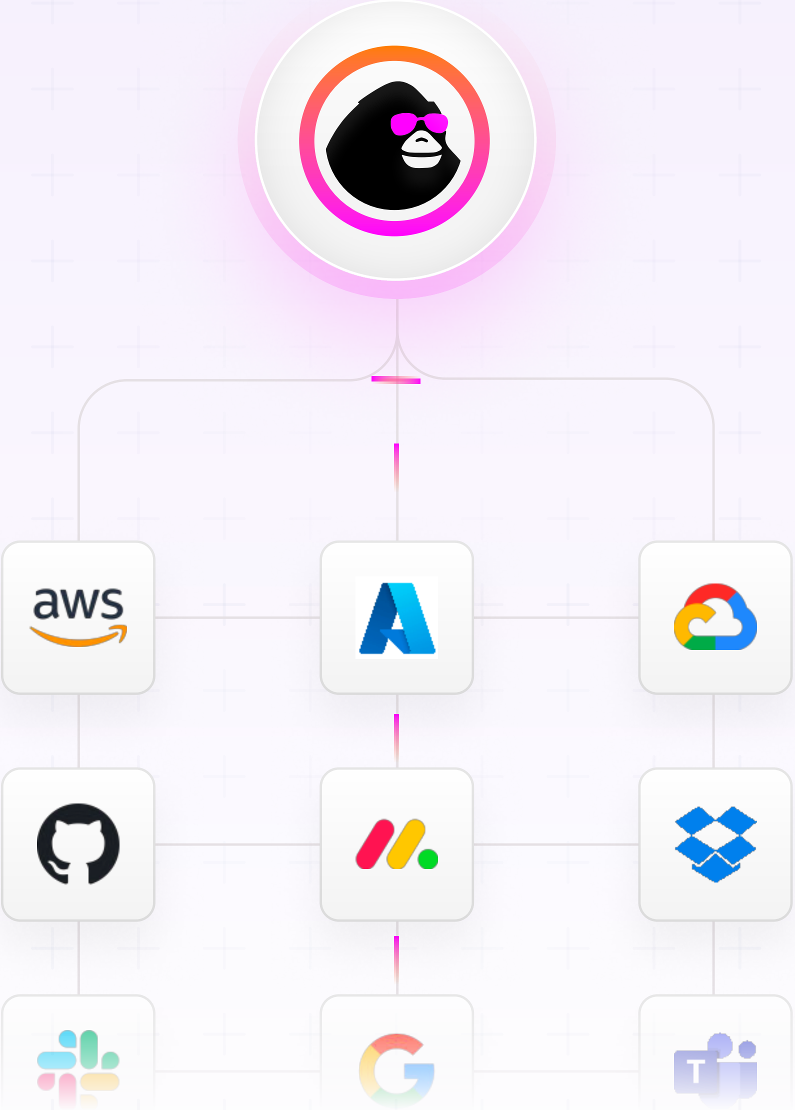
Cyber Upgrade

Template

Cloud security risk 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. Customize

Tailor the questions to match the unique requirements of your organization. This can include adding specialized questions for industries like healthcare, finance, or government.

2. Prioritize

Focus on the highest-risk areas based on your context. For example, if your organization handles sensitive personal information, give priority to data encryption, data residency, and privacy sections.

3. Analyze gaps

Map each question to a control objective or compliance requirement (e.g., ISO 27001: A.12.1.1). This helps you quickly see if the cloud provider meets the control or if remediation steps are required.

4. Document

Document the answers in a formal assessment report. Highlight any concerns, recommended actions, and deadlines for remediation.

5. Follow up

Request clarifications or remediation plans for weak areas.

1. General & Organizational Overview

1.1. Service Description

- What specific cloud services (IaaS, PaaS, SaaS) do you offer or are you consuming?
- What geographical regions do you operate in (data centers, offices, etc.)?

