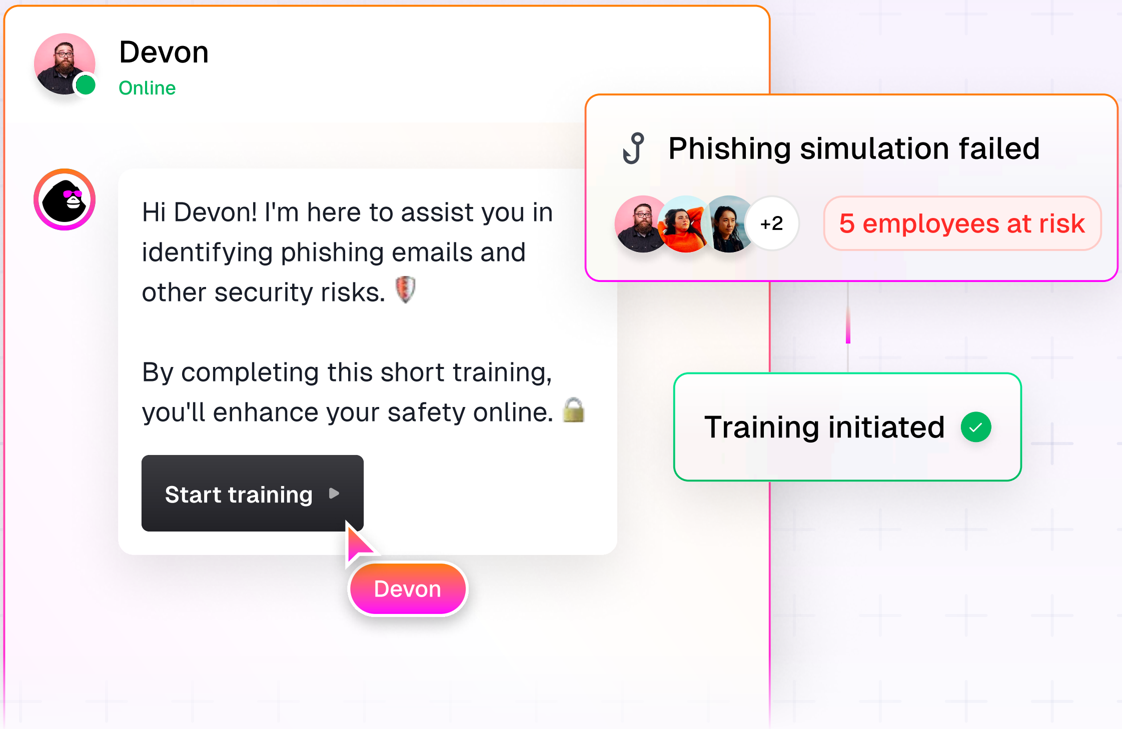
Cyber Upgrade

Questionnaire

Third-party security questionnaire template

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



Devon
Online

Hi Devon! I'm here to assist you in identifying phishing emails and other security risks. 🛡️

By completing this short training, you'll enhance your safety online. 🔒

How to use this questionnaire

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

① Distribute

- Identify all vendors or third parties delivering critical services or handling sensitive data.
- Send them a copy of this questionnaire, requesting a completion deadline.

② Collect

- Gather responses in a standardized format (fillable PDF or editable Word doc).
- Maintain a central repository (e.g., a vendor management system) to track and archive responses.

③ Review & score

- Evaluate each response for completeness, accuracy, and risk level (e.g., high, medium, low).
- Compare answers against your internal policies, regulatory requirements (DORA), and industry best practices.

④ Follow-up

- For any incomplete or concerning answers, schedule a follow-up discussion or ask for additional documentation.
- If major gaps are identified, consider on-site audits, pen tests, or partial remedial measures.

⑤ Document & decide

- Summarize key findings in a risk assessment report.
- Determine whether the vendor meets your risk appetite and if additional controls or contractual clauses are needed.

