THREATNEXIS
Cybersecurity Intelligence & Advisory

IMPLEMENTATION TEMPLATE

NIST RMF / ISO 27001

Implementation Roadmap & Compliance Template

A practitioner-grade template for aligning your organization's security program with NIST Risk Management Framework (RMF) and ISO/IEC 27001:2022. Includes gap analysis, control mapping, implementation tracking, and executive reporting.

Framework Version	NIST RMF Rev 2 | ISO 27001:2022	**Document Version**	1.0
Target Audience	CISOs, IT Managers, GRC Teams, Consultants	**Classification**	Confidential

threatnexis.com | Enterprise Cybersecurity Advisory | GRC | vCISO Services

1. Purpose & Scope

1.1 Purpose

This template provides a structured, practitioner-grade roadmap for implementing the NIST Risk Management Framework (RMF) and achieving ISO/IEC 27001:2022 certification. It bridges the gap between framework theory and real-world execution — giving your security team actionable worksheets, gap analysis tools, control mapping tables, and executive reporting artifacts.

Whether you're pursuing formal ISO 27001 certification, aligning to NIST RMF for federal compliance, or simply maturing your security program, this template provides a structured path forward.

1.2 Scope

This document applies to:

- Organizations pursuing ISO/IEC 27001:2022 certification
- Federal agencies and contractors subject to NIST RMF requirements
- Organizations seeking dual-framework alignment (NIST + ISO)
- SMBs implementing a formal Information Security Management System (ISMS)
- GRC teams building or maturing their risk management programs
- Security consultants advising clients on framework implementation

1.3 How to Use This Template

Getting Started

Step 1: Complete the organizational context section (Section 3)
Step 2: Conduct the NIST RMF step-by-step assessment (Section 4)
Step 3: Map your current controls to ISO 27001 Annex A (Section 5)
Step 4: Identify gaps and populate the gap analysis table (Section 6)
Step 5: Build your implementation roadmap (Section 7)
Step 6: Use the executive summary template for board reporting (Section 9)

2. Key Definitions

The following terms are used throughout this document. Plain-English explanations are provided to support practitioners at all experience levels.

Term	Definition
NIST RMF	NIST Risk Management Framework — a 7-step process for managing information security risk in federal systems. Steps: Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor.
ISO 27001	International standard for Information Security Management Systems (ISMS). The 2022 revision includes 93 controls across 4 themes: Organizational, People, Physical, and Technological.
ISMS	Information Security Management System — the collection of policies, procedures, and controls an organization uses to manage information security risk systematically.
Annex A	The control reference set in ISO 27001:2022 containing 93 controls organized into 4 control themes and 11 control categories.
Control	A measure that modifies risk. Controls can be preventive, detective, corrective, or compensating in nature.
SoA	Statement of Applicability — an ISO 27001 requirement listing all Annex A controls, whether each applies, and the justification for inclusion or exclusion.
Risk Register	A documented inventory of identified risks, including likelihood, impact, risk rating, treatment decision, and ownership.
Risk Treatment	The decision made for each identified risk: Mitigate, Accept, Transfer, or Avoid.
Gap Analysis	A structured assessment comparing your current security posture against framework requirements to identify what's missing.
Maturity Level	A scale (typically 1–5) rating how developed and consistent your security practices are for a given control domain.
POAM	Plan of Action and Milestones — an artifact required by NIST RMF listing known weaknesses, planned remediation, and target completion dates.
ATO	Authorization to Operate — a formal decision by an authorizing

Term	Definition
	official that a system's risk is acceptable for operation (NIST RMF specific).
vCISO	Virtual CISO — a fractional or outsourced Chief Information Security Officer who provides strategic security leadership on a part-time basis.

3. Organizational Context

Complete this section before beginning any framework assessment. Understanding your organization's context is foundational to scoping the ISMS and selecting appropriate controls.

3.1 Organization Profile

Field	Response
Organization Name	
Industry / Sector	
Number of Employees	
Number of Locations	
Annual Revenue Range	
Regulatory Environment	(e.g., HIPAA, PCI-DSS, CMMC, SOX)
Data Types Processed	(e.g., PII, PHI, Financial, Classified)
Cloud Provider(s)	
Primary IT Contact	
Assessment Lead	
Assessment Date	
Target Completion Date	
External Auditor / Certifying Body	

3.2 ISMS Scope Statement

Instructions

Define the boundaries of your Information Security Management System (ISMS). The scope determines what assets, processes, locations, and services are covered by your

ISO 27001 certification or NIST RMF authorization boundary.

Be specific. Auditors will test everything within scope. Exclude systems or locations only if there is a documented, justified rationale.

