NIS2
Survival
Guide

NIS2 Survival Guide for CISOs and Board Administrators

NIS2 Survival Guide
for CISOs and Board Administrators

A Practical Approach to NIS2 Compliance and Governance in Italian Public Administrations, Leveraging NIST CSF 2.0 for Enhanced Protection

Introduction

The evolving digital landscape presents unprecedented challenges to the security and resilience of critical infrastructure. In the European Union, the Directive on measures for a high common level of cybersecurity across the Union (**NIS2 Directive, (EU) 2022/2555**) establishes a new baseline for cybersecurity risk management and incident reporting **obligations for essential and important entities**. **Italy**, having transposed NIS2 into national law via Legislative **Decree No. 138 of September 4, 2024** (effective October 16, 2024), places significant new responsibilities on organizations operating critical infrastructure, including Public Administration (PA) entities designated as "essential entities".

This guide provides Chief Information Security Officers (CISOs) and management within Italian critical infrastructure PAs a practical roadmap for developing and implementing a robust cybersecurity governance strategy aligned with both NIS2 obligations and the comprehensive structure of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) version 2.0. Adherence to these frameworks is not merely a compliance exercise but a strategic imperative to ensure the continuity of essential services, protect sensitive data, and maintain public trust in an era of increasing cyber threats, including sophisticated state-sponsored attacks, ransomware, and supply chain compromises.

This document outlines a ten-chapter approach, integrating legal requirements, governance structures, policy development, risk management, technical and organizational measures (TOMs), incident handling, supply chain security, monitoring, reporting, and inspection preparedness, specifically tailored for the Italian PA context operating critical IT and Operational Technology (OT) systems.

Chapter 1: Understand the NIS2 Obligations

The foundation of any effective cybersecurity strategy under the new regulatory landscape is a thorough understanding of the specific obligations imposed by the NIS2 Directive and its Italian transposition (Legislative Decree 138/2024). For Italian Public Administration entities operating critical infrastructure, this understanding is paramount.

1.1 Know Your Scope: An "Essential Entity"

Under NIS2 and the Italian decree, organizations are classified as either "essential entities" (soggetti essenziali - EE) or "important entities" (soggetti importanti - EI) based on their sector, size, and the criticality of the services they provide. Critical infrastructure PAs typically fall under the essential entity category. This designation carries significant implications, primarily subjecting the entity to proactive (ex-ante) supervision by the competent national authority and potentially higher penalties for non-compliance compared to important entities, which face ex-post supervision. The Agenzia per la Cybersicurezza Nazionale (ACN) is the designated national competent authority in Italy responsible for overseeing NIS2 implementation, registration, and supervision. Entities were required to self-assess their status by December 31, 2024, and register via the ACN portal between January and February 2025, with ACN publishing the official list by March 31, 2025.

1.2 Understand Your Obligations

Being classified as an essential entity under Italian Law No. 138/2024 entails several core obligations derived directly from the NIS2 Directive:

- **Cybersecurity Risk Management Measures (Art. 21, NIS2 / Art. 21, D.Lgs. 138/2024):** Entities must implement "appropriate and proportionate technical, operational and organizational measures" to manage risks to their network and information systems used for service provision. This requires an "all-hazards approach," considering both cyber threats and physical disruptions. Measures must be based on risk assessment, state-of-the-art practices, relevant standards (e.g., ISO/IEC 27001, NIST CSF), and cost, ensuring a security level appropriate to the identified risks. Article 21 explicitly lists minimum required measures, including policies for risk analysis and security, incident handling, business continuity / disaster recovery, supply chain security, secure system development /

maintenance (including vulnerability management), effectiveness assessment procedures, cyber hygiene and training, cryptography / encryption use, HR security / access control / asset management, and MFA / secure communications.

- **Incident Notification (Art. 23, NIS2 / Art. 25, D.Lgs. 138/2024):** Significant incidents impacting service provision must be reported to the national Computer Security Incident Response Team (CSIRT Italia, managed by ACN) or the competent authority (ACN). The Italian decree mandates compliance with these reporting obligations starting January 1, 2026. The multi-stage reporting process includes:
  - **Early Warning:** Within **24 hours** of becoming aware of the significant incident, indicating potential malicious cause or cross-border impact.
  - **Incident Notification:** Within **72 hours** of becoming aware, providing an initial assessment (severity, impact, indicators of compromise).
  - **Intermediate Report:** Upon request from CSIRT Italia/ACN.
  - **Final Report:** Within **one month** of the incident notification (or one month after handling if ongoing), detailing the incident, root cause, mitigation measures, and cross-border impact.
- **Governance and Accountability (Art. 20, NIS2 / Art. 20, D.Lgs. 138/2024):** Management bodies (e.g., Board of Directors, Executive Committee) must approve the cybersecurity risk management measures, oversee their implementation, and can be held liable for infringements. This elevates cybersecurity to a strategic board-level concern. Management must also undergo specific cybersecurity training. Compliance with governance requirements is mandated within 18 months of receiving ACN notification.
- **Regular Audits and Supervision (Art. 32, 33 NIS2 / Art. 34-37, D.Lgs. 138/2024):** Essential entities are subject to proactive supervision by ACN. This includes regular and ad-hoc audits, on-site inspections, and requests for information / evidence to verify compliance. ACN can issue binding instructions and corrective orders.
- **Penalties for Non-Compliance** (Art. 34, NIS2 / Art. 38, D.Lgs. 138/2024): Significant administrative fines can be imposed for non-compliance. For essential entities, fines can reach up to €10 million or 2% of the total worldwide annual turnover, whichever is higher. Italy also sets minimum fines and specific (lower) caps for public administrations (€25,000 to €125,000 for EEs). Repeated violations or failure to act on binding instructions can lead to higher penalties. **Management liability** is also a key enforcement mechanism.

1.3 Aligning Legal Interpretation

CISOs must ensure their governance strategy is grounded in the official text of Directive (EU) 2022/2555 and, critically, the specific requirements of the Italian Legislative Decree 138/2024. It is also advisable to monitor guidance and implementing acts issued by the European Commission and ACN. Engaging with legal and compliance teams is essential to ensure accurate interpretation and application of these requirements within the specific context of the PA critical infrastructure. Italy's transposition includes some national specificities, such as annual registration periods, expanded sector definitions in annexes, a dedicated NIS2 implementation committee, and specific audit powers for ACN.

Chapter 2: Build the Cybersecurity Governance Model

A clearly defined and formally documented cybersecurity governance model is essential for meeting NIS2 requirements, particularly the emphasis on management accountability (Art. 20), and for effectively managing cybersecurity risk across the organization. It provides structure, clarifies responsibilities, and ensures alignment between strategic objectives and operational activities. The NIST CSF 2.0 Govern (GV) function provides a strong foundation for establishing this model, focusing on organizational context, strategy, roles, policy, and oversight.

2.1 Define a Clear Governance Structure

A multi-tiered governance structure helps delineate responsibilities and decision-making authority across different organizational levels. For a critical infrastructure PA, a suitable model includes:

- Strategic Cybersecurity (Board + CISO):
  - **Responsibility:** Setting the overall cybersecurity direction, defining risk appetite and tolerance, approving the cybersecurity strategy and policies, allocating resources, overseeing program effectiveness, and ensuring compliance with NIS2 (including management liability). The Board (or equivalent PA Executive Committee/Director General) is ultimately accountable.
  - **Actors:** Board of Directors/Executive Committee, Director General/CEO, CISO. The CISO provides strategic advice and reports directly to the highest executive level (CEO/DG or equivalent).
- Tactical Cybersecurity (CISO + Cyber Risk Committee):
  - **Responsibility:** Translating strategic direction into actionable plans, developing and maintaining policies and standards, managing the cybersecurity budget, overseeing the risk management program (Chapter 4), coordinating cross-functional security initiatives, and reporting on posture and incidents to the strategic level.
  - **Actors:** CISO, Cyber Risk Committee (or Cybersecurity Steering Committee), representatives from IT, OT, Legal, Compliance, Risk Management, HR, Physical Security, and key business units.
- Operational Cybersecurity (SOC, IT, OT Security Teams):
  - **Responsibility:** Implementing and operating security controls (TOMs - Chapter 5), monitoring for threats and incidents (Chapter 6), managing

vulnerabilities (Chapter 4), responding to security events, maintaining security infrastructure, and executing day-to-day security tasks.
    - **Actors:** Security Operations Center (SOC) / SIEM team, IT Security team, OT Security team, Network Operations, System Administrators, Application Security specialists.

This structure ensures clear lines of communication and escalation, from operational teams detecting issues to tactical committees analyzing risks and strategic leadership making informed decisions.

2.2 Create a Cybersecurity Governance Charter

A formal **Cybersecurity Governance Charter** is a concise document that codifies the governance model. It serves as the foundational document outlining how cybersecurity is managed within the organization.

Template: Cybersecurity Governance Charter Outline

1. **Introduction and Purpose**:
    - State the charter's objective: To establish the framework, roles, responsibilities, and processes for governing cybersecurity within <Organization Name>, ensuring alignment with strategic goals, NIS2 compliance, and effective risk management.
    - Reference relevant mandates (NIS2 Directive, D.Lgs. 138/2024, NIST CSF 2.0, organizational policies).
2. **Scope**:
    - Define the applicability of the charter (e.g., all departments, personnel, IT/OT systems, data, third parties involved in critical service delivery).
3. **Governance Structure**:
    - Describe the Strategic, Tactical, and Operational levels defined in Section 2.1.
    - Detail the composition, mandate, and frequency of meetings for key bodies (e.g., Board/Executive Committee oversight role, Cyber Risk Committee).
4. **Roles and Responsibilities**:
    - Clearly define the cybersecurity responsibilities for:
        - Board of Directors / Executive Committee (Strategic oversight, risk appetite, policy approval, accountability)
        - CEO / Director General (Overall responsibility, CISO reporting line)
        - Chief Information Security Officer (CISO) (Strategy development, program management, reporting, policy enforcement, incident oversight, liaison

        with ACN/CSIRT)
        - Cyber Risk Committee (Tactical oversight, risk review, policy recommendation, cross-functional coordination)
        - Chief Information Officer (CIO) (Technology infrastructure, collaboration with CISO)
        - IT/OT Security Teams (Operational implementation, monitoring, response)
        - Risk Management Function (Collaboration on risk assessment/treatment)
        - Compliance Function (Monitoring regulatory adherence)
        - Legal Department (Contract review, incident legal support)
        - Human Resources (Training, personnel security)
        - Physical Security (Coordination on physical controls)
        - All Personnel (Adherence to policies, reporting incidents)
    - Reference NIST CSF Govern Function (GV.RR)
5. **Decision-Making Processes**:
    - Outline how key cybersecurity decisions are made (e.g., policy approval, risk acceptance, major security investments, incident escalation thresholds).
    - Specify quorum and voting rules for committees.
6. **Reporting Lines**:
    - Explicitly state that the CISO reports directly to the CEO/Director General or equivalent highest executive level. This ensures visibility and authority.
    - Define reporting flows from operational teams to tactical committees, and from the CISO/Committee to the strategic leadership (Board/Executive Committee). Detail frequency and format (e.g., quarterly board reports - Chapter 9).
7. **Link with Risk Management and Compliance Functions**:
    - Describe the interaction and collaboration mechanisms between cybersecurity governance bodies and the established Enterprise Risk Management (ERM) and Compliance functions.
    - Ensure alignment of risk assessment methodologies (Chapter 4) and compliance monitoring (Chapter 8).
8. **Charter Review and Updates**:
    - Specify the frequency (e.g., annually) and process for reviewing and updating the charter to ensure continued relevance and effectiveness.
9. **Approval**:
    - Signature block for formal approval by the Board/Executive Committee or Director General.