⑥ Ongoing monitoring

- Re-issue or refresh this questionnaire periodically (annually or at contract renewal).
- Track updates to the vendor's security posture, certifications, or incident history.

1. General & corporate Information

1.1 Legal entity & registration

- Please provide the legal name of your organization, address, and registration details.
- Indicate your organizational structure (e.g., parent company, subsidiaries).
- Please provide the primary contacts for contract management, compliance, security, and escalation.

1.2 Business profile & services

- Describe the services and/or products you will be providing.
- Outline how these services integrate with or support our critical business functions.

1.3 Financial stability

- Provide a summary of your organization’s financial status or relevant financial statements.
- Have you experienced any significant financial difficulties in the past 3 years? If so, please describe.

1.4 Compliance readiness

- List relevant regulatory frameworks and standards you are currently compliant with (e.g., ISO 27001, SOC 2, PCI-DSS, GDPR).
- Do you have a dedicated compliance or governance team overseeing adherence to these standards?

2. Governance & organizational resilience

2.1 Governance framework

- How is your information security governance structured (e.g., committees, executive oversight, reporting lines)?
- Do you have board-level or senior management sponsorship of operational resilience and cybersecurity programs?

2.2 Policy & procedures

- Please provide or summarize your security policies (e.g., information security policy, acceptable use policy, supplier management policy).
- How often are policies reviewed and updated?

2.3 Risk management program

- Describe your enterprise risk management methodology and framework.
- How do you identify, assess, and document ICT and operational risks relevant to the services you provide?
- Do you conduct periodic risk assessments? How frequently, and who oversees these?

2.4 Roles and responsibilities

- Describe the roles and responsibilities for security, resilience, and compliance within your organization.
- Provide an overview of staff training and awareness programs related to cybersecurity and resilience.

3. ICT security & risk management

3.1 ICT infrastructure overview

- Describe your ICT architecture, including on-premises data centers, cloud environments, and major applications.
- Are you using any cloud service providers? If so, which ones, and for what functions?

3.2 Access control & identity management

- How are user accounts, privileges, and roles managed and revoked in your systems?
- Do you enforce multi-factor authentication (MFA) for all critical system access?

3.3 Network & system security

- Which methods do you use to segment your network?
- Do you perform regular vulnerability scanning and penetration testing? Please describe frequency and scope.
- How do you secure remote access for staff or subcontractors?

3.4 Data encryption & protection

- Do you encrypt data at rest and in transit? Please specify protocols and algorithms used.
- How do you manage encryption keys? Are Hardware Security Modules (HSMs) used?

3.5 Logging & monitoring

- Describe your logging, monitoring, and alerting capabilities (e.g., SIEM solutions).
- How do you detect and respond to potential intrusions or anomalies in real time?

3.6 Malware & threat protection

- What anti-malware, intrusion detection, or intrusion prevention systems do you use?
- How frequently are these tools updated and tested?

4. Physical security

4.1 Facility security

- Describe how you secure your physical premises (e.g., badge access, guards, surveillance cameras).
- Do you have a documented process for facility access management (visitor logs, authorized personnel)?

4.2 Hardware & equipment protection

- How do you secure servers, networking equipment, and backup media in your data centers or server rooms?
- Do you maintain any hardware in shared colocation facilities? If yes, how do you ensure physical segregation?

5. Data protection & privacy

5.1 Data classification & handling

- Do you follow a data classification scheme (e.g., public, internal, confidential, highly confidential)?
- How do you ensure data is handled according to its classification level?

5.2 Privacy regulations & compliance

- If handling personal data, how do you ensure compliance with GDPR or other relevant privacy laws?
- Do you have processes for handling data subject requests (e.g., right to access, erasure)?

5.3 Data retention & disposal

- What is your data retention policy for sensitive or business-critical data?
- How do you securely dispose of or sanitize data (digital and physical media)?