ISMS Scope Statement (describe in detail below)
Locations covered:
Business units covered:
Systems and applications in scope:
Systems and locations explicitly excluded:
Justification for exclusions:

3.3 Interested Parties (Stakeholder Analysis)

ISO 27001 requires identifying internal and external parties whose needs and expectations must be considered in your ISMS.

Interested Party	Type	Relevant Needs / Expectations
Board of Directors / Leadership	Internal	Risk visibility, regulatory compliance, business continuity
IT Department	Internal	Technical control guidance, clear security standards
Employees	Internal	Security awareness, acceptable use policies, incident reporting
Customers / Clients	External	Data protection, privacy, service availability
Regulators / Government	External	Compliance with applicable laws and standards
Third-Party Vendors	External	Vendor requirements, data handling agreements
Cyber Insurers	External	Minimum security controls, risk posture evidence
Auditors / Certifying	External	ISMS documentation, evidence of

Interested Party	Type	Relevant Needs / Expectations
Bodies		control operation
[Add Additional Party]		

4. NIST Risk Management Framework — Implementation Tracker

The NIST RMF provides a 7-step process for managing cybersecurity risk. Use this section to document your progress through each step, capture key decisions, and maintain an audit trail.

Step	Name	Objective	Status	Owner
1	PREPARE	Establish context, roles, risk strategy, and resources before the RMF process begins	⬜ Not Started	
2	CATEGORIZE	Categorize the system based on the potential impact of a security compromise	⬜ Not Started	
3	SELECT	Select a set of controls to protect the system based on risk assessment	⬜ Not Started	
4	IMPLEMENT	Implement the controls and document how they are deployed	⬜ Not Started	
5	ASSESS	Determine whether controls are implemented correctly and producing desired outcomes	⬜ Not Started	
6	AUTHORIZE	Senior official makes a risk-based decision to authorize system operation	⬜ Not Started	
7	MONITOR	Continuously monitor control effectiveness, document changes, conduct ongoing assessments	⬜ Not Started	

Step 1 — PREPARE

The Prepare step establishes the organizational context needed to manage security and privacy risk effectively. It should be completed before proceeding to system-level activities.

Task	Description	Status	Evidence / Notes
Assign Authorizing Official (AO)	Senior official accountable for accepting system risk	⬜	
Assign System Owner	Individual responsible for the overall system	⬜	
Assign ISSO / Security Officer	Individual responsible for ISMS/security program day-to-day	⬜	
Define Risk Tolerance	Document acceptable risk levels for the organization	⬜	
Establish Risk Management Strategy	Identify how risk will be managed, monitored, and reported	⬜	
Conduct Organization-Level Risk Assessment	Identify threats, vulnerabilities, and organizational risk	⬜	
Identify Common Controls	Document controls inherited from the organization or shared services	⬜	
Define Security Requirements	Capture requirements from laws, regulations, and policies	⬜	
Mission / Business Process Identification	Document critical business processes that rely on the system	⬜	
Supply Chain Risk Considerations	Identify supply chain threats and establish SCRM strategy	⬜	

Step 2 — CATEGORIZE

Categorize information and the system using FIPS 199 / NIST SP 800-60. The impact level (Low, Moderate, High) drives control baseline selection in Step 3.

FIPS 199 System Categorization

Security Objective	Confidentiality	Integrity	Availability
Potential Impact Level	[ ] Low [ ] Mod [ ] High	[ ] Low [ ] Mod [ ] High	[ ] Low [ ] Mod [ ] High
Justification / Rationale			
Overall System Categorization	[ ] Low [ ] Moderate [ ] High (highest water mark)		

Categorization Guidance
LOW Impact: Limited adverse effect on operations, assets, or individuals MODERATE Impact: Serious adverse effect — significant degradation of mission capability HIGH Impact: Severe or catastrophic adverse effect — loss of primary mission capabilities The overall system categorization = the HIGHEST impact level across all three security objectives

Step 3 — SELECT

Select the appropriate security control baseline from NIST SP 800-53 Rev 5, then tailor controls based on your risk assessment and organizational requirements.

Control Baseline Selection	Applicable Baseline	Controls Scoped In	Controls Scoped Out
Selected Baseline	[ ] Low [ ] Moderate [ ] High		
Overlays Applied	(e.g., Privacy, SCIF, Healthcare)		
Tailoring Rationale			
Common Controls Inherited			

Step 4 — IMPLEMENT

Document how each selected control is implemented. This section serves as the basis for assessment and authorization activities.

Use the Control Implementation Tracker in Section 5 to document implementation details for each control family. Key outputs of this step include:

- System Security Plan (SSP) — documents the control implementation
- Privacy Plan — addresses privacy controls if applicable
- SCRM Plan — addresses supply chain risk management
- Configuration Management Plan — documents baselines and change management

Step 5 — ASSESS

Determine whether controls are implemented correctly, operating as intended, and producing the desired outcomes.

