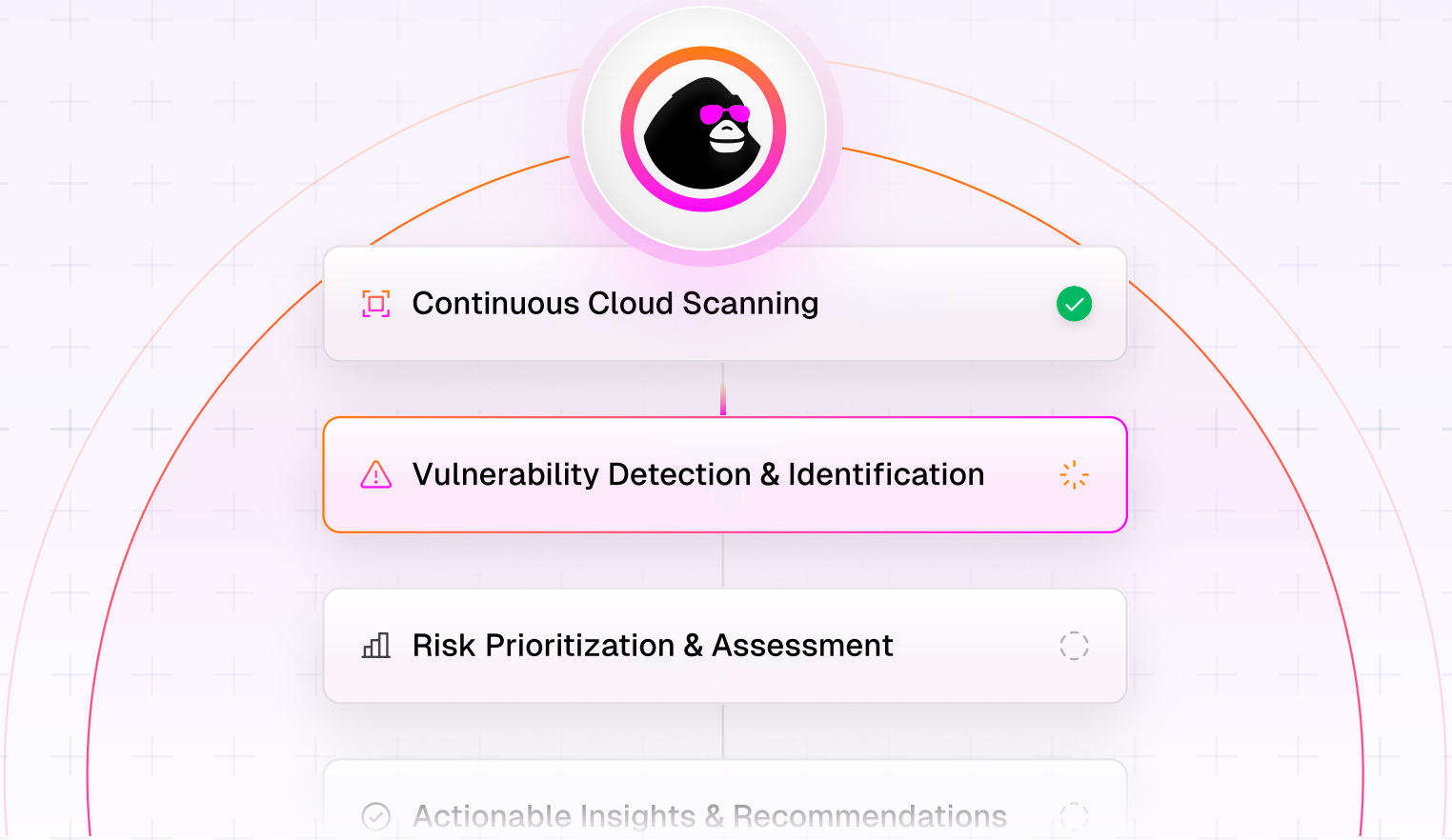
Cyber Upgrade

Template

Cybersecurity maturity assessment questionnaire template

Aligned with DORA, ISO 27001, NIS2, and industry best practices



How to score and analyze

1. Assign maturity levels

For each question, assign a maturity score from 1 to 5 based on the defined scale.

2. Average and weighted scores

- Calculate an average score for each domain.
- If some domains are more critical to your organization, you may assign weights to calculate an overall maturity score.

3. Identify gaps & prioritize improvements

- Focus first on areas with low maturity scores that also have a high impact on your organization's overall risk profile.
- Develop a remediation plan with clear owners, timelines, and resource requirements.

4. Document and track progress

- Retain evidence for each rating.
- Schedule periodic reassessments (annually or semi-annually) to track your improvement trajectory.

Maturity scale

Most maturity scales range from 1 (Non-Existent) to 5 (Optimized). You can customize each level as appropriate for your organization, but a commonly used scale is:

---

1. **Level 1 – Non-existent/Ad hoc**

   For each question, assign a maturity score from 1 to 5 based on the defined scale.

