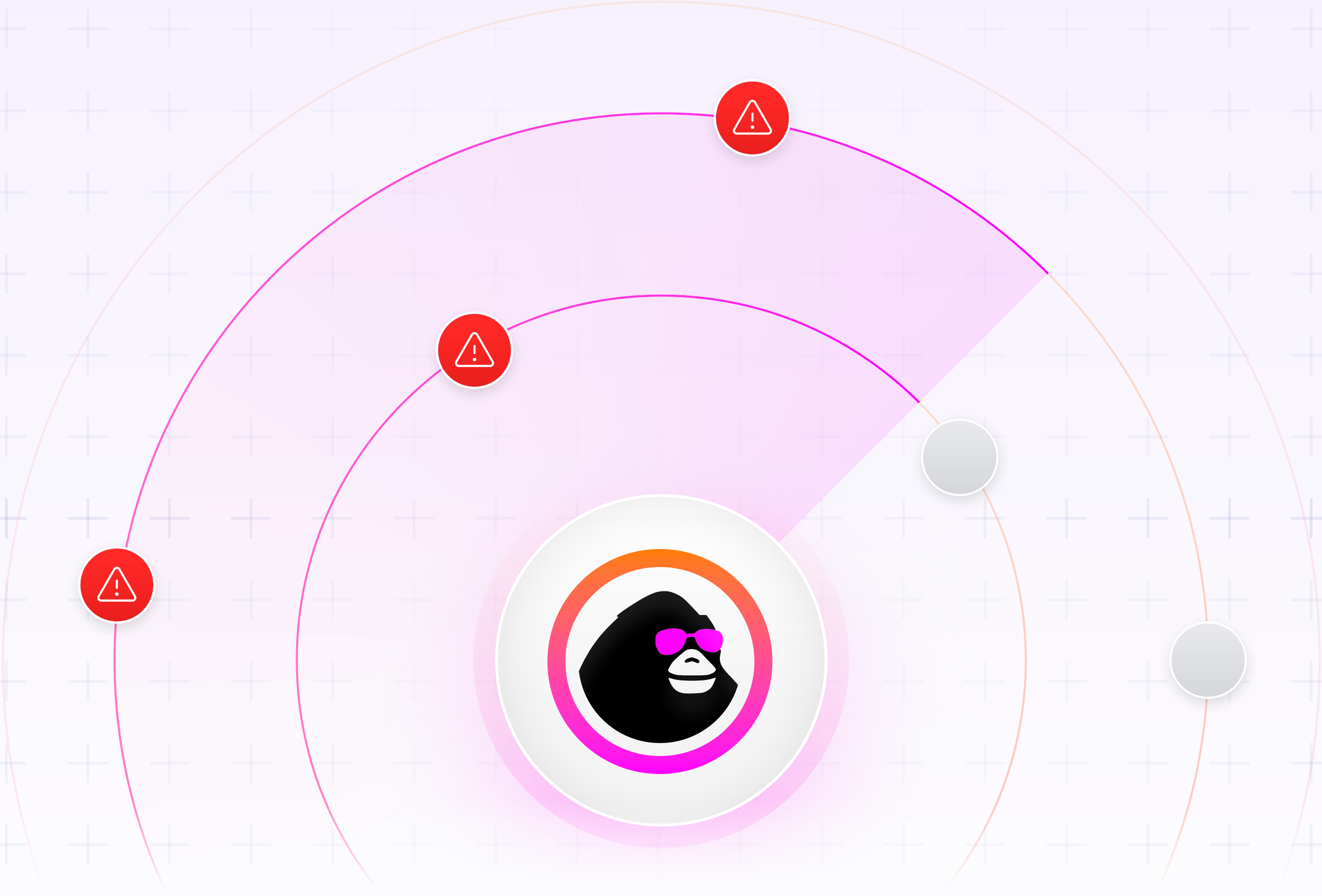
Cyber Upgrade

Template

SaaS security 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. Customize Questions

Tailor the questions to align with your organization’s specific regulatory and industry requirements (e.g., HIPAA, PCI DSS, GDPR). Remove sections that aren’t relevant.

2. Distribute to Vendors

Send the questionnaire to the SaaS provider as part of the initial due diligence or procurement process.

3. Request Evidence

For critical controls, request evidence such as documented procedures, certifications, or redacted architecture diagrams to confirm that controls are in place.

4. Evaluate Responses

Assess the completeness and clarity of responses. Follow up on any unclear or insufficient answers. If needed, conduct an on-site visit or request a live demonstration of critical controls.

