Cybersecurity Maturity Report

Created by CyberResilient for , 2025-12-09 14:56

This security assessment has been generated by CyberResilient – an AI-driven platform developed with support from NCC-SE and the Swedish Civil Contingencies Agency (MSB).

Total Cybersecurity Maturity Level **29%**

Executive Summary

The organisation's overall cybersecurity maturity is assessed as **29/100**, a **very low** position relative to expected capabilities under the *NIS2* Directive. This composite score reflects multiple categories that are at planning stages or not implemented, indicating limited operational readiness to meet NIS2 governance, reporting and resilience obligations.

Key strengths are narrow but meaningful: a largely complete central asset register provides baseline visibility, patch management and backup processes are reported as largely implemented, and several personnel controls (disciplinary measures and confidentiality agreements) are functioning. However these strengths are outweighed by critical gaps: governance and an operational **ISMS** are not implemented (governance score: **13/100**); incident management and external reporting are effectively absent (incident score: **15/100**); training and awareness is minimal (training score: **8/100**); continuity and crisis capabilities are not in place (continuity score: **13/100**); and supply chain security is critically weak (supply chain score: **10/100**). Information protection shows low maturity (**42/100**) with important control gaps such as MFA, secure procurement and complete access control processes. Risk management is partial and inconsistent (**31/100**), and there is no evidence of independent reviews or a testing regime for controls.

Several areas lack documented evidence required by NIS2 — for example, formal offboarding processes, timely regulatory reporting procedures, a maintained supplier registry and records of regular testing or independent audits. The current posture

exposes the organisation to regulatory non compliance, prolonged operational disruption and unmanaged third party risk. Immediate attention is required to close governance, incident response, continuity and supplier risk deficiencies.

Strategically, the priority must be to secure senior commitment, assign accountable owners and resource a concise delivery roadmap that addresses the highest compliance and operational risks first. Establishing a documented ISMS and formal risk management framework, operationalising incident reporting and internal communications, completing asset classification, and delivering mandatory baseline training are the most urgent steps to create a foundation for sustained improvement and to demonstrate intent to regulators under NIS2.

Table of Contents

Governance 13%

Observations

• The overall governance maturity for information security is **very low**, reflected by the composite score of **13/100**, with the ISMS only at a **planned** stage and management reporting **not implemented**.

• There is evidence that planning for an **information security management system (ISMS)** has begun, but there is no indication that a scope, timeline, accountable owner or secured resources have been formalised and communicated.

• The absence of a continuous, documented reporting process to management represents a significant oversight: **management visibility and decision-making** on cyber risk is currently unsupported, which is inconsistent with NIS2 expectations for governance and oversight.

• Key governance elements are missing or unreported, including **defined roles and responsibilities**, a documented review cycle for policies and compliance, and evidence of integration between risk assessment outputs and management reporting.

Recommendations:

HIGH PRIORITY

Establish and Implement an ISMS

Begin by formally establishing an **Information Security Management System (ISMS)** that is documented, resourced and communicated across the organisation. The ISMS should set the policy framework, define scope, align to business objectives and provide the foundation for consistent risk treatment and control implementation.

Implementing an ISMS demonstrates compliance intent with NIS2 governance requirements and provides a structured approach to identify, assess and manage cybersecurity risks. A clear, time-bound implementation plan reduces the risk of fragmented or ad-hoc security measures and enables measurable progress.

- Define and document the ISMS **scope** (business processes, services, assets and locations) within 4–6 weeks
- Appoint an accountable owner (e.g. **CISO** or senior information security lead) and a small implementation team
- Develop an ISMS policy suite that maps directly to NIS2 requirements and organisational objectives
- Create an implementation roadmap with milestones, resource estimates and a target date for initial operation
- Communicate the ISMS scope, objectives and governance structure to senior management and relevant staff

HIGH PRIORITY

Implement Continuous Management Reporting

Design and deploy a simple, repeatable management reporting process to provide regular, documented updates on the status of information security activities. Reports should be tailored to the audience (management bodies vs operational teams) and include key indicators that enable oversight and informed decisions.

Regular reporting closes the visibility gap identified in the assessment and ensures that the management body receives the information necessary to meet NIS2 obligations, including oversight of policy compliance, risk posture and significant incidents.

- Develop a concise reporting template covering **incidents, risk status, patching/maintenance, compliance metrics** and outstanding remediation actions
- Define reporting cadence (e.g. monthly operational, quarterly board-level) and required attendees/recipients
- Assign a report owner responsible for data collection, validation and timely distribution
- Include escalation criteria for significant incidents or trends that require immediate executive attention
- Pilot the report for two cycles and adjust content based on management feedback

MEDIUM PRIORITY

Define Roles, Responsibilities and Secure Resources

Ensure accountability by defining and documenting clear roles and responsibilities for information security across the organisation. This includes identifying the management body responsibilities, the ISMS owner, process owners and operational teams.

Securing appropriate resources — people, budget and tools — is essential to move from planning to implementation and to sustain ongoing governance activities.

- Create a RACI matrix that maps security responsibilities to specific roles (including the management body) for core ISMS processes
- Formally appoint an ISMS owner (e.g. **CISO**) with delegated authority and define their objectives
- Estimate and obtain a baseline budget for ISMS implementation and early operations
- Define required competencies and schedule targeted training for accountable personnel

MEDIUM PRIORITY

Establish Compliance Monitoring and Review Cycles

Introduce an ongoing compliance monitoring and policy review process to measure adherence to the ISMS and topic-specific policies. Ensure that results of assessments and independent reviews are documented and fed back into risk assessments and management reporting.

A defined review cycle and compliance reporting process will help demonstrate to regulators and senior management that controls are effective and that corrective actions are tracked to closure.

- Define a compliance monitoring plan with scope, frequency and acceptance criteria for policy and control checks
- Schedule regular management reviews of ISMS performance and policy updates (e.g. annual or after significant incidents)
- Document results of audits and reviews, and integrate findings into the risk register and remediation plans
- Implement a simple compliance dashboard to feed management reports with objective evidence

Risk Management 31%

Observations

- The overall maturity for **Risk Management** is assessed at **31/100**, which denotes significant gaps in the formalisation and execution of core risk processes.
- The organisation has only a **planned** risk management methodology and has not yet established a fully implemented, documented framework that defines roles, responsibilities and procedures.
- Risk reporting to risk owners and top management is **ongoing** but appears inconsistent and ad hoc rather than driven by a documented cadence and standardised reporting content.
- There is **no implemented** comprehensive threat (environmental) assessment, while the network and information systems risk analysis is reported as **ongoing**, indicating partial coverage but incomplete risk treatment and documentation.

Recommendations:

HIGH PRIORITY

Adopt and formalise a risk management framework

Establish a documented, organisation-wide **risk management framework** that defines the methodology for identification, analysis, evaluation, treatment and monitoring of cybersecurity risks. The framework should explicitly assign roles and responsibilities (including risk owners) and specify interfaces between IT, security and business units.

Formalising the framework will create the foundation required by NIS2 and enable consistent decision-making, traceability of risk treatment and measurable improvement over time.