Assessment Activity	Method	Assessor	Target Date
Security Assessment Plan (SAP)	Document assessment scope and methodology		
Control Testing	Interview, examine, test per SP 800-53A		
Penetration Testing	External/internal technical testing		
Vulnerability Scanning	Automated scanning of in-scope systems		
Security Assessment Report (SAR)	Document findings and recommendations		
POAM Development	Document weaknesses and remediation plan		

Step 6 — AUTHORIZE

The Authorizing Official (AO) reviews the authorization package and makes a formal risk-based decision to authorize system operation.

Authorization Package Component	Description	Status
System Security Plan (SSP)	Complete documentation of system, controls, and implementation	⬜
Security Assessment Report (SAR)	Results of control assessment including findings	⬜
Plan of Action & Milestones (POA&M)	Known weaknesses and remediation schedule	⬜
Risk Assessment	Organization and system-level risk findings	⬜
AO Risk Acceptance Decision	Formal Authorization to Operate (ATO) or denial	⬜
Authorization Decision Document	Signed authorization with conditions and expiration	⬜

Step 7 — MONITOR

Ongoing monitoring ensures the security posture of the system remains acceptable over time. This is not a one-time activity — it's a continuous program.

Monitoring Activity	Frequency	Responsible Party	Last Completed
Ongoing Control Assessment	Continuous / Annual		
Vulnerability Scanning	Monthly		
Penetration Testing	Annual		
Security Log Review	Daily / Weekly		
Configuration Change Review	Per change		
Incident Response Activities	As needed		
POA&M Updates	Monthly		
Annual Risk Assessment Update	Annual		

Monitoring Activity	Frequency	Responsible Party	Last Completed
Authorization Renewal Review	Per ATO conditions		

5. ISO 27001:2022 — Annex A Control Tracker

Use this tracker to document the implementation status and maturity level for each of the 93 ISO 27001:2022 Annex A controls. This tracker also serves as the foundation for your Statement of Applicability (SoA).

Maturity Scale Reference

1 — Initial: Ad hoc, undocumented, or absent. Relies on individual heroics.
2 — Developing: Some documented procedures but inconsistently applied.
3 — Defined: Documented, communicated, and consistently applied across the organization.
4 — Managed: Measured and monitored. Metrics in place. Regular management review.
5 — Optimized: Continuously improved. Industry-leading practice. Proactively evolving.