5. Incorporate into Contracts

If moving forward with a vendor, ensure that important security requirements (e.g., breach notification timelines, DR capabilities, etc.) are included in contract language.

1. Organizational Security & Governance

1.1 Security Policies & Governance

- Do you maintain written information security policies (ISP) covering confidentiality, integrity, and availability of data?
  - Request copies of relevant security policies if appropriate.
- How often are your security policies reviewed and updated?
- Is there an internal security governance board or committee responsible for overseeing information security?
- How do you communicate security policies and expectations to your employees, contractors, and partners?

1.2 Information Security Roles & Responsibilities

- Do you have a dedicated Chief Information Security Officer (CISO) or equivalent role?
- Are there specific security roles and responsibilities assigned across the organization (e.g., data privacy officer, incident response lead)?
- What training do employees receive regarding information security and data privacy?

1.3 Risk Management

- Describe your risk assessment process. How often do you perform risk assessments?
- How do you prioritize remediation items from risk assessments?
- Do you follow any recognized frameworks (e.g., ISO 27001, NIST CSF, SOC 2, CSA STAR)?

2. Human Resources & Personnel Security

2.1 Employee Screening & Onboarding

- Do you conduct background checks on employees before hire?
- What level of background check is performed (e.g., criminal, credit, references)?

2.2 Security Awareness & Training

- Describe your security awareness program.
  - Is training formal, frequent, and mandatory?
- Do employees undergo specific training for secure coding, handling customer data, or privacy?

2.3 Termination or Role Change

- What is your process for revoking system access when employees leave the company or change roles?
- How quickly are access privileges revoked?

3. Compliance & Regulatory Requirements

- Which industry standards, frameworks, or certifications do you hold?
  - Examples: SOC 2 Type II, ISO 27001, PCI DSS, HIPAA, FedRAMP, GDPR compliance.
- Are third-party audit reports (e.g., SOC 2 report, ISO 27001 certification, PCI AoC) available for review?
- How do you handle data subject requests (e.g., under GDPR, CCPA)?

4. Data Protection & Privacy

4.1 Data Classification & Handling

- How do you classify and label sensitive, confidential, and public data?
- What methods are used to protect data in transit and at rest (e.g., encryption algorithms, key management)?

4.2 Data Residency & Geolocation

- Where will our data be stored geographically (e.g., data centers, cloud regions)?
- Does your service offer data residency options for specific regions (e.g., EU)?

4.3 Data Retention & Disposal

- How long is data retained? Can customers define retention policies?
- What is your process for secure data disposal (e.g., wiping or destruction methods)?

4.4 Privacy & Consent

- Do you use personal data for analytics, marketing, or other secondary purposes? If yes, how do you manage user consent?
- Do you have a process for handling privacy-related inquiries or user requests (e.g., data subject access requests)?

5. Infrastructure & Network Security

5.1 Cloud Infrastructure Overview

- Which cloud service provider(s) or data centers do you use?
- How is your infrastructure segmented to prevent lateral movement between different environments (e.g., dev, test, production)?

5.2 Network Security Controls

- Do you use firewalls, IDS/IPS systems, or other perimeter security controls?
- How do you monitor network traffic for anomalies or suspicious activity?
- Do you have a documented network architecture diagram you can share (redacted if necessary)?

5.3 Configuration & Patch Management

- How do you ensure servers, applications, and other components are securely configured (e.g., hardening guidelines)?
- Describe your patch management process and timelines.

5.4 DDoS & Threat Protection

- What measures are in place to protect against DDoS attacks?
- Do you leverage a Web Application Firewall (WAF) or Content Delivery Network (CDN)?

6. Application Security

6.1 Secure Development Lifecycle (SDLC)

- Describe your SDLC. At which stages do you incorporate security reviews or threat modeling?
- How do you ensure secure coding practices (e.g., code reviews, static/dynamic analysis)?

6.2 Testing & Vulnerability Management

- Do you perform regular penetration tests or vulnerability assessments?
- How quickly do you address discovered vulnerabilities?
- Do you have a bug bounty or responsible disclosure program?

6.3 Third-Party & Open-Source Components

- What is your process for tracking and patching vulnerabilities in open-source or third-party libraries?
- How do you evaluate and monitor the security posture of your critical suppliers or partners?

7. Access Control & Identity Management

7.1 Authentication Mechanisms

- Which authentication methods do you support (e.g., SSO, MFA, OAuth)?
- Do you enforce strong password policies?

7.2 Authorization & Role-Based Access

- How are user privileges managed and enforced within the application?
- Is there support for role-based or attribute-based access control?
- Can customers customize role definitions and permissions?