- Document and approve a risk management framework aligned to the organisation's size, structure and threat landscape
- Define and publish roles and responsibilities for **risk owners**, business units and the security function
- Adopt a standard risk taxonomy and scoring model (likelihood, impact, risk rating) for consistent assessments
- Approve the framework at executive or board level and make it a mandatory part of policy documentation

HIGH PRIORITY

Implement regular risk reporting and governance cadence

Introduce a formal reporting cadence that delivers risk assessment results, risk treatment status and key risk indicators to **risk owners** and **top management** on a scheduled basis (for example, quarterly), and after significant changes or incidents.

This strengthens governance, ensures senior awareness and supports the requirement to regularly review compliance with security policies and the effectiveness of measures.

- Define a reporting template covering risk ratings, treatment plans, progress, residual risk and obstacles
- Schedule recurring risk reporting (e.g. quarterly) to the management board and ad-hoc reports for critical changes
- Assign responsibility for producing and validating reports (e.g. Chief Risk Officer or Head of Security)
- Integrate report outputs into decision-making processes (budget, resource allocation, project prioritisation)

HIGH PRIORITY

Establish a comprehensive threat and environmental assessment process

Develop and operationalise a process to collect, analyse and report **threat intelligence** and environmental factors relevant to the organisation. The process should identify credible external and internal threats, trends and threat actor activity and produce a concise report for senior management.

Regular threat assessments enable prioritisation of controls, inform testing and remediation activities, and demonstrate alignment with NIS2 obligations to monitor the threat landscape and technical vulnerabilities.

- Identify reliable threat sources (CERTs, sector ISACs, commercial feeds, open-source intelligence)
- Create a simple, repeatable threat assessment template for management-level reporting
- Schedule periodic threat assessments (e.g. monthly operational summaries; quarterly executive briefings)
- Map identified threats to critical assets and update the risk register with threat-driven risk scenarios

MEDIUM PRIORITY

Complete and document the network & information systems risk analysis and treatment plan

Finalise the ongoing risk analysis for network and information systems so that all identified vulnerabilities, exposures and dependencies are documented, rated and assigned treatment actions. The output should be a clear remediation plan with timelines, owners and acceptance criteria.

Documented results and an actionable treatment plan are necessary to support business continuity, security testing and segmentation decisions, and to meet NIS2 expectations on risk-informed security measures.

- Complete the outstanding threat and vulnerability mapping for network and information systems
- Produce a consolidated risk register entry per asset/system including residual risk after proposed treatment
- Define and schedule remediation activities (patching, segmentation, access controls) with owners and deadlines
- Conduct periodic reviews to confirm remediation progress and update the register when changes occur

MEDIUM PRIORITY

Build capability through resourcing, training and continuous assurance

Allocate resources and provide targeted training to the teams responsible for risk management activities. Implement continuous assurance activities (compliance monitoring, independent reviews and measurement) so that the effectiveness of the risk-management lifecycle is assessed and improved.

Strengthening capability reduces reliance on ad hoc work, increases institutional knowledge and supports sustainable compliance with NIS2 reporting and review obligations.

- Assign or recruit dedicated personnel for risk management and threat intelligence functions
- Provide role-specific training on the adopted risk methodology and NIS2 requirements for key staff and risk owners
- Establish periodic independent reviews or compliance checks and document the results for management
- Implement tooling or dashboards to monitor risk metrics and track remediation status continuously

Asset Management 50%

Observations

- The organisation maintains a **central register** of information assets that is largely complete and mapped to core operational services, reflecting a reasonable baseline for asset visibility.
- There is **no completed classification** of information assets; classification activity is currently planned but not executed, leaving asset criticality and sensitivity unconfirmed.
- Key inventory attributes required by NIS2 (for example, unique identifiers, owners/custodians, physical locations and explicit classification levels) appear to be **partially captured** or not yet consistently documented.
- The current state suggests a risk of **inconsistent application of security controls** because asset classification and formal assignment of owners/custodians are incomplete, limiting the organisation's ability to align protection measures to asset criticality.

Recommendations:

HIGH PRIORITY

Implement an operational asset classification scheme

Completing and operationalising an **asset classification scheme** is essential to meet NIS2 requirements and to ensure security controls are applied proportionately to asset criticality and sensitivity.

Classification should be documented, repeatable and backed by clear criteria so that each asset in the register has an assigned protection level that drives technical and organisational controls.

- **Appoint accountable owners** for the classification programme and assign custodians for asset categories.
- **Define a classification matrix** with levels (e.g. public, internal, confidential, restricted) and explicit criteria for each level.
- **Apply the classification** to the existing asset register, recording the classification value as a mandatory attribute for each asset entry.
- **Map required security controls** to each classification level and update control implementation plans accordingly.
- **Document and publish** the classification policy and procedures for ongoing use and auditability.

MEDIUM PRIORITY

Formalise and maintain the central asset register

The central register is a strong foundation but requires formal processes to ensure accuracy, integrity and appropriate access controls. Regular maintenance is necessary to prevent drift between documented assets and the live estate.

Bringing the register under consistent lifecycle management will improve incident response, change management and regulatory reporting capabilities.

- **Establish a change-control process** to update the register whenever assets are introduced, modified or retired.
- **Ensure mandatory attributes** are recorded for each asset (unique identifier, type/description, owner/custodian, physical/logical location, classification).
- **Restrict and log access** to the register so only authorised personnel can modify entries and all changes are auditable.
- **Integrate the register** with CMDB, ITSM and security tooling where feasible to reduce manual effort and improve accuracy.
- **Schedule periodic reviews** (for example quarterly) to reconcile the register against production systems and estate discovery scans.

MEDIUM PRIORITY

Embed asset ownership and align assets with risk management

Assigning clear ownership and integrating assets into the organisation's risk management processes will ensure accountability for protection decisions and that resources are prioritised effectively.

Linking asset data to business processes and threat modelling enables evidence-based selection of controls and demonstrates compliance with NIS2 expectations for asset-based risk treatment.

- **Assign owners and custodians** for all critical assets and record their contact details in the register.
- **Incorporate asset data** into the organisation's risk register and conduct risk assessments that reference asset classification and business impact.
- **Use asset classification** to prioritise remediation, patching and monitoring activities within operational procedures.
- **Include asset update and ownership checks** in change management and procurement workflows to maintain governance over time.

Training and Security Awareness 8%

Observations

- The overall maturity for **Training and Security Awareness** is very low, with a composite score of **8/100**, indicating material gaps against NIS2 expectations.
- There is a **planned** training plan for employees and top management, but it appears incomplete and not yet implemented beyond planning stage.
- No regular cybersecurity training is currently delivered to the general employee population, creating an immediate operational and compliance risk.
- Board and senior management have **no regular training** in place, which risks inadequate strategic oversight and failure to meet NIS2 role-specific awareness obligations.

Recommendations:

HIGH PRIORITY

Establish a formal, risk based training strategy

Develop a documented, organisation wide training strategy that is explicitly **aligned to the results of your risk assessment** and the NIS2 requirements. The strategy should define scope, target audiences, roles and responsibilities, delivery methods and success metrics.

This approach ensures training is not generic but *role specific* and proportionate to the risks identified across operational units. A formal strategy also creates the basis for governance, budget allocation and measurable improvement.

- **Document the training strategy** that maps training needs to risk assessment outcomes and NIS2 obligations.
- **Identify and classify roles** (e.g. operational staff, IT, OT, executives) and define required competency levels for each.
- **Assign ownership** for the training programme to a specific function (e.g. CISO, HR or a joint governance board).
- **Set measurable objectives** (completion rates, assessment scores, phishing click rates) and reporting cadence.