This charter provides the necessary clarity and authority to drive cybersecurity initiatives effectively within the PA. Establishing clear reporting lines, particularly ensuring the CISO reports to the highest executive level, is critical for the visibility and influence needed to implement NIS2-level security. Furthermore, integrating cybersecurity governance with existing ERM and compliance functions prevents silos and ensures a holistic approach to managing organizational risk.

Chapter 3: Establish Policies and Procedures

Formal policies and procedures are the bedrock of a standardized and compliant cybersecurity program. NIS2 explicitly requires certain policies (e.g., Art. 21 mandates policies on risk analysis, information system security, incident handling, BCDR, supply chain security, effectiveness assessment, cryptography, HR security, access control, asset management). These documents translate strategic intent and governance decisions into actionable requirements for personnel and systems. For a critical infrastructure PA, these must cover both Information Technology (IT) and Operational Technology (OT) environments.

3.1 Standardization Through Formal Documentation

Policies define *what* needs to be done and *why*, setting high-level direction and requirements. Procedures detail *how* specific tasks are performed, providing step-by-step instructions. Standards specify mandatory technical configurations or rules. Guidelines offer recommended practices. Using established templates and frameworks (like those from SANS, NIST, or based on ISO 27001/27002) can accelerate development, but they **must** be customized to the organization's specific context, technologies (IT/OT), risks, and regulatory obligations (NIS2, GDPR, PSNC).

3.2 Policy Structure Example

Each policy should follow a consistent structure for clarity and usability:

- **Policy Title:** Clear and descriptive (e.g., Incident Response Policy).
- **Version Control:** Document version, date, author, approver, review cycle.
- **Purpose:** State the policy's main goal and rationale. Example (Incident Response): "To establish a consistent and effective approach for detecting, responding to, and recovering from cybersecurity incidents, minimizing impact and ensuring timely reporting as required by NIS2."
- **Scope:** Define who and what the policy applies to (e.g., all personnel, systems, data, locations, third parties handling PA data). *Example (Incident Response): "This policy applies to all personnel, contractors, IT and OT systems, and data managed by <Organization Name>, and covers all suspected or confirmed cybersecurity incidents."*
- **Policy Statements / Requirements:** The core rules and mandates. These should be clear, concise, and mandatory. Example (Incident Response): "All suspected

cybersecurity incidents must be reported immediately to the designated internal point of contact (e.g., SOC/Help Desk)."; "The Incident Response Team (IRT) must follow the defined phases: Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned."; "Significant incidents, as defined by NIS2 criteria, must be reported to CSIRT Italia/ACN within the mandated timeframes (24h early warning, 72h notification, 1-month final report)."

- **Roles and Responsibilities:** Define who is responsible for implementing, enforcing, and complying with the policy (e.g., CISO, IT/OT teams, SOC, users, management). *Example (Incident Response): "The CISO is responsible for overseeing the Incident Response Program. The IRT Lead coordinates response activities. All personnel are responsible for reporting suspected incidents."*
- **Compliance Criteria / Enforcement:** State how compliance will be monitored (e.g., audits, log reviews) and the consequences of non-compliance (e.g., disciplinary action, linkage to performance reviews).
- **Related Documents:** List relevant procedures, standards, guidelines, or other policies.
- **Definitions:** Define key terms used in the policy.
- **Approval:** Signature of the approving authority (e.g., CISO, Cyber Risk Committee, Board).

3.3 Core Policies for NIS2 Compliance

While numerous policies are needed, NIS2 compliance necessitates at least:

1. **Information Security Policy (ISP):** The overarching policy establishing management's commitment to information security, defining objectives, and referencing other specific policies. *Mandatory reference point.*
   - *Example Requirement:* "All organizational units shall implement security controls commensurate with the value and sensitivity of the information assets they manage, in alignment with the organization's risk management framework."
2. **Risk Management Policy:** Defines the organization's approach to identifying, assessing, evaluating, and treating cybersecurity risks (linking to Chapter 4). *Mandatory under NIS2 Art. 21(2)(a).*
   - *Example Requirement:* "Cybersecurity risk assessments shall be conducted at least annually, or upon significant changes to the IT/OT environment, threats, or business objectives, following the methodology outlined in the Cybersecurity Risk Management Procedure."

3. **Incident Response Policy:** Governs the detection, analysis, containment, eradication, recovery, and post-mortem analysis of security incidents (linking to Chapter 6). *Mandatory under NIS2 Art. 21(2)(b)*. Must explicitly include notification procedures for CSIRT Italia/ACN according to NIS2 timelines.
   - *Example Requirement:* "The Incident Response Team shall classify incidents based on severity and impact, and escalate significant incidents according to the defined procedure, ensuring compliance with NIS2 reporting deadlines to CSIRT Italia/ACN."
4. **Business Continuity and Disaster Recovery (BCDR) Policy:** Outlines how the organization will maintain critical operations during disruptions and recover IT/OT systems and data afterwards (linking to NIST CSF Recover function). *Mandatory under NIS2 Art. 21(2)(c)*.
   - *Example Requirement:* "Business Impact Analyses (BIAs) shall be conducted to identify critical processes and systems and define Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs)."; "BCDR plans, including backup restoration, shall be tested at least annually."
5. **Third-Party Cybersecurity Policy (Supply Chain Security):** Defines requirements for managing cybersecurity risks associated with suppliers, vendors, and partners (linking to Chapter 7). *Mandatory under NIS2 Art. 21(2)(d)*.
   - *Example Requirement:* "Cybersecurity requirements, including incident notification obligations and right-to-audit clauses, shall be included in contracts with critical suppliers."; "Regular risk assessments shall be performed on critical third parties based on the sensitivity of data accessed or services provided."

Developing these core policies, ensuring they cover both IT and OT domains where applicable, and customizing them using a structured approach provides a solid foundation for NIS2 compliance and effective cybersecurity management. These policies must be communicated effectively and integrated into employee training programs (Chapter 5).

Chapter 4: Risk Management Program

NIS2 mandates a proactive and systematic approach to cybersecurity risk management. Article 21 requires essential entities to implement appropriate measures based on risk analysis. As CISO, establishing a continuous Risk Management program aligned with recognized frameworks is fundamental. This program informs policy development (Chapter 3), guides the selection and implementation of controls (Chapter 5), and provides crucial input for governance reporting (Chapter 9). The NIST CSF 2.0 Govern (GV.RM, GV.SC) and Identify (ID.RA, ID.AM, ID.TH, ID.VU) functions provide a structured approach.

4.1 The Continuous Risk Management Cycle

A robust risk management program operates as a continuous cycle, adapting to changes in assets, threats, vulnerabilities, and business objectives. Key phases include:

1. **Context Establishment (ISO 27005):** Define the scope, risk criteria (impact and likelihood scales), risk appetite/tolerance, and roles/responsibilities for risk management, aligned with the governance model (Chapter 2).
2. **Asset Identification (NIST CSF ID.AM):** Compile and maintain a comprehensive inventory of critical assets supporting essential services. This **must** include both IT assets (servers, networks, applications, data) and OT assets (SCADA, DCS, PLCs, sensors, industrial networks). The inventory should detail attributes like owner, location, criticality, data sensitivity, dependencies, and current security posture. *Action: Develop an Asset Inventory, potentially starting with critical services and mapping dependencies. Consider using existing tools or templates.*
3. **Threat Analysis (NIST CSF ID.TH):** Identify potential threat sources (adversarial, accidental, structural, environmental) and relevant threat events targeting critical infrastructure PAs. Key threats to consider include:
   - **Nation-State Actors / Advanced Persistent Threats (APTs):** Targeting critical infrastructure for espionage, disruption, or strategic advantage.
   - **Ransomware:** Increasingly targeting critical sectors, including healthcare and energy, causing operational disruption and data exfiltration. Italy has seen a rise in ransomware attacks.
   - **Supply Chain Attacks:** Exploiting vulnerabilities in third-party software or services to compromise downstream targets. NIS2 places strong emphasis here.
   - **Distributed Denial-of-Service (DDoS):** Often used by hacktivists (e.g., pro-

Russian groups targeting Italian entities) to disrupt services and gain visibility.
   - **Insider Threats:** Malicious or accidental actions by employees or contractors.
   - **OT-Specific Threats:** Targeting ICS protocols, manipulating physical processes, causing safety incidents.
   - Action: Leverage threat intelligence from ACN, ENISA, CSIRT Italia, ISACs, and commercial providers.

4. **Vulnerability Management (NIST CSF ID.VU):** Systematically identify, assess, and remediate vulnerabilities in IT and OT systems. This involves:
   - **Regular Vulnerability Scanning:** Automated scanning of networks and systems to detect known vulnerabilities (CVEs). Frequency depends on risk and compliance requirements (e.g., quarterly for PCI DSS, potentially monthly or weekly for critical systems).
   - **Penetration Testing:** Simulated attacks to identify exploitable weaknesses. NIS2 implies the need for regular testing. While some sources suggest a specific frequency like every 6 months for Italian entities, others indicate ACN has discretion or recommend annual/biannual tests or testing after significant changes. A risk-based approach is prudent.
   - **Patch Management:** Timely application of security patches (see Chapter 5).
   - Action: Establish formal vulnerability scanning and penetration testing procedures, defining frequency based on risk assessment and regulatory guidance (monitor ACN specifics). Implement a patch management process with clear SLAs (Chapter 5).
5. **Risk Assessment (NIST CSF ID.RA / ISO 27005):** Analyze identified threats and vulnerabilities in the context of specific assets to determine the likelihood of a threat event occurring and the potential impact (confidentiality, integrity, availability, safety for OT).
   - **Methodologies:** Can be qualitative (e.g., High/Medium/Low using a 5x5 matrix), semi-quantitative, or quantitative (e.g., FAIR model). NIST RMF and ISO 27005 provide detailed guidance.
   - **Calculation:** Risk = Likelihood x Impact.
   - Action: Select and document a risk assessment methodology appropriate for the PA context. Conduct assessments systematically.
6. **Risk Treatment (ISO 27005):** Based on the assessed risk level and the organization's risk appetite, decide on a course of action for each significant risk:
   - **Mitigate/Reduce:** Implement security controls (TOMs - Chapter 5) to lower likelihood or impact.
   - **Transfer/Share:** Shift risk to a third party (e.g., cyber insurance, outsourcing

specific functions).
  - **Accept:** Formally acknowledge and accept the risk (typically for low risks or where treatment cost exceeds potential impact), requiring management approval.
  - **Avoid:** Discontinue the activity or system generating the risk.
  - Action: Develop Risk Treatment Plans documenting the chosen strategy and specific controls/actions for each prioritized risk.
7. **Monitoring and Review (ISO 27005 / NIST CSF GV.OV):** Continuously monitor the risk environment, control effectiveness (Chapter 8), and the status of risk treatment plans. Regularly review and update risk assessments and the overall program.

4.2 Implement a Risk Register

A Risk Register is a central repository for documenting and tracking the entire risk management process. While sophisticated GRC tools exist, a structured spreadsheet (e.g., Excel) can be an effective starting point.

