ChatGPT

# NIS2 Directive (Belgium) – CyberFundamentals Knowledge Base

## Introduction to NIS2 and Belgian Context

The **NIS2 Directive** is an EU-wide cybersecurity law that imposes obligations on organizations in key sectors to strengthen their cyber resilience [1]. It introduces requirements in four main areas: **risk management measures**, **corporate accountability**, **incident reporting**, and **business continuity** [2]. In Belgium, NIS2 has been transposed into national law ("la loi NIS2") as of mid-2024, with full enforcement by end of 2024 [3]. Crucially, the Belgian NIS2 law explicitly references the **CyberFundamentals Framework** as a baseline for the required security measures [4]. The CyberFundamentals framework, developed by the Centre for Cybersecurity Belgium (CCB), provides a comprehensive set of concrete cybersecurity controls aligned with NIS2 requirements [4] [5].

**Scope:** NIS2 applies to *essential* and *important entities* across 17 sectors (energy, transport, health, finance, digital infrastructure, public administration, etc.). Organizations should first determine if they fall in scope (based on sector and size criteria). If yes, they must implement **baseline cybersecurity measures** and meet governance and reporting obligations under NIS2 [6] [7]. Non-compliance can lead to fines and management liability [8].

**Core obligations:**
- **Risk Management Measures:** Entities must assess cyber risks and implement measures addressing at least ten domains (asset inventory, access control, incident handling, business continuity, supply chain security, etc.) [9] [10]. These measures should minimize cyber risks like incidents, data breaches, etc.
- **Top Management Accountability:** NIS2 places responsibility on management boards to **approve cybersecurity policies** and oversee their implementation. Management must also undergo cybersecurity training [11]. In Belgium, this means executives should be involved in risk assessments and allocation of resources for security. Failure by management can result in personal liability or temporary disbarment from roles [8].
- **Incident Reporting:** Organizations must have processes to detect and **report significant incidents**. NIS2 specifies strict timelines – an initial notification ("early warning") within **24 hours** of awareness of a significant incident, a more detailed incident report within **72 hours**, and a final report within one month [12]. These reports are made to the relevant CSIRT or authority and should include incident severity, impact, and remediation status.
- **Business Continuity & Recovery:** Entities need plans to ensure operations during and after cyber incidents [13]. This includes maintaining reliable **backups**, disaster recovery plans, and crisis management procedures to quickly recover and restore services after an attack.

The **CyberFundamentals Framework** is a practical tool to achieve NIS2 compliance in Belgium. It breaks down the broad NIS2 requirements into actionable controls and tasks. By obtaining a **CyberFundamentals certification/label** at the appropriate level, an organization can demonstrate it meets NIS2's baseline security measures. CCB defines four assurance levels in CyberFundamentals – **Small, Basic, Important,**

**Essential** – with each level adding more controls. The highest level, **Essential**, includes all prior measures and aligns with NIS2's full requirements [5] [14]. Most SMEs are encouraged to reach at least the Basic level, while NIS2 in Belgium effectively mandates the Essential level for in-scope entities [4] [15].

## Framework Overview: Core Functions and Levels

CyberFundamentals organizes security controls under the five NIST Cybersecurity Framework functions: **Identify, Protect, Detect, Respond, Recover** [16]. This structure helps cover all aspects of cybersecurity: from understanding what needs protection, to deploying safeguards, detecting incidents, responding to crises, and recovering operations. Below, the NIS2/CyberFundamentals requirements are listed by function, with their identifiers (mapping to NIST CSF categories) and a brief description. Under each requirement, we outline key **tasks** – concrete actions or controls – that an organization should implement. These tasks are the "deep dive" measures ensuring the requirement is met. (Each task can be marked by priority: in CyberFundamentals, tasks are categorized as *Low, Normal, High,* or *Critical* importance, corresponding to the Small→Essential level progression, though those labels are omitted here for brevity.)

**Note:** If any question is unclear or too broad, the chatbot should politely ask for clarification (e.g. *"Did you mean X or Y?"*) before drawing from this knowledge base. After answering a query, the chatbot can suggest relevant next steps or related topics to guide the user. (See the **Chatbot Interaction Guidelines** at the end.)

---

## Identify ➔ (Understanding the Organization)

*(Identify and manage assets, business environment, governance, risk, and supply chain.)*

- **ID.AM-1 – Inventory Physical Devices/Systems:** All physical devices and systems within the organization are identified and inventoried [17]. *Tasks:* Maintain an up-to-date register of hardware assets (computers, servers, network equipment, etc.), including asset owner, location, and criticality. Perform regular asset audits to ensure new devices are tracked and unauthorized devices are detected.
- **ID.AM-2 – Inventory Software Platforms/Applications:** All software platforms and applications in use are inventoried [18]. *Tasks:* Create and update an inventory of software (including OS, applications, services) with version info. Identify authorized software and detect unauthorized or outdated applications.
- **ID.AM-3 – Map Data Flows:** Organizational communication channels and data flows are mapped [19]. *Tasks:* Document data flow diagrams showing how data moves between systems, networks, and external parties. Identify key data inputs/outputs and ensure data flow maps are reviewed when systems change.
- **ID.AM-4 – Catalog External Information Systems:** External information systems (cloud services, third-party systems, etc.) are catalogued [20]. *Tasks:* Keep a list of external IT services in use, with details of the provider, purpose, and data involved. Ensure third-party systems are approved and meet security requirements.
- **ID.AM-5 – Prioritize Resources:** Resources are prioritized based on classification, criticality, and business value [21]. *Tasks:* Classify information assets (e.g. public, internal, confidential) and systems (critical vs. non-critical). Perform impact assessments to rank which systems/data are most vital to operations or pose highest risk, focusing security efforts accordingly.

