anecdotes

The NIS2 Starter Pack

A comprehensive list of controls and the requirements necessary to satisfy them for organizations looking to comply with NIS2.

NIS2 covers a wide range of industries, including critical infrastructure, banking, healthcare, energy, digital infrastructure and ICT providers. While it does not have reach outside of the EU, any international organizations with security decision-makers or large security teams in the EU fall into its scope. If you meet those criteria, starting October 17th, 2024, you will need to ensure compliance with NIS2.

Unlike some previous regulations, NIS2 requires some organizations to submit evidence of compliance annually. Regulators can also choose to audit for NIS2 compliance at any time with minimal notice provided. It is also highly likely that partners and customers will require evidence of compliance before agreeing to terms in the future. This means organizations that need to comply with NIS2 need to collect and retain evidence and monitor controls on an ongoing basis.

To help you get started and save you time and effort, our NIS2 starter pack provides a breakdown of the legal text, transforming it into an actionable framework. For each article that requires action on behalf of 'essential and important entities', we have split each clause into a 'control'. Each control can be monitored and audited by ensuring that the expected evidence (requirements) are always readily available and in a positive state.

Naturally, as there is no one-size-fits-all approach to security and compliance, the controls outlined in this document may need to be modified or adapted to meet your organization's precise needs.

NIS2 - Controls and Expected Evidence (Requirements)

Article 20 - Governance

CONTROL NAME

20.1 Approval of cybersecurity risk-management measures

CONTROL DESCRIPTION

Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions and the liability of public servants and elected or appointed officials.

SIMILAR CONTROLS

ISO 27001:2022
5.1 Leadership and commitment
9.3.1 Management review

NIST 800-53 REV 5
PM-1 Information Security Program Plan
PM-9 Risk Management Strategy

REQUIREMENTS

- **Board of Directors responsibility document** — Outlines the areas in which the Board of Directors takes overall responsibility for information security.
- **Management review documentation** — Meeting minutes that present management with information security updates, internal audit findings, the status of actions from previous reviews, changes in external and internal issues, risk assessment/treatment statuses, etc.

CONTROL NAME

20.2 Cybersecurity training for management bodies and employees

CONTROL DESCRIPTION

Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training and shall encourage essential and important entities to offer similar training to their employees regularly so that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

SIMILAR CONTROLS

ISO 27001:2022
A.6.3 Information security awareness, education and training

NIST 800-53 REV 5
AT-2 Literacy Training and Awareness
AT-4 Training Records

REQUIREMENTS

- **Security awareness and training policy** — Policy that defines training requirements for organizational employees, both in terms of training content and training frequency.
- **Board training curriculum** — Topics covered in the training are specifically designed to ensure that board members are aware of information security risks and their responsibilities in ensuring information security requirements are met (discharging effective oversight).
- **Board member training completion** — Register of attendance for each training within the curriculum.
- **Information security awareness training curriculum** — Topics covered within the training that all employees undergo. Commonly includes acceptable use of assets, handling sensitive data (e.g., PII/PHI), recognizing phishing attempts, etc.
- **Information security awareness training completion** — Register of attendance for each training within the curriculum.

Article 21 - Cybersecurity risk-management measures

CONTROL NAME

20.1 Technical, operational and organizational measures to manage network and information system security risk

CONTROL DESCRIPTION

Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems that those entities use for their operations or the provision of their services and to prevent or minimize the impact of incidents on recipients of their services and other services.

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed. When assessing the proportionality of those measures, due account shall be taken of the degree of the entity's exposure to risks, the entity's size, the likelihood of occurrence of incidents and their severity, including the societal and economic impact.

SIMILAR CONTROLS

ISO 27001:2022
6.1.2 Information security risk assessment
8.2 Information security risk assessment

NIST 800-53 REV 5
RA-3 Risk Assessment
RA-7 Risk Response

REQUIREMENTS

- **List of completed audits and assessment activity** — List of all internal and external audits conducted over the last year, as well as any additional security assessments (such as penetration tests, red team exercises, etc.).
- **Risk register (with assessments per risk)** — Risk assessment that has been performed, updated and reviewed within the past year. The risk assessment should include the following:
  a. Identification of risks to service/product/organization that is the subject of the audit
  b. Quantification of likelihood and impact of risk occurring
  c. Identification of mitigation strategies and controls for each risk identified
  d. Evidence of review and approval of the risk assessment
  e. Date risk assessment was performed

CONTROL NAME

20.2a Policies

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: policies on risk analysis and information system security.

