SECURITY LEADERSHIP FRAMEWORK

CISO Master Checklist

A comprehensive security leadership framework covering 243 controls across 16 domains. Mapped to ISO 27001:2022, NIST CSF 2.0, NIS2, DORA, ISO 27701:2025, ISO 42001:2023, and the EU AI Act. All controls sorted by severity: Critical first, then High, then Medium.

243	16	8+	3
CONTROLS	DOMAINS	FRAMEWORKS	PRIORITY LEVELS

ISO 27001:2022 · NIST CSF 2.0 · ISO 27701:2025 · ISO 42001:2023 · NIS2 · DORA · CIS Controls v8 · EU AI Act · GDPR · MITRE ATT&CK · PCI DSS 4.0.1 · GCC Regional Laws · NIST AI RMF

INTRODUCTION

Building a Security Programme That Actually Works

Security leadership has never been more demanding. CISOs today are expected to navigate an expanding threat landscape, a growing web of global regulations, rapid cloud and AI adoption, and board rooms that require clear, business aligned reporting. The CISO Master Checklist was created to give security leaders a single, practical reference that cuts through the noise.

This framework consolidates the most critical controls from internationally recognised security standards into one actionable document. Whether you are building a security programme from the ground up, preparing for an ISO 27001 audit, responding to NIS2 obligations, implementing ISO 42001 AI management, or presenting a board level security strategy, this checklist provides the structure to move forward with confidence.

Each control is sorted by severity within its domain so you always address the most urgent items first. Controls are grouped Critical, then High, then Medium, with a visual divider between each group. Every control is mapped to its source framework for direct use in audit evidence and board papers.

Who This Is For

Designed for CISOs, Security Directors, vCISOs, IT Directors, and senior security professionals responsible for enterprise security programmes across industries and geographies.

How to Use It

Work through each domain starting with Critical controls. Check off completed items and note gaps. Use the framework references to connect each control back to its regulatory requirement for audit evidence.

What You Will Get

A clear picture of your current security posture, a prioritised list of gaps, and a structured basis for your security roadmap, board reporting, and budget justification.

Keeping It Current

Reassess all controls quarterly and after any major security incident, regulatory update, or significant change to your technology environment.

SEVERITY LEVELS — SORTING ORDER

1 — CRITICAL

Address immediately. Represents material risk. Remediate within 30 days and escalate to board if resource constrained. Listed first in every domain.

2 — HIGH

Important controls to address in the near term. Include in your 90 day security roadmap with clear ownership and timelines. Listed second.

3 — MEDIUM

Good practice controls for a mature security programme. Plan into your annual security strategy and budget cycle. Listed last.

RECOMMENDED ASSESSMENT APPROACH

1. **Initial Assessment (Weeks 1 to 2):** Work through all Critical controls across all domains first. Mark each as Complete, In Progress, or Not Started.
2. **Gap Analysis (Week 3):** Compile all incomplete items into a prioritised remediation roadmap with assigned owners, timelines, and cost estimates.
3. **Board Presentation (Week 4):** Present your gap analysis and 90 day remediation plan to leadership with supporting resource and budget requirements.
4. **Quarterly Review (Ongoing):** Reassess all controls every quarter, updating completion status and incorporating new threat intelligence or regulatory changes.

CONTENTS

Table of Contents

DOMAIN 01 OF 16

Governance, Risk and Compliance

6 Critical 7 High 2 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Establish and document an information security governance framework aligned to business objectives ISO 27001:2022 Cl.5 / NIST CSF GV.OC	CRITICAL
☐	2	Define, approve, and communicate security policies, standards, and procedures across the organisation NIST CSF GV.PO / ISO 27001 A.5.1	CRITICAL
☐	3	Align the security strategy with business objectives and formally document the organisational risk appetite ISO 27001:2022 Cl.4.1 / NIST CSF GV.OC	CRITICAL
☐	4	Conduct annual security risk assessments using an accepted methodology such as ISO 27005 or NIST ISO 27001:2022 Cl.6.1 / ISO 27005:2022	CRITICAL
☐	5	Maintain a risk register that includes treatment plans, risk owners, and regular review dates NIST CSF ID.RA / ISO 27001 Cl.6.1.2	CRITICAL
☐	6	Implement a regulatory compliance tracking programme covering GDPR, PDPL, NCA, and all applicable laws NIS2 / DORA / GDPR Art.5 / GCC Laws	CRITICAL
HIGH CONTROLS			
☐	7	Establish board level security oversight with a defined reporting cadence of at least quarterly NIS2 Art.20 / DORA Art.5 / ISO 27001 Cl.5.1	HIGH
☐	8	Define a RACI matrix for all security functions and ensure accountability is assigned to named individuals ISO 27001:2022 Cl.5.3 / NIST CSF GV.RR	HIGH
☐	9	Integrate information security risk management with the enterprise risk management framework ISO 27005:2022 / NIST RMF	HIGH
☐	10	Establish Key Risk Indicators and build leadership dashboards to track the security risk posture over time NIST CSF GV.RM / ISO 27001 Cl.9.1	HIGH
☐	11	Schedule internal and external security audits with documented scope, findings, and remediation tracking ISO 27001:2022 Cl.9.2 / NIS2 Art.21	HIGH

DOMAIN 01 OF 16 — CONTINUED

Governance, Risk and Compliance

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Maintain a centralised evidence repository for all compliance artefacts and audit logs ISO 27001:2022 Cl.7.5 / DORA Art.12	HIGH
☐	13	Align the security programme to at least one major framework such as ISO 27001, NIST CSF, or CIS Controls v8 Multi-framework alignment	HIGH
		MEDIUM CONTROLS	
☐	14	Review and formally update all security policies annually and after every significant security incident ISO 27001:2022 Cl.9.3 / NIST CSF GV.PO	MEDIUM
☐	15	Establish a formal exception management process for policy deviations with documented approvals and time limits CIS Controls v8 / ISO 27001 A.5.1	MEDIUM