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1–5)
5. Organizational Controls (5.1 – 5.37)				
5.1	**Policies for information security**	Written IS policies approved by leadership	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.2	**Information security roles and responsibilities**	Security roles defined and assigned	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.3	**Segregation of duties**	Conflicting duties identified and separated	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.4	**Management responsibilities**	Management support for IS documented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.5	**Contact with authorities**	Process for contacting authorities during incidents	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.6	**Contact with special interest groups**	Participation in security information sharing	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5	**Threat**	Process for collecting and acting on threat intelligence	[ ] Implemented [ ] Partial [ ] Not	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
.7	**intelligence**		Implemented [ ] N/A	
5.8	**IS in project management**	Security integrated into project lifecycle	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.9	**Inventory of assets**	Asset inventory maintained and owned	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.10	**Acceptable use of assets**	Rules for acceptable use documented and communicated	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.11	**Return of assets**	Process for recovering assets on termination/exit	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.12	**Classification of information**	Information classification scheme defined	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.13	**Labelling of information**	Information labeled according to classification	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.14	**Information transfer**	Policies for transferring information to external parties	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.15	**Access control**	Access control policy documented and enforced	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.16	**Identity management**	Identity lifecycle management process in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.17	**Authentication information**	Passwords and authentication managed securely	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5	**Access rights**	Access rights provisioned,	[ ] Implemented [ ]	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
5.18		reviewed, and revoked	Partial [ ] Not Implemented [ ] N/A	
5.19	**Information security in supplier relationships**	IS requirements included in supplier agreements	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.20	**Addressing IS in supplier agreements**	IS controls contractually required from suppliers	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.21	**Managing IS in the ICT supply chain**	Supply chain security requirements defined	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.22	**Monitoring and review of supplier services**	Supplier performance regularly reviewed	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.23	**IS for use of cloud services**	Cloud security requirements and oversight in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.24	**IS incident management planning**	Incident response plan documented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.25	**Assessment and decision on IS events**	Process for categorizing and prioritizing incidents	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.26	**Response to IS incidents**	Documented incident response procedures	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.27	**Learning from IS incidents**	Post-incident review process exists	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.2	**Collection of evidence**	Procedures for evidence collection and preservation	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1–5)
8				
5.29	**IS during disruption**	IS maintained during disruptions and crises	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.30	**ICT readiness for business continuity**	ICT recovery capabilities tested and documented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.31	**Legal, statutory, regulatory requirements**	Applicable legal requirements identified and tracked	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.32	**Intellectual property rights**	Procedures to protect IP and licensed software	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.33	**Protection of records**	Records retention and protection procedures	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.34	**Privacy and PII protection**	Privacy requirements addressed and PII protected	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.35	**Independent review of IS**	Independent IS reviews conducted regularly	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.36	**Compliance with IS policies**	Compliance with IS policies reviewed regularly	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
5.37	**Documented operating procedures**	Operating procedures documented and maintained	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6. People Controls (6.1 – 6.8)				
6.	**Screening**	Background checks performed for relevant roles	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
1				
6.2	**Terms and conditions of employment**	IS responsibilities included in employment agreements	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.3	**IS awareness, education and training**	Security awareness training program in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.4	**Disciplinary process**	Disciplinary process for IS violations	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.5	**Responsibilities after termination**	Post-employment IS obligations enforced	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.6	**Confidentiality or NDA agreements**	NDAs in place for employees and contractors	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.7	**Remote working**	Security controls for remote working documented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
6.8	**IS event reporting**	Easy channel for reporting IS events exists	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7. Physical Controls (7.1 – 7.14)				
7.1	**Physical security perimeters**	Secure perimeters defined for sensitive areas	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.2	**Physical entry**	Physical access controlled and logged	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.3	**Securing offices, rooms and facilities**	Offices and sensitive areas physically secured	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.4	**Physical security monitoring**	CCTV / monitoring of physical facilities	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.5	**Protecting against physical and**	Controls for fire, flood, environmental threats	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
	environmental threats			
7.6	**Working in secure areas**	Procedures for working in secure areas	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.7	**Clear desk and clear screen**	Policy for clear desk and screen locking	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.8	**Equipment siting and protection**	Equipment protected from physical threats	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.9	**Security of assets off-premises**	Controls for assets used outside facilities	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.10	**Storage media**	Secure handling and disposal of storage media	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.11	**Supporting utilities**	Power, HVAC, and other utilities protected	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.12	**Cabling security**	Power and data cabling protected	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.13	**Equipment maintenance**	Maintenance performed and documented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
7.14	**Secure disposal or re-use of equipment**	Equipment sanitized before disposal or reuse	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8. Technological Controls (8.1 – 8.34)				
8.1	**User endpoint devices**	Endpoint security policies and controls in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8	**Privileged access**	Privileged accounts	[ ] Implemented [ ]	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
.2	**rights**	managed and monitored	Partial [ ] Not Implemented [ ] N/A	
8.3	**Information access restriction**	Access to information restricted by business need	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.4	**Access to source code**	Source code access restricted and logged	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.5	**Secure authentication**	MFA and strong authentication implemented	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.6	**Capacity management**	Capacity monitored and planned proactively	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.7	**Protection against malware**	Anti-malware controls deployed and updated	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.8	**Management of technical vulnerabilities**	Vulnerability management program exists	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.9	**Configuration management**	Secure configurations documented and enforced	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.10	**Information deletion**	Procedures for secure data deletion in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.11	**Data masking**	Sensitive data masked or anonymized as required	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.12	**Data leakage prevention**	DLP controls implemented for sensitive data	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.13	**Information backup**	Backup policy and procedures documented and tested	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
8.14	**Redundancy of IT**	IT redundancy implemented for critical systems	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.15	**Logging**	Security events logged and logs protected	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.16	**Monitoring activities**	Systems and networks monitored for anomalies	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.17	**Clock synchronization**	Clocks synchronized across systems (NTP)	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.18	**Use of privileged utility programs**	Privileged tools access restricted and logged	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.19	**Installation of software on operational systems**	Software installation restricted and controlled	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.20	**Networks security**	Network security controls and architecture in place	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.21	**Security of network services**	Network services identified and security requirements defined	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.22	**Segregation of networks**	Networks segmented based on risk and sensitivity	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.23	**Web filtering**	Web filtering controls implemented for users	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.	**Use of cryptography**	Cryptography policy and key management in place	[ ] Implemented [ ] Partial [ ] Not	1 2 3 4 5