- **ID.AM-6 – Define Security Roles & Responsibilities:** Cybersecurity roles, responsibilities, and authorities for the entire workforce and third-party stakeholders are established [22]. *Tasks:* Define and document security-related roles (e.g. CISO, IT admin, Data Protection Officer). Assign responsibilities for risk management, incident response, compliance, etc., including for vendors or partners as applicable. Communicate these responsibilities in job descriptions and security policies.
- **ID.BE-1 – Identify Role in Supply Chain:** The organization's role in the supply chain is identified and communicated [23]. *Tasks:* Determine your organization's position in critical infrastructure and sector supply chains (e.g. as a supplier, service provider, or end-user). Communicate to relevant staff and partners what critical services you rely on and provide, so that dependencies are understood.
- **ID.BE-2 – Identify Critical Sector & Infrastructure Dependencies:** The organization's place in critical infrastructure and its industry sector is identified and communicated [24]. *Tasks:* If applicable, confirm which nationally critical sector(s) you operate in. Identify any critical infrastructure or essential services your operations support. Share this context internally so personnel understand the importance of certain systems.
- **ID.BE-3 – Establish Mission Priorities:** Priorities for the organizational mission, objectives, and activities are established and communicated [25]. *Tasks:* Define what the most important business functions and objectives are (e.g. "ensure 24/7 availability of service X"). Communicate these priorities so that cybersecurity efforts can focus on protecting them.
- **ID.BE-4 – Identify Critical Services and Functions:** Dependencies and critical functions for delivery of critical services are established [26]. *Tasks:* Identify which business services are critical and what underlying functions or processes they depend on (e.g. key IT systems, facilities, personnel). Document these dependencies for business continuity planning.
- **ID.BE-5 – Establish Resilience Requirements:** Resilience requirements to support delivery of critical services are established for all operating states (normal, under attack, during recovery) [27]. *Tasks:* Define performance and availability requirements for critical services (e.g. maximum downtime or data loss). Set recovery time objectives (RTOs) and recovery point objectives (RPOs) and ensure plans meet these targets even under cyber-attack conditions.
- **ID.GV-1 – Establish Security Policies:** An organizational cybersecurity policy is established and communicated [28]. *Tasks:* Develop comprehensive information security policies approved by senior management [29]. Include roles and responsibilities, acceptable use rules, and security objectives. Make policies readily available to employees and provide training on them. Update policies annually or when major changes occur [30]. *(The policy should cover management commitment, coordination between departments, and integration with business processes [29].)*
- **ID.GV-3 – Understand Legal & Regulatory Requirements:** Legal and regulatory cybersecurity requirements (including data privacy and other obligations) are understood and managed [31]. *Tasks:* Identify all laws/regulations applicable (e.g. GDPR, sector-specific rules). Maintain compliance documentation (e.g. records of processing, regulatory filings). Monitor for updates to laws and adjust policies accordingly.
- **ID.GV-4 – Integrate Cyber into Risk Management:** Governance and enterprise risk management processes address cybersecurity risks [32]. *Tasks:* Include cyber risks in the corporate risk register. Regularly brief top management on cyber risk exposure. Ensure there is a governance forum or committee overseeing cybersecurity (e.g. risk steering group including IT and business leaders) so that cyber risk decisions align with business risk appetite.
- **ID.RA-1 – Identify Asset Vulnerabilities:** Asset vulnerabilities are identified and documented [33]. *Tasks:* Conduct vulnerability assessments on systems and software (e.g. vulnerability scanning, penetration testing). Keep a log of known vulnerabilities (and patches available) for each asset. Prioritize and remediate vulnerabilities based on risk (see PR.IP-12).

- **ID.RA-2 – Gather Threat Intelligence:** Cyber threat intelligence is received from information-sharing forums and sources [34]. *Tasks:* Subscribe to threat intel feeds or CERT alerts relevant to your sector. Participate in information-sharing communities (ISACs) if available. Continuously update your understanding of emerging threats (TTPs) and adjust defenses accordingly.
- **ID.RA-5 – Analyze Risks (Threats & Impacts):** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk [35]. *Tasks:* Perform periodic risk assessments combining asset vulnerabilities (technical weaknesses), threat scenarios, and potential business impacts. Use a risk scoring methodology to quantify risk levels. Document and review these risk assessment results with stakeholders.
- **ID.RA-6 – Identify Risk Responses:** Risk responses are identified and prioritized [36]. *Tasks:* Decide how to treat identified risks – e.g. mitigate (by implementing controls), transfer (insurance), accept, or avoid. Prioritize treatment of risks above the organization's risk tolerance. Create a risk treatment plan mapping specific controls (tasks) to each high risk.
- **ID.RM-1 – Establish Risk Management Program:** Risk management processes are established, managed, and agreed to by stakeholders [37]. *Tasks:* Implement a formal risk management program (policy, procedure). Engage leadership and relevant departments in the risk management process (so they buy into risk decisions). Ensure ongoing risk monitoring and reporting to stakeholders (e.g. regular risk reports to management).
- **ID.RM-2 – Determine Risk Tolerance:** Organizational risk tolerance is determined and clearly expressed [38]. *Tasks:* Define the organization's risk appetite/tolerance in qualitative or quantitative terms (e.g. "no more than X days downtime" or "no critical vulnerabilities unpatched beyond 1 month"). Document this in risk management policy and use it to guide which risks need immediate action.
- **ID.RM-3 – Contextualize Risk Tolerance:** The determination of risk tolerance is informed by the organization's role in critical infrastructure and sector-specific risk analysis [39]. *Tasks:* Adjust your risk tolerance based on external context – e.g. if you operate critical services, you may require a lower tolerance for downtime or data loss. Consider sector risk assessments or national risk scenarios when setting your thresholds.
- **ID.SC-1 – Manage Supply Chain Risks:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by stakeholders [40]. *Tasks:* Develop a **supply chain cybersecurity risk management plan**. This includes procedures to evaluate suppliers' security, incorporate security requirements into contracts, and monitor third-party risks. Get management approval for this plan since third-party disruptions can impact business [41] [42].
- **ID.SC-2 – Assess Suppliers and Partners:** Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a risk-based process [43]. *Tasks:* Keep an inventory of suppliers/partners (especially those with network or data access). For each, assess their criticality and perform due diligence (e.g. security questionnaires, audits, require compliance with standards). Prioritize deeper assessments for those supporting critical functions [44] [45].
- **ID.SC-3 – Secure Contracts with Suppliers:** Contracts with suppliers and partners are used to implement appropriate cybersecurity measures and supply chain risk controls [46]. *Tasks:* Update supplier contracts to include cybersecurity clauses (e.g. compliance with your security policy or standards, right to audit, breach notification requirements). Ensure contracts align with your Cyber Supply Chain Risk Management Plan (for example, requiring suppliers to have incident response plans) [47].
- **ID.SC-4 – Monitor Supplier Compliance:** Suppliers and third-party partners are routinely assessed via audits, test results, or other evaluations to confirm they meet their cybersecurity obligations [48]. *Tasks:* Conduct periodic reviews or audits of key suppliers. Obtain evidence of their security controls

(e.g. penetration test results, certifications, compliance reports). If issues are found, work with the supplier on corrective actions or consider alternate suppliers.

- **ID.SC-5 – Include Suppliers in Response/Recovery Planning:** Response and recovery planning and testing are conducted with suppliers and third-party providers [49]. *Tasks:* Involve critical suppliers in your incident response and business continuity exercises. For example, test how a cloud provider would support you during a cyber incident. Ensure contact information and escalation paths for third parties are in your incident plans. Coordinate disaster recovery tests that include key vendors.