DOMAIN 02 OF 16

Identity and Access Management

7 Critical 7 High 1 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement multi-factor authentication for all privileged accounts without any exceptions CIS Control 6 / NIS2 Art.21 / NIST SP 800-63B	CRITICAL
☐	2	Deploy multi-factor authentication across all remote access methods and cloud service portals NIST SP 800-63B / ISO 27001 A.8.5	CRITICAL
☐	3	Establish a Privileged Access Management solution to control, monitor, and audit all privileged sessions CIS Control 5 / ISO 27001 A.8.2	CRITICAL
☐	4	Conduct quarterly user access reviews and certifications across all critical systems and applications ISO 27001 A.5.18 / CIS Control 6.7	CRITICAL
☐	5	Enforce the principle of least privilege consistently across all systems, applications, and cloud environments CIS Control 6.8 / ISO 27001 A.8.2	CRITICAL
☐	6	Enforce a password policy requiring a minimum of 14 characters, complexity, and no reuse across last 12 passwords NIST SP 800-63B / CIS Control 5.2	CRITICAL
☐	7	Monitor and alert on all privileged account activity in real time using a SIEM or dedicated PAM tooling NIST CSF DE.AE / CIS Control 8.5	CRITICAL
HIGH CONTROLS			
☐	8	Implement Zero Trust Architecture principles starting with identity verification for every access request NIST SP 800-207 / ISO 27001 A.8.3	HIGH
☐	9	Implement a role-based access control framework with clearly defined roles mapped to business functions ISO 27001 A.5.15 / NIST SP 800-53 AC-2	HIGH
☐	10	Automate the joiner, mover, and leaver process to ensure access is provisioned and revoked consistently ISO 27001 A.6.1 / CIS Control 6	HIGH
☐	11	Deploy Single Sign-On for enterprise applications to reduce password fatigue and improve audit trail quality CIS Control 12 / ISO 27001 A.8.5	HIGH

DOMAIN 02 OF 16 — CONTINUED

Identity and Access Management

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Implement an Identity Governance and Administration platform to manage access lifecycle at scale ISO 27001 A.5.18 / NIST SP 800-53	HIGH
☐	13	Establish a service account management policy including documentation, ownership, and regular rotation CIS Control 5.4 / ISO 27001 A.5.17	HIGH
☐	14	Identify and disable all dormant accounts that have been inactive for more than 30 days CIS Control 5.3 / ISO 27001 A.5.18	HIGH
		MEDIUM CONTROLS	
☐	15	Implement just-in-time access for sensitive systems to reduce standing privilege exposure NIST SP 800-207 / Zero Trust Principles	MEDIUM

DOMAIN 03 OF 16

Network and Infrastructure Security

7 Critical 8 High

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement network segmentation and micro-segmentation to limit lateral movement in the event of a breach CIS Control 12 / ISO 27001 A.8.22	CRITICAL
☐	2	Deploy Next Generation Firewalls with application awareness and threat intelligence integration at all perimeters CIS Control 13 / ISO 27001 A.8.20	CRITICAL
☐	3	Implement Intrusion Detection and Prevention Systems across all critical network segments CIS Control 13.3 / ISO 27001 A.8.16	CRITICAL
☐	4	Enforce TLS 1.3 for all data in transit and formally deprecate TLS 1.1, TLS 1.2, and all SSL versions ISO 27001 A.8.24 / NIST SP 800-52	CRITICAL
☐	5	Conduct network vulnerability scanning at a minimum of quarterly frequency across all in-scope assets CIS Control 7 / NIS2 Art.21	CRITICAL
☐	6	Harden all network devices including routers, switches, and firewalls to CIS benchmark standards CIS Benchmarks / ISO 27001 A.8.9	CRITICAL
☐	7	Conduct annual penetration testing of the full network infrastructure using a qualified third party NIS2 Art.21 / ISO 27001 A.5.34	CRITICAL
HIGH CONTROLS			
☐	8	Establish a DMZ architecture for all internet facing services to isolate them from internal networks ISO 27001 A.8.22 / NIST SP 800-41	HIGH
☐	9	Deploy a Web Application Firewall in front of all public facing web applications and APIs CIS Control 16 / OWASP	HIGH
☐	10	Implement DDoS protection and tested mitigation capabilities for all critical internet facing services NIST CSF PR.DS / ISO 27001 A.8.20	HIGH
☐	11	Implement Zero Trust Network Access as the primary remote access mechanism for all staff and third parties NIST SP 800-207 / ISO 27001 A.6.7	HIGH

DOMAIN 03 OF 16 — CONTINUED

Network and Infrastructure Security

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Deploy DNS security controls including DNSSEC, DNS filtering, and protection against DNS based threats CIS Control 9.2 / ISO 27001 A.8.20	HIGH
☐	13	Implement network traffic analysis and anomaly detection to identify unusual patterns and lateral movement NIST CSF DE.AE / CIS Control 13	HIGH
☐	14	Disable all unused ports, protocols, and services on every network device and server across the environment CIS Control 4.8 / ISO 27001 A.8.8	HIGH
☐	15	Implement secure Wi-Fi using WPA3, EAP-TLS authentication, and maintain a separate guest SSID CIS Control 12 / ISO 27001 A.8.20	HIGH