Ctrl	Control Name	Key Implementation Evidence	Status	Maturity (1-5)
24			Implemented [ ] N/A	
8.25	**Secure development lifecycle**	Security integrated into development lifecycle (SDLC)	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.26	**Application security requirements**	Security requirements defined for applications	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.27	**Secure system architecture and engineering principles**	Security-by-design principles applied	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.28	**Secure coding**	Secure coding standards defined and followed	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.29	**Security testing in development and acceptance**	Security testing in UAT and pre-production	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.30	**Outsourced development**	Security requirements in outsourced dev contracts	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.31	**Separation of development, test and production**	Dev/Test/Prod environments separated	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.32	**Change management**	Change management process documented and followed	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.33	**Test information**	Production data protected in test environments	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5
8.34	**Protection of IS during audit testing**	IS controls maintained during audit activities	[ ] Implemented [ ] Partial [ ] Not Implemented [ ] N/A	1 2 3 4 5

6. Gap Analysis Worksheet

A gap analysis identifies the delta between your current security posture and the requirements of NIST RMF and ISO 27001. Documenting gaps creates a clear roadmap for remediation and provides evidence of due diligence to auditors.

6.1 Gap Scoring Methodology

Gap Rating	Risk Level	Description
Critical	Immediate Action Required	Control is absent. Significant exposure to breach, regulatory fine, or business disruption.
High	Remediate within 30 days	Control exists but has significant deficiencies. Material risk of exploitation.
Medium	Remediate within 90 days	Control partially implemented. Risk is manageable but should be improved.
Low	Remediate within 180 days	Minor gaps. Documentation or minor process improvements needed.

6.2 Gap Analysis Register

ID	Gap Description	Framework Reference	Gap Rating	Remediation Action	Owner	Target Date
G-01	No formal MFA enforcement on all privileged accounts	ISO 8.5 / NIST AC-2	Critical	Deploy MFA solution for all admin accounts within 30 days	[Owner]	
G-02	Incident response plan not documented or tested	ISO 5.24 / NIST IR-1	Critical	Develop IR plan; conduct tabletop exercise	[Owner]	
G-03	No vulnerability management program in place	ISO 8.8 / NIST RA-5	High	Implement monthly vulnerability scanning	[Owner]	
G-0	Asset inventory incomplete — cloud assets not	ISO 5.9 / NIST CM-8	High	Deploy cloud asset discovery tool;	[Owner]	

ID	Gap Description	Framework Reference	Gap Rating	Remediation Action	Owner	Target Date
4	tracked			update CMDB		
G-05	Vendor security assessments not conducted	ISO 5.19 / NIST SA-9	High	Implement vendor questionnaire process	[Owner]	
G-06	Security awareness training is ad hoc, not annual	ISO 6.3 / NIST AT-2	Medium	Deploy annual mandatory security awareness program	[Owner]	
G-07	No formal access review process (quarterly)	ISO 5.18 / NIST AC-2	Medium	Implement quarterly access certification reviews	[Owner]	
G-08	Backup testing not conducted or documented	ISO 8.13 / NIST CP-9	Medium	Schedule and document quarterly backup restoration tests	[Owner]	
G-09	Logging retention policy not defined	ISO 8.15 / NIST AU-11	Medium	Define and enforce log retention policy (minimum 90 days)	[Owner]	
G-10	No formal change management process	ISO 8.32 / NIST CM-3	Medium	Implement change advisory board (CAB) process	[Owner]	
[G-XX]	[Add identified gaps below]					

7. Risk Register & Risk Heat Map

7.1 Risk Scoring Methodology

Risk scores are calculated using the standard formula: Risk Score = Likelihood × Impact. Scores range from 1 (Very Low) to 25 (Critical).

5×5 Risk Heat Map

Impact → Likelihood ↓	1 Negligible	2 Minor	3 Moderate	4 Major	5 Severe
5 Almost Certain	5	10	15	20	25
4 Likely	4	8	12	16	20
3 Possible	3	6	9	12	15
2 Unlikely	2	4	6	8	10
1 Rare	1	2	3	4	5

Very Low (1-3)	Low (4-6)	Medium (8-15)	High / Critical (16-25)

7.2 Risk Register

ID	Risk Description	Asset / System Affected	L	I	Score	Treatment	Owner	Target Date
R-01	Ransomware attack encrypts production systems causing extended outage	All IT Systems	4	5	20	Mitigate		
R-02	Phishing attack leads to credential compromise and data	Email / Users	5	4	20	Mitigate		

ID	Risk Description	Asset / System Affected	L	I	Score	Treatment	Owner	Target Date
	breach							
R-03	Unpatched software exploited by external attacker	Servers / Endpoints	4	4	16	Mitigate		
R-04	Insider threat — unauthorized data exfiltration by employee	Data / Applications	2	5	10	Mitigate		
R-05	Third-party vendor breach exposes customer data	Vendor Systems	3	4	12	Transfer		
R-06	Loss of critical system availability due to hardware failure	Servers / Storage	2	4	8	Mitigate		
R-07	Business email compromise (BEC) results in financial fraud	Email / Finance	3	4	12	Mitigate		
R-08	Regulatory non-compliance results in significant fine	Compliance Program	2	3	6	Mitigate		
[R-XX]	[Add identified risks]							

Risk Treatment Options

MITIGATE — Implement controls to reduce likelihood or impact to an acceptable level

ACCEPT — Formally accept the risk (requires documented management sign-off)
TRANSFER — Shift risk to a third party (e.g., cyber insurance, contract clauses)
AVOID — Eliminate the activity or condition that gives rise to the risk

8. Implementation Roadmap

Use this roadmap to plan and track your NIST RMF / ISO 27001 implementation. Prioritize based on risk ratings from the gap analysis. Quick wins build momentum and demonstrate progress to leadership.