## Protect ➔ (Implement Safeguards to Ensure Delivery of Services)

*(Protective measures for access control, data security, training, maintenance, etc.)*

- **PR.AC-1 – Manage Identities and Credentials:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes [50]. *Tasks:* Implement an **Identity and Access Management (IAM)** system. This includes unique user IDs, secure credential issuance (passwords, keys, badges), multi-factor authentication for critical systems, and a process to disable credentials when employees or devices are decommissioned. Regularly audit accounts and privileges to ensure only authorized, active accounts exist.
- **PR.AC-2 – Physical Access Control:** Physical access to assets (offices, data centers, critical systems) is managed and protected [51]. *Tasks:* Control entry to facilities with locks, access badges, or biometric controls. Maintain visitor logs. Server rooms or sensitive areas should have additional restrictions. Regularly review who has keys/badge access and revoke access promptly when not needed.
- **PR.AC-3 – Remote Access Management:** Remote access is managed [52]. *Tasks:* Enforce secure remote access solutions (VPNs with MFA, secure remote desktop). Maintain a list of users with remote access privileges and restrict remote connections to only necessary personnel/services. Monitor remote login attempts and apply strict network segmentation for remote connections.
- **PR.AC-4 – Least Privilege Access:** Access permissions and authorizations are managed, incorporating **least privilege** and **separation of duties** [53]. *Tasks:* Grant users only the minimum rights required for their job. Use role-based access control to group permissions logically. Implement separation of duties for critical functions (no single person has end-to-end control that could be abused). Perform periodic access reviews and remove or downgrade excessive permissions.
- **PR.AC-5 – Network Segregation:** Network integrity (network segregation, segmentation, etc.) is protected [54]. *Tasks:* Segment networks into security zones (e.g. isolate critical servers, use VLANs or firewalls to separate IT and OT networks). Implement internal network access controls so that compromise of one segment does not easily lead to others. Regularly review network architecture for any segmentation gaps.
- **PR.AC-6 – Identity Proofing:** Identities are **proofed** and bound to credentials and asserted in interactions [55]. *Tasks:* For user accounts, verify identity of individuals (e.g. new hires) before issuing credentials. For devices, ensure devices have unique identities (certificates or device IDs) tied to your asset inventory. Use strong authentication protocols to assert identities when users/devices connect (to prevent impersonation).

- **PR.AC-7 – Identity Assurance (Advanced):** Identities are proofed, bound to credentials, and asserted in interactions (advanced/continuous) [56]. *Tasks:* This appears similar to PR.AC-6, potentially emphasizing ongoing or higher-assurance identity management. Implement measures like digital

certificates or federation for identity trust. Continuously monitor authentication events for anomalies (possible credential compromise).

- **PR.AT-1 – Security Awareness for All Users:** All users are informed and trained [57]. *Tasks:* Implement a security awareness training program for all employees. Topics should include basic cyber hygiene (strong passwords, phishing email recognition, safe Internet use) [58]. Train new hires upon onboarding and conduct annual refresher training for all staff. Keep records of completed trainings.

- **PR.AT-2 – Training for Privileged Users:** Privileged users (administrators or users with elevated access) understand their roles and responsibilities [59]. *Tasks:* Provide specialized training for administrators and IT staff on secure configuration, incident response procedures, and their extra responsibilities in protecting systems. Emphasize adherence to change control, administrative account security, and monitoring.
- **PR.AT-3 – Third-Party Stakeholder Awareness:** Third-party stakeholders (suppliers, customers, partners) understand their roles and responsibilities [60]. *Tasks:* Where applicable, educate partners or suppliers about your security expectations. For example, if vendors connect to your network, ensure they are aware of and trained on your security policies/procedures. Include security requirements in contracts and provide guidelines to suppliers for handling your data securely.
- **PR.AT-4 – Executive Security Training:** Senior executives understand their roles and responsibilities [61]. *Tasks:* Provide cybersecurity briefings or training to senior management and board members [62] [63]. Cover topics like NIS2 obligations, leadership's accountability for cyber risk, incident crisis management, and decision-making during major incidents. Ensure executives know their duty to approve security measures and the potential liabilities for non-compliance [11].

- **PR.AT-5 – Security Personnel Training:** Physical security and cybersecurity personnel understand their roles and responsibilities [64]. *Tasks:* Ensure that dedicated security staff (both IT security and physical security teams) receive ongoing training relevant to their specialties (e.g. new attack techniques, new security technologies, incident response skills). Clarify coordination procedures between physical security and IT security during incidents (for example, a physical breach accompanying a cyber incident).

- **PR.DS-1 – Protect Data-at-Rest:** Data at rest is protected (through access controls, encryption, etc.) [65]. *Tasks:* Implement measures like encryption for sensitive data stored on disks, databases, or backups. Apply strict file permissions to data repositories. Use full-disk encryption on laptops and mobile devices. Store encryption keys securely and separate from the data.

- **PR.DS-2 – Protect Data-in-Transit:** Data in transit is protected (e.g. via encryption/tunneling) [66]. *Tasks:* Use strong cryptographic protocols (TLS, VPN) for transmitting sensitive information over networks. Ensure website and application interfaces enforce HTTPS/TLS. For internal networks, consider encryption for especially sensitive links (or network segmentation to protect data flows).
- **PR.DS-3 – Manage Asset Disposal:** Assets are formally managed throughout removal, transfers, and disposition [67]. *Tasks:* Have procedures for secure disposal of IT assets (wiping or destroying disks before discarding, shredding paper records). Track assets during transfer (e.g. if equipment is sent for repair, ensure data is secured). Maintain chain-of-custody documentation for decommissioned hardware containing sensitive data.

- **PR.DS-4 – Ensure Capacity for Availability:** Adequate capacity to ensure availability is maintained [68]. *Tasks:* Monitor and plan for capacity needs (bandwidth, compute, storage) so that critical services don't fail due to resource exhaustion (whether accidental or due to DoS attacks). Use scalability and redundancy (e.g. load balancers, failover systems) to handle peak loads or disruptions. Test that backup systems can handle required capacity during primary system outages.
- **PR.DS-5 – Prevent Data Leaks:** Protections against data leaks (data leakage prevention) are implemented [69]. *Tasks:* Deploy Data Loss Prevention (DLP) tools or measures to detect and block unauthorized transfer of sensitive information (e.g. via email or USB). Implement policies like disabling auto-forwarding of corporate emails to external accounts, blocking unapproved cloud file sharing, and scanning outgoing traffic for sensitive data patterns.
- **PR.DS-6 – Verify Software Integrity:** Integrity checking mechanisms are used to verify software, firmware, and information integrity [70]. *Tasks:* Use checksums, code signing, or digital signatures to ensure software/firmware has not been tampered with. For critical files and configurations, use file integrity monitoring tools to detect unauthorized changes. Validate updates via signed patches.
- **PR.DS-7 – Separate Environments:** The development and testing environments are separate from the production environment [71]. *Tasks:* Maintain strictly separate development/test systems with no direct connection to production data. Use dummy or anonymized data in testing. Implement access controls so developers/testers cannot inadvertently affect live production systems. This prevents untested code or malware in dev from impacting operations.