SIMILAR CONTROLS

ISO 27001:2022
5.2 Policy
A.5.1 Policies for information security

NIST 800-53 REV 5
AC-1 Policy and Procedures

REQUIREMENTS

- **List of reviewed and approved policies/documents** — All policies/documents that have received their annual management approval.
- **Information security policy** — Policy governing information security as a whole within the organization. This policy references the general approach to security across a wide array of relevant domains such as protection of assets and sensitive data (e.g. PII/PHI), human resources practices, network security, etc.

CONTROL NAME

20.2b Incident handling

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: incident handling.

SIMILAR CONTROLS

ISO 27001:2022
A.5.24 Information security incident management planning and preparation
A.5.26 Response to information security incidents

NIST 800-53 REV 5
IR-1 Policy and Procedures
IR-4 Incident Handling

REQUIREMENTS

- **Incident response procedure** — Formal procedure outlining the stages for response once an information security event is classified as an incident.
- **Incident response team documentation** — Define the team to be responsible for incident response, with a clear division of responsibilities (can be included within the incident response policy). A team member must be available 24/7 to respond to any critical detections/alerts.
- **List of external contacts for incident reporting** — List of organizations to be contacted in the event of an incident that requires external communication (e.g. law enforcement, regulatory bodies, supervisory authorities).

CONTROL NAME

20.2c Business continuity

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: business continuity, such as backup management and disaster recovery, and crisis management.

SIMILAR CONTROLS

ISO 27001:2022
A.5.30 ICT readiness for business continuity
A.8.14 Redundancy of information processing facilities
A.8.13 Information backup

NIST 800-53 REV 5
CP-2(5) Contingency Plan | Continue Mission and Business Functions
CP-6 Alternate Storage Site
CP-9 System Backup

REQUIREMENTS

- **Business Continuity Plan (BCP)** — Plan developed to address specific scenarios that may arise that pose a risk to the continuity of business critical assets and processes (as classified by a business impact analysis). These plans are thoroughly detailed and periodically tested, with the testing documented such that lessons can be learned over time.
- **Disaster Recovery Plan (DRP)** — Plan developed to ensure systems can return to full operation following a significant incident. This plan is tested annually, with results analyzed, and the plan updated to reflect findings.
- **Backup schedule configuration** — Configuration of a backup schedule that validates that backups are performed as per policy (e.g. daily incremental backups plus weekly full backups).
- **Backup and restoration policy** — Policy that defines the frequency of backups per system and application, and the frequency for performing restorations from backups (as part of a test).
- **Multi-availability zones (redundancy configurations)** — Configurations per critical resource demonstrating an additional availability zone so that redundancy is ensured in the event of system downtime.

CONTROL NAME

20.2d Supply chain security

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers.

SIMILAR CONTROLS

ISO 27001:2022
A.5.19 Information security in supplier relationships
A.5.20 Addressing information security within supplier agreements
A.5.21 Managing information security in the ICT supply chain
A.5.22 Monitoring, review and change management of supplier services

NIST 800-53 REV 5
SR-1 Policy and Procedures
SR-2 Supply Chain Risk Management Plan
SR-3 Supply Chain Controls and Processes

REQUIREMENTS

- **Vendor management policy** — Policy defines the approach towards vendor evaluation before onboarding, as well as continuous security requirements and termination procedures.
- **Vendor agreement sample** — Sample of agreement/contract signed by the vendor, outlining security and confidentiality requirements, as well as a standard code of conduct.
- **List of vendors** — List of all vendors used by the organization. Includes date of start of service, service provided, contact information, vendor criticality (critical/not-critical) and status (active/inactive); Also includes requirements for annual compliance re-validation.
- **Review of vendor/sub-services compliance and agreements** — Documentation collected during annual review of audit reports/compliance attestations for vendors/sub-services. For SOC2 audit reports, impact of control exceptions and applicable complementary user entity controls (CUECs) are considered.
- **Third-party risk assessment** — Risk assessment of third parties, including an overall risk level for each vendor, reviewed and updated periodically.

CONTROL NAME

20.2e Network and information system security

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure.

SIMILAR CONTROLS

ISO 27001:2022
A.8.20 Networks security
A.8.21 Security of network services

NIST 800-53 REV 5
SC-7 Boundary Protection
SI-4 System Monitoring

REQUIREMENTS

- **Security operations and network security policy** — Policy defines guidelines for network access, as well as giving an overview of network architecture.
- **Network connections listing** — List of network connections (e.g., security groups) with their rules (services, ports and protocols allowed/blocked). By default, all network communications are disabled, and only those needed are enabled.
- **IDS/IPS configuration** — Configuration of intrusion detection or prevention systems in place to provide continuous monitoring of both the organizational network (NIDS) and the hosts on the network (HIDS) and to prevent potential security breaches (NIPS/HIPS).
- **Web-app firewall (WAF) configuration** — Configuration of firewall that blocks unwanted traffic to and from the organization's website/web application.