5.4 Data location & transfers

- In which jurisdictions is data stored, processed, or transmitted?
- How do you comply with cross-border data transfer requirements (e.g., Standard Contractual Clauses, adequacy decisions)?

6. Incident & crisis management

6.1 Incident response plan

- Do you have a formal incident response plan? How often is it tested and updated?
- Describe your procedures for detecting, responding to, containing, and remediating security incidents.

6.2 Incident escalation & reporting

- How quickly do you notify customers (including our organization) of potential or actual incidents that affect their data or operations?
- Describe your internal escalation paths for incident management.

6.3 Post-incident review & lessons learned

- Do you have a formal process for post-incident analysis and reporting?
- How do you incorporate lessons learned into your security controls and training?

7. Business continuity & disaster recovery

7.1 BCP & DR plans

- Provide an overview of your Business Continuity Plan (BCP) and Disaster Recovery (DR) strategy.
- What are the Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) for critical services?

7.2 Resilience testing

- How often do you test your BCP and DR plans (e.g., tabletop exercises, simulations, full failover tests)?
- Are test results reviewed by senior management, and how are improvements tracked?

7.4 Redundancy & high availability

- Do you have redundant systems, data centers, or cloud availability zones to mitigate single points of failure?
- How do you ensure continuous operations during maintenance or partial failures?

7.5 Supply chain continuity

- If you rely on subcontractors, how do you ensure their business continuity capabilities align with yours?
- Have you assessed potential single points of failure or concentration risk within your supply chain?

8. Third-party & subcontractor management

8.1 Downstream vendor oversight

- Do you outsource or subcontract any critical functions related to the services you will provide to us?
- How do you assess and monitor the security posture of your subcontractors?

8.2 Contractual obligations

- Do you have clauses in place requiring subcontractors to adhere to specific security and resilience standards?
- How do you ensure their compliance with DORA-like requirements?

8.3 Notification requirements

- How do you handle communication and reporting regarding incidents or significant changes in subcontractors’ security posture?

9. Compliance & regulatory alignment

9.1 Regulatory frameworks

- Are you aware of your obligations under DORA when providing services to financial entities?
- Which other regulatory standards (e.g., EBA Guidelines on ICT and security risk management) do you follow?

9.2 Audit & certification

- Do you have any relevant certifications or audits (e.g., ISO/IEC 27001, SOC 1/SOC 2 Type II)? Please provide recent reports or attestations.
- How frequently do you engage external auditors or conduct internal compliance audits?

9.3 Legal & contractual requirements

- Are there any known legal or regulatory proceedings or compliance issues in the past 5 years?
- How do you ensure contractual obligations regarding security, data protection, and resilience are met?

10. Testing & vulnerability management

10.1 Vulnerability scanning

- How often do you perform vulnerability scanning on networks, systems, and applications?
- How do you prioritize and remediate identified vulnerabilities?

10.2 Penetration testing

- Do you conduct regular penetration tests (external/internal)?
- How do you address the findings from these tests, and are results shared with clients?

10.3 Secure development practices (if applicable)

- Describe your Secure Software Development Lifecycle (SSDLC) practices.
- Which security testing (e.g., code reviews, static/dynamic analysis) do you conduct for internally developed software?

|** 11. Security awareness & training

11.1 Employee training programs

- Describe your cybersecurity and data protection training programs for employees, contractors, and third parties.
- How often is training conducted and refreshed?

11.2 Phishing & social engineering

- Do you conduct simulated phishing or social engineering tests?
- How do you address repeated failures or high-risk indicators among staff?

11.3 Insider threat management

- Do you have controls in place to monitor and mitigate insider threats (e.g., user behavior analytics)?

12. Monitoring & ongoing oversight

12.1 Continuous monitoring

- Do you employ continuous monitoring tools or processes to track changes in your environment?
- How do you maintain visibility into real-time security events?

12.2 Performance & SLA monitoring

- How do you monitor and report on service-level agreements (SLAs), uptime, and performance metrics?
- What is your procedure for SLA breach notifications and remediation?