Template: Risk Register (Excel Structure)

	Description	**Example Entry**
Risk ID	Unique identifier for the risk.	R-OT-001
Date Identified	Date the risk was first recorded.	2025-05-15
Risk Title	Concise name of the risk.	Unauthorized Remote Access to PLC Network
Risk Description	Detailed explanation of the risk scenario.	Attacker exploits unpatched VPN vulnerability (CVE-XXXX) to gain access to OT network, potentially disrupting PLC operations.
Asset(s) Affected	Critical IT/OT asset(s) impacted by the risk (Link to Asset Inventory).	PLC Network Segment A, Control Server X
Threat Source	Potential origin of the threat (e.g., External Attacker, Insider, Malware).	External Attacker (APT Group Y)
Vulnerability	Specific weakness being exploited (e.g., CVE, misconfiguration, lack of control).	Unpatched VPN Appliance (CVE-XXXX), Lack of Network

		Segmentation
Existing Controls	Current measures in place that partially mitigate the risk.	Perimeter Firewall, Basic VPN Authentication
Inherent Likelihood	Probability of the risk occurring *before* new treatment (e.g., Scale 1-5 or High/Med/Low).	4 (High)
Inherent Impact	Potential consequence if the risk occurs *before* new treatment (e.g., Scale 1-5 or High/Med/Low - consider operational, financial, safety, compliance).	5 (Critical - potential OT disruption, safety risk)
Inherent Risk Score	Calculated score (e.g., Likelihood x Impact).	20 (Critical)
Risk Treatment Strategy	Chosen approach (Mitigate, Transfer, Accept, Avoid).	Mitigate
Proposed Controls/Actions	Specific new measures to be implemented (Link to TOMs/Improvement Plan).	Patch VPN (P-001), Implement IT/OT Segmentation (P-002), Deploy OT IDS (P-003), Enforce MFA for VPN (P-004)
Control Owner	Person/Team responsible for implementing the new controls.	IT Security Team, OT Engineering
Due Date	Target date for control implementation.	2025-09-30
Residual Likelihood	Estimated probability *after* treatment implementation.	2 (Low)
Residual Impact	Estimated consequence *after* treatment implementation.	3 (Medium - disruption contained)
Residual Risk Score	Calculated score after treatment.	6 (Medium)
Risk Status	Current status (Open, In Progress, Mitigated, Accepted, Closed).	In Progress
Last Review Date	Date the risk was last reviewed.	2025-05-20
Next Review Date	Date for the next scheduled review.	2025-08-20
Comments	Additional notes or context.	Awaiting budget approval for OT IDS.

Note: Customize scales and fields based on the chosen methodology (e.g., ISO 27005, NIST RMF) and organizational needs.

4.3 Aligning with Established Frameworks

Aligning the risk management program with established frameworks like **ISO/IEC 27005** (Information security, cybersecurity and privacy protection — Guidance on managing information security risks) or the **NIST Risk Management Framework (RMF)** (particularly steps like Prepare, Categorize, Select, Implement, Assess, Authorize, Monitor outlined in NIST SP 800-37) lends significant credibility and structure. These frameworks provide detailed methodologies for each phase of the cycle, supporting a repeatable and defensible risk management process essential for NIS2 compliance and demonstrating due diligence.

Implementing a continuous, documented, and framework-aligned risk management program is not just a NIS2 requirement; it is the engine that drives informed cybersecurity decision-making and resource allocation within the critical infrastructure PA.

An example of a Risk Register is provided below, including only a selection of the columns described above due to space constraints.

Risk ID	Risk Description	Asset(s) Affected	Threat Source	Vulnerability	Existing Controls	Inherent Likelihood	Inherent Impact	Inherent Risk Score	Risk Treatment Strategy
R-PA-001	Attacker exploits unpatched VPN vulnerability (CVE-XXXX) to gain access to OT network, potentially disrupting PLC operations.	PLC Network Segment A, Control Server X	External Attacker (APT Group Y)	Unpatched VPN Appliance (CVE-XXXX), Lack of Network Segmentation	Firewall, Antivirus, Basic Security Policies	3	5	15	Mitigate
R-PA-002	Employee clicks on phishing email, leaking sensitive citizen data.	Employee Email Accounts, Citizen Database	External Attacker (Phishing Campaign)	Lack of Email Filtering, Insufficient User Training	Firewall, Antivirus, Basic Security Policies	3	5	15	Mitigate
R-PA-003	Hackers deface public administration website to spread misinformation.	Public Website Server	Hacktivist Group	Outdated CMS Software, Weak Admin Credentials	Firewall, Antivirus, Basic Security Policies	5	4	20	Mitigate
R-PA-004	Disgruntled employee accesses and leaks confidential	Internal Document Repository	Insider Threat	Excessive User Privileges, Lack of Monitoring	Firewall, Antivirus, Basic Security Policies	3	4	12	Mitigate

	internal documents.								
R-PA-005	Ransomware attack encrypts critical systems, halting public services.	Municipality IT Systems	External Attacker (Ransomware Group)	Unpatched Systems, Lack of Segmented Backup	Firewall, Antivirus, Basic Security Policies	3	4	12	Mitigate
R-PA-006	Compromised IoT devices provide a backdoor into the administration network.	IoT Surveillance Cameras, Smart Sensors	External Attacker (IoT Botnet)	Default Credentials, No Network Segmentation	Firewall, Antivirus, Basic Security Policies	3	5	15	Mitigate
R-PA-007	DDoS attack makes citizen services unavailable.	Citizen Services Portal	External Attacker (DDoS-for-Hire Group)	Lack of DDoS Protection	Firewall, Antivirus, Basic Security Policies	5	5	25	Mitigate
R-PA-008	Sensitive communication sent to wrong recipients.	Email Systems, Document Management Systems	Human Error	Lack of Verification Procedures	Firewall, Antivirus, Basic Security Policies	4	4	16	Mitigate
R-PA-009	Admin accounts use weak, guessable passwords.	Domain Controllers, Critical Servers	External Attacker	Lack of Strong Password Policy	Firewall, Antivirus, Basic Security Policies	5	4	20	Mitigate
R-PA-010	Personal data is mishandled, leading to regulatory fines.	Citizen Data Repositories	Organizational Weakness	Lack of Data Protection Impact Assessments	Firewall, Antivirus, Basic Security Policies	4	5	20	Mitigate

Chapter 5: Technical and Organizational Measures (TOMs)

NIS2 Article 21 explicitly requires essential and important entities to implement "appropriate and proportionate technical, operational and organizational measures" based on their risk assessment (Chapter 4). These measures, often referred to as TOMs or security controls, are the practical safeguards used to protect network and information systems (both IT and OT) and ensure the resilience of essential services. The NIST CSF 2.0 provides a comprehensive structure for organizing these measures across its Functions, particularly **Protect (PR)**, **Detect (DE)**, and supporting elements within **Govern (GV)**, **Identify (ID)**, **Respond (RS)**, and **Recover (RC)**.

5.1 Key Domains for TOMs under NIS2

Article 21(2) lists minimum areas that TOMs must cover. Aligning these with NIST CSF 2.0 Functions and Categories provides a practical implementation framework:

1. **Access Control** (NIST CSF PR.AA - Identity Management, Authentication, and Access Control): Controlling who can access systems and data is fundamental.
    - *NIS2 Requirements:* Human resources security, access control policies, asset management. Use of multi-factor authentication (MFA) or continuous authentication solutions.
    - *Implementation Examples:* Implement Role-Based Access Control (RBAC) based on the principle of least privilege. Enforce strong password policies and **mandate MFA** for all users, especially privileged accounts and remote access (IT and OT). Manage identities and credentials throughout their lifecycle (creation, modification, revocation). Regularly review access rights. Implement physical access controls coordinated with cybersecurity policies.
2. **Network Security** (NIST CSF PR.PS - Platform Security & PR.IR - Technology Infrastructure Resilience): Protecting the network infrastructure connecting IT and OT systems.
    - *NIS2 Requirements:* Policies on information system security.[21]
    - *Implementation Examples:* Implement robust **network segmentation**, critically separating IT and OT environments using firewalls, VLANs, and Demilitarized Zones (DMZs). Employ Intrusion Detection/Prevention Systems (IDS/IPS). Secure network device configurations. Protect remote access pathways (e.g., secure VPNs with MFA). Secure wireless communications.
3. **Security Monitoring** (NIST CSF DE.AE - Anomalies and Events & DE.CM - Security Continuous Monitoring): Detecting potential threats and incidents in real-time.

   - *NIS2 Requirements:* Implied by incident handling and effectiveness assessment requirements.
   - *Implementation Examples:* Implement centralized logging and monitoring using a **Security Information and Event Management (SIEM)** system covering both IT and relevant OT events. Establish a **Security Operations Center (SOC)** function (internal or outsourced) for 24/7 monitoring, analysis, and alert triage. Deploy Endpoint Detection and Response (EDR) solutions. Monitor network traffic for anomalies.
4. **Patch and Vulnerability Management** (NIST CSF ID.VU - Vulnerability Management): Addressing known weaknesses before they can be exploited.
   - *NIS2 Requirements:* Security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.
   - *Implementation Examples:* Establish a formal patch management program with defined **Service Level Agreements (SLAs)** based on vulnerability severity (critical, high, medium, low). Conduct regular vulnerability scanning (Chapter 4). For OT systems where patching is difficult or risky due to availability/safety concerns, implement and document **compensating controls** (e.g., network segmentation, stricter access control, increased monitoring, application allowlisting, virtual patching).
5. **Backup and Recovery** (NIST CSF RC.RP - Recovery Planning & PR.IR - Technology Infrastructure Resilience): Ensuring data and systems can be restored after an incident.
   - *NIS2 Requirements:* Business continuity, such as backup management and disaster recovery.
   - *Implementation Examples:* Implement regular, automated backups of critical data and system configurations (IT and OT). Follow the 3-2-1 rule (3 copies, 2 different media, 1 offsite/offline/immutable). Encrypt backups. **Test backup restoration procedures regularly** (e.g., annually or semi-annually) to ensure effectiveness. Align with BCDR policy (Chapter 3).
6. **Incident Response Capabilities (NIST CSF RS Function):** Having the plans, tools, and skills to handle incidents effectively.
   - *NIS2 Requirements:* Incident handling.
   - *Implementation Examples:* Develop and maintain an Incident Response Plan (IRP) and specific playbooks (Chapter 6). Ensure capabilities for **digital forensics** suitable for both IT and OT environments (recognizing OT data volatility and specialized systems). Maintain necessary tools for analysis and containment.

7. **Employee Training and Awareness** (NIST CSF PR.AT - Awareness and Training): Ensuring personnel understand their cybersecurity responsibilities.
   - *NIS2 Requirements:* Basic cyber hygiene practices and cybersecurity training. Management training is also mandated.
   - *Implementation Examples:* Implement a **continuous** security awareness training program covering topics like phishing, social engineering, password security, acceptable use, incident reporting, and OT-specific risks. Conduct regular phishing simulations. Provide role-based training for specialized functions (IT/OT security, developers, management). **Maintain records** of training completion and effectiveness (e.g., quiz results) as proof for audits.
8. **Cryptography and Encryption** (NIST CSF PR.DS - Data Security): Protecting data confidentiality and integrity.
   - *NIS2 Requirements:* Policies and procedures regarding the use of cryptography and, where appropriate, encryption.
   - *Implementation Examples:* Encrypt sensitive data at rest (e.g., databases, file storage) and in transit (e.g., TLS for network traffic, secure VPNs). Use validated cryptographic modules. Manage cryptographic keys securely. Define policies on acceptable encryption algorithms and standards.
9. **Other Measures:** NIS2 Art. 21 also requires policies on risk analysis and information system security (covered in Chapter 3 & 4), policies/procedures to assess TOM effectiveness (covered in Chapter 8), and secure communications (covered under Access Control/Network Security). Supply chain security is covered in Chapter 7.

5.2 Action: Build a Security Controls Matrix

A Security Controls Matrix is a tool to inventory implemented TOMs, track their ownership, and assess their maturity or compliance status. This is invaluable for managing the security program and demonstrating compliance during audits.