CONTROL NAME

20.2f Policies and procedures to assess effectiveness

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

SIMILAR CONTROLS

ISO 27001:2022
9.1 Monitoring, measurement, analysis and evaluation
A.8.8 Management of technical vulnerabilities

NIST 800-53 REV 5
CA-8 Penetration Testing,
RA-5 Vulnerability Monitoring and Scanning

REQUIREMENTS

- **Vulnerability management policy** — Policy outlines
  a. the schedule for vulnerability scanning (both infrastructure and application layers) and the configuration of scans
  b. the penetration testing schedule (both internal testing and testing conducted by third parties)
  c. the appropriate configuration and scan schedule for organizational antivirus
  d. the process for scanning code from third party libraries
  e. remediation methodologies for all types of found vulnerabilities.
- **Penetration test report** — Report produced following annual (at minimum) penetration test. Report includes scope of test and detailed findings, including remediation guidance.
- **Penetration test finding remediation tickets/approval** — Remediation tickets opened to track resolution of findings from the penetration test. Tickets are tracked and prioritized based on severity of finding.
- **Infrastructure vulnerability scan report** — Report of periodic vulnerability scan performed on infrastructure components (e.g., servers, VMs, endpoints) to identify vulnerabilities.
- **Infrastructure vulnerability scan configuration** — Configuration of the scope of the scan (to ensure that all production components are in scope) and the cadence at which the scan will occur.
- **Application vulnerability scan report** — Report of periodic vulnerability scan performed at the application layer (most commonly on a web app, commonly known as DAST) to identify vulnerabilities.
- **Application vulnerability scan configuration** — Configuration of the scope of the scan (to ensure that all production applications are in scope) and the cadence at which the scan will occur.

CONTROL NAME

20.2g Cyber hygiene and training

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: basic cyber hygiene practices and cybersecurity training.

SIMILAR CONTROLS

ISO 27001:2022
A.6.3 Information security awareness, education and training

NIST 800-53 REV 5
AT-2 Literacy Training and Awareness
AT-4 Training Records

REQUIREMENTS

- **Information security awareness training curriculum** — Topics covered within the training that all employees undergo. Commonly includes acceptable use of assets, handling sensitive data (e.g., PII/PHI), recognizing phishing attempts, etc.
- **Information security awareness training completion** — Register of attendance for each training within the curriculum.
- **Continuous awareness training curriculum** — Contents may include internal phishing campaigns, monthly/bi-monthly short training videos that employees are required to watch, and general security update emails.
- **Security awareness and training policy** — Policy that defines training requirements for organizational employees, both in terms of training content and training frequency.

CONTROL NAME

20.2h Cryptography and encryption

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: policies and procedures regarding the use of cryptography and, where appropriate, encryption.

SIMILAR CONTROLS

ISO 27001:2022
A.5.34 Privacy and protection of PII
A.8.24 Use of cryptography
A.8.3 Information access restriction
A.8.1 User endpoint devices

NIST 800-53 REV 5
SC-13 Cryptographic Protection
SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection

REQUIREMENTS

- **Encryption policy** — Policy defines encryption requirements (e.g., cipher strength) for data at rest and data in transit, as well as the requirements for key management (storage and rotation).
- **Encryption configuration of data at rest** — Configuration demonstrating that data at rest (e.g. database/storage) is encrypted using industry-accepted standards (e.g. AES256).
- **Encryption configuration of data in transit** — Configuration demonstrating that data in transit (e.g. being transmitted over a public network) is encrypted using industry-accepted standards (e.g. TLS 1.2 or newer). Deprecated protocols are avoided (e.g. TLS1.1 or older).
- **Endpoint disk encryption configuration** — Configuration demonstrating that disk encryption is enabled and enforced on all endpoints (as part of the IT setup process); decryption requires authentication.

CONTROL NAME

20.2i Human resources, access control and asset management

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents and shall include at least the following: human resources security, access control policies and asset management.