DOMAIN 04 OF 16

Security Operations and Incident Response

8 Critical 7 High

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Establish a 24 by 7 Security Operations Centre capability either in-house or via a managed security service provider NIS2 Art.21 / ISO 27001 A.5.25	CRITICAL
☐	2	Deploy a SIEM platform with use-case driven detection rules, tuned alert thresholds, and log retention policies CIS Control 8 / ISO 27001 A.8.16	CRITICAL
☐	3	Define, document, and test an Incident Response Plan at least once per year including all key stakeholders ISO 27001 A.5.26 / NIST SP 800-61	CRITICAL
☐	4	Establish a formal incident classification and severity matrix covering P1 through P4 with response SLAs NIST CSF RS.AN / ISO 27001 A.5.25	CRITICAL
☐	5	Define escalation procedures, communication trees, and response runbooks for each incident severity level NIS2 Art.23 / NIST SP 800-61	CRITICAL
☐	6	Define breach notification workflows covering NIS2 24 hour early warning and GDPR 72 hour formal report obligations NIS2 Art.23 / GDPR Art.33	CRITICAL
☐	7	Maintain a complete incident log and conduct a formal post-incident review for every P1 and P2 incident ISO 27001 A.5.27 / NIST SP 800-61	CRITICAL
☐	8	Deploy Endpoint Detection and Response or Extended Detection and Response on all managed endpoints CIS Control 13 / ISO 27001 A.8.7	CRITICAL
HIGH CONTROLS			
☐	9	Implement Security Orchestration, Automation and Response tooling to accelerate detection and response workflows NIST CSF RS.MA / ISO 27001 A.5.26	HIGH
☐	10	Conduct quarterly tabletop exercises simulating realistic threat scenarios with cross-functional participation NIST CSF RS.IM / DORA Art.26	HIGH
☐	11	Implement a threat intelligence platform with IoC management and integration into SIEM detection rules MITRE ATT&CK / NIST CSF ID.RA	HIGH

DOMAIN 04 OF 16 — CONTINUED

Security Operations and Incident Response

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Establish digital forensics investigation capabilities and a documented chain of custody process ISO 27001 A.5.28 / NIST SP 800-86	HIGH
☐	13	Integrate proactive threat hunting activities into regular SOC operations using MITRE ATT&CK as a guide MITRE ATT&CK / NIST CSF DE.AE	HIGH
☐	14	Monitor the dark web and threat intelligence feeds for credential leaks and brand impersonation NIST CSF ID.RA / CIS Control 17	HIGH
☐	15	Establish and track Mean Time to Detect and Mean Time to Respond KPIs with monthly reporting to leadership NIST CSF RS.MI / ISO 27001 Cl.9.1	HIGH

DOMAIN 05 OF 16

Cloud Security and Data Protection

8 Critical 7 High

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement a Cloud Security Posture Management platform to continuously monitor cloud configuration drift CIS Benchmarks / ISO 27001 A.5.23	CRITICAL
☐	2	Enforce cloud security baseline configurations aligned to CIS Benchmarks for all cloud accounts and services CIS Benchmarks / ISO 27001 A.8.9	CRITICAL
☐	3	Implement a four tier data classification framework covering Public, Internal, Confidential, and Restricted data ISO 27001 A.5.12 / NIST SP 800-60	CRITICAL
☐	4	Encrypt all data at rest using AES-256 or equivalent with encryption keys stored separately from the data ISO 27001 A.8.24 / NIST FIPS 197	CRITICAL
☐	5	Implement Data Loss Prevention controls across email, endpoint, and cloud channels to prevent data exfiltration NIST CSF PR.DS / ISO 27001 A.8.12	CRITICAL
☐	6	Implement data residency controls to ensure PII is stored within approved jurisdictions per applicable regulations GDPR Art.44 / UAE PDPL / ISO 27701	CRITICAL
☐	7	Implement backup encryption and verify offsite backup restoration successfully at least monthly ISO 27001 A.8.13 / CIS Control 11	CRITICAL
☐	8	Establish data retention, archival, and secure disposal policies aligned to regulatory and business requirements GDPR Art.5 / ISO 27701 / ISO 27001 A.8.10	CRITICAL
HIGH CONTROLS			
☐	9	Deploy a Cloud Access Security Broker to gain visibility and control over all sanctioned and unsanctioned SaaS usage ISO 27001 A.5.23 / NIST CSF PR.AC	HIGH
☐	10	Establish and document the cloud shared responsibility model for each cloud provider and service category ISO 27001 A.5.23 / CSA CCM	HIGH
☐	11	Conduct cloud infrastructure security assessments quarterly using automated tooling and manual review CIS Benchmarks / ISO 27001 A.8.8	HIGH

DOMAIN 05 OF 16 — CONTINUED

Cloud Security and Data Protection

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Implement cloud workload protection for all containers, virtual machines, and serverless workloads CIS Kubernetes Benchmark / ISO 27001	HIGH
☐	13	Deploy a secrets management solution to eliminate hardcoded credentials and manage API keys centrally CIS Control 18 / ISO 27001 A.8.24	HIGH
☐	14	Deploy Infrastructure as Code security scanning in all CI/CD pipelines before code reaches production CIS DevSecOps / NIST SP 800-218	HIGH
☐	15	Monitor and control Shadow IT by maintaining a current inventory of all unsanctioned cloud services in use NIS2 Art.21 / NIST CSF ID.AM	HIGH

DOMAIN 06 OF 16

Vulnerability Management and Application Security

6 Critical 7 High 2 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement continuous vulnerability scanning across all assets in the environment including cloud and on-premises CIS Control 7 / NIS2 Art.21	CRITICAL
☐	2	Establish SLA-based remediation timelines requiring Critical fixes within 24 hours and High fixes within 7 days NIST CSF RS.MI / CIS Control 7.7	CRITICAL
☐	3	Deploy an automated patch management programme covering all operating systems, applications, and firmware CIS Control 7.4 / ISO 27001 A.8.8	CRITICAL
☐	4	Conduct external and internal penetration testing at least annually using a qualified independent third party NIS2 Art.21 / DORA Art.26	CRITICAL
☐	5	Maintain a comprehensive and continuously updated asset inventory covering all hardware, software, and cloud resources CIS Control 1 / ISO 27001 A.5.9	CRITICAL
☐	6	Subscribe to CVE feeds and zero-day alert services for all technologies deployed in the production environment CISA KEV / NVD / NIST CSF ID.RA	CRITICAL
HIGH CONTROLS			
☐	7	Implement a Secure Software Development Lifecycle framework covering all stages from design through deployment NIST SP 800-64 / OWASP SAMM	HIGH
☐	8	Integrate Static Application Security Testing into all CI/CD pipelines with quality gates blocking high severity findings OWASP DevSecOps / CIS Control 16	HIGH
☐	9	Implement Dynamic Application Security Testing for all web applications before every major production release OWASP Testing Guide v4 / CIS Control 16	HIGH
☐	10	Deploy Software Composition Analysis tooling to identify and manage open source component vulnerabilities CIS Control 16.3 / NIST SP 800-218	HIGH
☐	11	Implement container image scanning and runtime protection for all Kubernetes and containerised workloads CIS Kubernetes Benchmark / NIST SP 800-190	HIGH