HIGH PRIORITY

Deploy a mandatory baseline cybersecurity course for all employees

Introduce a compulsory, baseline cybersecurity awareness course for all personnel covering cyber hygiene, phishing, credential security and the organisation's reporting mechanisms. Ensure the content is practical, concise and linked to day to day tasks.

Mandatory baseline training reduces common human risks quickly and delivers an auditable record of awareness. Pair training with short, periodic refreshers and real world exercises to maintain vigilance and measure behavioural change.

- **Create or procure a baseline course** that covers cyber hygiene, incident reporting, social engineering and data handling.
- **Make completion mandatory** for all staff within a defined timeframe (for example, 30–60 days) and include it in onboarding.
- **Integrate brief refresher modules** (e.g. 15–30 minutes) to be completed at least annually.
- **Run simulated phishing campaigns** and use results to target further training.

HIGH PRIORITY

Introduce regular, tailored training for the board and senior management

Design and deliver a concise, executive level training programme for the board and senior management that focuses on strategic cyber risks, legal and regulatory obligations under NIS2, incident escalation and decision making in cyber incidents.

Executive training should be tailored, case based and repeated at regular intervals to ensure continuity of oversight and to enable informed risk decisions. This reduces the risk of inadequate governance and demonstrates due diligence to regulators.

- **Develop a short executive programme** (e.g. 1–2 hours) covering NIS2 obligations, strategic risks and reporting responsibilities.
- **Schedule sessions** at least biannually and after material changes to the threat or business landscape.
- **Include scenario tabletop exercises** to practice decision making during incidents.
- **Record attendance and assessment outcomes** as evidence of oversight.

MEDIUM PRIORITY

Implement training records, monitoring and continuous improvement

Establish a centralised recordkeeping process for all cybersecurity training activities and results, including attendance, completion rates, assessment scores and exercise outcomes. Ensure records are retained to demonstrate compliance and to inform audits.

Use these records to define KPIs, identify training gaps, and update course content based on incident trends and changes in the risk assessment. This creates a feedback loop for continuous improvement and regulatory evidence.

- **Implement a training register or LMS** that logs enrolments, completions and assessment results.
- **Define KPIs** (e.g. 90% completion within X days, reduction in phishing click through) and report them to senior management.
- **Review and update content annually** or after significant incidents or risk assessment changes.
- **Retain records** in line with NIS2 audit expectations and local retention policies.

Personnel Security 67%

Observations

- The organisation has initiated a **background-check** programme, but implementation is **ongoing** and presently incomplete (score: 50/100), indicating inconsistent application across recruitment and personnel management.
- There is an established disciplinary process for information-security non compliance that is **largely implemented** and used as required (score: 75/100); this represents a clear governance strength.
- Confidentiality and secrecy agreements are **largely implemented** (score: 75/100) and appear to function in practice, though there is limited evidence of systematic review and alignment with evolving legal or operational changes.
- Overall maturity is **moderate** (aggregate score 67/100). Key gaps include the incomplete background checking process and missing evidence in the questionnaire about *offboarding* or change of employment procedures and consistent documentation of enforcement and review activities.

Recommendations:

HIGH PRIORITY

Finalise and formalise the background check programme

The organisation should complete the rollout of a risk based background checking policy that clearly defines when and how checks are applied according to role sensitivity.

Formalising this process reduces insider risk, ensures consistent legal compliance and supports recruitment decisions for roles with access to critical systems or sensitive data.

- Develop and publish a **Background Checking Policy** that defines checks by role sensitivity and legal requirements
- Define clear vetting levels (e.g. basic, enhanced) mapped to job roles and access privileges
- Integrate checks into the HR recruitment workflow and require documented approval before granting elevated access
- Conduct a legal review to ensure compliance with local employment and data protection laws and record retention rules
- Maintain a secure register of completed checks and schedule periodic re checks where justified by risk

HIGH PRIORITY

Implement formal offboarding and change of employment procedures

The questionnaire did not provide evidence of comprehensive processes to manage termination or role changes. The organisation should implement formal offboarding and role change routines to revoke access, collect assets and update privileges promptly.

Such procedures are essential to prevent residual access and ensure rapid mitigation of insider and supply chain risks, aligning personnel controls with NIS2 expectations for employment lifecycle management.

- Create a documented **Offboarding and Role Change Procedure** covering access revocation, asset recovery and account deactivation timescales
- Ensure HR, IT and security teams have clearly defined responsibilities and an automated checklist for each leaver or role change
- Log and audit completion of offboarding steps and periodically test the effectiveness of the process
- Include contractual clauses and supplier notifications where third parties or contractors are affected

MEDIUM PRIORITY

Enhance preventive controls through targeted training and integration with disciplinary measures

While disciplinary measures exist, emphasis should shift towards prevention by strengthening role based security training and awareness. This reduces incidents that require disciplinary action and supports a security conscious culture.

Integrating training outcomes into personnel records and ensuring disciplinary measures are proportionate and consistently applied will improve fairness and effectiveness.

- Introduce **role based security training** during onboarding and at regular intervals for privileged and sensitive roles
- Publish clear guidance on acceptable behaviour and link training completion to access privileges where appropriate
- Review disciplinary procedures to ensure transparency, proportionality and documented escalation paths
- Establish KPIs to measure training uptake, behavioural improvement and reductions in policy breaches

LOW PRIORITY

Schedule periodic reviews of confidentiality agreements and governance documents

The confidentiality agreements are in place but should be subject to a formal review cycle to ensure they remain aligned with legal changes and evolving business operations.

Regular review reduces legal risk, ensures protection of sensitive information and maintains consistency across employment contracts and third party arrangements.

- Implement an annual review cycle for confidentiality and secrecy agreement templates
- Conduct a legal and business impact review following significant regulatory or organisational changes
- Ensure third party contracts and contractor agreements reflect the same confidentiality standards and are tracked centrally
- Document sign off and maintain a versioned repository of current agreements

Information Protection 42%

Observations

- The overall maturity for **Information Protection** is **low (42/100)**, with several critical controls either not implemented or only planned.
- The organisation demonstrates operational strengths in *patch management* and *backup processes*, both rated as largely implemented, providing a basic resilience foundation.
- Key gaps include the absence of a **secure system development** process during procurement and maintenance, limited deployment of **MFA**, incomplete **access control** processes, and immature policies for **encryption in transit** and **key management**.
- Several controls are in progress (network segmentation, anti-malware, identity lifecycle, logging and encryption at rest), but their **partial state** creates residual risk and may not meet NIS2 requirements without formal policies, testing and documentation.

Recommendations:

HIGH PRIORITY

Establish a secure development and procurement policy (Secure SDLC)

Implement a formal **secure development lifecycle (SDLC)** and procurement policy that mandates security requirements be defined at specification and acquisition stages. This should cover both in house development and outsourced suppliers, ensuring security clauses, acceptance criteria and testing obligations are contractually enforced.

Adopting an SDLC reduces vulnerabilities introduced during acquisition and maintenance and aligns the organisation with NIS2 expectations for risk management in procurement and lifecycle security.