PHASE 1 — IMMEDIATE (0–30 Days) | Critical Gaps Only

Action Item	Framework Control	Owner	Status
Enforce MFA on all privileged and admin accounts	ISO 8.5 / NIST IA-2		⬜ Not Started
Document and communicate Incident Response Plan	ISO 5.24 / NIST IR-1		⬜ Not Started
Implement automated vulnerability scanning	ISO 8.8 / NIST RA-5		⬜ Not Started
Conduct emergency security awareness training	ISO 6.3 / NIST AT-2		⬜ Not Started
Assign formal security roles and responsibilities	ISO 5.2 / NIST PM-2		⬜ Not Started

PHASE 2 — SHORT-TERM (30–90 Days) | High Priority Gaps

Action Item	Framework Control	Owner	Status
Complete and test asset inventory (CMDB)	ISO 5.9 / NIST CM-8		⬜ Not Started
Implement vendor security assessment process	ISO 5.19 / NIST SA-9		⬜ Not Started
Deploy endpoint protection (EDR) on all devices	ISO 8.7 / NIST SI-3		⬜ Not Started
Establish quarterly access review process	ISO 5.18 / NIST AC-2		⬜ Not Started
Define and implement network segmentation	ISO 8.22 / NIST SC-7		⬜ Not Started

Action Item	Framework Control	Owner	Status
Implement security information and event monitoring (SIEM)	ISO 8.16 / NIST AU-6		⬜ Not Started
Develop and communicate security policies	ISO 5.1 / NIST PM-1		⬜ Not Started
Test data backups and document results	ISO 8.13 / NIST CP-9		⬜ Not Started

PHASE 3 — MEDIUM-TERM (90–180 Days) | Program Maturation

Action Item	Framework Control	Owner	Status
Conduct full internal audit against ISO 27001 controls	ISO 9.2 / NIST CA-2		⬜ Not Started
Implement data loss prevention (DLP) controls	ISO 8.12 / NIST SI-12		⬜ Not Started
Complete ISMS documentation package	ISO 4–10 / NIST All		⬜ Not Started
Conduct management review of ISMS	ISO 9.3 / NIST PM-3		⬜ Not Started
Run incident response tabletop exercise	ISO 5.26 / NIST IR-3		⬜ Not Started
Engage external auditor for Stage 1 audit (ISO)	ISO Certification		⬜ Not Started
Define KPIs and metrics for security program	ISO 9.1 / NIST PM-6		⬜ Not Started

PHASE 4 — LONG-TERM (180–365 Days) | Certification & Continuous Improvement

Action Item	Framework Control	Owner	Status
External ISO 27001 Stage 2 certification audit	ISO Certification		⬜ Not Started

Action Item	Framework Control	Owner	Status
Establish continuous monitoring program	ISO 10 / NIST CA-7		⬜ Not Started
Implement security metrics dashboard for board	ISO 9.1 / NIST PM-6		⬜ Not Started
Complete RMF authorization package (ATO)	NIST RMF Step 6		⬜ Not Started
Annual penetration test and report	ISO 8.8 / NIST CA-8		⬜ Not Started
Conduct annual security awareness training	ISO 6.3 / NIST AT-2		⬜ Not Started

9. Executive Summary Template

Use this section to communicate your ISMS status and risk posture to leadership, the board, and external stakeholders. Replace bracketed fields with your organization's actual data.