DOMAIN 06 OF 16 — CONTINUED

Vulnerability Management and Application Security

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Conduct API security testing against the OWASP API Top 10 and implement an API gateway with rate limiting OWASP API Top 10 / CIS Control 16	HIGH
☐	13	Establish a secure code review process and embed security training into the developer onboarding programme NIST SP 800-64 / OWASP SAMM	HIGH
		MEDIUM CONTROLS	
☐	14	Establish a bug bounty or responsible disclosure programme with a clearly published security contact NIST CSF / ISO 27001 A.5.8	MEDIUM
☐	15	Implement mobile application security testing aligned to the OWASP Mobile Application Security Verification Standard OWASP MASVS / CIS Control 16	MEDIUM

DOMAIN 07 OF 16

Third-Party and Supply Chain Security

6 Critical 6 High 3 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement a vendor risk assessment framework with defined criteria for evaluating and tiering all third parties ISO 27001 A.5.19 / DORA Art.28	CRITICAL
☐	2	Classify all vendors into risk tiers of Critical, High, Medium, and Low based on data access and service criticality ISO 27001 A.5.19 / DORA Art.30	CRITICAL
☐	3	Include mandatory security requirements and right to audit clauses in all vendor contracts and master agreements ISO 27001 A.5.20 / NIS2 Art.21	CRITICAL
☐	4	Conduct formal annual security assessments of all Critical and High tier vendors using questionnaires or audits NIS2 Art.21 / DORA Art.28	CRITICAL
☐	5	Include mandatory security incident notification obligations with defined timelines in all vendor agreements NIS2 Art.21 / DORA Art.28	CRITICAL
☐	6	Maintain a vendor register with current risk ratings, assessment dates, and named relationship owners ISO 27001 A.5.19 / DORA Art.30	CRITICAL
HIGH CONTROLS			
☐	7	Implement fourth-party risk monitoring to understand the security posture of your vendors key sub-processors DORA Art.28 / ISO 27001 A.5.21	HIGH
☐	8	Require and review SOC 2 Type II reports, ISO 27001 certificates, and penetration test executive summaries annually ISO 27001 A.5.21 / DORA Art.28	HIGH
☐	9	Establish a formal vendor offboarding process that includes data deletion confirmation and access revocation ISO 27701 Cl.8 / ISO 27001 A.5.20	HIGH
☐	10	Implement a Software Bill of Materials for all critical applications to understand open source and commercial dependencies NIST SP 800-218 / Executive Order 14028	HIGH
☐	11	Send vendor security questionnaires based on SIG Lite or CAIQ at least annually for all in-scope vendors ISO 27001 A.5.19 / CSA CAIQ	HIGH

DOMAIN 07 OF 16 — CONTINUED

Third-Party and Supply Chain Security

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Implement continuous vendor monitoring using external threat intelligence to detect vendor compromise early DORA Art.28 / NIST CSF ID.SC	HIGH
		MEDIUM CONTROLS	
☐	13	Verify vendor cyber insurance coverage, policy limits, and that your organisation is named where appropriate DORA Art.28 / ISO 27001 A.5.20	MEDIUM
☐	14	Define concentration risk limits for critical ICT service providers and document your exit strategy for each DORA Art.29 / ISO 27001 A.5.19	MEDIUM
☐	15	Identify and manage Shadow AI by inventorying all unsanctioned SaaS AI tools being used across the organisation NIS2 Art.21 / EU AI Act	MEDIUM

DOMAIN 08 OF 16

Business Continuity and Cyber Resilience

7 Critical 8 High

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Develop and maintain a comprehensive Business Continuity Plan covering all critical business functions and systems ISO 22301:2019 / DORA Art.11	CRITICAL
☐	2	Establish a Disaster Recovery Plan and test it at least annually with documented results and lessons learned ISO 22301 / DORA Art.11 / NIS2 Art.21	CRITICAL
☐	3	Define and formally document Recovery Time Objectives and Recovery Point Objectives for all critical systems ISO 22301 Cl.8.4 / DORA Art.11	CRITICAL
☐	4	Implement a 3-2-1 backup strategy with three copies of data, two different media types, and one copy offsite CIS Control 11 / ISO 27001 A.8.13	CRITICAL
☐	5	Test backup restoration successfully at least monthly and document the results including any issues found ISO 22301 Cl.8.5 / CIS Control 11	CRITICAL
☐	6	Implement ransomware resilient backups using immutable storage and air-gapped copies that cannot be encrypted remotely CISA Ransomware Guide / CIS Control 11	CRITICAL
☐	7	Maintain an up-to-date emergency contacts list, escalation matrix, and crisis war room setup instructions ISO 22301 Cl.8.4 / NIST SP 800-61	CRITICAL
HIGH CONTROLS			
☐	8	Conduct annual BCP and DR tabletop exercises with board and executive participation to test decision making NIS2 Art.21 / ISO 22301 Cl.8.5	HIGH
☐	9	Establish alternate communication channels for use during a crisis when primary systems may be unavailable ISO 22301 Cl.8.4 / NIS2 Art.23	HIGH
☐	10	Define a crisis communication plan including media response protocols and pre-approved statement templates ISO 22301 Cl.8.4 / DORA Art.14	HIGH
☐	11	Conduct a formal Business Impact Analysis annually to keep recovery priorities aligned to current business needs ISO 22301 Cl.8.2 / DORA Art.11	HIGH