- **PR.DS-8 – Verify Hardware Integrity:** Integrity checking mechanisms are used to verify hardware integrity [72]. *Tasks:* For critical hardware (network devices, servers), use techniques to ensure they are genuine and unaltered (e.g. check hardware firmware for known-good versions, use hardware security modules). Inspect new equipment for signs of tampering. Maintain an inventory of hardware serial numbers and verify during maintenance that hardware hasn't been swapped maliciously.

- **PR.IP-1 – Secure Configuration Baselines:** A baseline configuration of IT/OT systems is created and maintained, incorporating security principles [73]. *Tasks:* Develop secure configuration standards for all systems (e.g. server baseline hardening guides, firewall rule baselines). Ensure new systems are configured according to these baseline settings (disable unnecessary services, enforce strong settings). Regularly review and update baselines as threats evolve.

- **PR.IP-2 – System Development Life Cycle:** A System Development Life Cycle (SDLC) to manage systems is implemented [74]. *Tasks:* Follow a formal SDLC for software and systems—from design to deployment and retirement—that embeds security at each stage. This includes security requirements in design, code review, security testing before production, and change management. Ensure updates and patches go through change control and testing.
- **PR.IP-3 – Change Control:** Configuration change control processes are in place [75]. *Tasks:* Implement a change management process for IT configurations. Require documentation, testing, and approval for significant changes to systems or network configs. Keep a log of changes and have a rollback plan in case a change causes issues. This prevents unauthorized or harmful changes that could introduce vulnerabilities.
- **PR.IP-4 – Backups and Restoration:** Backups of information are performed, maintained, and tested [76]. *Tasks:* Regularly back up critical data and system images. Store backups securely off-site or in cloud with appropriate encryption. **Test** restoration procedures periodically to ensure backups are usable (e.g. simulate restoring a server from backup). Keep backups updated to meet your recovery point objectives [77].

- **PR.IP-5 – Physical Environment Policies:** Policy and regulations regarding the physical operating environment for organizational assets are met [78] . *Tasks:* Ensure compliance with requirements for physical security, power, climate control, and other environmental factors in places where critical IT assets reside. For instance, maintain UPS and generator systems for power outages, ensure server rooms have fire suppression and cooling according to standards, etc.
- **PR.IP-6 – Data Destruction:** Data is destroyed according to policy [79] . *Tasks:* Establish a data retention and destruction policy. When data (or media containing data) reaches end-of-life or is no longer needed, destroy it securely (shredding, secure erase) as per policy. Maintain records of destruction for sensitive information to prove it has been rendered unrecoverable.
- **PR.IP-7 – Improve Protection Processes:** Protection processes are continuously improved [80] . *Tasks:* Regularly evaluate the effectiveness of existing security controls and processes. Use insights from incidents, testing, or audits to update policies and procedures [81] . For example, if a phishing test reveals weaknesses, strengthen email filtering and training. Establish a cycle for management review of security program performance and implement enhancements.
- **PR.IP-8 – Share Effectiveness of Security Technologies:** The effectiveness of protection technologies is shared (within or across communities) [82] . *Tasks:* Collect metrics on security control performance (e.g. blocked attacks, incident response times) and share appropriate information with stakeholders or industry peers. Participate in information-sharing groups to exchange what's working or not. For instance, if a new antivirus solution significantly reduced malware incidents, communicate that success story internally and consider sharing lessons learned with industry forums.
- **PR.IP-9 – Incident & Business Continuity Plans: Response plans** (incident response, business continuity) and **recovery plans** (disaster recovery) are in place and managed [83] . *Tasks:* Develop formal **Incident Response Plans** and **Business Continuity/Disaster Recovery Plans**. Include clear steps for different incident types, roles (incident response team members), communication flows, and external notification contacts [7] . Ensure these plans are approved by management and updated regularly. Train the response team and test these plans via drills or tabletop exercises.
- **PR.IP-11 – Cyber in HR Practices:** Cybersecurity is included in human resources practices (e.g. personnel screening, offboarding) [84] . *Tasks:* Integrate security into HR processes: background check employees (especially for sensitive roles) in accordance with law, include confidentiality and cybersecurity clauses in employment agreements, provide security training during onboarding (see PR.AT-1). Have strict offboarding procedures (revoke access, collect badges/devices immediately when staff leave) [85] [30] .

- **PR.IP-12 – Vulnerability Management Plan:** A vulnerability management plan is developed and implemented [86] . *Tasks:* Establish a documented plan for regularly scanning for vulnerabilities and patching systems. Define roles and timelines for applying critical patches (e.g. within 14 days). Include processes for handling zero-day vulnerabilities (temporary mitigations) and keep an exception log for any delayed patches, documented as accepted risks if necessary.

- **PR.MA-1 – Maintenance and Repair:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools [87] . *Tasks:* Only use authorized tools and personnel for system maintenance. Keep detailed logs of maintenance activities (what was done, by whom, when). For example, when servicing a server, use vetted software/firmware and ensure the maintenance session is monitored. Verify the integrity of systems after repairs (no unauthorized changes).

- **PR.MA-2 – Secure Remote Maintenance:** Remote maintenance of assets is approved, logged, and performed in a manner that prevents unauthorized access [88]. *Tasks:* If equipment is maintained remotely (by vendors or IT staff), enforce secure channels (VPN, one-time access credentials). Require scheduling and approval for remote maintenance sessions. Monitor these sessions in real-time if possible, and log all actions. Immediately revoke remote access after the maintenance window.

- **PR.PT-1 – Audit Logs:** Audit/log records are determined, documented, implemented, and reviewed in line with policies [89]. *Tasks:* Define which security events must be logged (login attempts, admin actions, etc.) and ensure systems are configured to produce those logs. Centralize log collection (e.g. SIEM system) and protect log integrity. Regularly review logs or automated alerts for signs of incidents. Retain logs for a period per policy to support investigations.