Template: Security Controls Matrix (Excel Structure):

Control ID	Control Description	Implemented Measure(s)	Owner (Team/Role)	Maturity Level	Last Reviewed Date
PR.AA-01	Asset inventory is maintained	CMDB maintained	IT Asset Management	4 - Managed	01/01/2025
PR.AA-06	Access permissions are reviewed	Quarterly access reviews	IAM Team	3 - Defined	01/02/2025
PR.PS-05	Personnel security policies are established	Background checks	HR Department	2 - Developing	15/01/2025
DE.CM-01	Security monitoring is performed	SIEM solution deployed	SOC Team	5 - Optimized	01/03/2025

ID.VU-04	Vulnerability management processes are implemented	Regular vulnerability scans	Vulnerability Management	3 - Defined	20/01/2025
RC.RP-01	Incident response plan is established	IR plan approved	IR Team	4 - Managed	15/02/2025
PR.AT-01	Security awareness training is conducted	Annual training sessions	Training Department	2 - Developing	30/01/2025
PR.IP-01	Information protection processes are maintained	DRP and ISMS maintained	IT Security	5 - Optimized	01/03/2025
DE.DP-01	Detection processes are tested	Tabletop exercises	SOC Team	3 - Defined	10/01/2025
ID.AM-01	Asset management procedures are documented	Asset database with ownership	IT Asset Management	3 - Defined	25/01/2025
PR.DS-01	Data-at-rest is protected	Encryption of hard drives	Data Protection Officer	4 - Managed	05/02/2025
PR.MA-01	Maintenance activities are performed securely	Secure maintenance contracts	Maintenance Team	2 - Developing	05/01/2025
DE.CM-02	Monitoring for unauthorized access	IDS/IPS solutions	SOC Team	4 - Managed	10/03/2025
RS.RP-01	Response plans are executed during incidents	Runbook executed	IR Team	4 - Managed	20/02/2025
ID.RA-01	Risk assessment processes are established	Annual risk assessments	Risk Management	3 - Defined	18/01/2025
RS.CO-01	Coordinated communication during incidents	Crisis communication plan	Communication Officer	5 - Optimized	01/03/2025
PR.PT-01	Physical access to assets is restricted	Access controls and logging	Facilities Management	2 - Developing	07/01/2025
DE.CM-03	Monitoring for malicious code	Anti-malware solutions	SOC Team	4 - Managed	12/03/2025
RS.IM-01	Incident mitigation processes are established	Incident playbooks	IR Team	4 - Managed	18/02/2025
RC.IM-01	Incident recovery plans are improved	Post-incident reviews	IR Team	3 - Defined	12/01/2025

Implementing and documenting these TOMs, guided by risk assessment and structured using frameworks like NIST CSF 2.0, is central to achieving NIS2 compliance and building genuine cyber resilience for critical infrastructure. The effectiveness of these measures must be continuously assessed (Chapter 8).

Chapter 6: Incident Detection and Reporting

Effective incident detection and reporting are critical components of NIS2 compliance, particularly given the strict notification timelines mandated by Article 23. A well-defined process ensures that incidents are identified early, assessed accurately, escalated appropriately, and reported to authorities like CSIRT Italia and ACN within the required deadlines. This chapter focuses on establishing the necessary internal procedures, communication plans, and reporting workflows, leveraging the NIST CSF Detect (DE), Respond (RS), and Govern (GV) functions.

6.1 Internal Procedures for Early Detection and Categorization

Rapid detection minimizes the potential impact of an incident. This requires:

- **Monitoring Capabilities:** Leveraging tools implemented in Chapter 5, such as SIEM, IDS/IPS, EDR, and log analysis, to identify anomalies and potential threats across IT and OT environments.
- **Defined Detection Processes (NIST CSF DE.DP):** Establishing clear procedures for analyzing alerts, correlating events, and confirming whether a security event constitutes a genuine incident.
- **User Reporting:** Training all personnel (Chapter 5) to recognize and immediately report suspicious activities or potential incidents through a designated channel (e.g., SOC hotline, dedicated email).
- **Incident Categorization/Classification:** Developing a clear framework to classify incidents based on type (e.g., malware, ransomware, DDoS, data breach, unauthorized access, OT disruption) and severity/impact (e.g., Critical, High, Medium, Low). This classification determines the required response level, escalation path, and whether the incident qualifies as "significant" under NIS2.
    - *NIS2 Significance Criteria (Art. 23(3) / Art. 25(4) D.Lgs. 138/2024):* An incident is significant if it (a) has caused or is capable of causing severe operational disruption or financial loss, OR (b) has affected or is capable of affecting other persons by causing considerable material or non-material damage.[21]

6.2 Communication Plan for Fast Escalation

Clear and timely communication during an incident is crucial for effective coordination and decision-making.

- **Internal Escalation Paths:** Define clear triggers and pathways for escalating incidents from the operational level (SOC/IT/OT teams) to the tactical level (Incident Response Team Lead, CISO, Cyber Risk Committee) and, for significant incidents, to the strategic level (CEO/DG, Board/Executive Committee, Legal, Communications).
- **Communication Channels:** Establish primary and backup communication methods (e.g., dedicated chat channels, conference bridges, secure email, phone trees) for incident response coordination, especially if primary systems are compromised.
- **Stakeholder Communication Matrix:** Identify key internal stakeholders (Management, Legal, HR, PR/Communications, Business Units) and external stakeholders (ACN/CSIRT Italia, Law Enforcement, affected service recipients, suppliers, media) and define what information needs to be communicated to whom, when, and by whom.

Template: Simple Internal Escalation Matrix

Incident Severity	Initial Responder	First Escalation (within X mins)	Second Escalation (within Y mins)	Strategic Notification (within Z hours)
Low	SOC Analyst	SOC Lead	-	-
Medium	SOC Analyst	SOC Lead / IRT Member	IRT Lead / CISO	CISO (Informational)
High	SOC Analyst	IRT Lead	CISO / Cyber Risk Committee	CEO/DG, Legal, Comms (Briefing)
Critical (NIS2 Sig.)	SOC Analyst	IRT Lead (Immediate)	CISO (Immediate)	CEO/DG, Board Committee, Legal, Comms (Immediate)

6.3 Notification Workflows to CSIRT Italy / ACN

Compliance with NIS2 reporting timelines is mandatory. Establish a documented workflow:

1. **Incident Confirmed & Classified as Significant:** IRT Lead/CISO confirms the incident meets NIS2 significance criteria.
2. **Early Warning** (within 24h of awareness):
   - *Responsibility:* CISO or designated IRT member.
   - *Recipient:* CSIRT Italia (info@csirt.gov.it, emergency phone +39 06 4213 88895) or ACN via designated portal/method. *Note: Confirm the official ACN reporting channel.*
   - *Content:* Indicate if suspected malicious/unlawful cause, potential cross-border impact. Use official forms/templates if provided by ACN/CSIRT.
3. **Incident Notification** (within 72h of awareness):
   - *Responsibility:* CISO or designated IRT member.
   - *Recipient:* CSIRT Italia/ACN.
   - *Content:* Update early warning information, provide initial assessment (severity, impact), indicators of compromise (IoCs) if available.
4. **Intermediate Report(s)**:
   - *Responsibility:* CISO or designated IRT member.
   - *Recipient:* CSIRT Italia/ACN.
   - *Trigger:* Upon request from CSIRT/ACN.
   - *Content:* Status updates on the ongoing incident.
5. **Final Report** (within 1 month of Notification):
   - *Responsibility:* CISO or designated IRT member.
   - *Recipient:* CSIRT Italia/ACN.
   - *Content:* Detailed description (severity, impact), likely threat/root cause, mitigation measures applied/ongoing, cross-border impact.
   - *If Ongoing:* Submit a progress report at the 1-month mark, and a final report within 1 month of handling completion.

Note: Italy's D.Lgs. 138/2024 sets the deadline for compliance with these notification obligations as January 1, 2026. However, preparation should begin immediately.

6.4 Action: Draft Incident Response Playbooks

While the overall IRP provides the framework, specific playbooks offer step-by-step guidance for common or high-impact incident types. These should be tailored to the PA's IT and OT environments.

Template: Incident Response Playbook Outline (Example: Ransomware)

1. **Playbook Title:** Ransomware Incident Response Playbook

2. **Version & Approval:** Version control details.
3. **Incident Type:** Ransomware (Data Encryption, Data Exfiltration/Extortion).
4. **Objectives:** Contain spread, prevent data loss, restore operations, preserve evidence, meet reporting obligations.
5. **Triggers:** How ransomware is typically detected (e.g., user reports ransom note, EDR alerts, SIEM detects encryption activity, file share inaccessibility).
6. **Roles & Responsibilities:** Specific actions for IRT Lead, Security Analysts, Network Admins, System Admins, Legal, Comms, CISO, OT Engineers (if OT impacted).
7. Response Phases (Aligned with NIST SP 800-61 / SANS):
   - **Preparation:** (Covered by IRP, training, backups). Ensure offline/immutable backups exist and are tested. Identify critical systems.
   - **Identification:** Confirm ransomware presence, identify affected systems/data (IT & OT), determine variant (if possible), assess scope and impact, check for data exfiltration evidence.
   - **Containment: Immediately isolate** affected systems/segments (disconnect from network, disable accounts). Prevent lateral movement. Secure backups.
   - **Eradication:** Identify and remove malware components (reimage systems from trusted sources preferred over cleaning). Address the root cause (e.g., patch vulnerability, reset compromised credentials). *Do NOT pay ransom (CISA recommendation, check organizational policy)*.
   - **Recovery:** Restore systems and data from clean backups. Validate system integrity before reconnecting. Monitor closely for re-infection. Prioritize critical systems.
   - **Post-Incident Activity (Lessons Learned):** Conduct post-mortem, document findings, update IRP/playbooks, improve controls.
8. **Communication Plan:** Internal updates, external notifications (CSIRT/ACN, Law Enforcement, affected parties if data breached) following Communication Plan (Section 6.2) and NIS2 workflow (Section 6.3).
9. **Evidence Handling:** Procedures for collecting and preserving forensic evidence (system images, logs, memory captures, ransom notes).
10. **Specific Tools:** List relevant tools (EDR, SIEM, Forensics software, Backup solution).

Develop similar playbooks for other critical scenarios like DDoS, Data Breach, OT System Compromise, Major Vulnerability Exploitation.

Establishing robust detection, clear communication and escalation pathways, documented reporting workflows, and practical playbooks is essential for minimizing incident impact and meeting NIS2's stringent reporting requirements. These processes must be regularly tested and refined through drills and exercises.

Chapter 7: Supply Chain Security

The NIS2 Directive significantly elevates the importance of supply chain cybersecurity, recognizing that vulnerabilities within suppliers and service providers can pose substantial risks to essential and important entities. Article 21(2)(d) explicitly mandates measures addressing "security-related aspects concerning the relationships between each entity and its direct suppliers or service providers". For critical infrastructure PAs, securing the supply chain involves managing risks associated with IT and OT vendors, software providers, cloud services, managed service providers (MSPs), and other third parties integrated into their operations or service delivery. NIST CSF 2.0 also incorporates Cybersecurity Supply Chain Risk Management (C-SCRM) within the Govern function (GV.SC).

7.1 NIS2 Requirements for Supply Chain Security

Entities must:

- **Assess Supplier Risk:** Take into account the vulnerabilities specific to each direct supplier and service provider.
- **Evaluate Supplier Practices:** Consider the overall quality of products and cybersecurity practices of suppliers, including their secure development procedures.
- **Incorporate Risk Assessments:** Utilize results from coordinated security risk assessments of critical supply chains (as potentially mandated by authorities, Art. 22 NIS2).
- **Implement Measures:** Take appropriate and proportionate measures based on these assessments to manage supply chain risks.

7.2 Steps for Managing Supply Chain Risk

A systematic approach is required:

1. **Map Critical Suppliers:** Identify suppliers and service providers critical to the PA's essential functions or those handling sensitive data or having privileged access to IT/OT systems. Prioritize based on criticality and risk exposure. *Action: Maintain an inventory of critical third parties, detailing the services provided and data accessed.*
2. **Define Cybersecurity Requirements:** Establish clear cybersecurity standards

and requirements that critical suppliers must meet. These should align with the PA's own security policies (Chapter 3) and NIS2 obligations. *Action: Develop a Supplier Security Standard document*.