DOMAIN 08 OF 16 — CONTINUED

Business Continuity and Cyber Resilience

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Establish a cyber insurance policy with coverage limits and terms aligned to your documented risk profile DORA Art.12 / ISO 27001	HIGH
☐	13	Implement geographic or cloud redundancy for all systems classified as Critical or High in the Business Impact Analysis DORA Art.11 / ISO 22301	HIGH
☐	14	Define supply chain resilience strategies to manage the impact of a critical technology provider outage DORA Art.28 / NIS2 Art.21	HIGH
☐	15	Perform annual cyber resilience testing through threat-led penetration testing or red team exercises DORA Art.26 / NIS2 Art.21	HIGH

DOMAIN 09 OF 16

Security Awareness and Human Risk Management

4 Critical 8 High 3 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement mandatory annual security awareness training for every member of staff including contractors and board members ISO 27001 A.6.3 / NIS2 Art.21	CRITICAL
☐	2	Conduct monthly phishing simulations with automatic enrolment of those who click into targeted remedial training CIS Control 14 / NIS2 Art.21	CRITICAL
☐	3	Include specific security responsibilities and acceptable use obligations in every employee onboarding and offboarding process ISO 27001 A.6.2 / CIS Control 14	CRITICAL
☐	4	Maintain an Acceptable Use Policy and obtain annual written acknowledgment from all staff confirming compliance ISO 27001 A.5.10 / CIS Control 14	CRITICAL
HIGH CONTROLS			
☐	5	Deliver role based security training covering specific threats and responsibilities for IT, finance, HR, and executives NIS2 Art.20 / ISO 27001 A.6.3	HIGH
☐	6	Establish an insider threat detection, monitoring, and structured response programme with clear escalation paths NIST SP 800-53 AT / ISO 27001 A.6.6	HIGH
☐	7	Track security awareness KPIs including training completion rates and phishing click rates and report quarterly ISO 27001 Cl.9.1 / NIST CSF PR.AT	HIGH
☐	8	Establish an anonymous security reporting mechanism such as a hotline or portal to encourage early disclosure ISO 27001 A.6.4 / NIS2 Art.21	HIGH
☐	9	Conduct social engineering assessments including vishing campaigns and physical security testing at least annually NIST CSF PR.AT / ISO 27001 A.5.34	HIGH
☐	10	Provide board and executive level cybersecurity briefings at least quarterly covering threat landscape and programme status NIS2 Art.20 / DORA Art.5	HIGH
☐	11	Enforce BYOD security policy through technical controls and annual training for all staff using personal devices CIS Control 4 / ISO 27001 A.6.7	HIGH

DOMAIN 09 OF 16 — CONTINUED

Security Awareness and Human Risk Management

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Train all staff on data handling, classification, and secure disposal procedures relevant to their role ISO 27701 Cl.6 / GDPR Art.32	HIGH
		MEDIUM CONTROLS	
☐	13	Implement a security champion programme with trained representatives embedded in each business unit OWASP SAMM / ISO 27001 A.6.3	MEDIUM
☐	14	Develop security culture KPIs and conduct an annual security culture benchmarking exercise across the organisation ISO 27001 Cl.9.1 / NIST CSF GV.OC	MEDIUM
☐	15	Measure and actively work to reduce the organisational human risk score using behavioural analytics tooling CIS Control 14 / ISO 27001 A.6.3	MEDIUM

DOMAIN 10 OF 16

Data Privacy and ISO 27701:2025

9 Critical 5 High 1 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Establish a Privacy Information Management System aligned to ISO 27701:2025 covering all PII processing activities ISO 27701:2025 Cl.4-5	CRITICAL
☐	2	Appoint a named Data Protection Officer with direct board access and documented independence in their role GDPR Art.37 / ISO 27701:2025 Cl.5	CRITICAL
☐	3	Maintain Records of Processing Activities for all PII covering purposes, categories, recipients, and retention periods GDPR Art.30 / ISO 27701:2025 Cl.7	CRITICAL
☐	4	Conduct Data Protection Impact Assessments for all processing activities that present a high risk to individuals GDPR Art.35 / ISO 27701:2025 Cl.7	CRITICAL
☐	5	Establish, document, and review the lawful basis for every PII processing activity across the organisation GDPR Art.6 / ISO 27701:2025 Cl.7.2	CRITICAL
☐	6	Implement data subject rights procedures enabling access, erasure, rectification, and portability requests within legal timeframes GDPR Art.15-22 / ISO 27701:2025 Cl.7	CRITICAL
☐	7	Document all international PII transfers with appropriate safeguards and maintain transfer impact assessments ISO 27701:2025 Cl.7 / GDPR Chapter V	CRITICAL
☐	8	Classify all processing activities as PII Controller or PII Processor and apply the corresponding ISO 27701 obligations ISO 27701:2025 Cl.7 and Cl.8	CRITICAL
☐	9	Align the privacy programme to all applicable GCC regulations including UAE PDPL, Bahrain PDPL, and NCA requirements UAE PDPL / Bahrain PDPL 2022 / KSA NCA ECC	CRITICAL
HIGH CONTROLS			
☐	10	Implement a consent management platform that captures, stores, and provides a complete audit trail for all consents GDPR Art.7 / ISO 27701:2025 Cl.7.2	HIGH
☐	11	Maintain accurate and current privacy notices across all touchpoints where PII is collected from individuals GDPR Art.13-14 / ISO 27701:2025	HIGH