- Draft a **Secure Development & Procurement Policy** that includes security requirements, acceptance criteria and supplier obligations
- Integrate security requirements into procurement templates and contracts for all ICT acquisitions
- Require threat modelling and security review at design/specification phases for new systems
- Define acceptance tests for security controls and include them as contract milestones with suppliers
- Maintain an up to date register of outsourced development and suppliers with documented security ratings

HIGH PRIORITY

Complete and test network segmentation and zoning

Formalise network architecture documentation and complete segmentation into zones that reflect criticality and trust levels. Segmentation must be informed by the risk assessment and include controls to limit lateral movement.

Regular testing (vulnerability assessments, segmentation validation exercises and red team tests) will confirm that segmentation works as intended and will identify misconfigurations or insufficient isolation.

- Document an up to date network architecture and data flows with zone definitions
- Define segmentation rules and permissible traffic flows between zones
- Perform a segmentation validation exercise (internal test or third party assessment)
- Remediate identified gaps and repeat testing on a scheduled basis
- Review segmentation after significant changes or incidents

MEDIUM PRIORITY

Deploy comprehensive anti malware and endpoint detection controls

Move from partial anti malware coverage to an organisation wide capability that includes updated malware detection, endpoint detection and response (*EDR*), and automated remediation where possible. Ensure signature and behavioural engines are regularly updated and centrally managed.

Comprehensive coverage reduces the likelihood of successful malware incidents and shortens detection and response times.

- Inventory endpoints and ensure anti malware/EDR is deployed to all relevant devices
- Centralise management of anti malware signatures and behavioural rules
- Implement automated quarantining and remediation workflows for detected threats
- Schedule regular scans and threat hunting activities informed by threat intelligence
- Integrate anti malware alerts with the central logging and incident response process

MEDIUM PRIORITY

Harden patching process with pre deployment testing and third party tracking

Although patch routines are largely implemented, introduce formal pre deployment testing and explicit tracking of third party software and firmware. Define acceptable timelines for high severity vulnerabilities and an exception process where patching is deferred.

This approach balances stability with security and ensures that patching decisions are auditable and aligned with NIS2 expectations for vulnerability management.

- Establish a pre production test environment and test critical patches before broad deployment
- Classify patch criticality and define target timeframes for deployment per severity
- Maintain an inventory of third party software/hardware and subscribe to vulnerability feeds for those products
- Document the patch exception process with risk acceptance and compensating controls
- Report patch status regularly to senior management

HIGH PRIORITY

Implement identity lifecycle and access management controls including MFA

Consolidate identity management by integrating HR and identity systems to ensure unique, person bound user identities and automated onboarding/offboarding. Formalise registration and deregistration processes and introduce periodic entitlement reviews.

Deploy multifactor authentication for all critical systems and privileged users to significantly reduce account compromise risk and satisfy NIS2 access control expectations.

- Integrate HR and identity systems to automate user provisioning and deprovisioning
- Document and enforce registration and deregistration procedures with defined SLAs
- Implement periodic access reviews and remediate orphaned or excessive privileges
- Deploy MFA for all critical systems and privileged accounts, starting with administrative access
- Implement privileged access management controls for documented privileged accounts

HIGH PRIORITY

Define and implement encryption policies and key management

Put in place a formal cryptography policy covering when to use encryption, approved algorithms and protocols, and minimum key lengths. Pair this with a documented key management policy that defines generation, storage, rotation and destruction of keys, and roles and responsibilities.

Strong cryptographic governance closes gaps in protection of data at rest and in transit and supports compliance with NIS2 requirements for cryptography policies.

- Develop an organisational cryptography policy specifying approved algorithms and use cases
- Implement a centralised key management solution or use HSMs where appropriate
- Define key lifecycle procedures: generation, backup, rotation, compromise handling and destruction
- Ensure encryption in transit is enabled for all sensitive services and define permitted protocols
- Train relevant staff on key handling responsibilities and implement access controls for key stores

MEDIUM PRIORITY

Formalise backup testing and recovery objectives

While backups are largely implemented, formal disaster recovery and backup testing is required. Define recovery time objectives (*RTOs*) and recovery point objectives (*RPOs*) by asset class, conduct regular restore tests and ensure offsite or immutable copies are maintained.

Regular testing validates the ability to recover and supports business continuity obligations under NIS2.

- Define RTOs and RPOs for critical assets and document backup responsibilities
- Implement offsite or cloud backups and ensure they are protected against tampering
- Schedule and perform regular restore tests and document outcomes
- Integrate backup status and test results into business continuity plans
- Adjust backup capacity and processes based on test findings

MEDIUM PRIORITY

Complete central logging, monitoring and retention policies

Accelerate the rollout of central log management and define logging requirements, retention periods and protection measures. Ensure logs cover user lifecycle events, network traffic and critical system changes, and that time synchronisation is in place for reliable correlation.

Centralised logs are essential for incident detection, investigation and demonstrating compliance with NIS2 auditing and reporting obligations.

- Define log sources, minimum log fields and retention requirements in a logging policy
- Deploy centralised log aggregation and ensure logs are protected from unauthorised changes
- Ensure system clocks are synchronised (NTP) across infrastructure for correlation
- Create use cases for monitoring and integrate alerts with incident response processes
- Conduct regular reviews of log coverage and retention against compliance needs

Incident Management and Reporting 15%

Observations

• The organisation's overall maturity for **Incident Management and Reporting** is very low, with an aggregate score of **15/100**, indicating substantial gaps across key NIS2 requirements.

• There is an **ongoing** incident management process in place (50/100) but internal reporting is only **planned** (25/100) and not yet operationalised, creating a risk that incidents are not escalated or handled consistently.

• Critical obligations are currently **not implemented**: there is no formal process for reporting significant incidents to authorities, no procedure to promptly inform affected users, and no regular incident exercises (all 0/100), exposing the organisation to regulatory non compliance and operational disruption.

• The lack of post incident testing and exercises, and the absence of defined external reporting and user notification routines, mean lessons are unlikely to be captured and business continuity arrangements may not be validated under realistic conditions.

Recommendations:

HIGH PRIORITY

Establish a documented incident handling policy and procedure

Develop and approve a formal **incident handling policy** that defines scope, roles, responsibilities, incident categories, severity/impact criteria and escalation paths. This policy should be aligned with NIS2 requirements and integrated with existing risk management and business continuity plans.

The expected benefit is consistent, auditable incident handling that enables timely containment and eradication of threats and provides a foundation for regulatory reporting and internal communication.

- **Within 30 days:** Convene a working group (IT security, legal, operations, risk) to draft the incident handling policy.
- **Within 60 days:** Finalise and publish the policy, including a clear **categorisation and triage matrix** for incidents.
- **Ongoing:** Ensure the policy is formally owned by a senior manager and reviewed annually or after major incidents.

HIGH PRIORITY

Implement internal reporting and communication routines

Turn the planned internal reporting arrangements into operational routines that ensure all employees and contractors know how to report incidents 24/7 and understand escalation paths. Provide clear contact channels and ensure duty rosters for incident responders.

Operationalising internal communication reduces mean time to detect and respond and supports compliant escalation to senior management and relevant stakeholders.

- **Create a single internal reporting channel** (e.g. dedicated email/portal and phone rota) and publish it organisation wide within 14 days.
- **Run a communications campaign** (e.g. email, intranet, quick reference cards) to ensure staff know how and when to report incidents within 30 days.
- **Document escalation matrices and response SLAs** and include out of hours procedures and on call responsibilities.