- **PR.PT-2 – Protect Removable Media:** Removable media is protected and its use restricted according to policy [90]. *Tasks:* Control the use of USB drives, external disks, etc. through policy (e.g. prohibit unencrypted USBs, or disable USB ports if possible). Encrypt data on any approved removable media. Train employees about risks of malware via USB. If removable media must be used, scan it for malware and keep an inventory if containing sensitive data.
- **PR.PT-3 – Least Functionality (Secure Config):** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities [91]. *Tasks:* Disable or remove all unnecessary software, services, and default accounts on systems. For example, turn off guest accounts, uninstall unused applications, turn off unused ports/services. This minimizes the attack surface. Use group policies or configuration management tools to enforce uniform hardened configurations.
- **PR.PT-4 – Secure Networks & Email (Filtering):** Communications and control networks are protected. Web and email filters are installed and used [92]. *Tasks:* Deploy network security controls like firewalls, intrusion prevention systems (IPS), and filtering solutions. Implement email security gateways to block spam, phishing emails, and malicious attachments. Use web proxy/filtering to block access to known malicious sites and content. Keep these protective technologies updated with the latest threat intelligence. *(This control is critical for preventing common attacks)* [93] [94].

## Detect ➔ (Activities to Identify Cyber Events)

*(Timely discovery of incidents through continuous monitoring and detection processes.)*

- **DE.AE-1 – Anomalies and Events: Establish Baselines:** *"A baseline of network operations and expected data flows for users and systems is established and managed."* [95] This means the organization defines what "normal" behavior looks like on its networks and systems, to help detect anomalies. **Tasks:** Establish normal baseline profiles for network traffic and system usage. For example, document typical data flow patterns and volumes between key systems and networks. Implement continuous logging and automated analysis of logs to detect deviations from the baseline (unexpected spikes, unusual connections) [96] [97]. Maintain up-to-date interface documentation (which systems connect to which) to know what traffic is expected [98]. Periodically review and adjust the baseline as the environment changes.
- **DE.AE-2 – Detect Anomalous Events:** *"Detected events are analyzed to understand attack targets and methods."* [99] This involves investigating alerts to determine if they represent security incidents. **Tasks:** When an alert or anomaly is detected (e.g. by an IDS or SIEM), analyze the event data to

identify what the target was and how the attack might be unfolding. Use automated log analysis tools to correlate events from multiple sources [100] . Have an incident analysis process (playbooks) for common event types. Tasks may include triaging the event severity, performing root-cause analysis, and documenting findings. Ensure **incident handling procedures** are in place to follow up on detected events [101] [102] . For example, if malware is detected on a host, analyze how it got there and what it did, to inform containment.

- **DE.AE-3 – Event Correlation:** *"Event data are collected and correlated from multiple sources and sensors."* [103] **Tasks:** Deploy multiple detection mechanisms (network-based sensors, host-based agents, log collectors) and aggregate their data. Use a SIEM or log management system to correlate events across these sources (e.g. link an IDS alert with a corresponding firewall log and endpoint alert) [104] . This improves detection accuracy and context. Key tasks include setting up centralized log collection (from servers, firewalls, IDS, etc.), normalizing log data, and creating correlation rules or use-cases to detect complex attack patterns.
- **DE.AE-4 – Determine Impact:** *"Impact of events is determined."* [105] When an event/incident is detected, the organization assesses the scope and potential damage. **Tasks:** Define criteria for impact levels (e.g. High – affecting critical systems or data loss, Low – minor isolated issue). During incident analysis, gather information on what systems/data were affected and estimate the operational, financial, or reputational impact. Have an incident severity matrix to consistently classify incidents. For example, a malware outbreak on 10 PCs might be medium impact, whereas ransomware on a server hosting critical data is high impact. This impact determination guides the response priorities and notifications (significant incidents may trigger NIS2 reporting to authorities).

- **DE.AE-5 – Establish Incident Alert Thresholds:** *"Incident alert thresholds are established."* [106] This means defining what kinds of events trigger alerts to the security team (and possibly to management). **Tasks:** Configure monitoring systems with thresholds and rules for alert generation – e.g. **failed login attempts** threshold that triggers an alert if exceeded, or an alert when a critical server goes offline. Define which conditions warrant immediate incident response versus just logging. Document these thresholds in the incident response plan and adjust them over time to balance sensitivity (avoiding too many false positives but ensuring serious events aren't missed).

- **DE.CM-1 – Network Monitoring:** *"The network is monitored to detect potential cybersecurity events."* [106] **Tasks:** Use network monitoring tools (IDS/IPS, traffic analyzers) to continuously watch for suspicious traffic patterns (port scans, data exfiltration, malware communications). Ensure key network segments are covered by monitoring sensors. Analyze network logs (flow data, firewall logs) for anomalies. For example, implement an Intrusion Detection System that generates alerts on known attack signatures or unusual traffic flows.

- **DE.CM-2 – Physical Environment Monitoring:** *"The physical environment is monitored to detect potential cybersecurity events."* [107] **Tasks:** Monitor physical security systems for signs of intrusions that could lead to cyber events (e.g. unauthorized entry into server room). Use cameras, access logs, motion sensors, etc., and integrate alerts (like a door forced open) into security operations. Ensure that physical breaches that could compromise IT (theft of hardware, unauthorized person near critical terminals) are treated as security incidents.
- **DE.CM-3 – Personnel Activity Monitoring:** *"Personnel activity is monitored to detect potential cybersecurity events."* [108] **Tasks:** Implement user activity monitoring especially for privileged users. This could include reviewing admin actions, using Data Loss Prevention (DLP) to catch employees emailing out large sensitive files, or analyzing work hours access (to spot suspicious use of

someone's credentials after hours). Insider threat detection programs and audit trails for user actions on critical systems help fulfill this.