DOMAIN 10 OF 16 — CONTINUED

Data Privacy and ISO 27701:2025

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Implement privacy by design and privacy by default principles in all new systems, products, and services GDPR Art.25 / ISO 27701:2025 Cl.7.4	HIGH
☐	13	Conduct privacy risk assessments integrated with the information security risk process and documented in the risk register ISO 27701:2025 Cl.8 / GDPR Art.32	HIGH
☐	14	Enforce data minimisation and purpose limitation principles across all systems that process personal information GDPR Art.5 / ISO 27701:2025 Cl.7.2	HIGH
		MEDIUM CONTROLS	
☐	15	Perform an annual PIMS management review covering performance, risks, and opportunities for continual improvement ISO 27701:2025 Cl.9-10	MEDIUM

DOMAIN 11 OF 16

Cryptography and Key Management

6 Critical 6 High 3 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Define and enforce a cryptographic standards policy specifying approved algorithms, key lengths, and usage contexts ISO 27001 A.8.24 / NIST SP 800-57	CRITICAL
☐	2	Implement certificate lifecycle management with automated alerting and a fully documented enterprise PKI NIST SP 800-57 / ISO 27001 A.8.24	CRITICAL
☐	3	Establish formal key rotation schedules, key escrow procedures, and documented key ceremony processes NIST SP 800-57 / ISO 27001 A.8.24	CRITICAL
☐	4	Monitor certificate expiry continuously and automate renewal alerts at 90, 30, and 7 day thresholds ISO 27001 A.8.24 / CIS Control 16	CRITICAL
☐	5	Enforce TLS 1.3 as the minimum acceptable protocol version and formally deprecate all legacy SSL and TLS versions NIST SP 800-52 / PCI DSS v4	CRITICAL
☐	6	Implement encrypted channels for all privileged and administrative access to systems and network infrastructure ISO 27001 A.8.24 / CIS Control 12	CRITICAL
HIGH CONTROLS			
☐	7	Deploy Hardware Security Modules for the storage and management of all critical cryptographic keys NIST FIPS 140-3 / ISO 27001 A.8.24	HIGH
☐	8	Conduct a post-quantum cryptography readiness assessment and develop a migration roadmap aligned to NIST standards NIST FIPS 203/204/205 / NSA CNSA 2.0	HIGH
☐	9	Implement code signing and digital signature management for all software releases and critical communications CIS Control 16 / NIST SP 800-218	HIGH
☐	10	Deploy tokenisation and data masking for all sensitive PII and payment card data across applications and databases PCI DSS v4 / ISO 27001 A.8.11	HIGH
☐	11	Implement formal key destruction and disposal procedures to ensure cryptographic material cannot be recovered after use NIST SP 800-57 / ISO 27001 A.8.10	HIGH

DOMAIN 11 OF 16 — CONTINUED

Cryptography and Key Management

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Audit all cryptographic implementations across applications and infrastructure on an annual basis CIS Control 16 / ISO 27001 A.8.24	HIGH
		MEDIUM CONTROLS	
☐	13	Review cryptographic requirements and key management obligations in all third-party vendor contracts annually ISO 27001 A.5.20 / DORA Art.28	MEDIUM
☐	14	Align cryptographic implementations with NSA CNSA 2.0 quantum-resistant algorithm suite requirements by 2030 NSA CNSA 2.0 / NIST PQC 2024	MEDIUM
☐	15	Test the quantum resilience of current encryption implementations and begin planning migration to PQC algorithms NIST PQC Standard 2024 / NSA CNSA 2.0	MEDIUM

DOMAIN 12 OF 16

Physical and Environmental Security

6 Critical 6 High 3 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Implement multi-factor physical access controls for all data centres, server rooms, and sensitive office areas ISO 27001 A.7.1 / NIS2 Art.21	CRITICAL
☐	2	Deploy CCTV surveillance covering all entry and exit points with tamper alerts and at least 90 days of retention ISO 27001 A.7.4 / NIS2 Art.21	CRITICAL
☐	3	Implement secure physical media destruction processes aligned to NIST 800-88 for all decommissioned storage devices ISO 27001 A.7.10 / NIST SP 800-88	CRITICAL
☐	4	Deploy environmental controls covering fire suppression, temperature monitoring, flood detection, and power protection ISO 27001 A.7.5 / ISO 27001 A.7.11	CRITICAL
☐	5	Deploy N+1 UPS and generator backup power for all data centres and critical infrastructure locations ISO 27001 A.7.11 / DORA Art.11	CRITICAL
☐	6	Define and consistently enforce secure disposal procedures for all IT equipment and removable storage media ISO 27001 A.7.14 / NIST SP 800-88	CRITICAL
HIGH CONTROLS			
☐	7	Enforce clean desk and clear screen policies with regular unannounced spot checks across all office locations ISO 27001 A.7.7 / CIS Control 4	HIGH
☐	8	Establish a formal visitor management process including pre-registration, identity verification, and escort requirements ISO 27001 A.7.2 / NIS2 Art.21	HIGH
☐	9	Conduct annual physical penetration testing of all critical facilities to identify physical security vulnerabilities ISO 27001 A.7 / NIS2 Art.21	HIGH
☐	10	Review and audit all physical badge access rights at least quarterly and revoke access immediately upon role change ISO 27001 A.7.2 / CIS Control 6	HIGH
☐	11	Implement mantrap or secure entry zones with anti-tailgating controls for all data centres and high security areas ISO 27001 A.7.1 / NIS2 Art.21	HIGH

DOMAIN 12 OF 16 — CONTINUED

Physical and Environmental Security

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Conduct an annual review of all physical and environmental security controls with findings reported to leadership ISO 27001 A.7 / NIS2 Art.21	HIGH
		MEDIUM CONTROLS	
☐	13	Establish secure print release and document handling procedures to prevent sensitive information being left unattended ISO 27001 A.7.7 / GDPR Art.32	MEDIUM
☐	14	Implement equipment asset tagging, physical inventory tracking, and regular reconciliation across all sites CIS Control 1 / ISO 27001 A.7.9	MEDIUM
☐	15	Establish cabling security standards, labelling conventions, and cable management procedures across all facilities ISO 27001 A.7.12 / NIST SP 800-53	MEDIUM