3. **Impose Requirements in Contracts:** Embed specific cybersecurity clauses into contracts and service level agreements (SLAs) with suppliers. Key clauses should cover:
    - Adherence to defined security standards (e.g., ISO 27001, NIST CSF, PA's specific requirements).
    - Data protection obligations (confidentiality, integrity, availability, compliance with GDPR).
    - Incident notification requirements (mandating timely reporting of breaches affecting the PA).
    - Vulnerability management expectations.
    - Right-to-audit clauses or requirements for third-party attestations (e.g., SOC 2 reports, ISO 27001 certification).
    - Secure software development practices (if applicable).
    - Data handling upon contract termination (secure deletion/return).
    - Liability and indemnification for security breaches caused by the supplier.
    - Action: Work with Legal and Procurement teams to develop standard cybersecurity contract addendums.
4. **Assess Supplier Compliance (Due Diligence):** Evaluate the cybersecurity posture of potential and existing critical suppliers before onboarding and periodically thereafter. Methods include:
    - **Security Questionnaires:** Using standardized questionnaires (e.g., SIG Lite/Core, CAIQ) or custom templates to gather information on the supplier's controls.
    - **Documentation Review:** Assessing supplier policies, procedures, certifications (ISO 27001), and audit reports (SOC 2).
    - **Security Ratings Platforms:** Utilizing external platforms (e.g., BitSight, SecurityScorecard) that provide objective, continuously monitored security scores based on externally observable data.
    - **Penetration Test Results:** Requesting summaries of recent penetration tests.
    - **Technical Assessments/Audits:** Conducting deeper assessments or audits for very high-risk suppliers.
    - Action: Implement a **Third-Party Risk Management (TPRM)** process incorporating these assessment methods.
5. **Monitor Supplier Compliance Periodically:** Cybersecurity is not static.

Continuously or periodically monitor the security posture of critical suppliers.

  - **Methods:** Regular questionnaire updates, reviewing updated certifications/audits, continuous monitoring via security ratings platforms, monitoring public threat intelligence and breach notifications.
  - Action: Define monitoring frequency based on supplier risk level.

7.3 Action: Create a Third-Party Risk Assessment Template

A standardized template helps ensure consistency and thoroughness in supplier assessments. It can be based on established questionnaires or customized.

Template: Third-Party Risk Assessment Questionnaire (Key Sections Example)

Section A: Vendor Information & Relationship Context

- Vendor Name, Contact Information
- Services/Products Provided to PA
- Criticality Level (High, Medium, Low - based on BIA/PA assessment)
- Data Accessed/Processed (Types, Sensitivity - e.g., PII, Operational Data)
- System Access Granted (Level of privilege, Network connectivity IT/OT)
- Sub-processors Used? (List critical ones)

Section B: Governance & Compliance

- Does the vendor have a formal Information Security Policy? (Request copy)
- Is there a designated CISO or equivalent security lead?
- Does the vendor hold relevant certifications (e.g., ISO 27001, SOC 2)? (Provide evidence)
- Is the vendor subject to specific regulations (e.g., GDPR)? How is compliance managed?
- How are cybersecurity responsibilities defined and communicated internally?

Section C: Risk Management

- Does the vendor conduct regular cybersecurity risk assessments? (Describe process/frequency)
- How are risks tracked and mitigated? (Provide Risk Register example if possible)
- Does the vendor have a formal vulnerability management program (scanning, patching)? (Describe process/frequency)
- Does the vendor conduct regular penetration testing? (Provide

summary/attestation)

Section D: Security Controls (Aligned with NIS2 Art. 21 / NIST CSF)

- **Access Control:** Describe identity management, authentication (MFA required?), and authorization processes. How is least privilege enforced?
- **Data Security:** How is PA data protected at rest and in transit (encryption methods)? How is data segregated? Describe data disposal procedures.
- **Network Security:** Describe network segmentation, firewall management, IDS/IPS usage.
- **Endpoint Security:** Describe endpoint protection measures (antivirus, EDR, patching).
- **Secure Development (if applicable):** Describe secure coding practices, code reviews, vulnerability testing in SDLC.
- **Physical Security:** Describe controls for data centers or facilities handling PA assets/data.

Section E: Incident Response & Business Continuity

- Does the vendor have a documented Incident Response Plan? (Request summary/outline)
- What are the procedures and timelines for notifying the PA of a security incident affecting PA data or services? (Must align with PA contractual requirements)
- Does the vendor have a documented Business Continuity/Disaster Recovery Plan? (Request summary/outline)
- How often are IR and BCDR plans tested? (Provide test summary/attestation)

Section F: Personnel Security & Training

- Are background checks conducted for personnel handling sensitive PA data?
- Is regular cybersecurity awareness training provided to employees? (Describe topics/frequency)

Section G: Supply Chain Security (Fourth-Party Risk)

- How does the vendor assess and manage cybersecurity risks associated with its own critical suppliers (sub-processors)?

Section H: Attestation

- Signature of authorized vendor representative confirming accuracy of responses.

Section	Question	Vendor Response
A. Vendor Information & Relationship Context	Vendor Name, Contact Information	
	Services/Products Provided to PA	
	Criticality Level (High, Medium, Low - based on BIA/PA assessment)	Medium
	Data Accessed/Processed (Types, Sensitivity - e.g., PII, Operational Data)	
	System Access Granted (Level of privilege, Network connectivity IT/OT)	
	Sub-processors Used? (List critical ones)	
B. Governance & Compliance	Does the vendor have a formal Information Security Policy? (Request copy)	Yes
	Is there a designated CISO or equivalent security lead?	
	Does the vendor hold relevant certifications (e.g., ISO 27001, SOC 2)? (Provide evidence)	Yes
	Is the vendor subject to specific regulations (e.g., GDPR)? How is compliance managed?	
	How are cybersecurity responsibilities defined and communicated internally?	
C. Risk Management	Does the vendor conduct regular cybersecurity risk assessments? (Describe process/frequency)	No
	How are risks tracked and mitigated? (Provide Risk Register example if possible)	
	Does the vendor have a formal vulnerability management program (scanning, patching)? (Describe process/frequency)	Yes
	Does the vendor conduct regular penetration testing? (Provide summary/attestation)	No
D. Security Controls	Access Control: Describe identity management, authentication (MFA required?), and authorization processes. How is least privilege enforced?	
	Data Security: How is PA data protected at rest and in transit (encryption methods)? How is data segregated? Describe data disposal procedures.	
	Network Security: Describe network segmentation, firewall management, IDS/IPS usage.	
	Endpoint Security: Describe endpoint protection measures (antivirus, EDR, patching).	
	Secure Development (if applicable): Describe secure coding practices, code reviews, vulnerability testing in SDLC.	
	Physical Security: Describe controls for data centers or facilities handling PA assets/data.	
E. Incident Response & Business Continuity	Does the vendor have a documented Incident Response Plan? (Request summary/outline)	Yes
	What are the procedures and timelines for notifying the PA of a security incident affecting PA data or services? (Must align with PA contractual requirements)	
	Does the vendor have a documented Business Continuity/Disaster Recovery Plan? (Request summary/outline)	Yes

	How often are IR and BCDR plans tested? (Provide test summary/attestation)	
F. Personnel Security & Training	Are background checks conducted for personnel handling sensitive PA data?	Yes
	Is regular cybersecurity awareness training provided to employees? (Describe topics/frequency)	Yes
G. Supply Chain Security (Fourth-Party Risk)	How does the vendor assess and manage cybersecurity risks associated with its own critical suppliers (sub-processors)?	
H. Attestation	Signature of authorized vendor representative confirming accuracy of responses.	

Note: This is illustrative. Use standardized questionnaires where feasible, supplemented by specific questions relevant to the PA's critical infrastructure context (especially OT aspects if applicable) and NIS2 requirements.

Effectively managing supply chain risk is a complex but non-negotiable aspect of NIS2 compliance. It requires ongoing effort, collaboration between Cybersecurity, Procurement, Legal, and business units, and a risk-based approach to prioritize resources on the most critical third-party relationships.

Chapter 8: Audit, Monitoring, and Continuous Improvement

NIS2 compliance is not a one-time achievement but an ongoing process requiring demonstrable evidence of effectiveness. Essential entities face proactive supervision, including potential audits and inspections by ACN. Therefore, establishing robust internal audit mechanisms, continuous monitoring through relevant metrics, and a formal continuous improvement cycle is crucial. This aligns directly with the NIST CSF 2.0 Govern (GV.OV - Oversight) and Identify (ID.IM - Improvement) functions.

8.1 Internal Audit Program

Regular internal audits provide assurance to management and the Board that cybersecurity policies and controls are implemented effectively and operating as intended. They also help identify gaps before external scrutiny.

- **Frequency:** Plan internal cybersecurity audits at least **annually**, or more frequently for high-risk areas.
- **Scope:** Audits should cover key NIS2 compliance areas: governance, risk management processes, implementation and effectiveness of TOMs (Chapter 5), incident response procedures and reporting (Chapter 6), supply chain security practices (Chapter 7), and training effectiveness (Chapter 5).
- **Methodology:** Align audit procedures with recognized frameworks like ISACA standards, NIST CSF, or ISO 27001. The process typically involves planning, fieldwork (interviews, documentation review, control testing), reporting findings (identifying non-conformities or weaknesses), and tracking remediation.
- **Independence:** Ensure auditors (internal audit team or co-sourced/outsourced experts) have sufficient independence from the functions they are auditing.
- Action: Develop an Internal Cybersecurity Audit Plan/Program.

Template: Internal Cybersecurity Audit Work Plan (Simplified Example)

1. **Audit Title:** NIS2 Compliance Audit - Q3 2025
2. **Audit Objective:** To assess the design and operating effectiveness of controls implemented to meet key requirements of D.Lgs. 138/2024 (NIS2) and the organization's cybersecurity policies.
3. **Scope**:
   - Governance: Review of Charter, Committee minutes, CISO reporting.
   - Risk Management: Review of Risk Register, assessment process

    documentation, treatment plans for top 5 risks.
   - TOMs (Sample): Test MFA implementation for critical systems, review IT/OT segmentation rules, verify patch status for critical vulnerabilities, inspect backup logs and last restore test report.
   - Incident Reporting: Review IRP, sample incident tickets, verify documentation for one simulated significant incident notification workflow.
   - Supply Chain: Review TPRM policy, sample contract clauses, assessment records for 3 critical suppliers.
   - Training: Verify training completion records for selected departments.
4. **Criteria:** D.Lgs. 138/2024, Relevant Organizational Policies (ISP, Risk Mgt, IR, BCDR, TPRM), NIST CSF 2.0, ISO 27001/27002.
5. **Audit Team:** Internal Audit Lead, IT Auditor, OT Security SME (Consultant).
6. **Timeline:** Fieldwork: - [End Date]; Draft Report: [Date]; Final Report: [Date].
7. **Key Stakeholders:** CISO, IT Security Manager, OT Security Lead, Risk Manager, Compliance Officer.
8. Audit Procedures (Examples):
   - *GV.OV:* Interview CISO regarding board reporting; review Board Pack contents.
   - *ID.RA:* Inspect Risk Register; walkthrough risk assessment procedure with Risk Manager.
   - *PR.AA-06:* Sample user accounts for critical systems; verify MFA enrollment and usage logs.
   - *RS.RP:* Simulate incident report escalation; review IR team communication logs.
   - *GV.SC:* Examine contracts for 3 critical suppliers for required security clauses.
9. **Reporting:** Document findings, classify by severity, provide recommendations, agree on management action plans and timelines.

8.2 Monitoring KPIs and KRIs

Continuous monitoring using Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) provides near real-time insight into security posture and potential issues.

- **KPIs (Performance):** Measure the effectiveness and efficiency of security processes and controls. *Example: Patching Time, Training Completion Rate, Backup Success Rate.*
- **KRIs (Risk):** Indicate the level of exposure to specific risks. Example: Number of Critical Vulnerabilities, Number of Successful Phishing Clicks, Mean Time to Detect Incidents.

