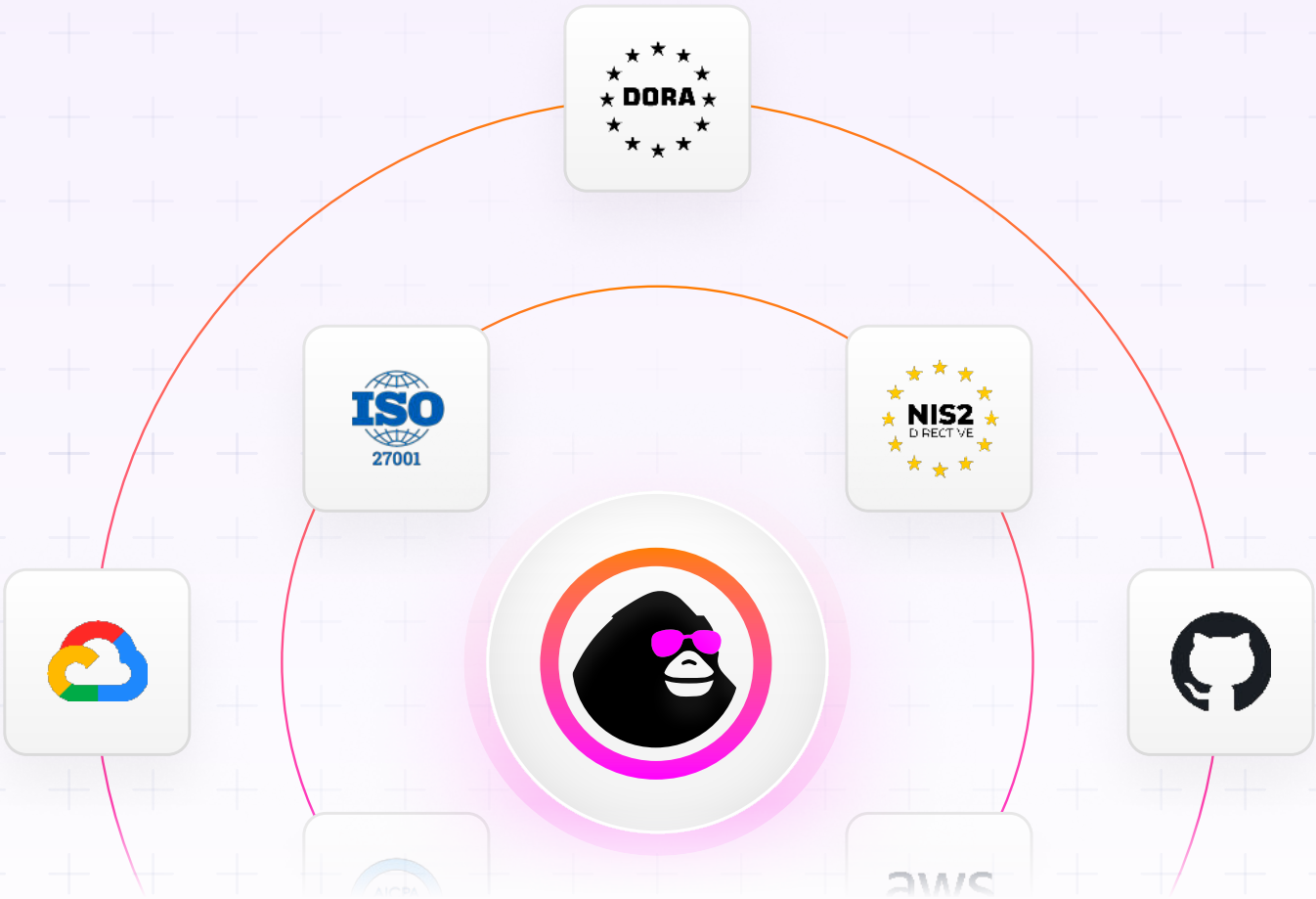
Cyber Upgrade

Template

# Information and cybersecurity risks assessment questionnaire template

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



# How to use the questionnaire

To get the most out of this template, follow the steps below.

### 1. Define the scope

Identify the purpose (vendor review, internal audit) and applicable frameworks (DORA, ISO 27001, NIS2)

### 2. Involve key stakeholders

Engage security, risk, compliance, and IT teams.

### 3. Distribute & collect responses

Send the questionnaire and request complete, documented answers.

### 4. Review & assess risks

Check for compliance, identify gaps, and evaluate security posture.

### 5. Follow up

Request clarifications or remediation plans for weak areas.

### 6. Approve or request improvements

Decide if the vendor/process meets security standards.