- **DE.CM-4 – Malicious Code Detection:** *"Malicious code is detected."* [109] **Tasks:** Deploy anti-malware solutions on endpoints, servers, and at network gateways to detect viruses, ransomware, spyware, etc. Keep signature databases updated and leverage heuristic or behavior-based detection. Monitor for alerts of malware and take immediate action (isolate infected system, clean or reimage as needed). Incorporate threat intelligence to update detection rules for new malware strains.
- **DE.CM-5 – Unauthorized Mobile Code Detection:** *"Unauthorized mobile code is detected."* [110] **Tasks:** "Mobile code" refers to things like scripts, ActiveX controls, Java applets that execute on systems. Use security settings to restrict or prompt before running such code from untrusted sources (e.g. browser settings to control ActiveX, use whitelisting for allowed scripts). Deploy host-based intrusion prevention that can detect unauthorized code execution in memory. Monitor endpoints for indications of unauthorized scripts or macros (for instance, detect if an Office macro tries to spawn a shell).
- **DE.CM-6 – External Service Provider Monitoring:** *"External service provider activity is monitored to detect potential cybersecurity events."* [111] **Tasks:** If third-party providers have access to your systems or network (e.g. managed service providers, cloud admins), monitor their activity. This could mean reviewing logs of vendor remote access sessions, using privileged access management tools that record vendor actions, and setting up alerts for any unusual activity from vendor accounts. Essentially, treat external providers' accounts with the same (or higher) level of scrutiny as internal admin accounts.
- **DE.CM-7 – Monitoring for Unauthorized Access:** *"Monitoring for unauthorized personnel, connections, devices, and software is performed."* [112] **Tasks:** Implement continuous scanning to detect any unauthorized devices connected to the network (e.g. rogue Wi-Fi access points or unknown laptops). Use NAC (Network Access Control) to only allow known devices. Monitor for unauthorized software installation on endpoints via application whitelisting or EDR (Endpoint Detection & Response) tools. Also monitor physical premises for unauthorized personnel as noted, since that could lead to unauthorized devices being plugged in.

- **DE.CM-8 – Vulnerability Scans:** *"Vulnerability scans are performed."* [113] **Tasks:** Conduct automated vulnerability scans of systems and networks regularly (e.g. monthly or quarterly). Use reputable scanning tools to identify missing patches or insecure configurations. Make sure to scan all in-scope systems (including web applications, databases, network devices). Treat scanning results as input to your vulnerability management plan (see PR.IP-12) – i.e., remediate discovered vulnerabilities in a timely manner. Scans should also be done after significant changes and occasionally from an external perspective to find exposures.

- **DE.DP-2 – Compliance with Detection Requirements:** *"Detection activities comply with all applicable requirements."* [114] **Tasks:** Ensure your monitoring and detection processes themselves meet any legal or regulatory obligations. For instance, privacy laws might require informing employees of monitoring. Sector regulations might dictate specific logging (like financial services needing to log certain transactions). Document your compliance in this area – e.g., maintain logging policies that account for data protection (only security team accesses certain personal data in logs if justified).

- **DE.DP-3 – Test Detection Processes:** *"Detection processes are tested."* [115] **Tasks:** Regularly test your detection and monitoring systems to ensure they are effective. This can include **penetration testing** or red-team exercises to see if malicious activity is caught by your SOC, or simply simulating alerts to drill the incident response. Conduct exercises where you inject test events (like a fake malware

signature) to verify the SOC analysts or automated systems properly detect and escalate. Address any gaps discovered during these tests (tuning sensors, improving playbooks).

- **DE.DP-4 – Communication of Detection Information:** *"Event detection information is communicated."* [116] **Tasks:** Establish clear reporting channels for detected incidents. When an event is detected, ensure the right people are notified according to the incident severity (e.g. operations team for a minor outage, CISO and management for a serious breach). Set up automated alerting (emails, tickets, SMS) for critical events to on-call staff. Also, communicate detection trends and summary reports to leadership periodically (e.g. monthly security dashboard highlighting number of attacks detected and thwarted).
- **DE.DP-5 – Continuous Improvement of Detection:** *"Detection processes are continuously improved."* [117] **Tasks:** Just as with PR.IP-7 for protection, regularly review how well your detection program is performing and update it. After each incident or false alarm, hold a brief "lessons learned" session: Did we catch it early enough? Were there missed indicators? Update detection rules, thresholds, or processes accordingly. Keep up with evolving threats by adding new use cases to your SIEM or new monitoring tools if needed (for example, if attackers start using a new technique, adjust your sensors to detect that). Also consider user feedback – if certain alerts are consistently low-value, tune or eliminate them to reduce fatigue.

## Respond ➔ (Take Action Regarding a Detected Cybersecurity Incident)

*(Contain and mitigate incidents, communicate as needed, and improve response processes.)*

- **RS.RP-1 – Execute Response Plan:** *"Response plan is executed during or after a cybersecurity incident."* [118] [119] When an incident occurs, the organization's incident response plan is put into action without delay. **Tasks:** Activate the incident response team and follow the steps in the IR plan (e.g. identification, containment, eradication, recovery, lessons learned). Ensure that roles (incident lead, comms lead, etc.) carry out their assigned tasks. Use checklists from the plan so nothing is overlooked (like preserving evidence or notifying stakeholders). If an incident exceeds a certain threshold (significant incident), trigger required notifications (regulators per NIS2, customers if personal data involved per GDPR, etc.).
- **RS.CO-1 – Coordinate Personnel During Response:** *"Personnel know their roles and order of operations when a response is needed."* [120] **Tasks:** Train staff on the incident response **procedures** so that in a crisis everyone knows what to do. For example, IT ops knows to collect system images for forensics, communications team knows to prepare holding statements for media, management knows how to make key decisions. Conduct incident response drills to reinforce this. This requirement emphasizes having a well-orchestrated response where each team member's responsibilities are clear to avoid chaos during an incident.
- **RS.CO-2 – Incident Reporting Criteria:** *"Incidents are reported consistent with established criteria."* [121] **Tasks:** Define what constitutes a notifiable incident (both internally and externally). For internal reporting: ensure employees report any suspected incident to the security team immediately (establish an internal reporting channel). For external: determine triggers for reporting to authorities (e.g. incidents meeting NIS2 "significant" criteria) and ensure reports are made within required timelines (24h/72h as discussed). Keep templates ready for incident notification to streamline this process.
- **RS.CO-3 – Information Sharing in Response:** *"Information is shared consistent with response plans."* [122] **Tasks:** During incident response, share information with internal and external

stakeholders as planned. Internally, that means keeping management and affected business units updated. Externally, it could mean sharing indicators of compromise with other companies or CERTs to help broader community defense. Ensure any **public communication** is coordinated (so as not to release unapproved info). Essentially, follow the communication part of your incident response plan regarding who to inform and when [7].

- **RS.CO-4 – Coordinate with Stakeholders:** *"Coordination with stakeholders occurs consistent with response plans."* [123] **Tasks:** Involve relevant stakeholders in response actions according to your plan. For example, if a cloud service is impacted, coordinate with that provider's support. If customer data is compromised, coordinate with customer support or legal teams on notifying customers. Ensure legal, PR, HR, or other departments are pulled in as needed (for instance, HR if an insider is suspected, or PR for managing external communications). Document these coordination steps in the plan and practice them in simulations.