1.2. Organizational Governance

- Do you have a formal security governance structure (e.g., a Chief Information Security Officer, Security Steering Committee)?
- How often are security policies and standards reviewed and updated?

1.3. Compliance and Regulatory Requirements

- 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?

1.4. Security Policies & Procedures

- Do you have documented cloud security policies?
- How do you ensure employees, contractors, and third parties understand and follow these policies?

1.5. Risk Management Program

- Do you have a formal risk management program (risk assessment, risk treatment, risk acceptance)?
- How do you ensure continuous risk assessment and mitigation?

2. Infrastructure & Architecture

2.1. Data Centers & Physical Security

- Where are your primary data centers located? Are secondary (backup) data centers located in different regions?
- What physical security measures are enforced at each data center (access controls, CCTV, guards, etc.)?

2.2. Isolation & Multi-Tenancy

- Do you have a formal security governance structure (e.g., a Chief Information Security Officer, Security Steering Committee)?
- How often are security policies and standards reviewed and updated?

2.3. Network Design & Segmentation

- Can you describe the network design and segmentation strategies (VPCs, subnets, firewalls, SDN)?
- How are external connections secured (VPN, dedicated lines, secure gateways)?

2.4. Virtualization/Container Security

- What type of virtualization or container technology is used?
- How do you ensure hypervisor/container security?
- Do you have controls to prevent breakout or privilege escalation between virtual machines or containers?

3. Data Management & Protection

3.1. Data Classification

- Do you have a data classification policy (e.g., public, internal, confidential, restricted)?
- How is data classified, labeled, and handled in the cloud environment?

3.2. Data Encryption

- Is data encrypted at rest? What encryption algorithms and key lengths are used?
- How is data encrypted in transit? What protocols (TLS versions, cipher suites) are supported?
- How are encryption keys generated, stored, and managed? Do you use Hardware Security Modules (HSMs)?

3.3. Data Residency

- Can you specify the location(s)/regions where data is stored?
- Are there options for customers to choose data residency for compliance reasons?

3.4. Data Retention & Deletion

- What is your data retention policy?
- How do you ensure secure data deletion (both logical and physical) upon contract termination?

3.5. Data Backup & Recovery

- What backup methods are used, and how frequently are backups performed?
- Where are backups stored, and how are they protected?
- How do you test backup restoration processes?

4. Identity & Access Management (IAM)

4.1. Authentication & Authorization

- What IAM solutions or services are used (e.g., integrated directory, SSO, federated identity solutions)?
- Do you support MFA/2FA for admin and user access?

4.2. Privilege Management

- How do you handle privileged user accounts and access (role-based access control, time-bound privileges)?
- Are separate administrative accounts used for admin tasks vs. normal activities?

4.3. Account Provisioning & Deprovisioning

- What is the process for creating, modifying, and revoking access for users and administrators?
- How quickly can you revoke access if a security risk is identified?

4.4. Logging & Monitoring of IAM

- Do you log all authentication and authorization attempts?
- How do you monitor for anomalous access patterns?

5. Network Security & Connectivity

5.1. Perimeter Security

- What perimeter security controls do you have in place (firewalls, WAFs, IDS/IPS)?
- Are these services or devices managed by the provider or the customer?

5.2. Segmentation & Zoning

- Are production, staging, and development environments separated?
- How are different network zones (DMZ, internal, external) segregated?

5.3. Secure Communications

- Which secure protocols are enforced for administration and data transfer (e.g., SSH, TLS)?
- What measures are used to prevent eavesdropping, man-in-the-middle, or session hijacking attacks?

5.4. Remote Access

- How is remote administrative access to the cloud environment secured?
- Do you use VPN, jump boxes/bastion hosts, or other secure remote connectivity solutions?

6. Logging, Monitoring, & Incident Response

6.1. Logging & Audit Trails

- What logs are collected (system, network, application, IAM events)?
- How long are logs retained, and where are they stored?
- Are logs protected from tampering or unauthorized access?