### 7. Monitor & update

Identify the purpose (vendor review, internal audit) and applicable frameworks (DORA, ISO 27001, NIS2)

# 1. Organizational & governance

## 1.1 Security governance & leadership

- Is there a documented information security governance framework or policy in place?
- Does the organization have a designated Chief Information Security Officer (CISO) or equivalent role?
- How often does the governing body (e.g., board, executive leadership) review security risks and strategies?

---

## 1.2 Security policies & procedures

- Are information security policies formally approved, reviewed, and updated on a regular basis?
- Are all employees and contractors required to acknowledge understanding of the security policies?
- Do policies exist for acceptable use, password management, and remote work?

---

## 1.3 Regulatory compliance

- Which regulations, standards, or frameworks (e.g., ISO 27001, NIST, HIPAA, GDPR) does the organization follow?
- Is there a process to monitor changes in relevant laws, regulations, or standards?
- Does the organization perform periodic compliance audits or assessments?

# 2. Risk management process

## 2.1. Risk assessment methodology

- Is there a formal, documented risk assessment methodology in place?
- How frequently are risk assessments conducted (annually, semi-annually, etc.)?
- Does the methodology include asset identification, threat modeling, vulnerability analysis, impact analysis, and likelihood assessment?

---

## 2.2. Risk treatment & acceptance

- Are risk treatment options (accept, mitigate, transfer, avoid) documented and approved by senior management?
- Is there a risk register or log tracking identified risks, owners, and treatment progress?
- How does the organization ensure residual risks are formally approved or accepted at the appropriate level?

---

## 2.3. Third-party risk management

- Are third-party vendors or suppliers required to meet specific security requirements or certifications?
- Do contracts with third parties include security clauses (e.g., data handling, breach notification)?
- Is there a periodic assessment process to evaluate the security posture of third-party vendors?

# 3. Asset management & classification

## 3.1. Asset inventory

- Is there a maintained and up-to-date inventory of all IT assets (hardware, software, data)?
- Does the organization track ownership and location of these assets?

## 3.2. Classification & labeling

- Are information assets classified (e.g., public, internal, confidential, restricted) based on sensitivity and criticality?
- Are data handling and labeling procedures defined based on classification (e.g., encryption for confidential data)?

## 3.3. Data retention & disposal

- Is there a data retention schedule defining how long different categories of data should be stored?
- Are secure disposal methods in place for end-of-life assets (e.g., shredding, wiping, degaussing)?

# 4. Access control & identity management

## 4.1. User provisioning & deprovisioning

- Is there a formal process for granting, modifying, and revoking access rights?
- Are privileges promptly revoked when employees leave or change roles?

## 4.2. Authentication mechanisms

- Is multi-factor authentication (MFA) enabled for critical systems and remote access?
- Are password policies (e.g., length, complexity, expiration) enforced across the environment?

## 4.3. Privileged access management

- Is there a separate privileged account management solution or process?
- Are privileged actions logged and monitored for anomalies?

## 4.4. Remote access & BYOD

- Are employees allowed to use personal devices for business purposes? If so, what security controls (e.g., MDM) are in place?
- Is remote access to internal systems restricted and monitored?

# 5. Network security

## 5.1. Network architecture & segmentation

- Is there documented network architecture showing DMZs, internal networks, and segregated environments (e.g., PCI network)?
- Are critical systems isolated or segmented from the corporate network?

## 5.2. Firewall & perimeter security

- Are firewalls configured with a default deny rule set, only allowing necessary traffic?
- How often are firewall rules reviewed and updated?
- Are intrusion detection or intrusion prevention systems (IDS/IPS) deployed and monitored?

## 5.3. Wireless network security

- Is wireless access restricted using WPA2/WPA3 or equivalent encryption?
- Is guest Wi-Fi segregated from internal corporate networks?

## 5.4. Network monitoring & logs

- Are network traffic logs reviewed regularly for suspicious or unauthorized activities?
- Does the organization have a Security Information and Event Management (SIEM) system or log management solution?

# 6. Endpoint & system security

## 6.1. Endpoint protection

- Are antivirus/anti-malware solutions installed and kept up to date on all endpoints?
- Are endpoints (e.g., laptops, desktops, servers) configured with host-based firewalls?

## 6.2. Patch management

- Is there a formal patch management policy covering operating systems, applications, and firmware?
- How quickly are critical or high-severity patches applied?

## 6.3. Secure configuration

- Does the organization follow a secure baseline or benchmark (e.g., CIS Benchmarks) for servers, workstations, and network devices?
- Are administrative tools (e.g., PowerShell, Remote Desktop) restricted and monitored?