- **RS.CO-5 – Voluntary External Information Sharing:** *"Voluntary information sharing occurs with external stakeholders to achieve broader situational awareness."* [124] **Tasks:** As part of responding, consider sharing anonymized incident details or threat information with industry peers or information-sharing forums (as long as it's safe and legal to do so). This can help others be aware of ongoing threats (for example, sharing that a specific malware is targeting companies in your sector). Also maintain relationships with external incident response organizations or CERTs; sharing info can help you receive help or additional intel.

- **RS.AN-1 – Analysis: Investigate Notifications:** *"Notifications from detection systems are investigated."* [125] [126] **Tasks:** Ensure that every security alert or notification received (from SIEM, IDS, anti-virus, etc.) is promptly analyzed by the security team. Develop triage procedures to validate whether an alert is a true incident or a false positive. Document the outcome of each investigation. For significant alerts, perform deeper forensic analysis (see RS.AN-3). Use a trouble-ticket system to track investigations. This requirement is basically making sure alerts are not ignored – they must feed into an analytic process by responders.

- **RS.AN-2 – Understand Incident Impact:** *"The impact of the incident is understood."* [127] **Tasks:** As part of incident analysis, determine what the incident has affected and how badly. Identify all systems, data, and business processes impacted. For example, in a ransomware attack, ascertain which servers and files are encrypted and what business operations are disrupted. Update the impact assessment as more information becomes available. Communicate this impact assessment to decision-makers to inform the response (e.g. whether to failover systems, declare disaster recovery, etc.).
- **RS.AN-3 – Perform Forensic Analysis:** *"Forensics are performed."* [128] **Tasks:** If an incident is confirmed, carry out forensic analysis to understand the attack and prevent recurrence. This includes collecting and preserving evidence (disk images, memory dumps, log files), analyzing malware or tools used by the attacker, and determining the root cause and timeline of the incident. Use specialized tools or external forensic experts if needed. The goal is to learn exactly how the intrusion happened and what the adversary did, which will feed into recovery and improvement.
- **RS.AN-4 – Incident Classification:** *"Incidents are categorized consistent with response plans."* [129] **Tasks:** Classify each incident into a category or severity level as defined in your incident response plan. For instance, categories might be "Malware Infection," "Unauthorized Access," "Denial of Service," etc., and severity could be low/medium/high. Ensure responders label the incident accordingly early in the process, as this can trigger certain actions (like high-severity incidents

notifying top management and regulators). Use consistent criteria so that everyone speaks the same language about the incident's nature and urgency.

- **RS.AN-5 – Vulnerability Disclosure Response:** *"Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization (from internal or external sources)."* [130] **Tasks:** Set up a **vulnerability disclosure** or intake process. This could include a public-facing channel (like a security@ email or web form) for external researchers to report vulnerabilities in your products or infrastructure. Internally, encourage employees to report security issues they discover. Have a procedure to acknowledge such reports, quickly analyze the reported vulnerability, and take mitigation action or patch development as needed. Also, coordinate with the reporter for public disclosure if applicable. (This aligns with having a **vulnerability management** and bug-bounty process, ensuring you don't ignore reports of weaknesses.)

- **RS.MI-1 – Contain Incidents:** *"Incidents are contained."* [131] **Tasks:** Upon detection of an active threat, take immediate actions to **contain** it and limit damage. This can include isolating affected systems (e.g. remove from network), blocking malicious IP addresses or accounts, applying temporary firewall rules, etc. For example, if malware is spreading, promptly segment or shut down parts of the network to stop propagation. Follow predefined containment strategies in your IR plan for different incident types.

- **RS.MI-2 – Mitigate Incidents:** *"Incidents are mitigated."* [132] **Tasks:** After containment, work on **eradication** of the threat and mitigation of vulnerabilities that allowed it. This could mean removing malware from systems, applying patches to fix exploited flaws, strengthening security controls to prevent similar attacks. Ensure that backups are clean before restoring. Mitigation may also involve short-term fixes (e.g. disabling a vulnerable service) until a permanent solution is in place. Document all mitigation steps taken.
- **RS.MI-3 – Address Newly Identified Vulnerabilities:** *"Newly identified vulnerabilities are mitigated or documented as accepted risks."* [133] **Tasks:** During or after incidents, you often uncover new vulnerabilities (for instance, a misconfiguration exploited by an attacker). This requirement ensures you either fix those promptly or formally accept the risk if it cannot be fixed immediately. Create a remediation plan for each newfound vulnerability (patch, configuration change, upgrade). If a decision is made to accept a risk (perhaps due to business constraints), document the rationale and obtain management sign-off. Integrate these discoveries into the **vulnerability management plan** (PR.IP-12) and continuously improve your security posture.

## Recover ➔ (Restore Normal Operations After an Incident)

*(Recovery planning, improvements, and coordination after a cybersecurity incident.)*

- **RC.RP-1 – Execute Recovery Plans:** *"Recovery plan is executed during or after a cybersecurity incident."* [118] [119] After an incident has been contained and mitigated, activate your **recovery plans** to restore systems and return to normal operations. **Tasks:** Follow the Disaster Recovery (DR) procedures: restore data from backups, rebuild systems, re-establish network connectivity, etc., in a prioritized order (most critical services first). Communicate status to stakeholders (internal and external) as you recover services. Verify systems are fully functional and not compromised before returning them to production. Continue business continuity measures (manual workarounds,

alternate processes) until IT systems are back. Keep management informed of progress and any resources needed for recovery.

- **RC.IM-1 – Incorporate Lessons Learned:** *"Recovery plans incorporate lessons learned."* [134] **Tasks:** After an incident, review how the recovery went and update your Business Continuity and Disaster Recovery plans with any lessons learned. If you found that certain systems weren't prioritized correctly, or a backup process failed, adjust the plans. Also integrate technical lessons: e.g., if a particular failover mechanism didn't work as expected, fix it and note it in the plan. Essentially, improve your recovery strategies based on real-world experience so you're better prepared next time.
- **RC.IM-2 – Update Recovery Strategies:** *"Recovery strategies are updated."* [135] **Tasks:** Similar to RC.IM-1, ensure the overarching recovery strategies (not just the detailed plans) are kept current. For example, if your business adopts a new critical cloud service, your recovery strategy must account for a contingency if that service fails. Regularly (at least annually) review the recovery architecture – are the backup sites, redundancy, and failover technologies still sufficient given changes in the business or threat landscape? Update strategies to possibly include newer solutions (like cloud disaster recovery services, more frequent backups, etc.).
- **RC.CO-1 – Public Relations Management:** *"Public relations are managed."* [136] **Tasks:** After a significant incident, managing public perception and communication is crucial. Work with PR or communications teams as part of the recovery to issue public statements if needed (especially if customers or the public are aware of the incident). Ensure messaging is transparent but controlled – acknowledge the issue, what is being done, and any support for affected parties. Good PR management can help repair reputation damage. This task may include preparing media talking points, handling press inquiries, and communicating on social media if appropriate.
- **RC.CO-2 – Repair Reputation:** *"Reputation is repaired after an incident."* [137] **Tasks:** Beyond the immediate PR, take longer-term actions to rebuild trust with clients, partners, and the public. This could involve offering support to affected customers (credit monitoring if data was leaked, for example), undergoing independent security audits and sharing those results, or achieving certifications to demonstrate improved security. It may also include marketing or outreach highlighting the improvements made post-incident. The goal is to show stakeholders that the incident was taken seriously and the organization's security posture is now stronger.
- **RC.CO-3 – Communicate Recovery Activities:** *"Recovery activities are communicated to internal and external stakeholders as well as executive and management teams."* [138] **Tasks:** During the recovery phase, regularly inform all relevant parties about the status. Internally, brief executives and employees on what has been restored and what remains to be done. Externally, if customers or regulators were notified of the incident, update them when services are restored or when the incident is fully resolved. Provide a summary report to management detailing the incident, response, and recovery actions taken. This transparency ensures everyone knows when operations are back to normal and any follow-up steps.