DOMAIN 13 OF 16

AI Security and Governance

7 Critical 6 High 2 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Establish an AI governance policy, assign AI risk ownership, and integrate AI risk into the enterprise risk framework EU AI Act / NIST AI RMF 1.0 / ISO 42001	CRITICAL
☐	2	Create and maintain a complete inventory of all AI, Generative AI, and machine learning tools in use including Shadow AI NIS2 Art.21 / NIST AI RMF / EU AI Act Art.49	CRITICAL
☐	3	Assess and classify every AI system by risk level according to the EU AI Act taxonomy before deployment EU AI Act Art.9 / Annex III	CRITICAL
☐	4	Implement Generative AI data leakage controls preventing staff from entering PII or confidential data into AI prompts ISO 27701 / GDPR Art.32 / EU AI Act	CRITICAL
☐	5	Deploy a distinct managed identity for every AI agent with scoped permissions and no shared credential reuse NIST SP 800-207A / Zero Trust	CRITICAL
☐	6	Register all high-risk AI systems in the EU AI Act compliance database and maintain documentation for audit EU AI Act Art.49 / Art.51	CRITICAL
☐	7	Enforce least privilege access scoping for all AI agent and automation service accounts across all environments NIST SP 800-207A / CIS Control 5	CRITICAL
HIGH CONTROLS			
☐	8	Implement the NIST AI Risk Management Framework across all four functions of Govern, Map, Measure, and Manage NIST AI RMF 1.0 / ISO 42001:2023	HIGH
☐	9	Establish an AI vendor risk assessment process covering all external model providers and AI platform vendors NIST AI RMF / EU AI Act / DORA Art.28	HIGH
☐	10	Implement prompt injection detection and prevention controls for all Generative AI deployments and integrations MITRE ATLAS 2025 / OWASP LLM Top 10	HIGH
☐	11	Conduct AI model security assessments using the MITRE ATLAS framework for all internally deployed AI systems MITRE ATLAS v2 2025 / NIST AI RMF	HIGH

DOMAIN 13 OF 16 — CONTINUED

AI Security and Governance

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Establish an AI specific incident response playbook covering model compromise, data poisoning, and output manipulation NIST AI RMF RS / ISO 27001 A.5.26	HIGH
☐	13	Monitor AI deployments for model extraction attempts, adversarial attacks, and training data poisoning indicators MITRE ATLAS / NIST AI RMF ME	HIGH
		MEDIUM CONTROLS	
☐	14	Implement AI output validation, hallucination logging, and audit trails for all high-risk AI assisted decisions NIST AI RMF MG / EU AI Act Art.13	MEDIUM
☐	15	Establish an AI ethics and bias review process for all AI systems that influence decisions affecting individuals EU AI Act Art.10 / NIST AI RMF GV	MEDIUM

DOMAIN 14 OF 16

ISO 42001 AI Management System

6 Critical 8 High 4 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Establish an AI Management System scope statement covering all AI systems, stakeholders, and organisational boundaries ISO 42001:2023 Cl.4.3	CRITICAL
☐	2	Define the organisational context for AI including internal and external issues that affect AI objectives ISO 42001:2023 Cl.4.1	CRITICAL
☐	3	Identify all interested parties for AI systems and document their requirements and expectations formally ISO 42001:2023 Cl.4.2	CRITICAL
☐	4	Establish top management commitment to AI management including a formal AI policy signed by senior leadership ISO 42001:2023 Cl.5.1 / Cl.5.2	CRITICAL
☐	5	Assign AI management roles, responsibilities, and authorities to named individuals across the organisation ISO 42001:2023 Cl.5.3	CRITICAL
☐	6	Conduct AI risk assessments using a documented methodology to identify and treat risks from all AI systems ISO 42001:2023 Cl.6.1	CRITICAL
HIGH CONTROLS			
☐	7	Define AI objectives that are measurable, monitored, communicated, and updated when conditions change ISO 42001:2023 Cl.6.2	HIGH
☐	8	Ensure staff responsible for AI systems have documented competency requirements and evidence of meeting them ISO 42001:2023 Cl.7.2	HIGH
☐	9	Make staff aware of the AI policy, their contribution to AI management objectives, and implications of non-conformity ISO 42001:2023 Cl.7.3	HIGH
☐	10	Establish documented information controls for all AI management system documents and records ISO 42001:2023 Cl.7.5	HIGH
☐	11	Implement operational planning and controls for all AI system development, deployment, and monitoring activities ISO 42001:2023 Cl.8.1	HIGH

DOMAIN 14 OF 16 — CONTINUED

ISO 42001 AI Management System

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Conduct AI impact assessments before deploying AI systems that could significantly affect individuals or society ISO 42001:2023 Cl.8.4 / Annex B	HIGH
☐	13	Monitor, measure, analyse, and evaluate AI system performance against defined criteria and objectives ISO 42001:2023 Cl.9.1	HIGH
☐	14	Conduct internal audits of the AI management system at planned intervals to verify conformity and effectiveness ISO 42001:2023 Cl.9.2	HIGH
		MEDIUM CONTROLS	
☐	15	Conduct management reviews of the AI management system at least annually to ensure its continuing suitability ISO 42001:2023 Cl.9.3	MEDIUM
☐	16	Address nonconformities in AI systems promptly and implement corrective actions to prevent recurrence ISO 42001:2023 Cl.10.1	MEDIUM
☐	17	Implement continual improvement processes to enhance the suitability, adequacy, and effectiveness of the AI management system ISO 42001:2023 Cl.10.2	MEDIUM
☐	18	Document responsible AI principles covering fairness, transparency, accountability, and human oversight ISO 42001:2023 Annex A / EU AI Act	MEDIUM