2. **Level 2 – Repeatable but intuitive**

   Some awareness and basic processes, but they are inconsistent.

3. **Level 3 – Defined**

   Documented procedures, standards, and guidelines in place.

4. **4. Document and track progress**

   Processes are consistently followed and measured for effectiveness.

1. Organizational Security & Governance

1.1 Security governance structure

- Does your organization have a defined cybersecurity governance structure (e.g., designated CISO, security committee)?
- Is there an executive sponsor or board-level involvement in cybersecurity strategy?

1.2 Policies and standards

- Are cybersecurity policies, procedures, and standards formally documented and regularly reviewed?
- Does your organization have a process to ensure these policies and standards are communicated and enforced?

1.3 Risk management program

- Is there a documented, organization-wide risk management program that includes cybersecurity risk?
- How often are security risk assessments conducted, and is there a formal methodology (e.g., NIST RMF, ISO 27005)?

1.4 Compliance & regulatory requirements

- Are legal and regulatory requirements (e.g., GDPR, HIPAA, PCI-DSS, SOX) identified, tracked, and integrated into cybersecurity policies?
- Is there a formal process to monitor changes in relevant regulations and ensure ongoing compliance?

2. Asset & data management

2.1 Asset inventory

- Does your organization maintain a comprehensive, up-to-date inventory of critical assets (hardware, software, data)?
- Are critical assets classified based on sensitivity and business value?

2.2 Data classification & handling

- Is there a formal data classification policy that defines handling requirements for different data types (e.g., public, internal, confidential)?
- Are there guidelines or technical controls for data at rest and data in transit, especially for sensitive data?

2.3 Data retention & disposal

- Are data retention periods defined and enforced for all data types?
- Are secure data disposal methods (e.g., secure wipe, shredding) consistently applied?

3. Access control

3.1 Identity & access management (IAM)

- Does your organization have centralized IAM solutions (e.g., single sign-on, directory services)?
- Are strong authentication methods (e.g., MFA) implemented for critical systems?

3.2 Privilege management

- Are privileged accounts (e.g., administrator, superuser) managed with strict controls and monitoring?
- Is there a process for periodic review of user access rights to ensure least privilege is maintained?

3.3 Remote access

- Is remote access (VPN, RDP, etc.) secured with multi-factor authentication and encryption?
- Are remote sessions monitored or logged for potential security events?

4. Network & endpoint security

4.1 Network segmentation & security

- Are critical systems and data segregated from general network segments (e.g., through VLANs, DMZ architecture)?
- Are network traffic logs and alerts centrally collected and monitored?

4.2 Endpoint security

- Are endpoint protection tools (antivirus, EDR, patch management) consistently deployed across the enterprise?
- Are endpoints regularly scanned for vulnerabilities, and are patches applied in a timely manner?

4.3 Secure configuration management

- Are secure baseline configurations defined and implemented for servers, workstations, and network devices?
- Is there a process to verify and document all configuration changes?

5. Threat & vulnerability management

5.1 Vulnerability assessment

- Are regular vulnerability scans performed on internal and external systems?
- Does the organization have a formal process to prioritize and remediate identified vulnerabilities?

5.2 Penetration testing & red team exercises

- Are penetration tests conducted periodically to identify weaknesses in applications, networks, and systems?
- Does the organization conduct advanced exercises (e.g., red team/blue team) to assess detection and response capabilities?

5.3 Threat intelligence

- Does your organization subscribe to threat intelligence feeds or participate in information-sharing communities (ISACs)?
- Is threat intelligence integrated into security monitoring and incident response workflows?

6. Security operations & monitoring

6.1 Security operations center (SOC)

- Do you have a dedicated SOC (internal or outsourced) responsible for threat monitoring and incident response?
- Is SOC staff properly trained and equipped with the necessary tools (SIEM, SOAR, etc.)?

6.2 Logging & monitoring

- Are critical systems and applications configured to generate logs that are centrally aggregated?
- Are logs monitored in real-time for anomalous behavior, and is there a defined log retention policy?

6.3 Metrics & reporting

- Does your organization track and report on key security metrics (e.g., number of incidents, mean time to detect/respond)?
- Are these metrics regularly reviewed by management to drive improvement?

7. Incident response & business continuity

7.1 Incident response plan (IRP)

- Is there a formally documented Incident Response Plan that defines roles, responsibilities, and procedures?
- Are tabletop exercises and incident simulations conducted periodically to validate and refine the IRP?

7.2 Business continuity & disaster recovery

- Does the organization have a documented Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)?
- Are critical systems regularly backed up, and is backup data tested for integrity/restoration?

7.3 Lessons learned & continuous improvement

- After a security incident, is a post-incident review conducted to capture lessons learned?
- Are improvements from incident reviews consistently integrated into policies and controls?