Examples of Relevant KPIs/KRIs for NIS2/CISO Reporting:

- Governance & Compliance:
  - KRI: # Overdue audit findings.
  - KPI: Policy review cycle adherence %.
  - KPI: NIS2 Training completion rate %.
- Risk Management:
  - KRI: # Critical vulnerabilities unpatched > SLA.
  - KRI: % High-risk suppliers not assessed in last 12 months.
  - KPI: Risk assessment completion rate (by scope).
  - KPI: % Risks with approved treatment plans.
- TOMs Effectiveness:
  - KPI: Mean Time to Patch critical vulnerabilities.
  - KRI: # Systems missing critical patches.
  - KRI: # Unidentified devices detected on network.
  - KPI: MFA enrollment %.
  - KRI: # Failed login attempts (brute force indicator).
  - KPI: Endpoint protection coverage %.
  - KPI: Backup success rate. Backup test success rate.
- Incident Management:
  - KPI: Mean Time to Detect (MTTD).
  - KPI: Mean Time to Respond/Resolve (MTTR).
  - KPI: Mean Time to Contain (MTTC).
  - KRI: # Security incidents (by severity/type).
  - KPI: % Incidents reported to CSIRT Italy within NIS2 timelines.
  - KRI: Phishing test click rate.

Note: Select a manageable number of meaningful metrics. Tailor to organizational context and ensure they are measurable and actionable.

8.3 Continuous Improvement (NIST CSF ID.IM)

The insights gained from audits and monitoring must feed a continuous improvement loop.

- **Identify Gaps:** Use audit results, KPI/KRI trends, incident post-mortems, threat intelligence (ACN, ENISA), and risk assessment updates to identify weaknesses, non-conformities, or areas for enhancement.
- **Develop Improvement Plans:** Create corrective action plans detailing the issue,

proposed solution, owner, timeline, and required resources. Track these plans systematically.

- **Implement Changes:** Execute the improvement plans, which might involve updating policies/procedures (Chapter 3), enhancing TOMs (Chapter 5), refining risk assessments (Chapter 4), or improving training (Chapter 5).
- **Verify Effectiveness:** Monitor KPIs/KRIs or conduct follow-up audits to confirm that the implemented changes have effectively addressed the identified gaps.

This cycle ensures the cybersecurity program evolves and adapts to the changing threat landscape and business needs, moving beyond static compliance towards genuine resilience.

8.4 Action: Compliance Dashboard

A compliance dashboard provides a high-level, visual summary of the organization's NIS2 compliance status and key cybersecurity metrics, primarily for management and governance oversight.

- **Purpose:** Offer a quick overview of posture, highlight trends, identify areas needing attention.
- **Tools:** Can range from dedicated Governance, Risk, and Compliance (GRC) platforms, Business Intelligence (BI) tools like Tableau or PowerBI, or even well-structured spreadsheets or presentation slides for initial stages.
- **Audience:** CISO, Cyber Risk Committee, Senior Management, Board (as input to Chapter 9 reporting).

Template: Example Compliance Dashboard Elements

- **Overall NIS2 Compliance Score/Maturity:** (e.g., % completion against a NIS2 checklist or maturity rating based on Controls Matrix) - *Gauge or Scorecard*.
- **Compliance % by Key Area:** (e.g., Governance, Risk Mgt, TOMs, Incident Reporting, Supply Chain, Training) - *Bar Chart or Radar Chart*.
- Key KRI Trends:
  - Critical Vulnerabilities Over Time (Trend Line).
  - MTTD / MTTR Trend (Trend Line).
  - Phishing Simulation Click Rate Trend (Trend Line).
- **Open Audit Findings:** (Count by Severity, Ageing Chart) - *Table or Bar Chart*.
- **Patching Status:** (# Critical Patches Pending SLA, % Systems Compliant with Patch Policy) - *Scorecards or Gauges*.

- **Training Compliance:** (Overall Completion Rate %, Rate by Department) - *Gauges or Bar Chart*.
- **Recent Incidents:** (Count by Severity for the Quarter) - *Scorecard or simple table*.
- **Supplier Risk:** (% High-Risk Suppliers Assessed in last 12 months, # Open High-Risk Findings) - *Scorecards*.

Keep the dashboard visual, focused on key indicators, and easy to understand at a glance. Ensure data accuracy and consistency.

The integration of auditing, monitoring, and continuous improvement is vital. Monitoring provides the ongoing pulse check, audits provide the periodic health check, and the improvement cycle ensures the organization learns and adapts. Selecting meaningful metrics is paramount; focusing solely on compliance checkboxes without understanding underlying risk or control effectiveness provides a false sense of security. Metrics should tell a story about risk reduction and program maturity, informing both operational adjustments and strategic decisions. Furthermore, while internal audits are essential for preparation and management assurance, the ultimate validation often comes from external assessments or regulatory inspections, emphasizing the need for robust documentation and evidence-keeping (Chapter 10).

Chapter 9: Governance Reporting to Top Management

Effective communication with top management and the Board of Directors (or equivalent executive committee in a PA) is a critical component of cybersecurity governance, especially under NIS2, which explicitly places oversight responsibility and **potential liability on these bodies** (Art. 20). Regular, clear, and concise reporting ensures that leadership is informed about the organization's cybersecurity risk posture, compliance status, and the effectiveness of the security program, enabling them to fulfill their oversight duties and make strategic decisions. This aligns with the NIST CSF Govern function (GV.OV - Oversight).

9.1 NIS2 Requirement for Management Oversight

Article 20 of NIS2 mandates that management bodies approve cybersecurity risk-management measures and oversee their implementation. This cannot be achieved without adequate information flow from the CISO and the cybersecurity function to the highest levels of the organization. Reporting provides the necessary visibility for this oversight.

9.2 Reporting Frequency and Audience

- **Audience:** The primary audience is the Board of Directors or the PA's equivalent senior executive committee (e.g., Comitato di Direzione). The CISO is typically responsible for presenting this report.
- **Frequency: Quarterly reporting** is a widely accepted best practice for providing regular updates without overwhelming leadership.
- **Supervisory Authority:** The competent authority (ACN in Italy) may also request specific reports or information as part of its supervisory activities. The structure and content of Board reports can often be adapted for regulatory submissions.

9.3 Key Content for Board-Level Reporting

Board reports must translate technical cybersecurity information into business context, focusing on risk, impact, and strategic alignment. Avoid excessive technical jargon. Key content areas include:

- Risk Status:
    - **Top Risks:** A summary of the top 3-5 cybersecurity risks facing the

organization, linked to the Risk Register (Chapter 4). Explain the potential business impact (financial, operational, reputational, safety) in clear terms.

  - **Emerging Threats:** A brief overview of significant threats in the landscape relevant to the PA's sector (leveraging ACN/ENISA intelligence) and how they might impact the organization.
  - **Risk Appetite:** Comparison of the current residual risk level against the Board-defined risk appetite.
- Incident Status:
  - **Significant Incidents:** Summary of any significant incidents occurring during the reporting period, focusing on business impact, response effectiveness (e.g., MTTD/MTTR metrics if meaningful to the Board), and key lessons learned.
  - **Trends:** Any notable trends in incident types or frequency.
  - **NIS2 Reporting:** Confirmation of compliance with NIS2 notification requirements to CSIRT Italia/ACN for any relevant incidents.
- Compliance Maturity:
  - **NIS2 Status:** High-level overview of progress towards full NIS2 compliance, highlighting key milestones achieved or upcoming deadlines.
  - **Dashboard Snapshot:** Key visuals from the Compliance Dashboard (Chapter 8) showing overall posture and trends in critical KPIs/KRIs.
  - **Audit Findings:** Status update on the remediation of significant internal or external audit findings.
- Key Projects & Program Performance:
  - **Initiatives Update:** Progress summary for major cybersecurity projects (e.g., new technology rollouts, major policy updates, C-SCRM program implementation) tied to strategic objectives or risk reduction.
  - **Budget:** High-level overview of cybersecurity budget spend versus plan.
  - **Resource Needs/Roadblocks:** Identify any significant resource constraints or issues requiring executive support or decision.

9.4 Action: Prepare a Cybersecurity Board Pack

The Board Pack is the formal deliverable for quarterly reporting. It should be concise, visually oriented, and structured for executive consumption.

Template: Quarterly Cybersecurity Board Pack Outline (PowerPoint/Word)

1. **Title Slide:** Cybersecurity Program Update – Q[X][Year]
   - Date, Presenter (CISO)

2. Executive Summary (1 Slide):
    - Overall cybersecurity posture assessment (e.g., using a Red/Amber/Green status).
    - Key achievements in the quarter (e.g., major project milestone, significant risk reduction).
    - Critical risks or incidents requiring Board attention.
    - Summary of key decisions needed from the Board.
3. Threat Landscape Update (1 Slide):
    - Brief overview of 1-2 major external threats relevant to the PA sector (citing ACN/ENISA).
    - Key internal threat/incident trends observed.
4. Risk Posture (1-2 Slides):
    - Visual representation of top 3-5 risks (e.g., heatmap or table summarizing risk, impact, mitigation status).
    - Trend chart showing overall residual risk level over time vs. risk appetite.
5. Incident Summary (1 Slide, if applicable):
    - Brief description of significant incidents (max 1-2).
    - Business impact (operational downtime, data compromised, cost).
    - Response effectiveness highlights (MTTD/MTTR if appropriate).
    - Key lessons learned and remediation actions.
    - Confirmation of NIS2 reporting compliance.
6. Compliance & Maturity (1-2 Slides):
    - Visual snapshot from the Compliance Dashboard (Chapter 8).
    - Highlight NIS2 compliance progress/status against deadlines.
    - Status of critical audit findings remediation (e.g., # open, % resolved).
7. Key Initiatives Update (1 Slide):
    - Bulleted list of 2-3 major strategic projects.
    - Status (On track, At risk, Delayed) and brief progress update.
    - High-level budget overview (e.g., % spent vs. budget).
8. Training & Awareness Metrics (Optional, 1 Slide):
    - Training completion rates.
    - Phishing simulation click rates (trend).
9. Supply Chain Risk (Optional, 1 Slide):
    - Status of high-risk supplier assessments or key issues identified.
10. Forward Look / Decisions Needed (1 Slide):
    - Key priorities for the next quarter.
    - Anticipated challenges or emerging risks.

    - Specific questions or decisions required from the Board (e.g., approval of risk acceptance, budget allocation for a new initiative).
11. Appendix (Optional):
    - Detailed metrics tables.
    - Full list of top risks from the register.
    - Project summaries.

Use charts, graphs, icons, and minimal text per slide. Focus on clarity and impact.

The effectiveness of Board reporting hinges on the CISO's ability to bridge the gap between technical security details and strategic business implications. Executives need to understand cybersecurity not as an IT cost center, but as a critical enabler of the PA's mission and a significant area of enterprise risk. Consistent, transparent reporting using clear language and relevant metrics builds credibility and trust, which is essential for securing necessary resources and support, and critically, helps the Board fulfill its NIS2-mandated oversight responsibilities. The **report should not be a mere data dump but a curated narrative that guides strategic discussion** and facilitates informed decision-making on **risk appetite, priorities, and investments**.

Chapter 10: Prepare for NIS2 Inspections

Under NIS2 and the Italian transposition (D.Lgs. 138/2024), ACN has the authority to conduct audits and inspections of essential entities, potentially with little notice, to verify compliance. Being prepared for such inspections is crucial to demonstrate due diligence and avoid potential sanctions. This involves having well-organized documentation and evidence readily available.

10.1 The Possibility of Inspection

ACN's supervisory powers for essential entities are proactive (ex-ante). This means inspections are not necessarily triggered only by incidents but can be part of regular oversight or targeted assessments.[5] Preparedness should be a continuous state, not a last-minute scramble. Auditors may request documentation in advance or review materials on-site.