DOMAIN 15 OF 16

Security Metrics and Board Reporting

5 Critical 7 High 3 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Define a security KPI framework that directly connects security programme health to business risk and strategic objectives NIST CSF GV.OC / ISO 27001 Cl.9.1	CRITICAL
☐	2	Implement a board level security reporting cadence of at least quarterly with a consistent and board appropriate format NIS2 Art.20 / DORA Art.5 / ISO 27001 Cl.5.1	CRITICAL
☐	3	Track and trend Mean Time to Detect, Mean Time to Respond, patch compliance percentage, and phishing click rate monthly CIS Control 17 / NIST CSF DE.AE	CRITICAL
☐	4	Report on regulatory compliance status covering all in-scope regulations to leadership at least monthly NIS2 Art.20 / DORA Art.5 / GDPR	CRITICAL
☐	5	Review and formally update the security strategy with board participation at least once per year ISO 27001 Cl.9.3 / NIS2 Art.20	CRITICAL
HIGH CONTROLS			
☐	6	Develop a cyber risk quantification model using the FAIR methodology to express security risk in financial terms NIST CSF ID.RA / FAIR Standard	HIGH
☐	7	Implement a security programme maturity assessment using CMMI or NIST CSF tiers and repeat annually NIST CSF / CMMI / ISO 27001 Cl.9.1	HIGH
☐	8	Establish a cybersecurity budget justification framework that connects security investment to risk reduction outcomes NIST CSF GV.RM / ISO 27001 Cl.9.3	HIGH
☐	9	Develop standardised executive security briefing templates and a live dashboard covering the most important metrics NIST CSF GV.OC / ISO 27001 Cl.9.3	HIGH
☐	10	Implement a real-time security operations dashboard with the key metrics visible to SOC and management at all times NIST CSF DE.AE / CIS Control 17	HIGH
☐	11	Track third-party risk scores and vendor compliance percentages as a standing item in board security reporting DORA Art.28 / ISO 27001 A.5.19	HIGH

DOMAIN 15 OF 16 — CONTINUED

Security Metrics and Board Reporting

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Establish a process for tracking the financial impact of security incidents and present this data annually to the board NIST CSF RS.MI / FAIR	HIGH
		MEDIUM CONTROLS	
☐	13	Measure and report the return on security investment to the board at least annually using quantified risk data NIST CSF GV.RM / FAIR	MEDIUM
☐	14	Benchmark the organisational security posture against industry peers using publicly available framework maturity data CIS Benchmarks / NIST CSF Tiers	MEDIUM
☐	15	Report security awareness training completion rates and phishing simulation trend data to leadership quarterly ISO 27001 Cl.9.1 / CIS Control 14	MEDIUM

DOMAIN 16 OF 16

NIS2, DORA and Regulatory Compliance

9 Critical 5 High 1 Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
CRITICAL CONTROLS			
☐	1	Map all entities, subsidiaries, and services to determine which are in scope of NIS2 as essential or important entities NIS2 Art.2-3 / Annex I-II	CRITICAL
☐	2	Implement the NIS2 all-hazards approach to risk management covering physical, cyber, and supply chain threats NIS2 Art.21 / Recital 79	CRITICAL
☐	3	Establish NIS2 incident reporting workflows enabling a 24 hour early warning and a 72 hour full incident report NIS2 Art.23 / ENISA Guidelines	CRITICAL
☐	4	Complete mandatory board and management level cybersecurity training to satisfy the NIS2 director liability requirement NIS2 Art.20 / Director liability	CRITICAL
☐	5	Implement the DORA ICT risk management framework with all required policies, procedures, and governance structures DORA Art.6 / RTS on ICT Risk	CRITICAL
☐	6	Establish a DORA operational resilience testing programme with annual testing and documented remediation tracking DORA Art.25 / RTS on TLPT	CRITICAL
☐	7	Register and manage all Critical ICT Third-Party Providers as required by DORA with documented oversight plans DORA Art.28-30 / EBA Register	CRITICAL
☐	8	Establish DORA ICT incident classification, reporting workflows, and root cause analysis processes for major incidents DORA Art.17-19 / ITS on Incidents	CRITICAL
☐	9	Continuously monitor and track regulatory changes across all applicable GCC jurisdictions and update controls accordingly UAE PDPL / Bahrain PDPL / NCA ECC	CRITICAL
HIGH CONTROLS			
☐	10	Implement DORA Threat-Led Penetration Testing at least once every three years using TIBER-EU methodology DORA Art.26 / TIBER-EU	HIGH
☐	11	Achieve and maintain PCI DSS 4.0.1 compliance for all systems involved in the processing of payment card data PCI DSS v4.0.1 / PCI SSC	HIGH

DOMAIN 16 OF 16 — CONTINUED

NIS2, DORA and Regulatory Compliance

Severity sorted: Critical → High → Medium

CHK	#	CONTROL · FRAMEWORK REFERENCE	SEVERITY
☐	12	Achieve or maintain SOC 2 Type II attestation to demonstrate trust service criteria compliance to customers AICPA SOC 2 / AICPA TSC	HIGH
☐	13	Establish an NCA Essential Cybersecurity Controls compliance programme for operations within Saudi Arabia NCA ECC 2:2020 / Saudi Arabia	HIGH
☐	14	Align the security programme with CBB cybersecurity requirements for financial sector entities operating in Bahrain CBB Rulebook Vol.6 / Module CY	HIGH
		MEDIUM CONTROLS	
☐	15	Implement CMMC v2 Level requirements if operating within or supplying to the US Department of Defense supply chain CMMC v2 / DFARS 252.204-7012	MEDIUM

CODE DEFENCE

Cybersecurity & Data Privacy

Consultancy · GCC · Global

codedefence.in
hello@codedefence.in

Need help implementing these controls?

Code Defence offers vCISO, vDPO, ISO 27001, ISO 42001, and VMaaS services for organisations across the GCC. Book a free consultation at codedefence.in.