## 6.4. Vulnerability scanning

- Is vulnerability scanning performed on a regular schedule (internal and external)?
- How are vulnerabilities prioritized for remediation, and what is the typical remediation timeline?

# 7. Application & software development

## 7.1. Secure software development lifecycle

- Are security requirements integrated into the SDLC, including design, development, testing, and deployment?
- Is code reviewed for security weaknesses (e.g., peer code reviews, automated static analysis)?

## 7.2. Application testing

- Do you conduct regular penetration testing or code scanning for critical applications?
- Are open-source or third-party components scanned for known vulnerabilities?

## 7.3. Change management

- Is there a formal change control process to document, assess, and approve changes?
- Are changes tested and reviewed for security impact before implementation?

## 7.4. Encryption & key management

- Is sensitive data encrypted at rest and in transit?
- How are encryption keys generated, stored, and rotated?
- Are industry standards (e.g., AES-256) used for encryption?

# 8. Physical & environmental controls

## 8.1. Facilities security

- Are physical access controls (e.g., badges, biometric readers) in place for sensitive areas?
- Is there a visitor management process (badges, escorts, logs)?

## 8.2. Equipment protection

- Are critical devices (servers, networking equipment) located in secure areas with restricted access?
- Is environmental control (temperature, humidity) and fire suppression available in data centers?

## 8.3. Monitoring & surveillance

- Are CCTV or other surveillance systems in place, and are footage logs retained for a defined period?
- Is on-premises security staffed or monitored 24/7?

# 9. Incident management & response

## 9.1. Incident response plan

- Is there a documented incident response plan (IRP) detailing roles, responsibilities, and procedures?
- How often is the IRP tested (e.g., tabletop exercises, simulations)?
- Is there a defined process for breach notification to regulators and affected parties?

## 9.2. Detection & reporting

- Are intrusion detection tools and logs actively monitored to identify potential incidents?
- Is there a clear process for employees to report suspected security events?

## 9.3. Forensics & investigation

- Does the organization have internal forensic capabilities or retain third-party expertise?
- Are investigation procedures documented and tested, including evidence handling?

# 10. Business continuity & disaster recovery

## 10.1. Business impact analysis (BIA)

- Has the organization conducted a BIA to identify critical processes and define RTO and RPO?
- When was the last BIA review or update conducted?

## 10.2. Business continuity plan (BCP)

- Is there a documented BCP addressing continuity strategies for essential functions?
- Are BCP tests or exercises conducted at least annually?

## 10.3. Disaster recovery (DR)

- Is there a DR plan with defined recovery procedures for critical systems and data?
- Are backups performed regularly, tested, and stored securely offsite?
- Have recovery time (RTO) and recovery point objectives (RPO) been defined and tested?

# 11. Security awareness & training

## 11.1. Training program

- Is there a formal security awareness program for all employees and contractors?
- How frequently is cybersecurity training provided (e.g., onboarding, annual refreshers)?

---

## 11.2. Phishing & social engineering

- Are regular phishing simulation campaigns conducted to measure and improve employee resilience?
- Is there a mechanism for employees to report suspicious emails or messages?

---

## 11.3. Role-based training

- Do employees in specialized roles (e.g., developers, administrators) receive additional security training relevant to their duties?
- Are training records maintained for auditing and compliance purposes?

# 12. Logging, monitoring & metrics

## 12.1. Logging policies

- Are critical system and application logs retained for a defined period (e.g., 90 days, 1 year)?
- Is log collection centralized (e.g., using a SIEM or log management tool)?

---

## 12.2. Monitoring & alerts

- Are real-time alerts configured for critical events or threshold breaches?
- Are logs reviewed regularly by trained personnel, with suspicious events escalated promptly?

---

## 12.3. Security metrics & reporting

- Are key security metrics (e.g., patch compliance, incident response time) tracked and reported to management?
- Does the organization have defined KPIs or KRIs (Key Performance/ Risk Indicators) for cybersecurity?

# 13. Cloud security

## 13.1. Cloud service provider selection

- Are cloud providers vetted for compliance with relevant security frameworks (e.g., SOC 2, ISO 27017)?
- Do contractual agreements with cloud providers address data security, privacy, and breach notifications?

## 13.2. Cloud architecture & responsibilities

- Is there a clear understanding of the shared responsibility model between the organization and the cloud provider?
- How are network and endpoint security controls extended to cloud environments?

## 13.3. Data security in the cloud

- Are encryption and key management processes implemented in cloud services?
- Are cloud-based workloads regularly scanned for vulnerabilities?