10.2 Essential Documentation and Evidence

Inspectors will seek tangible proof that the PA has implemented the required governance structures, risk management processes, and security measures mandated by NIS2. Key documentation to have readily accessible includes:

- Governance Model Documentation:
  - Cybersecurity Governance Charter (Chapter 2).
  - Organizational charts showing cybersecurity roles and reporting lines (CISO to CEO/DG).
  - Minutes from Cyber Risk Committee meetings.
  - Board packs/reports demonstrating management oversight (Chapter 9).
- Policies and Procedures:
  - The core policies developed in Chapter 3 (ISP, Risk Mgt, IR, BCDR, TPRM) and related procedures.
  - Evidence of policy communication and employee acknowledgment.
- Risk Management Program Documentation:
  - Risk Management Policy and Methodology (Chapter 3 & 4).
  - Asset Inventory (IT & OT) (Chapter 4).
  - Completed Risk Assessments (Chapter 4).
  - The up-to-date Risk Register (Chapter 4).
  - Risk Treatment Plans (Chapter 4).

- Technical and Organizational Measures (TOMs) Evidence:
    - Security Controls Matrix (Chapter 5).
    - Network diagrams showing segmentation (especially IT/OT).
    - Configuration standards/baselines.
    - Results of vulnerability scans and penetration tests (Chapter 4).
    - Patch management records/reports.
    - Backup logs and restore test reports (Chapter 5).
    - Access control lists/reviews.
    - MFA implementation evidence.
    - SIEM/SOC monitoring logs and reports (samples).
- Incident Management Records:
    - Incident Response Plan and Playbooks (Chapter 6).
    - Incident log/ticketing system records.
    - Records of NIS2 notifications made to CSIRT Italia/ACN.
    - Post-incident review reports/lessons learned documentation.
- Supply Chain Security Documentation:
    - Third-Party Risk Management Policy (Chapter 3 & 7).
    - Critical supplier inventory (Chapter 7).
    - Sample contracts with cybersecurity clauses (Chapter 7).
    - Completed supplier risk assessment questionnaires/reports (Chapter 7).
    - Evidence of supplier monitoring (e.g., security ratings reports).
- Audit Reports:
    - Internal cybersecurity audit reports and management responses/remediation tracking (Chapter 8).
    - External audit or assessment reports (if applicable).
- Evidence of Staff Training:
    - Security Awareness Training Policy (Chapter 3 & 5).
    - Training materials content.
    - Records of employee participation and completion (e.g., LMS reports, attendance sheets).
    - Phishing simulation results and follow-up actions.

10.3 Action: Create a NIS2 Compliance Folder

To facilitate efficient retrieval during an inspection, consolidate all relevant documentation and evidence into a dedicated **NIS2 Compliance Folder**, which can be physical, digital (e.g., a structured folder on a shared drive or document management system), or ideally within a GRC platform.

Template: NIS2 Compliance Evidence Folder Structure (Example)

```
NIS2_Compliance_Evidence/
│
├──── 01_Governance/
│     ├──── Cybersecurity_Governance_Charter.pdf
│     ├──── Org_Chart_Cybersecurity.pdf
│     ├──── Cyber_Risk_Committee_Minutes/
│     │     └──── Q1_2025_Minutes.pdf
│     │     └────...
│     └──── Board_Reports/
│         └──── Q1_2025_Board_Pack.pdf
│         └────...
│
├──── 02_Policies_Procedures/
│     ├──── Information_Security_Policy_v3.0.pdf
│     ├──── Risk_Management_Policy_v2.1.pdf
│     ├──── Incident_Response_Policy_v2.5.pdf
│     ├──── BCDR_Policy_v1.8.pdf
│     ├──── Third_Party_Risk_Policy_v1.5.pdf
│     ├──── Access_Control_Procedure_v2.0.pdf
│     ├──── Patch_Management_Procedure_v1.7.pdf
│     └────... (Other relevant policies/procedures)
│
├──── 03_Risk_Management/
│     ├─── Risk_Assessment_Methodology.pdf
│     ├──── Asset_Inventory_IT_OT.xlsx
│     ├──── Risk_Register.xlsx
│     ├──── Risk_Assessment_Report_2025.pdf
│     └──── Risk_Treatment_Plans/
│         └──── RTP_R-OT-001.pdf
│         └────...
│
├──── 04_TOMs_Evidence/
│     ├──── Security_Controls_Matrix.xlsx
│     ├──── Network_Diagram_IT_OT_Segmentation.vsdx
│   ├─── Vulnerability_Scan_Reports/
│   │   └─── Q1_2025_Scan_Summary.pdf
│   ├─── Penetration_Test_Reports/
│   │   └─── Annual_PenTest_Report_2024.pdf
│   ├─── Patch_Compliance_Reports/
│   │   └─── April_2025_Patch_Report.pdf
│   ├─── Backup_Restore_Tests/
│   │   └─── Annual_Restore_Test_Report_2024.pdf
│   └─── MFA_Implementation_Proof/
│     └─── Okta_Config_Screenshots.pdf
│
├─── 05_Incident_Management/
│   ├─── Incident_Response_Plan_v2.5.pdf
│   ├─── Playbooks/
│   │   └─── Ransomware_Playbook_v1.2.pdf
│   │   └─── DDoS_Playbook_v1.0.pdf
│   ├─── Incident_Log_Export_2025.csv
│   ├─── NIS2_Notifications_Log/
│   │   └─── Incident_2025-05-10_Notification_Record.pdf
│   └─── Post_Incident_Reviews/
│     └─── PIR_Incident_2025-02-15.pdf
│
├─── 06_Supply_Chain/
│   ├─── Critical_Supplier_List.xlsx
│   ├─── Standard_Contract_Cyber_Addendum.pdf
│   └─── Supplier_Assessments/
│     └─── Vendor_A_Assessment_2025.pdf
│     └─── Vendor_B_SIG_Lite_2024.xlsx
│
├─── 07_Audits/
│   ├─── Internal_Audit_Plan_2025.pdf
│   ├─── Internal_Audit_Report_NIS2_Q3_2025.pdf
│   └─── External_Assessment_Report_2024.pdf
│
└─── 08_Training_Awareness/
  ├─── Training_Policy_v1.3.pdf
```

```
├── Training_Material_Samples/
│   └── Annual_Awareness_Module.pdf
├── Training_Completion_Records_2025.xlsx
└── Phishing_Simulation_Results/
    └── Q1_2025_Phishing_Report.pdf
```

Structure based on ISO 27001 evidence concepts. Maintain version control and ensure easy searchability.

Being inspection-ready requires more than just having documents; it necessitates a culture of continuous compliance and documentation. Evidence should be generated as part of routine operations (e.g., logs, reports from tools, meeting minutes, updated risk registers) rather than created solely for an audit.

Conclusions and Recommendations

The NIS2 Directive, transposed into Italian law by D.Lgs. 138/2024, represents a significant evolution in cybersecurity regulation for critical infrastructure, including Public Administration entities designated as essential. Compliance is not merely a legal obligation carrying substantial penalties and management liability, but a strategic necessity for ensuring the resilience of essential services upon which society depends.

This guide provides a practical, ten-chapter roadmap for CISOs within Italian critical infrastructure PAs to establish a robust cybersecurity governance strategy aligned with NIS2 and leveraging the comprehensive structure of NIST CSF 2.0. Key recommendations derived from this guide include:

1. **Establish Strong Governance:** Define a clear governance structure (Strategic, Tactical, Operational) and formalize it through a Cybersecurity Governance Charter. Ensure the CISO has a direct reporting line to the highest executive level (CEO/Director General) to guarantee visibility and authority. Embed cybersecurity into executive decision-making, recognizing the Board's ultimate accountability under NIS2.
2. **Core Policy Development:** Develop and maintain core policies mandated or implied by NIS2 (Information Security, Risk Management, Incident Response, BCDR, Third-Party/Supply Chain Security), ensuring they cover both IT and OT environments and include clear roles, responsibilities, and compliance criteria.
3. **Implement Continuous Risk Management:** Adopt a continuous, framework-aligned (ISO 27005 or NIST RMF) risk management cycle encompassing asset identification (IT/OT), threat analysis (APT, ransomware, supply chain, DDoS), vulnerability management (scanning, penetration testing, patching with compensating controls for OT), risk assessment, and treatment. Maintain a comprehensive Risk Register.
4. **Deploy Robust TOMs:** Implement appropriate technical and organizational measures across key domains (access control/MFA, IT/OT network segmentation, security monitoring/SOC, patch management, backup/recovery, incident response/forensics, continuous training) guided by risk assessment and aligned with NIST CSF 2.0. Track implementation and maturity using a Security Controls Matrix.
5. **Prepare for Incident Reporting:** Establish clear internal detection, categorization, and escalation procedures. Develop specific incident response playbooks (e.g., ransomware, DDoS) and ensure strict adherence to NIS2's multi-

stage notification timeline (24h/72h/1m) to CSIRT Italia/ACN.

6. **Secure the Supply Chain:** Implement a rigorous Third-Party Risk Management (TPRM) program involving supplier mapping, contractual security requirements, due diligence assessments (using questionnaires like SIG/CAIQ and security ratings), and ongoing monitoring.
7. **Foster Continuous Improvement:** Conduct regular internal audits, monitor relevant KPIs and KRIs, and use these insights, along with incident lessons learned and threat intelligence, to drive continuous improvement of policies, controls, and processes, aligning with NIST CSF's ID.IM function. Utilize compliance dashboards for effective monitoring.
8. **Ensure Effective Board Reporting:** Communicate regularly (quarterly) with the Board/Executive Committee using concise, visual Board Packs that translate technical data into business risk language, focusing on risk posture, incident impact, compliance status, and strategic initiatives.
9. **Maintain Inspection Readiness:** Consolidate all necessary documentation and evidence (policies, risk assessments, logs, reports, training records) into a well-organized NIS2 Compliance Folder (physical or digital) for efficient retrieval during potential ACN inspections.

Successfully navigating NIS2 requires a holistic, risk-based, and continuous approach. It demands collaboration across IT, OT, legal, compliance, risk, procurement, and executive leadership. By following the practical steps and leveraging the frameworks outlined in this guide, CISOs in Italian critical infrastructure PAs can build a resilient cybersecurity posture, meet regulatory requirements, and ultimately safeguard the essential services they provide.