HIGH PRIORITY

Implement legal and regulator reporting checklists and contacts

Design and implement a **reporting checklist** that identifies incident types and thresholds that must be notified to CSIRTs or supervisory authorities under NIS2, including information to be provided, timeframes and responsible contacts.

This measure addresses immediate compliance gaps and reduces the risk of late or insufficient notifications that could attract regulatory sanctions.

- **Identify applicable authorities and CSIRT contacts** for each jurisdiction in which the organisation operates and compile an authorised contact list within 14 days.
- **Draft a regulator notification checklist** (data required, timelines, decision gate for reportability) and integrate it into the incident handling policy within 30 days.
- **Train incident response leads** on legal notification obligations and run a tabletop scenario to validate the checklist within 60 days.

HIGH PRIORITY

Define user/customer notification procedures

Establish procedures and templates for timely communication to users and customers when service affecting incidents occur, including criteria for when to notify, approved message templates, and preferred channels (email, SMS, service status page).

Proactive user notification reduces customer impact, maintains trust and fulfils NIS2 expectations around transparency and risk mitigation support for users.

- **Define notification criteria and escalation triggers** for customer communications within 21 days.
- **Create standardised message templates** (initial alert, status updates, remediation guidance) and agree legal/regulatory sign off rules.
- **Deploy and test communication channels** (e.g. status page, bulk email/SMS) in a controlled exercise within 60 days.

MEDIUM PRIORITY

Start regular incident management exercises and testing

Introduce a programme of incident exercises, beginning with simple tabletop exercises and progressing to full technical simulations. Exercises should validate procedures, decision making, communications and recovery plans, and must be scheduled at planned intervals.

Regular testing ensures the response remains effective, identifies procedural weaknesses and provides evidence of continuous improvement required by NIS2.

- **Within 30 days:** Develop an exercise plan for the next 12 months with at least one tabletop and one technical simulation.
- **Conduct the first tabletop exercise** within 60 days to validate roles, escalation and notification procedures, capture lessons and assign remediation actions.
- **Maintain an exercise log and integrate lessons learned** into policies, training and the risk register after each exercise.

MEDIUM PRIORITY

Implement post incident review and continuous improvement loop

Ensure every incident is subject to a documented post incident review that identifies root causes, corrective actions and updates to controls, processes and training. Link these outcomes to risk treatment and change management processes.

This closes the improvement loop, reduces recurrence risk and provides documented evidence of remediation efforts for auditors and regulators.

- **Mandate a post incident review** for all incidents above a defined severity within the incident handling policy.
- **Define a template** for reviews that includes root cause analysis, remediation plan, owner and due date, and capture these items in a central repository.
- **Review and report trends** quarterly to senior management and update risk treatment plans accordingly.

MEDIUM PRIORITY

Integrate incident management with business continuity and supplier oversight

Align incident response procedures with the business continuity and disaster recovery plans and ensure supplier incident obligations are enforced and monitored. This integration ensures service restoration objectives and supply chain risks are managed during incidents.

Better alignment reduces recovery times, protects critical services and demonstrates to regulators that the organisation maintains coordinated resilience arrangements.

- **Map critical services** and ensure incident playbooks reference relevant BCP/DR procedures within 30 days.
- **Obtain incident response contact and notification commitments** from key suppliers and incorporate them into contracts or SLAs within 90 days.
- **Test supplier dependencies** during at least one exercise per year and remediate identified gaps.

Continuity and Crisis Management 13%

Observations

• The overall maturity score of **13/100** indicates a **very low implementation** level: several foundational activities are only *planned* while core operational capabilities are **not implemented**.

• Asset mapping, continuity planning and disaster recovery processes are recorded as **planned** (each scoring 25/100) but have not been executed to an operational standard; there is no evidence the organisation has completed a **business impact analysis (BIA)** or a maintained inventory that supports continuity decisions.

• Critical capabilities for responding to major incidents are missing: there is **no implemented crisis management plan**, no programme for testing continuity and incident plans, and no provision for secure communications during crises (each scoring 0/100). This creates a material operational and compliance risk.

• These gaps expose the organisation to prolonged disruption, unclear decision-making in incidents, and potential non compliance with NIS2 requirements on **continuity, disaster recovery and incident handling**.

Recommendations:

HIGH PRIORITY

Establish a continuity and crisis management governance & roadmap

Immediate governance is required to coordinate the planned activities and address the unimplemented capabilities. A clear governance structure and a prioritised roadmap will ensure resources are allocated, owners are identified and milestones are tracked towards NIS2 compliance.

Creating a concise roadmap reduces ambiguity, shortens time to implementation and provides evidence for management and regulators that continuity and crisis measures are being actively delivered.

- Appoint an accountable owner (senior executive) for continuity and crisis management with delegated operational leads.
- Develop a 6–12 month roadmap that prioritises: (1) asset mapping and BIA, (2) business continuity and disaster recovery (BC/DR) plans, (3) crisis management plan, and (4) testing and secure communications.
- Define explicit milestones, success criteria and resourcing (budget, people, external support) for each roadmap item.
- Establish a governance meeting cadence (e.g. fortnightly during mobilisation, then monthly) and reporting to the senior management/board.

HIGH PRIORITY

Perform asset inventory and business impact analysis (BIA)

A documented asset inventory and BIA are prerequisites for all continuity, DR and crisis planning. The inventory should identify the systems, suppliers and processes that support critical services and include owners, classifications and recovery requirements.

Outputs from the BIA will define recovery time objectives (RTO), recovery point objectives (RPO) and prioritisation of restoration activities — essential inputs for effective BC/DR plans and for meeting NIS2 expectations.

- Conduct an asset inventory covering systems, applications, data, third party services and infrastructure; record unique identifiers, owners and criticality.
- Run a formal BIA workshop with process owners to capture service dependencies, impact thresholds and target RTOs/RPOs.
- Document and approve the inventory and BIA outputs, and store them in a controlled repository accessible to continuity planners.
- Map supplier criticality and contractual recovery commitments for each third party identified as supporting critical services.

HIGH PRIORITY

Develop and formalise Business Continuity and Disaster Recovery (BC/DR) plans

Translate the BIA and asset inventory into actionable BC and DR plans that describe procedures to restore operations. Plans must address technical recovery, data backup assurance and supplier failover arrangements.

Plans should be documented, approved by management and integrated with incident response procedures so that recovery activities align with operational triage and escalation processes.

- Create a business continuity plan (BCP) that defines recovery priorities, roles and communication channels for different disruption scenarios.
- Develop disaster recovery procedures for mission critical systems: documented restart steps, backup verification, and alternate site or cloud failover instructions.
- Define and document RTO and RPO targets in the BCP/DR plans aligned to the BIA outputs.
- Ensure contractual measures and SLAs with suppliers support the required recovery capabilities; update contracts or implement compensating controls where gaps exist.

HIGH PRIORITY

Establish a crisis management plan with roles, decision paths and contact points

A crisis management plan defines how the organisation will operate under major incidents, including clear decision making pathways, communication responsibilities and escalation thresholds. Given the current absence of an implemented plan, this is critical to reduce confusion and response time in a real crisis.

The plan should be practical, map to the incident response process and identify who is authorised to make operational and external communications decisions during a crisis.