12.3 Periodic reporting

- Will you provide regular updates or reports on your security posture, risk assessments, and incident statistics?
- How frequently will you provide these reports?

13. Exit strategy & service termination

13.1 Termination planning

- How is data returned, transferred, or destroyed at the end of the contract?
- Do you have a formal plan to ensure minimal disruption if the service is terminated unexpectedly?

13.2 Transition assistance

- Will you provide migration or transition support if we move to another vendor or bring the service in-house?
- How do you ensure knowledge transfer and timely handover of documentation?

14. Additional documentation & attestations

14.1 Supporting documents

- Please attach or reference any relevant policies, procedures, audit reports, penetration test summaries, or certifications.

14.2 Attestation & signature

- Please confirm that the information provided in this questionnaire is accurate and complete.
- Provide contact details for the person(s) responsible for answering additional due diligence questions.

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)

Additional resources

Critical questions or red flags

In reviewing the completed questionnaire, pay particular attention to the following high-impact items. A negative or unclear response in any of these areas might indicate significant risk or require immediate follow-up:

① Lack of established governance

- No formal security policies, unclear risk management framework, no senior management oversight.

② Weak incident response capability

- No documented IR plan, slow or vague notification timelines, or no post-incident reviews.

③ Missing or outdated certifications

- No recent SOC/ISO audits, outdated or invalid certificates, suspicious refusal to provide audit reports.

④ Poor data protection measures

- No clear data classification, uncertain encryption practices, or non-compliance with GDPR.

⑤ Insufficient business continuity/DR

- No tested BCP/DR plan, incomplete failover strategies, or uncertain RTO/RPO.

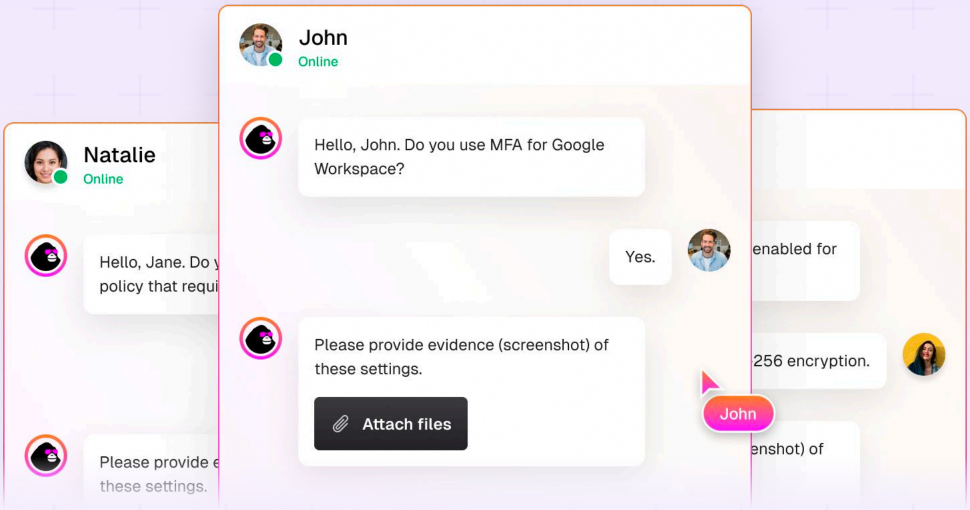
⑥ Unclear subcontractor oversight

- Failure to vet downstream service providers, unknown compliance statuses, or no contractual flow-down clauses.

⑦ Financial instability or legal/regulatory proceedings

- Vendor under investigation, recent bankruptcies, or multiple legal disputes.

If any of these red flags are identified, consider a heightened due diligence process or alternative service providers.



Hello, Jane. Do y
policy that requi

Please provide e
these settings.

Hello, John. Do you use MFA for Google Workspace?

Yes.

Please provide evidence (screenshot) of these settings.

enabled for

256 encryption.

enshot) of

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