# 14. Emerging threats & continuous improvement

## 14.1. Threat intelligence

- Does the organization subscribe to threat intelligence feeds or participate in information-sharing communities (e.g., ISACs)?
- Is there a process to integrate threat intelligence into security controls and risk assessments?

## 14.2. Continuous improvement

- Are lessons learned from incidents, audits, or assessments used to update security policies and procedures?
- Does the organization periodically benchmark against industry best practices or peers?

# Final review & action plan

## 15.1. Risk prioritization

- Which risks discovered during the assessment are deemed highest priority?
- What are the timelines and resources required to address these risks?

## 15.2. Management sign-off

- Who (roles or individuals) will review and approve the security assessment findings?
- Is there a defined process for escalating unresolved high-risk issues to executive management?

## 15.3. Ongoing governance

- How will progress on remediation items be tracked, reported, and validated?
- When will the next assessment or review take place (continuous assessment, annual formal review, etc.)?

Additional resources

# Checklist for key documents

Use this table as a quick-reference to request or verify documents mentioned in the questionnaire. Adjust as needed.

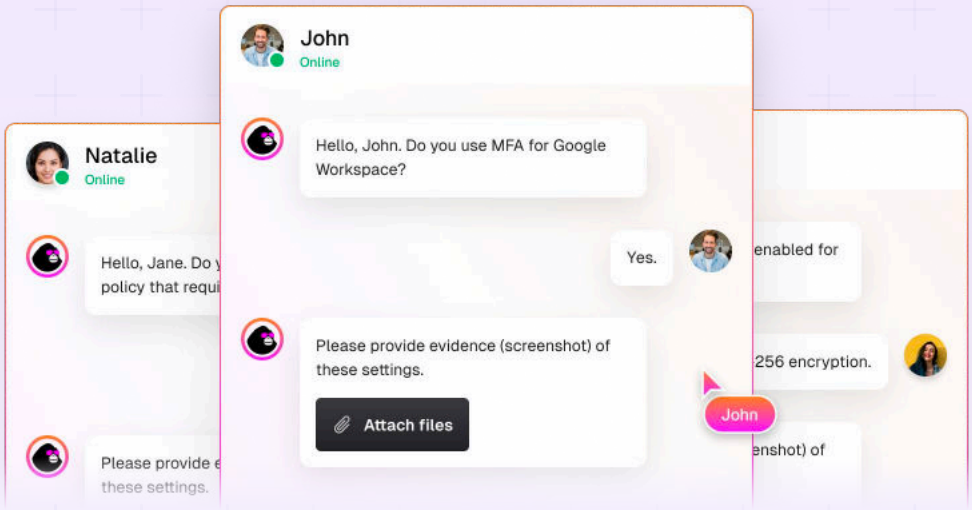
| Document / Certification | Requested | Received |
|---|---|---|
| Corporate registration / Legal certificates | ☐ | ☐ |
| Financial statements (last 2-3 years) | ☐ | ☐ |
| ISO 27001 certification | ☐ | ☐ |
| SOC 2 type II report (or equivalent) | ☐ | ☐ |
| PCI-DSS attestation (if applicable) | ☐ | ☐ |
| GDPR/Data protection policy | ☐ | ☐ |
| Information security policy & procedures | ☐ | ☐ |
| BCP/DR plan & testing reports | ☐ | ☐ |
| Incident response plan | ☐ | ☐ |
| Vendor/Subcontractor management policies | ☐ | ☐ |
| Latest penetration test report | ☐ | ☐ |
| Risk assessment & treatment plan | ☐ | ☐ |

Additional resources

# Roles & responsibilities matrix

Below is a sample matrix to illustrate who in your organization should review or approve different parts of the questionnaire.

| Role | Responsibility | Action required |
|---|---|---|
| IT Security Lead | Review technical security controls & incident response processes | Ensures vendor aligns with internal security standards |
| Compliance Officer | Check regulatory adherence (DORA, GDPR, etc.) | Confirms documentation & certifications are valid |
| Procurement Manager | Oversee vendor sourcing & contract negotiations | Coordinates distribution, collects responses, arranges follow-ups |
| Legal Counsel | Validate contractual clauses, ensure no legal risks or liabilities | Reviews contract addendums, compliance with data protection laws |
| Risk Management Officer | Conduct overall risk rating (high/medium/low) | Determines if additional oversight or mitigations are needed |
| Executive Sponsor | Ultimate approval of critical vendor relationships | Signs off on final decisions (e.g., proceed/terminate) |




# 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