- Define a crisis organisation: crisis lead, deputies, subject matter experts and spokespeople; publish a contact directory with 24/7 reachability details.
- Document decision making authorities and escalation criteria for operational, legal, regulatory and public communications actions.
- Integrate the crisis plan with the incident response policy so that cyber incidents trigger the appropriate crisis governance when thresholds are met.
- Provide concise, role specific playbooks for senior leaders and incident handlers to follow during the initial 24–72 hours of a major incident.

MEDIUM PRIORITY

Implement a testing programme for incident, BC and DR plans

Testing is essential to validate plans, expose gaps and train personnel. The organisation currently reports no testing of incident management or continuity plans, which leaves recovery assumptions unverified and increases the risk of failure during a real incident.

Start with low complexity tabletop exercises and progressively run live recoveries of backups and technical failovers. Capture lessons learned and feed them back into plan revisions.

- Define a test policy that sets the scope, frequency and types of tests (tabletop, technical restore, full failover) based on risk and criticality.
- Schedule and execute an initial tabletop exercise covering a plausible major cyber incident; document outcomes and action items.
- Perform a technical recovery test for at least one mission critical system (backup restore or failover) and validate RTO/RPO assumptions.
- Maintain test records, track remediation actions and update plans after each exercise.

MEDIUM PRIORITY

Establish secure, resilient communication channels for crises

Reliable and secure communications are indispensable during incidents when primary systems may be unavailable. The absence of any implemented secure communications capability increases the likelihood of miscoordination and data exposure.

Implement alternative channels and cryptographic protections for sensitive exchanges, and control access to those channels to prevent misuse during a crisis.

- Identify and provision alternative communication channels (e.g. encrypted messaging, out of band telephone trees, secure satellite/backup internet where applicable).
- Define access control and authentication for crisis communications, and ensure key holders have secure credentials and tested devices.
- Include communication channel failover procedures in the crisis playbooks and rehearse their use in tabletop exercises.

Supply Chain and Third-Party Risks 10%

Observations

• The organisation's maturity for **Supply Chain and Third Party Risks** is critically low, as indicated by the overall score of **10/100**. Only *identification* of systems and the introduction of contractual requirements are at a planned stage; all other controls remain unimplemented.

• There is **no evidence of a supplier risk assessment** or segmentation process, which prevents the organisation from prioritising resources or applying proportionate controls to suppliers that support critical services.

• The organisation has not specified security measures tied to information classification nor implemented a programme of regular follow ups or deviation management with suppliers, creating significant operational and compliance risks under NIS2.

• Key documentation and operational artefacts appear missing or incomplete: a maintained supplier registry, asset to supplier mappings and formal supply chain security policy are either not implemented or only planned, limiting visibility and enforceability.

Recommendations:

HIGH PRIORITY

Establish a formal supply chain security policy and supplier registry

Define and approve a **Supply Chain Security Policy** that governs selection, contracting and ongoing management of suppliers supporting critical services. This policy should mandate a maintained supplier registry with contact points and roles to satisfy governance and incident response needs.

Implementing a clear policy and registry provides the foundation for all subsequent supplier risk management activities and helps demonstrate alignment with NIS2 obligations on governance and supplier oversight.

- Appoint a senior owner for supply chain security and publish the policy for stakeholders
- Compile an initial supplier registry listing all direct suppliers, contact points, contract owners and the services they provide
- Classify suppliers by criticality (e.g. high/medium/low) and publish the update cadence for the registry
- Define roles and responsibilities for maintaining the registry and integrating it with asset inventories

HIGH PRIORITY

Perform supplier risk assessments and segmentation

Introduce a documented supplier risk assessment process to evaluate the cyber risk posed by each supplier based on factors such as access to sensitive data, availability impact, past security performance and hosting location.

Prioritise assessments for suppliers that support critical services and use the results to determine control depth, contract requirements and monitoring frequency. This enables risk based decision making required by NIS2.

- Define risk assessment criteria and a simple scoring model (impact, likelihood, security posture, criticality)
- Run assessments for the top 20% of suppliers by criticality or spend first, then extend coverage
- Document results in the supplier registry and map to required control levels
- Integrate assessment outcomes into procurement and vendor onboarding processes

MEDIUM PRIORITY

Embed clear cybersecurity requirements into contracts and procurement

Ensure all supplier contracts and procurement templates contain **clear, enforceable cybersecurity requirements** (for example, patching, vulnerability disclosure, secure configurations, encryption, audit and access controls). Include rights to audit, security SLAs and obligations for incident notification.

Making requirements contractual ensures suppliers understand expectations and provides legal levers to enforce compliance or apply remediation measures.

- Draft baseline cybersecurity clauses for use in new contracts and renewals (patching, encryption, incident reporting timelines, audit rights)
- Conduct a legal and procurement review to ensure clauses are enforceable and proportionate
- Apply baseline clauses immediately to all new engagements and a prioritised set of renewal contracts
- Define contractual escalation and remediation processes for non compliance

MEDIUM PRIORITY

Classify shared assets and require controls based on sensitivity

Implement an asset and information classification scheme and map which assets and data are handled by each supplier. Specify minimum controls and protection levels for each classification tier (for example, encryption at rest/in transit, multi factor authentication, least privilege).

This measure ensures that suppliers are required to meet security levels proportionate to the value and sensitivity of the information they process, supporting compliance with NIS2 control requirements.

- Define an organisational classification scheme for data and assets (e.g. public, internal, confidential, critical)
- Map suppliers to the assets and data they process and identify required protection levels
- Specify baseline technical controls for each classification (encryption, access controls, logging)
- Require suppliers to evidence or attest to implementation of those controls

HIGH PRIORITY

Implement ongoing monitoring, reporting and remediation for suppliers

Establish a programme of regular follow ups that includes monitoring of SLAs, periodic security reviews, vulnerability scanning or questionnaires, and defined remediation timelines. Include a process for risk based escalation when deviations are identified.

Continual monitoring and enforceable remediation are essential to reduce supply chain risk and to meet NIS2 expectations for supplier oversight and incident prevention and management.

- Define monitoring methods and cadence (annual reviews, quarterly reports, evidence submission, targeted audits)
- Set measurable KPIs and SLAs for supplier security performance and reporting
- Establish a non compliance escalation and remediation workflow with owners and timeframes
- Integrate supplier monitoring outputs into the organisation's risk register and executive reporting

Continuous Improvement and Monitoring 0%

Observations

- The organisation currently has **no evidence of independent reviews** of its information security management system or security work, indicating a complete absence of external or internal audit activity against security controls.
- There are **no documented processes or routines**
- The absence of testing and independent review means the organisation cannot demonstrate **effectiveness, validation or continuous improvement** of policies, controls and incident responses as required by NIS2.
- Key programme elements are missing or undocumented: scope and frequency of reviews and tests, competent reviewers/testers, reporting lines to management, and a structured remediation/tracking process.

Recommendations:

HIGH PRIORITY

Establish an independent review (audit) programme

Implement a formal programme of independent reviews to assess the suitability and effectiveness of the information security management system. Independent reviews may be performed by internal audit teams with appropriate competence or by external auditors depending on available expertise and independence requirements.

Independent reviews provide an objective assessment of people, processes and technologies, and are a core NIS2 expectation for demonstrating governance and compliance.