SIMILAR CONTROLS

ISO 27001:2022
A.5.15 Access control
A.5.18 Access rights
A.6.1 Screening

NIST 800-53 REV 5
PS-3 Personnel Screening
AC-3 Access Enforcement,
AC-6 Least Privilege

REQUIREMENTS

- **Human resources policy** — Policy outlines HR requirements throughout the employment lifecycle — prior to employment, during onboarding, during the employment period and during the offboarding process.
- **Candidate screenings/background checks** — Background and professional reference checks completed for new employees and contractors.
- **Employee/contractor employment contract** — Template of the employee/contractor agreement/contract, clearly defining responsibilities regarding information security.
- **Access control policy -** Policy outlining the requirements for the provisioning, modification and revocation of user access rights. Policy also defines frequency and method used for user access reviews.
- **Employee termination checklist** — Checklist that covers each task that must be completed as part of employee termination, ensuring access is revoked for all employees as part of offboarding.
- **List of revoked users** — List of revoked users from production systems (applications, databases, servers and cloud platforms).
- **Inventory of assets** — Complete list of managed assets (this may include both physical and virtual assets). Each asset has a defined owner, classification and location.

CONTROL NAME

20.2j MFA/continuous authentication

CONTROL DESCRIPTION

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following: the use of multi-factor authentication or continuous authentication solutions, secured voice, video and text communications and secured emergency communication systems within the entity, where appropriate.

SIMILAR CONTROLS

ISO 27001:2022
A.8.5 Secure authentication

NIST 800-53 REV 5
IA-5(1) Authenticator Management | Password-based Authentication
IA-2 Identification and Authentication (Organizational Users)

REQUIREMENTS

- **Password policy configuration** — Configuration demonstrating that secure passwords are required for authentication to all systems and applications and that complexity requirements are technologically enforced and align with organizational policy.
- **MFA configuration** — Configuration demonstrating that MFA is enforced for the organization's production systems (e.g. cloud platforms, servers, databases).

CONTROL NAME

20.3 Supplier evaluations

CONTROL DESCRIPTION

Member States shall ensure that, when considering which measures referred to in paragraph 2, point (d), of this Article are appropriate, entities take into account the vulnerabilities specific to each direct supplier and service provider and the overall quality of products and cybersecurity practices of their suppliers and service providers, including their secure development procedures. Member States shall also ensure that, when considering which measures referred to in that point are appropriate, entities are required to take into account the results of the coordinated security risk assessments of critical supply chains carried out in accordance with Article 22(1).

SIMILAR CONTROLS

ISO 27001:2022
5.19 Information security in supplier relationships

NIST 800-53 REV 5
SR-6 Supplier Assessments and Reviews

REQUIREMENTS

- **Vendor management policy** — Policy defines the approach towards vendor evaluation before onboarding, as well as continuous security requirements and termination procedures.
- **Third-party risk assessment** — Risk assessment of third parties, including an overall risk level for each vendor, reviewed and updated periodically.

CONTROL NAME

20.4 Corrective measures

CONTROL DESCRIPTION

Member States shall ensure that an entity that finds that it does not comply with the measures provided for in paragraph 2 takes, without undue delay, all necessary, appropriate and proportionate corrective measures.

SIMILAR CONTROLS

ISO 27001:2022
10.1 Continual improvement
10.2 Nonconformity and corrective action

NIST 800-53 REV 5
CA-5 Plan of Action and Milestones

REQUIREMENTS

- **Corrective and preventive action (CAPA) form** — Documented form that outlines actions to be taken in the event of any non-conformities arising from internal or external auditing processes.
- **Information security work plan** — A formalized program (a work plan) that includes information security-related tasks for the upcoming year that aim to mitigate risks and ensure KPIs are met.

Article 23 - Reporting obligations

CONTROL NAME

23.1 Notification of incidents to CSIRT or competent authority

CONTROL DESCRIPTION

Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident). Where appropriate, entities concerned shall notify, without undue delay, the recipients of their services of significant incidents that are likely to adversely affect the provision of those services. Each Member State shall ensure that those entities report, inter alia, any information enabling the CSIRT or, where applicable, the competent authority to determine any cross-border impact of the incident. The mere act of notification shall not subject the notifying entity to increased liability.

Where the entities concerned notify the competent authority of a significant incident under the first subparagraph, the Member State shall ensure that that competent authority forwards the notification to the CSIRT upon receipt.

In the case of a cross-border or cross-sectoral significant incident, Member States shall ensure that their single points of contact are provided in due time with relevant information notified in accordance with paragraph 4.

SIMILAR CONTROLS

ISO 27001:2022
A.5.5 Contact with authorities
A.6.8 Information security event reporting

NIST 800-53 REV 5
IR-6 Incident Reporting

REQUIREMENTS

- **List of security incidents and system downtime issues** — List of any security events that have formally been classified as incidents, including system downtime issues, and their status (e.g. resolved/awaiting resolution). List should also offer details per incident (category, severity, relevant departments, etc.).
- **List of external contacts for incident reporting** — List of organizations to be contacted in case of an incident requiring external communication (e.g. law enforcement, regulatory bodies, supervisory authorities).
- **Notification of incident sent to stakeholders** — Notification that has been sent to internal/external stakeholders who must be made aware of any incident that has occurred.
- **Incident response procedure** — A formal procedure outlining the response steps that must be carried out once an information security event is classified as an incident.