7.3 Privileged Access Management (PAM)

- Who has administrative or privileged access to customer environments or data?
- How are privileged accounts monitored and logged?

7.4 Session Management

- How are user sessions handled (timeout, re-authentication requirements, session tokens)?
- What safeguards are in place to prevent session hijacking?

8. Logging, Monitoring & Incident Response

8.1 Logging & Monitoring

- Which events are logged (e.g., authentication, data access, configuration changes)?
- How long are logs retained? Are logs protected against tampering?
- Do you provide customers with audit logs or activity reports?

8.2 Security Monitoring & Detection

- Do you have a SIEM or similar system for real-time security event monitoring?
- How often are logs or alerts reviewed by a security team?

8.3 Incident Response & Notification

- Do you have a formal incident response plan? How often is it tested?
- What is your process for notifying customers if a security incident involves their data?
- Do you have defined SLAs for incident response and communication?

9. Business Continuity & Disaster Recovery

9.1 Business Continuity Planning (BCP)

- Do you have a documented BCP addressing critical resources, staff, and processes?
- When was the last time your BCP was tested, and what were the results?

9.2 Disaster Recovery (DR)

- Where is customer data backed up (e.g., offsite, cross-region)?
- What are your RTO (Recovery Time Objective) and RPO (Recovery Point Objective) commitments?
- How frequently do you test your disaster recovery plan?

9.3 Redundancy & High Availability

- Does your architecture include redundancy or failover for critical components?
- What SLAs or uptime guarantees do you offer?

10. Physical & Environmental Security

- Where are your physical data centers located? Are they owned or leased (e.g., colocation, cloud)?
- Describe the physical security controls in place (e.g., biometrics, CCTV, guards, locked cages).
- How do you handle visitor management and physical access logs?
- Are environmental controls (e.g., HVAC, fire suppression) in place and tested?

11. Vendor & Third-Party Management

- Do you outsource any part of your service (e.g., payment processing, data storage, support)?
- How do you evaluate and monitor the security posture of critical vendors?
- Do you flow down contractual security requirements to your subcontractors or partners?

12. Customer Control & Responsibilities

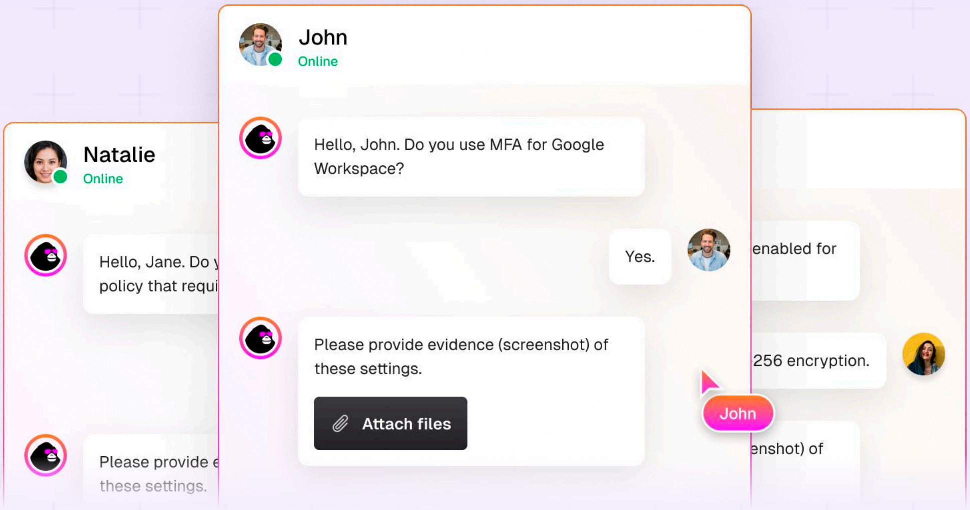
- Which security configurations can customers manage (e.g., encryption settings, access roles, logging)?
- Do you provide guidelines or best practices for customers to securely deploy and use the service?
- What responsibilities do customers retain for data protection, encryption, or compliance?

13. Insurance & Liability

- Do you carry cybersecurity insurance?
- Does your insurance cover data breaches or incidents that impact customers?
- Are you open to contractually defining liability limits for security incidents?

14. Additional Documentation & References

- Provide copies or summaries of relevant certifications (e.g., SOC 2, ISO 27001).
- Include any policy excerpts or publicly available security resources.
- Offer references or customer testimonials that speak to your security posture.



Natalie
Online

Hello, Jane. Do y
policy that requi

Please provide e
these settings.

John
Online

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