9.1 Program Status Scorecard

Domain	Prior Quarter	This Quarter	Trend	Status
Overall Security Maturity	[X.X / 5.0]	[X.X / 5.0]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
Organizational Controls (ISO 5)	[X.X / 5.0]	[X.X / 5.0]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
People Controls (ISO 6)	[X.X / 5.0]	[X.X / 5.0]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
Physical Controls (ISO 7)	[X.X / 5.0]	[X.X / 5.0]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
Technological Controls (ISO 8)	[X.X / 5.0]	[X.X / 5.0]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
NIST RMF Compliance	[XX%]	[XX%]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
Open Critical / High Gaps	[XX]	[XX]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind
Vendor Risk Coverage	[XX%]	[XX%]	↑ / ↓ / →	[ ] On Track [ ] At Risk [ ] Behind

9.2 Top Risks to the Business

The following risks represent the highest priority items requiring leadership awareness and/or decision:

#	Risk	Rating	Business Impact	Recommended Action
1	[Top risk — e.g., ransomware / credential compromise]	Critical	[e.g., Potential $X revenue loss, X days downtime]	[e.g., Deploy MFA; improve backup testing]
2	[Second risk]	High		
3	[Third risk]	High		
4	[Fourth risk]	Medium		
5	[Fifth risk]	Medium		

9.3 Certification Status

Certification / Framework	Current Status	Target Date	Notes
ISO 27001:2022	[ ] Certified [ ] In Progress [ ] Planned [ ] N/A		
NIST RMF (ATO)	[ ] Authorized [ ] In Progress [ ] Planned [ ] N/A		
SOC 2 Type II	[ ] Certified [ ] In Progress [ ] Planned [ ] N/A		
CMMC Level [X]	[ ] Certified [ ] In Progress [ ] Planned [ ] N/A		
PCI-DSS	[ ] Compliant [ ] In Progress [ ] Planned [ ] N/A		
HIPAA Security Rule	[ ] Compliant [ ] In Progress [ ] Planned [ ] N/A		

9.4 Key Recommendations for Leadership

Recommended Leadership Actions

1. Approve budget for MFA and endpoint detection and response (EDR) deployment — highest ROI controls
2. Assign formal ownership of the ISMS program to a named executive sponsor
3. Schedule a board-level tabletop exercise for ransomware / incident response
4. Authorize engagement with ISO 27001 certification auditor
5. Review and formally accept documented residual risks

Time and resource investment in these five actions will materially reduce organizational cyber risk within 90 days.

10. Statement of Applicability (SoA) — Summary

The Statement of Applicability (SoA) is a mandatory ISO 27001 artifact. It lists all Annex A controls, whether they are applicable to your ISMS, and the justification for inclusion or exclusion.

ISO 27001 Requirement (Clause 6.1.3)

The organization shall produce a Statement of Applicability that contains:
(a) The necessary controls (from Annex A)
(b) Justification for their inclusion
(c) Whether selected controls are implemented or not
(d) Justification for the exclusion of any Annex A controls

Controls may only be excluded if there is a documented justification AND the associated risk has been accepted by the authorizing official.

Ctrl	Control Name	Applicable?	Implemented?	Justification / Notes
5.1	Policies for information security	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
5.9	Inventory of information assets	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
5.15	Access control	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
5.24	IS incident management planning	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
6.3	IS awareness, education and training	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	

Ctrl	Control Name	Applicable?	Implemented?	Justification / Notes
7.1	Physical security perimeters	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.2	Privileged access rights	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.5	Secure authentication	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.7	Protection against malware	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.8	Management of technical vulnerabilities	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.13	Information backup	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.15	Logging	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.24	Use of cryptography	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
8.25	Secure development lifecycle	[ ] Yes [ ] No	[ ] Yes [ ] Partial [ ] No	
[...co				

Ctrl	Control Name	Applicable?	Implemented?	Justification / Notes
ntinuedforall93controlsinpremiumversion...]				

Note: The complete 93-control SoA worksheet is included in the Premium Implementation Toolkit.

11. Plan of Action & Milestones (POA&M)

The POA&M documents known weaknesses, planned remediation activities, resources required, and target completion dates. It is a mandatory artifact for NIST RMF and strongly recommended for ISO 27001 nonconformity tracking.

ID	Weakness / Finding	Control Reference	Severity	Resources	Remediation Steps	Target Date	Status
P-01	No MFA on privileged accounts	NIST IA-2 / ISO 8.5	Critical	$X / Xh	1. Evaluate MFA vendors 2. Deploy pilot 3. Full rollout		⬜ Open
P-02	Incident Response Plan not documented	NIST IR-1 / ISO 5.24	Critical	$X / Xh	1. Draft IRP 2. Review 3. Tabletop		⬜ Open
P-03	No formal vulnerability scanning program	NIST RA-5 / ISO 8.8	High	$X / Xh	1. Select scanner 2. Initial scan 3. Monthly cadence		⬜ Open
P-04	Asset inventory incomplete	NIST CM-8 / ISO 5.9	High	$X / Xh	1. Audit existing assets 2. Deploy discovery 3. Assign owners		⬜ Open
P-05	No annual security awareness training	NIST AT-2 / ISO 6.3	Medium	$X / Xh	1. Select LMS platform 2. Build curriculum 3. Deploy		⬜ Open
[P-XX]	[Add findings from gap analysis]						⬜ Open