CONTROL NAME

23.2 Notification of incidents to customer

CONTROL DESCRIPTION

Where applicable, Member States shall ensure that essential and important entities communicate, without undue delay, to the recipients of their services that are potentially affected by a significant cyber threat any measures or remedies that those recipients are able to take in response to that threat. Where appropriate, the entities shall also inform those recipients of the significant cyber threat itself.

SIMILAR CONTROLS

ISO 27001:2022
A.5.5 Contact with authorities

NIST 800-53 REV 5
IR-6 Incident Reporting

REQUIREMENTS

- **Notification of incident sent to stakeholders** — Notification that has been sent to internal/external stakeholders who must be made aware of any incident that has occurred.
- **Incident response procedure** — A formal procedure outlining the response steps that must be carried out once an information security event is classified as an incident.

CONTROL NAME

23.3 Incident classification

CONTROL DESCRIPTION

An incident shall be considered to be significant if:

(a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;

(b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.

SIMILAR CONTROLS

ISO 27001:2022
A.5.25 Assessment and decision on information security events

NIST 800-53 REV 5
IR-4 Incident Handling

REQUIREMENTS

- **Incident response policy** — Outlines organizational classification of different incident types, incident response responsibilities and high-level response actions that must occur.

CONTROL NAME

23.4 Incident updates and reports

CONTROL DESCRIPTION

Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:

(a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;

(b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;

(c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;

(d) a final report not later than one month after the submission of the incident notification under point (b), including the following:

(i) a detailed description of the incident, including its severity and impact;

(ii) the type of threat or root cause that is likely to have triggered the incident;

(iii) applied and ongoing mitigation measures;

(iv) where applicable, the cross-border impact of the incident;

(e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.

SIMILAR CONTROLS

ISO 27001:2022
A.5.24 Information security incident management planning and preparation
A.5.5 Contact with authorities

NIST 800-53 REV 5
IR-8(1) Incident Response Plan | Breaches

REQUIREMENTS

- **Incident notification procedures summary** — Document that summarizes clear procedures for formal notification of incidents: who needs to be notified within what timeframes and any follow-up notifications needed (e.g., incident final report submitted to formal authority).

Article 29 - Information sharing

CONTROL NAME

29.1 Exchange of relevant cybersecurity information

CONTROL DESCRIPTION

Member States shall ensure that entities falling within the scope of this Directive and, where relevant, other entities not falling within the scope of this Directive are able to exchange on a voluntary basis relevant cybersecurity information among themselves, including information relating to cyber threats, near misses, vulnerabilities, techniques and procedures, indicators of compromise, adversarial tactics, threat-actor-specific information, cybersecurity alerts and recommendations regarding configuration of cybersecurity tools to detect cyberattacks, where such information sharing:

(a) aims to prevent, detect, respond to or recover from incidents or to mitigate their impact;

(b) enhances the level of cybersecurity, in particular through raising awareness in relation to cyber threats, limiting or impeding the ability of such threats to spread, supporting a range of defensive capabilities, vulnerability remediation and disclosure, threat detection, containment and prevention techniques, mitigation strategies, or response and recovery stages or promoting collaborative cyber threat research between public and private entities.

SIMILAR CONTROLS

ISO 27001:2022
A.5.6 Contact with special interest groups
A.5.7 Threat intelligence

NIST 800-53 REV 5
PM-16 Threat Awareness Program
RA-10 Threat Hunting

REQUIREMENTS

- **Threat information sharing policy** — Defines organizational requirements for partnerships and collaboration that will result in access to maximal threat information.
- **Threat intelligence repository** — Documented, up-to-date repository of current cyber threats that is reflective of current trends and known exploits.

CONTROL NAME

29.4 Notification of participation

CONTROL DESCRIPTION

Member States shall ensure that essential and important entities notify the competent authorities of their participation in the cybersecurity information-sharing arrangements referred to in paragraph 2, upon entering into such arrangements, or, as applicable, of their withdrawal from such arrangements, once the withdrawal takes effect.

SIMILAR CONTROLS

ISO 27001:2022
A.5.6 Contact with special interest groups
A.5.7 Threat intelligence

NIST 800-53 REV 5
PM-16 Threat Awareness Program

REQUIREMENTS

- **Notification of participation in threat information sharing group** — Notification sent to competent authority with formal attestation to participation in threat information sharing with other relevant parties.