- **Define scope:** Document the scope of audits (policies, risk management, technical controls, incident handling, supplier security).
- **Appoint reviewers:** Select competent internal auditors or procure an external auditor with expertise in NIS2/ICT security.
- **Schedule reviews:** Create an annual audit calendar with milestones and review frequency tied to risk levels.
- **Report outcomes:** Ensure results are reported to the management body and retained as evidence for compliance.
- **Track remediation:** Assign owners and deadlines for remediation actions arising from reviews.

HIGH PRIORITY

Create and implement a documented security testing policy

Develop a policy and procedures that define the purpose, types, scope, frequency and responsible roles for security testing (e.g. vulnerability scanning, penetration testing, configuration checks, backup recovery tests).

A documented testing policy ensures tests are risk-driven, repeatable and auditable, meeting NIS2 requirements for assessing the effectiveness of cybersecurity measures.

- **Draft policy:** Produce a security testing policy that includes test types, frequency, approval rules and handling of findings.
- **Define criteria:** Base testing scope and frequency on the organisation's risk assessment.
- **Obtain approvals:** Have management and legal/HR sign-off for intrusive tests (e.g. penetration tests).
- **Integrate with procurement:** Ensure testing requirements are included in supplier contracts for hosted/managed services.

HIGH PRIORITY

Start immediate, pragmatic practical tests of basic controls

While policies and programmes are being established, perform immediate practical tests of critical/basic controls (password policies, endpoint protection, authentication, backup restore) to obtain quick assurance and to identify high-impact weaknesses.

These tactical tests deliver early risk reduction and create baseline evidence while the longer-term testing programme is implemented.

- **Perform vulnerability scanning:** Run authenticated and unauthenticated scans on critical assets and document results.
- **Test backups:** Execute at least one full restore from backup for a critical system and document recovery time and integrity.
- **Verify endpoint defences:** Confirm antivirus/EDR deployment and up-to-date signatures across representative systems.
- **Check access controls:** Validate password/ MFA enforcement on a sample of privileged and user accounts.
- **Record findings:** Log test outcomes and open tracked remediation tickets for each deficiency.

MEDIUM PRIORITY

Implement continuous monitoring and metrics for effectiveness

Establish continuous monitoring processes and measurable KPIs to assess effectiveness of security controls and to detect regression between periodic tests or audits. Monitoring should include vulnerability feeds, log aggregation, alerting and periodic evaluation against defined metrics.

Continuous monitoring supports early detection of issues and provides the data necessary for evidence-based decisions and regulatory reporting.

- **Define KPIs:** Establish measurable indicators (e.g. time to remediate critical vulnerabilities, percentage of systems with up-to-date EDR, backup restore success rate).
- **Deploy monitoring:** Implement or extend SIEM/log aggregation and vulnerability management tooling to collect relevant telemetry.
- **Subscribe to feeds:** Monitor vulnerability information channels (CSIRTs, CERT-EU, vendor advisories) and integrate into workflows.
- **Review periodically:** Produce a monthly management dashboard and escalate outliers to senior management.

MEDIUM PRIORITY

Establish governance: assign responsibilities and reporting lines

Define clear responsibilities for testing, independent reviews, monitoring and remediation, and ensure formal reporting of results to the management body. NIS2 requires that management bodies review policies and results at planned intervals and after significant incidents.

Clear governance reduces ambiguity, speeds remediation and demonstrates accountability to regulators.

- **Map roles:** Document owners for testing, audits, monitoring and remediation tracking.
- **Set reporting cadences:** Define how and when results are presented to senior management or the board.
- **Include in policy:** Update the security policy to state review responsibilities and intervals.
- **Ensure competence:** Provide training or procure expertise for reviewers and testers where gaps exist.

MEDIUM PRIORITY

Implement a documented remediation and evidence retention process

All findings from tests and reviews must be tracked, prioritised and remediated within defined timeframes. Retain evidence of tests, review reports and remediation actions to demonstrate due diligence and compliance with NIS2 requirements.

A formal remediation lifecycle ensures issues are closed and provides auditable trail for regulators and inspectors.

- **Create tracking system:** Use an issue tracker or GRC tool to log findings, assign owners, set deadlines and track status.
- **Define SLAs:** Establish remediation timeframes by severity (e.g. critical within 7 days, high within 30 days).
- **Retain evidence:** Archive test reports, audit reports and proof of remediation for a defined retention period.
- **Conduct closure validation:** Require independent verification of remediated high/critical findings before closing.

Physical Security and Access 75%

Observations

• The organisation has largely implemented physical protection measures for critical information systems, indicating defined security perimeters and basic safeguards against fire, flooding, burglary and sabotage.

• Physical access controls to IT spaces appear restrictive and traceable, with mechanisms in place to authorise entry; however, there is limited evidence that access logs are consistently integrated with central monitoring or that reviews are routinely documented.

• Redundancy for power, cabling and network paths is in place where justified, but active monitoring of environmental conditions and component health is not fully evidenced and lifecycle management of ageing infrastructure is unclear.

• There is partial or unspecified evidence of formalised inspection registers, owner assignments and regular testing of physical controls, which reduces assurance that current measures will sustain effectiveness and meet NIS2 audit expectations.

Recommendations:

MEDIUM PRIORITY

Formalise routine physical inspections and an asset protection register

Establishing a documented inspection regime and a centralised asset protection register will convert ad hoc checks into a repeatable, auditable process. This ensures owners are accountable for remediation and provides demonstrable evidence for regulators and auditors.

Routine inspections combined with automated sensor alerts will increase detection of physical hazards and accelerate corrective actions, improving the organisation's resilience and compliance posture under NIS2.

- Create a central **asset protection register** listing critical systems, their locations, assigned owners and remediation due dates
- Define and document a recurring inspection schedule (eg weekly visual checks, monthly functional tests) and capture results in the register
- Deploy or integrate environmental sensors (fire, flood, temperature, humidity) and configure automated alerts to the responsible owners
- Define escalation paths and SLAs for remediating inspection findings and ensure owners update the register on closure

HIGH PRIORITY

Integrate physical access logs with SIEM and enforce regular access reviews

Centralising physical access logs in the security information and event management (*SIEM*) platform enables correlation with logical security events and improves detection of anomalous activity. This provides a clearer audit trail for investigations and regulatory review.

Regular, documented access reviews aligned to job function and need-to-know will ensure that only authorised personnel retain access, reducing insider and credential risks.

- Identify all physical access log sources (card readers, biometric devices, door sensors) and enable secure log forwarding to the SIEM
- Implement SIEM use cases to detect anomalous entry patterns (eg after-hours access, door-held events, repeated failed access attempts) and create automated alerts
- Schedule and document quarterly access reviews with business owners; reconcile authorised lists against HR and IAM systems
- Automate deprovisioning processes for access when staff change role or leave the organisation

MEDIUM PRIORITY

Activate environmental and power monitoring and implement proactive lifecycle management

Continuous monitoring of power, temperature and link status is essential to detect early signs of failure and to validate redundancy mechanisms. Monthly review of these metrics will identify trends and support timely intervention.

Proactive replacement of ageing components and regular testing of failover measures will support recovery objectives and reduce the likelihood of interruptions that could affect availability obligations under NIS2.