References

- EUR-Lex. (n.d.). *Cybersecurity of network and information systems (2022)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=legissum:4637829
- NIS 2 Directive. (n.d.). *What is the NIS 2 Directive?* Retrieved from https://www.nis-2-directive.com/
- Sekoia.io Blog. (n.d.). *Navigating the NIS2 Directive: Key insights for cybersecurity compliance and how Sekoia.io can help*. Retrieved from https://blog.sekoia.io/navigating-the-nis2-directive-key-insights-for-cybersecurity-compliance-and-how-sekoia-io-can-help/
- EUR-Lex. (2022, December 27). *Directive (EU) 2022/2555*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/NIM/?uri=oj:JOL_2022_333_R_0002
- SEEBURGER Blog. (n.d.). *Implementing Regulation clarifies Articles 20, 21 and 23 of EU NIS2 2022/2555*. Retrieved from https://blog.seeburger.com/implementing-regulation-clarifies-articles-20-21-and-23-of-eu-nis2-2022-2555/
- CyberUpgrade Blog. (n.d.). *Compliance Regulations: NIS2 Directive Regulations and Implementation in Italy*. Retrieved from https://cyberupgrade.net/blog/compliance-regulations/nis2-directive-regulations-and-implementation-in-italy/
- Auxadi Blog. (2025, March 3). *Italy Cybersecurity Improvements*. Retrieved from https://www.auxadi.com/blog/2025/03/03/italy-cybersecurity-improvements/
- ECSO. (n.d.). *NIS2 Directive Transposition Tracker*. Retrieved from https://ecs-org.eu/activities/nis2-directive-transposition-tracker/
- OpenKRITIS. (n.d.). *EU NIS 2 Italy*. Retrieved from https://www.openkritis.de/eu/eu-nis-2-italy.html
- Advisera. (n.d.). *Overview of the Italian NIS2 Law and Comparison with the EU NIS2 Directive*. Retrieved from https://advisera.com/articles/overview-of-the-italian-nis2-law-and-comparison-with-the-eu-nis2-directive/
- Rexilience. (n.d.). *The NIS2 Directive: New Standards for IT Security in Italy*. Retrieved from https://rexilience.eu/the-nis2-directive-new-standards-for-it-security-in-italy/
- Tesisquare Blog. (n.d.). *Cybersecurity: The NIS2 Directive comes into force*. Retrieved from https://www.tesisquare.com/en/blog/cibersecurity-entra-in-vigore-la-direttiva-nis2
- Distline Blog. (n.d.). *NIS 2 Compliance: Everything You Need to Know*. Retrieved from https://www.distline.com/en/adeguamento-nis-2-tutto-quello-che-devi-sapere/
- Negg Blog. (n.d.). *ACN: National Competent Authority for NIS 2 in Italy*. Retrieved from https://negg.blog/en/acn-national-competent-authority-for-nis-2-in-italy/
- ASEE Cybersecurity Blog. (2025, April 25). *Incident reporting under NIS2: Entity Reporting Obligations*. Retrieved from https://cybersecurity.asee.io/blog/incident-reporting-under-nis2/
- Timelex Blog. (2025, January 23). *24 hours, 72 hours, 1 month: reporting cyber incidents under NIS2*. Retrieved from https://www.timelex.eu/en/blog/24-hours-72-hours-1-month-reporting-cyber-incidents-under-nis2
- NIS 2 Directive. (n.d.). *NIS 2 Directive Preamble 101 to 110*. Retrieved from https://www.nis-2-directive.com/NIS_2_Directive_Preamble_101_to_110.html
- RadarFirst Blog. (n.d.). *Navigating NIS2: A Comprehensive Guide to Incident Reporting Obligations*. Retrieved from https://www.radarfirst.com/blog/navigating-nis2-a-guide-to-incident-reporting-obligations/

- Advisera. (n.d.). *Reporting obligations according to NIS 2*. Retrieved from https://advisera.com/articles/reporting-obligations-nis2/
- Moody's. (n.d.). *Understanding the NIS2 Regulation: Staying Compliant - Key Insights*. Retrieved from https://www.moodys.com/web/en/us/kyc/resources/insights/understanding-the-nis2-regulation-staying-compliant-key-insights.html
- Tresorit Blog. (2025, January 14). *Penalties for non-compliance with NIS2: what businesses need to know*. Retrieved from https://tresorit.com/blog/penalties-for-non-compliance-with-nis2-what-businesses-need-to-know/
- The Cyphere Blog. (n.d.). *NIS2 Essential and Important Entities: What You Need to Know*. Retrieved from https://thecyphere.com/blog/nis2-essential-and-important-entities/
- Cyberday Blog. (n.d.). *Understanding NIS2 Supervision and Penalties of Non-Compliance*. Retrieved from https://www.cyberday.ai/blog/understanding-nis2-supervision-and-penalties-of-non-compliance
- National Institute of Standards and Technology. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0* (NIST CSWP 29). https://doi.org/10.6028/NIST.CSWP.29
- NIST. (n.d.). *Cybersecurity Framework Resources*. Retrieved from https://www.nist.gov/cyberframework/resources-0
- NIST. (n.d.). *Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework
- National Institute of Standards and Technology. (n.d.). *NIST CSF 2.0: Resource & Overview Guide* (NIST SP 1299). Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1299.pdf
- Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Cybersecurity Governance*. Retrieved from https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-governance
- MassCyberCenter. (n.d.). *Critical Infrastructure Toolkit*. Retrieved from https://masscybercenter.org/cyber-resilient-massachusetts/critical-infrastructure-toolkit
- SANS Institute. (n.d.). *Security Policy Templates*. Retrieved from https://www.sans.org/information-security-policy/
- U.S. Department of Energy. (2023, January). *Cybersecurity Plan Template - Medium Risk*. Retrieved from https://www.energy.gov/sites/default/files/2023-05/EXEC-2022-008113%20-%20Cybersecurity%20Plan%20Templates_Medium%20Risk.docx
- Info-Tech Research Group. (n.d.). *Templates and Policies*. Retrieved from https://www.infotech.com/browse/cio/strategy-governance/it-governance-risk-compliance/list/templates-and-policies?page=2
- National Cyber Security Centre NZ. (2019, November). *Charting Your Course: Governance Step 2 - Roles and Responsibilities*. Retrieved from https://www.ncsc.govt.nz/assets/NCSC-Documents/NCSC-Charting-Your-Course-Governance-Step-2-Nov-2019.pdf
- Augusta University. (n.d.). *Cybersecurity Charter Policy*. Retrieved from https://www.augusta.edu/services/legal/policyinfo/policy/cybersecurity-charter-policy.pdf
- Photronics, Inc. (n.d.). *Cybersecurity Risk Management Committee Charter*. Retrieved from https://photronicsinc.gcs-web.com/static-files/a167e6a3-5c3b-409e-9fcd-169ec352419d
- Unknown Author. (n.d.). *Italy's Cyber Security Architecture and Critical Infrastructure*. Retrieved from https://cris.unibo.it/bitstream/11585/800407/4/Italy%27s%20Cyber%20Security%20Architecture

%20and%20Critical%20Infrastructure.pdf (Note: Limited content preview available)

- European Commission Research & Innovation. (n.d.). *Public Deliverable Report*. Retrieved from https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5119187f1&appId=PPGMS (Note: Specific content not fully available)
- Syneto. (n.d.). *Cybersecurity: strategies and key roles in Italian companies*. Retrieved from https://syneto.eu/cybersecurity-strategies-and-key-roles-in-italian-companies/
- [1]Cybersecurity Dive. (2024, March 27). *CISA issues notice for long-awaited critical infrastructure reporting requirements*. Retrieved from https://www.cybersecuritydive.com/news/cisa-notice-critical-infrastructure/711506/
- [1]ENISA. (n.d.). *Network and Information Systems Directive 2 (NIS2)*. Retrieved from https://www.enisa.europa.eu/topics/awareness-and-cyber-hygiene/network-and-information-systems-directive-2-nis2
- SANS Institute. (n.d.). *All you need to know about the new NIS2 Directive*. Retrieved from https://www.sans.org/mlp/nis2/
- NIS 2 Directive. (n.d.). *Homepage*. Retrieved from https://www.nis-2-directive.com/
- Threat Modeling. (n.d.). *Cybersecurity Risk Assessment Template*. Retrieved from https://threat-modeling.com/cybersecurity-risk-assessment-template/
- ENISA. (2025, January 10). *Asking for your feedback: ENISA technical guidance for the cybersecurity measures of the NIS2 implementing act*. Retrieved from https://www.enisa.europa.eu/news/asking-for-your-feedback-enisa-technical-guidance-for-the-cybersecurity-measures-of-the-nis2-implementing-act
- Cyolo Videos. (n.d.). *How NIS2 Impacts the OT Domain*. Retrieved from https://cyolo.io/videos/how-nis2-impacts-the-ot-domain
- RadarFirst Blog. (n.d.). Navigating NIS2: A Comprehensive Guide to Incident Reporting Obligations. [28]
- ENISA. (n.d.). *Threats and Incidents*. Retrieved from https://www.enisa.europa.eu/topics/state-of-cybersecurity-in-the-eu/threats-and-incidents
- NIS 2 Directive. (n.d.). *NIS 2 Directive Article 23*. Retrieved from https://www.nis-2-directive.com/NIS_2_Directive_Article_23.html
- Distline Blog. (n.d.). NIS 2 Compliance: Everything You Need to Know. [6]
- IoT M2M Council. (2024, November 21). *ENISA issues guidance on NIS2 Directive*. Retrieved from https://www.iotm2mcouncil.org/iot-library/news/iot-in-public-policy/eu-issues-guidance-on-nis2-directive/
- Rockwell Automation Blog. (n.d.). *NIS2 and OT Cybersecurity: What Industrial Organizations Need to Know*. Retrieved from https://www.rockwellautomation.com/en-gb/company/news/blogs/nis2-ot-cybersecurity.html
- CIS Security. (n.d.). *NIST Cybersecurity Framework Policy Template Guide*. Retrieved from https://www.cisecurity.org/-/jssmedia/Project/cisecurity/cisecurity/data/media/img/uploads/2021/11/NIST-Cybersecurity-Framework-Policy-Template-Guide-v2111Online.pdf
- Mission Secure. (n.d.). *OT Cybersecurity*. Retrieved from https://www.missionsecure.com/ot-cybersecurity
- ENISA. (n.d.). *Good Practices for Supply Chain Cybersecurity*. Retrieved from https://www.enisa.europa.eu/sites/default/files/publications/Good%20Practices%20for%20Suppl

y%20Chain%20Cybersecurity.pdf

- Unknown Source (Mangum OK Meeting Attachment). (n.d.). *NIST Cybersecurity Framework Policy Template Guide*. Retrieved from https://mccmeetingspublic.blob.core.usgovcloudapi.net/mangumok-meet-4e68e0eeaa63422eba40bf865ed5bbf1/ITEM-Attachment-001-0e1cf20e7e734d34b9c7203f09bf3183.pdf [48]
- BitSight Blog. (n.d.). *Navigating NIS2 Requirements: Transforming Supply Chain Security*. Retrieved from https://www.bitsight.com/blog/navigating-nis2-requirements-transforming-supply-chain-security
- National Cybersecurity Authority (NCA). (n.d.). *Corporate Cybersecurity Policy Template*. Retrieved from https://cdn.nca.gov.sa/api/files/public/upload/6db9eb86-67ab-4d22-8afe-3db6855e3994_POLICY_Corporate-Cybersecurity-Policy_template_en-.pdf
- Cynet. (n.d.). *Creating Your Cyber Security Policy: Ultimate Guide*. Retrieved from https://www.cynet.com/cybersecurity/creating-your-cyber-security-policy-ultimate-guide/
- Cynomi Blog. (n.d.). *The Definitive Cyber Security Policy Template*. Retrieved from https://cynomi.com/blog/the-definitive-cyber-security-policy-template-xls-download/
- Stiftung Neue Verantwortung (SNV). (n.d.). *ENISA Fit for Purpose*. Retrieved from https://www.interface-eu.org/publications/enisa-fit-for-purpose
- Chambers and Partners Practice Guides. (n.d.). *Cybersecurity 2025 - Italy - Law and Practice*. Retrieved from https://practiceguides.chambers.com/practice-guides/comparison/971/15667/24449-24453-24458-24465-24468-24470
- Compliance Hub Wiki. (n.d.). *Navigating NIS2: A Comprehensive Guide to the EU's Cybersecurity Directive*. Retrieved from https://www.compliancehub.wiki/navigating-nis2-a-comprehensive-guide-to-the-eus-cybersecurity-directive/
- Cybersecurity and Infrastructure Security Agency (CISA). (n.d.). *Project Cyber Risk Assessment and Project Cybersecurity Risk Mitigation Activities Sample Template*. [Excel file]. Retrieved from https://www.cisa.gov/sites/default/files/2024-12/Project%20Cyber%20Risk%20Assessment%20and%20Project%20Cybersecurity%20Risk%20Mitigation%20Activities%20Sample%20Template_1.xlsx
- Federal Emergency Management Agency (FEMA). (2023, November). *Critical Cyber Asset Identification and Prioritization Checklist*. Retrieved from https://www.fema.gov/sites/default/files/documents/fema_cyber-asset-id-prioritization-checklist.pdf
- U.S. Department of Energy. (n.d.). *C2M2 V2.1 Practice and Help Text*. [Excel file]. Retrieved from https://c2m2.doe.gov/C2M2%20V2.1%20Practice%20and%20Help%20Text.xlsx
- Langner. (n.d.). *Simple Cyber Governance Program (SCGP)*. Retrieved from https://www.langner.com/scgp/