8. Security awareness & training

8.1 Security awareness program

- Does your organization have a formal, ongoing security awareness and training program for all employees?
- Is training content updated regularly to address current threats and organizational policies?

8.2 Phishing & social engineering tests

- Are regular simulated phishing campaigns or social engineering tests conducted?
- Is there a process to follow up with users who fail these tests, including targeted training?

8.3 Role-based training

- Do employees in high-risk roles (e.g., IT admins, developers) receive specialized security training?
- Are training completion records maintained and reviewed for compliance?

9. Third-party & supply chain risk

9.1 Third-party risk management

- Do you have a formal process to evaluate and onboard third parties or vendors (e.g., security questionnaires, contract clauses)?
- Is there a continuous monitoring or periodic reassessment of third-party security posture?

9.2 Supply chain security

- Are suppliers and service providers that handle sensitive data required to meet specific security standards?
- Do contracts or SLAs include clear cybersecurity requirements (e.g., right to audit, breach notification timelines)?

9.3 Cloud security governance

- Are security expectations defined for cloud providers (IaaS, PaaS, SaaS), including data protection, encryption, and incident response requirements?
- Are cloud environments reviewed and monitored for compliance with organizational policies?

10. Program maturity & continuous improvement

10.1 Formal assessment & benchmarking

- Does your organization routinely benchmark its cybersecurity program against recognized frameworks (e.g., NIST CSF, ISO 27001)?
- Is there a defined frequency (e.g., annually) to perform holistic security assessments?

10.2 Security roadmap & strategy

- Is there a long-term security roadmap aligned with business objectives and risk assessments?
- Are resources (budget, personnel) allocated in line with the roadmap and risk priorities?

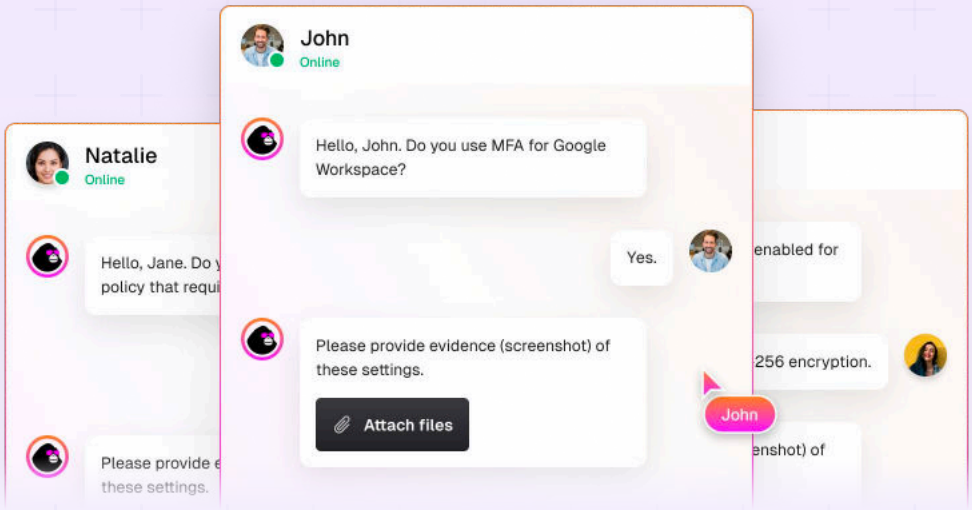
10.3 Continuous improvement cycle

- Do you have a mechanism (e.g., security steering committee) to oversee cybersecurity improvements?
- Is feedback from incidents, audits, and external assessments used to drive updates to the cybersecurity strategy?

Additional resources

Example summary table

Domain	Average maturity score	Priority areas for improvement
Information Security Policy	3.0	Formalize risk assessment schedule
Cloud Architecture Diagram(s)	2.5	Establish comprehensive asset inventory
Risk Management & Governance Policy	3.5	Implement MFA for all critical systems
Data Classification & Handling Guidelines	3.0	Enhance endpoint protection coverage
Incident Response Plan	2.5	Increase frequency of penetration tests
IAM Policy & Procedures	3.5	Improve real-time monitoring and alerting
Vulnerability & Patch Management Policy	2.0	Update incident response and DR plans
Business Continuity & Disaster Recovery Plan	4.0	Expand role-based training for technical staff
Vendor Management & Third-Party Agreements	2.5	Strengthen vendor due diligence process
Compliance / Audit Reports	3.0	Develop a long-term cybersecurity roadmap



Tired of endless custom security questionnaires? Ease the burden with CyberUpgrade

The CyberUpgrade team is deeply knowledgeable about DORA and the complexities of third-party risk management. We simplify these challenges with expertise and real-time support, ensuring your vendor ecosystem remains resilient and compliant. With an efficient AI questionnaire assistant, we automate up to 90% of the questionnaire process.

Book a demo

More info available on www.cyberupgrade.net

Further reading & resources

Learn about our Free AI Questionnaire Assistant

Download Mastering third-party risk management under DORA eBook

Visit our blog for more resources