12. References & Resources

Authoritative References

Resource	Source / Link
NIST Risk Management Framework	csrc.nist.gov/projects/risk-management
NIST SP 800-53 Rev 5 — Security Controls	csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
NIST SP 800-37 Rev 2 — RMF Guide	csrc.nist.gov/publications/detail/sp/800-37/rev-2/final
NIST SP 800-30 — Risk Assessment Guide	csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
NIST SP 800-61 — Incident Response Guide	csrc.nist.gov/publications/detail/sp/800-61/rev-2/final
ISO/IEC 27001:2022 Standard	iso.org/standard/27001
ISO/IEC 27005:2022 — Risk Management	iso.org/standard/80585.html
NIST Cybersecurity Framework 2.0	nist.gov/cyberframework
CIS Controls v8	cisecurity.org/controls
CISA Resources	cisa.gov/cybersecurity

Version History

Version	Date	Description	Author
1.0	[Date]	Initial release	Threatnexis
1.1		Next update — describe changes	

Want the Complete NIST RMF / ISO 27001 Premium Toolkit?

The premium version includes everything you need for full implementation:

- ✓ Complete 93-control SoA worksheet with auto-scoring
- ✓ Executive dashboard with maturity scores and trend charts
- ✓ Pre-populated sample findings and recommendations
- ✓ Industry-specific control guides (Healthcare, Finance, SaaS)
- ✓ Board-ready risk report templates (PPTX + DOCX)
- ✓ Automated risk scoring and heat maps (Excel)

threatnexis.com/nist-iso27001-premium-toolkit

Need Expert Guidance on Your Implementation?

Threatnexis provides hands-on cybersecurity advisory services:

- ✓ NIST RMF Assessment & ATO Support
- ✓ ISO 27001 Gap Analysis & Certification Readiness
- ✓ Virtual CISO (vCISO) Services
- ✓ Security Program Build-Out
- ✓ Ransomware Readiness & Tabletop Exercises

Book a Free Consultation: threatnexis.com/consult

Join the Threatnexis Insider Newsletter

Get free templates, checklists, breach analyses, and security tips delivered to your inbox.

Subscribe at: threatnexis.com/newsletter

Appendix A — SEO & Content Strategy

Internal use only. Use this appendix to guide content marketing and SEO efforts around this resource.

SEO Element	Value
Primary Keyword	NIST RMF implementation template
Secondary Keywords	ISO 27001 implementation guide, NIST RMF ISO 27001 mapping, ISMS implementation template, cybersecurity framework template
Meta Title	NIST RMF / ISO 27001 Implementation Template | Threatnexis
Meta Description	Free NIST RMF and ISO 27001 implementation template. Includes gap analysis, control tracker, risk register, and executive summary. Download now.
SEO Slug	/nist-rmf-iso-27001-implementation-template
Search Intent	Commercial / Informational — practitioner seeking implementation tools
Commercial Intent	High — users actively implementing frameworks likely to convert to premium or consulting
Content Cluster	Risk Management / GRC / Compliance

People Also Ask — Target Topics

- How do I implement the NIST Risk Management Framework?
- What is the difference between NIST RMF and ISO 27001?
- How long does it take to get ISO 27001 certified?
- What is an ISMS and how do I build one?
- What is a Statement of Applicability (SoA) in ISO 27001?
- How do I conduct a cybersecurity gap analysis?
- What are the 7 steps of the NIST RMF?
- What controls are in ISO 27001 Annex A?
- How much does ISO 27001 certification cost?
- What is the difference between NIST CSF and NIST RMF?

Suggested Supporting Blog Articles

1. NIST RMF vs ISO 27001: Which Framework Is Right for Your Organization?
2. How to Conduct a Cybersecurity Gap Analysis (Step-by-Step Guide)
3. ISO 27001 Annex A Controls Explained: The Complete Guide
4. What Is an ISMS? Building Your Information Security Management System
5. The NIST RMF 7 Steps Explained Simply (With Checklist)
6. How to Write a Statement of Applicability (SoA) for ISO 27001
7. ISO 27001 Certification Cost: What to Budget in 2025
8. NIST SP 800-53 Controls: A Plain-English Guide for IT Managers
9. How to Build a Vendor Risk Management Program
10. What Is a vCISO and Does Your Business Need One?

Related Templates (Suggested Companion Downloads)

- Cybersecurity Risk Assessment Template (NIST SP 800-30)
- Vendor Security Questionnaire & Scorecard
- Incident Response Plan Template
- Business Continuity Plan Template
- Cybersecurity Maturity Scorecard

THREATNEXIS
Cybersecurity Intelligence & Advisory
threatnexis.com | info@threatnexis.com