---

## Chatbot Interaction Guidelines (For Internal Use)

To provide the best assistance using the above knowledge base, the AI chatbot should follow these interaction practices:

- **Clarify Unclear Questions:** If the user's question is ambiguous or overly broad, ask a polite clarifying question before answering. For example: *"I want info on NIS2"* could mean compliance

requirements or scope or deadlines – so the bot might respond: *"Sure. To make sure I help you best, did you mean the general requirements of NIS2, or whether your organization falls under it?"*. This helps pinpoint the actual user need.

- **Disambiguate Multi-Part Queries:** If the user's request could refer to multiple distinct topics, the bot should break down the interpretation and ask the user to choose. For instance, *"Tell me about incident reporting"* might refer to internal incident processes *or* regulatory notifications. The bot can list the possible contexts: *"Did you want to know about how to internally report incidents within NIS2 compliance, or the external notification timelines to authorities?"*. Providing these options helps the user clarify their intent.

- **Confirm Understanding by Paraphrasing:** The bot can rephrase the user's question in its own words and ask for confirmation. E.g. *"Just to confirm, you're asking what cybersecurity measures a small business in Belgium needs to implement to comply with NIS2, is that right?"*. This "**Did you mean…**" approach ensures the bot's interpretation is correct before proceeding to give an answer from the knowledge base.

- **Suggest Next Steps:** After answering a query, the chatbot should be proactive in guiding the user on what to do next. For example, if a user asks about compliance gaps, after addressing the question the bot might add: *"Next steps: you might consider conducting a CyberFundamentals self-assessment to identify your gaps. I can provide information on how to do that if you're interested."*. If a user learns about one aspect (say incident reporting), the bot can suggest related topics (like *"Would you like to know about how to prepare an incident response plan as well?"*). This keeps the user engaged and supports them in a practical, action-oriented way.

By following these guidelines, the chatbot will ensure the user's questions are fully understood and addressed with accurate, context-relevant information from the NIS2/CyberFundamentals knowledge base, while also maintaining a helpful conversational flow. [4] [11]

---

[1] [2] [6] [7] [8] [9] [10] [11] [13] [58] [77] [81] NIS2 Requirements | 10 Minimum Measures to Address
https://nis2directive.eu/nis2-requirements/

[3] [15] [16] NIS2 & the Belgian CyberFundamentals ⋆ Brand Compliance
https://brandcompliance.com/en/docs/cyberfundamentals-nis2/

[4] (Product update) CyberFundamentals framework | Academy | Cyberday.ai
https://www.cyberday.ai/product-development/frameworks-cyberfundamentals-finalizations

[5] CyberFundamentals | Cyberday content library
https://www.cyberday.ai/frameworks/cyberfundamentals-belgium

[12] What is the NIS2 Directive? | Cybersecurity Regulations - Darktrace
https://www.darktrace.com/es/cyber-ai-glossary/nis2-directive

[14] CyberFundamentals Framework | CCB Safeonweb
http://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework

17 18 19 20 21 22 23 106 107 108 109 110 111 112 113 114 115 116 117 CyberFundamentals | Digiturvamallin sisältökirjasto
https://www.digiturvamalli.fi/vaatimuskehikot/cyberfundamentals-belgia

24 25 26 27 28 31 32 33 34 35 36 37 38 39 40 43 46 48 49 50 51 52 53 54 CyberFundamentals | Digiturvamallin sisältökirjasto
https://www.digiturvamalli.fi/vaatimuskehikot/cyberfundamentals-belgia?26e7756e_page=2

29 30 85 CyberFundamentals | ID.GV-1 | Organizational cybersecurity policy is established and communicated.
https://www.cyberday.ai/requirement/cyberfundamentals-id-gv-1-organizational-cybersecurity-policy-is-established-and-communicated

41 42 44 45 47 Supply chain cyber security risk management | Cyberday content library
https://www.cyberday.ai/library/supply-chain-cyber-security-risk-management?e1bc3a9a_page=2

55 56 57 59 60 61 64 65 66 67 68 69 70 71 72 73 74 75 76 78 79 80 84 86 CyberFundamentals | Digiturvamallin sisältökirjasto
https://www.digiturvamalli.fi/vaatimuskehikot/cyberfundamentals-belgia?26e7756e_page=3

62 NIS2: A Game-Changer for Senior Management and Boards
https://www.williamfry.com/knowledge/nis2-a-game-changer-for-senior-management-and-boards/

63 [PDF] CYBERSECURITY ROLES AND SKILLS FOR NIS2 ESSENTIAL ...
https://www.enisa.europa.eu/sites/default/files/2025-06/Mapping%20NIS%202%20obligations%20with%20ECSF%20role%20profiles.pdf

82 83 87 88 89 90 91 92 118 120 121 122 123 124 125 126 127 128 129 130 134 135 136 137 138 CyberFundamentals | Digiturvamallin sisältökirjasto
https://www.digiturvamalli.fi/vaatimuskehikot/cyberfundamentals-belgia?26e7756e_page=4

93 94 95 96 97 98 99 100 101 102 103 104 105 CyberFundamentals | Get compliant with Cyberday
https://www.cyberday.ai/frameworks/cyberfundamentals-belgium?3812fa91_page=3

119 131 132 133 CyberFundamentals | Digiturvamallin sisältökirjasto
https://www.digiturvamalli.fi/vaatimuskehikot/cyberfundamentals-belgia?26e7756e_page=5