- Deploy monitoring for power supplies, UPS status, ambient temperature and network link health and forward alerts to the operations team
- Review monitoring logs at least monthly and produce trend reports to identify components approaching end-of-life
- Define and maintain a lifecycle replacement plan for critical infrastructure and schedule proactive replacements before end-of-life
- Perform regular failover and restore exercises for power and network redundancy and record recovery times against business continuity objectives

Conclusion

To reach an acceptable NIS2 posture, the organisation should pursue a two phase strategic path: stabilise core governance and operational controls in the **short term (0–6 months)**, then consolidate, test and mature capabilities in the **medium term (6–24 months)**. Short term work must produce auditable artefacts (policies, owners, basic procedures) that mitigate the highest compliance and business risks. Medium term investments should embed assurance, automation and supplier governance to sustain resilience.

Immediate priorities are governance (establish an ISMS and management reporting), incident readiness (incident handling, internal reporting and regulatory notification checklists), continuity (BIA and BC/DR plans) and workforce awareness (baseline mandatory training). Over 6–24 months, the organisation should complete risk framework formalisation, operationalise supply chain risk management, implement secure procurement and development practices, roll out stronger identity and detection controls, and institute regular independent reviews and testing to demonstrate effectiveness and continuous improvement.

Short-Term Recommendations:

• Formally establish an Information Security Management System (ISMS) with an appointed owner, documented scope, timeline and secured resources.

• Implement a simple, repeatable management reporting process to provide regular, documented updates to the management body.

• Create and publish an incident handling policy and internal reporting procedures; define escalation paths and 24/7 reporting channels.

• Develop a regulator and user notification checklist aligned to **NIS2** thresholds and assign responsible contacts.

• Complete asset classification for the central register and assign clear owners/custodians for critical assets.

• Deploy a mandatory baseline cybersecurity awareness course for all staff and a concise executive briefing for senior management.

• Perform a Business Impact Analysis (BIA) and produce a prioritized continuity roadmap that identifies critical services and recovery objectives.

• Establish a supplier registry and begin high priority supplier identification for immediate risk assessment and contract review.

• Begin pragmatic practical tests of basic controls (backup restore, patch status checks, endpoint protection validation) and document results.

• Define and apply role based background check completion criteria and implement immediate offboarding checklists to revoke access on exits.

Long-Term Recommendations:

• Formalise and adopt a documented risk management framework that prescribes methodology, roles, cadence and KRI reporting to top management.

• Operationalise a mature BC/DR programme with documented plans, crisis management procedures, secure communications and regular exercises.

• Implement a secure development and procurement policy (secure SDLC) and embed enforceable cybersecurity clauses into supplier contracts.

• Roll out multi factor authentication and complete identity lifecycle and access control improvements organisation wide.

• Deploy centralised logging correlation (SIEM) integrating physical access logs, and introduce continuous monitoring and 24/7 detection capability.

• Establish a supplier risk assessment and segmentation programme with follow up monitoring, SLAs and audit rights for critical providers.

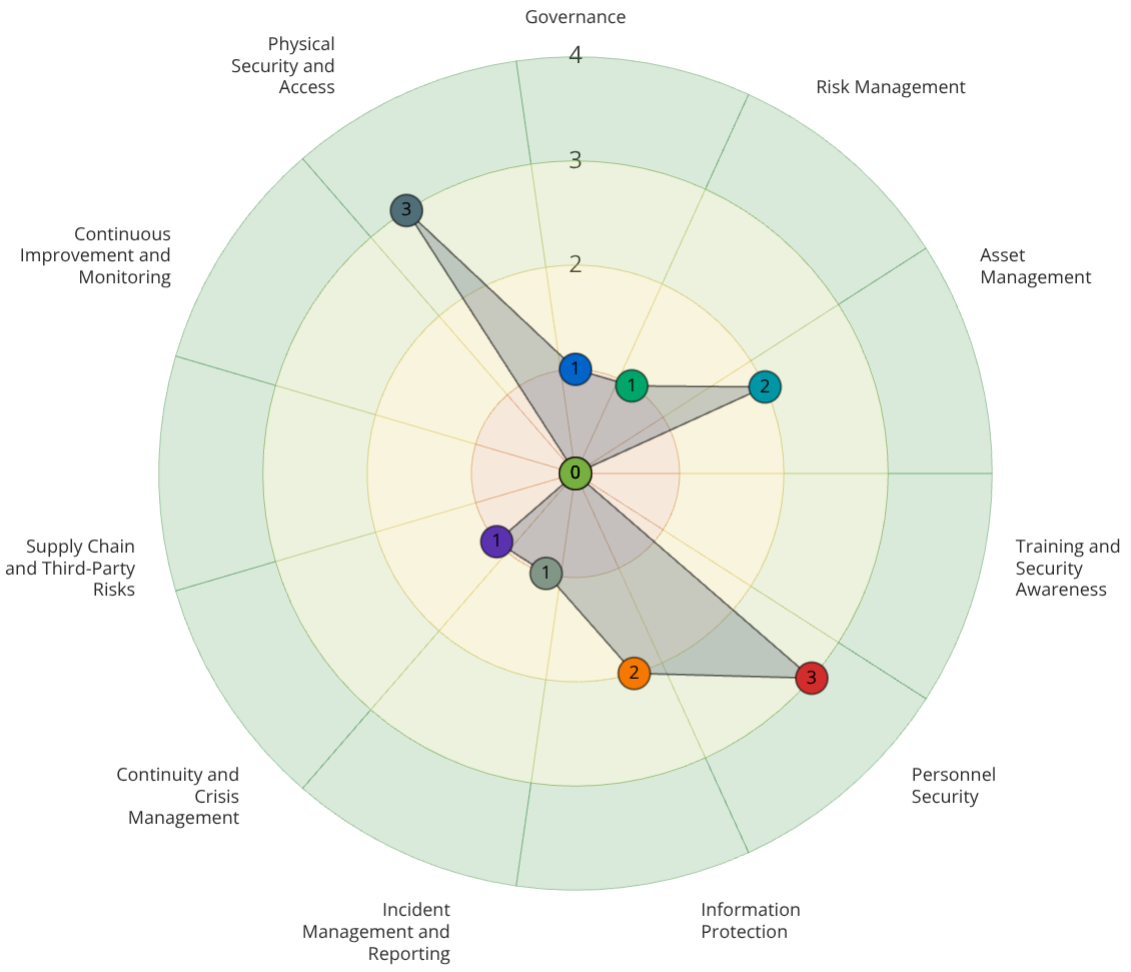
• Introduce a documented security testing policy and schedule regular vulnerability scanning, penetration testing and recovery tests; remediate via tracked tickets.

• Create an independent review programme (internal audit or external assessor) with defined scope, frequency and management reporting to evidence compliance.

• Institutionalise periodic incident exercises (tabletops, simulated incidents, red/blue team) to validate response, escalation and communication routines.

• Implement lifecycle management for physical infrastructure, environmental monitoring and routine documented access reviews integrated into overall security operations.

Charts



Not Implemented	Planned or Initiated	Ongoing	Largely Implemented	Optimized
Reactive or ad-hoc work; no formal approach or documentation.	Intent defined and first steps taken, but practice not yet established; documentation largely absent	Processes exist, are documented and understood, yet are only partly applied; effectiveness and coverage remain limited.	Practices are deployed and fully documented, staff are trained, and activities are managed, but systematic measurement and continuous improvement are still emerging.	Practices are fully implemented, documented, continually measured, and proactively improved; staff competence is verified and performance evidence is routinely reviewed.