANCED CONTROLS

Continuous monitoring systems

Regular security reviews

Integrated business processes

Performance metrics & KPIs

Automated control validation

IMPLEMENTATION TRACKING

Systematic implementation monitoring

Complete requirement coverage

Regular gap analysis

Documented corrective actions

Continuous improvement tracking

IMPLEMENTATION GUIDE

Phase over 6-12 months

Start with foundational controls

Build monitoring capabilities

Implement automation gradually

Measure and demonstrate value

COMPLIANCE ANALYTICS DASHBOARD

Framework	Mapped Categories	Coverage %	Status
ISO 27001:2022	0	0%	Needs Review
ISO 27002:2022	0	0%	Needs Review
CIS Controls IG3 v8.1	0	0%	Needs Review

EXECUTIVE RECOMMENDATIONS

- Prioritize categories with multi-framework coverage for maximum compliance ROI
- Focus implementation efforts on areas with highest regulatory impact
- Establish continuous monitoring for all mapped compliance requirements
- Schedule quarterly reviews to maintain compliance posture effectiveness