6.2. Security Monitoring & Alerting

- Do you have Security Information and Event Management (SIEM) or Extended Detection & Response (XDR) solutions in place?
- How quickly are alerts generated and responded to?
- Is there 24/7 monitoring by an in-house or outsourced Security Operations Center (SOC)?

6.3. Secure Communications

- Is there a formal Incident Response (IR) plan in place?
- How do you report and escalate security incidents to customers, and what is the SLA for incident notification?

6.4. Forensic Capabilities

- Are forensic images or logs preserved in the event of a security incident or investigation?
- Does the provider have a documented procedure for digital forensics?

7. Vulnerability & Patch Management

7.1. Vulnerability Scanning & Penetration Testing

- How often do you perform internal and external vulnerability scans?
- Do you allow customers to conduct or commission their own penetration testing? Under what conditions?

7.2. Patch Management

- How frequently do you apply patches and updates to the underlying infrastructure (OS, hypervisor, firmware)?
- What is the typical timeline for applying critical security patches?

7.3. Configuration Management

- Are secure baseline configurations applied to servers, network devices, and virtual machines?
- How are configuration changes tracked, tested, and approved (configuration control process)?

7.4. Disclosure of Vulnerabilities

- What is your process for disclosing vulnerabilities to customers, and how quickly do you typically notify them?

8. Business Continuity & Disaster Recovery

8.1. BC/DR Strategy

- Is there a documented business continuity and disaster recovery plan?
- How often is it tested, and are test results available for review?

8.2. Recovery Time Objective (RTO) & Recovery Point Objective (RPO)

- What are the stated RTO and RPO for each critical service?
- Have you met these objectives in past tests or actual incidents?

8.3. High Availability & Redundancy

- Are systems deployed in a high-availability configuration across multiple availability zones or regions?
- How do you ensure redundancy of critical infrastructure (network, power, cooling, etc.)?

8.4. Failover & Contingency Plans

- What is the failover process in the event of a major outage at a primary site?
- How are clients notified and supported during a failover or DR event?

9. Third-Party & Supply Chain Security

9.1. Vendor Management

- Do you use subcontractors or third-party providers for critical services (data storage, support, maintenance)?
- How do you assess the security of your third-party vendors?

9.2. SLAs and Security Clauses

- Do you maintain contractual SLAs for uptime, data handling, and incident response times?
- Are there specific security clauses in place that bind subcontractors to the same requirements?

9.3. Audits & Assessments

- Are vendors required to undergo regular audits, such as SOC 2 or ISO 27001?
- How are their compliance certifications validated and tracked?

9.4. Supply Chain Risk

- What processes are in place to identify and mitigate supply chain risks (hardware, software, network equipment)?

10. Application Security (for PaaS/SaaS)

10.1. Secure Development Lifecycle (SDLC)

- Do you follow a formal SDLC with security checkpoints (e.g., code reviews, static analysis, dynamic testing)?
- Which coding standards and frameworks do you use for secure development?

10.2. API Security

- Do you maintain contractual SLAs for uptime, data handling, and incident response times?
- Are there specific security clauses in place that bind subcontractors to the same requirements?

10.3. Application Vulnerability Management

- How do you manage application vulnerabilities discovered during scanning or testing?
- How frequently are applications tested for vulnerabilities (SAST, DAST, SCA)?

10.4. Supply Chain Risk

- Are secure configurations and best practices (e.g., OWASP Top Ten) applied by default?
- How is configuration drift monitored and corrected?

11. Privacy & Legal Considerations

11.1. Data Privacy

- How do you ensure compliance with data privacy regulations (GDPR, CCPA, etc.)?
- Do you offer Data Processing Agreements (DPAs) that clarify roles and responsibilities for data protection?

11.2. Legal Jurisdiction

- Which legal jurisdictions apply to the services?
- How do you handle requests for data from law enforcement or government agencies?

11.3. Customer Responsibilities

- Which security controls are the responsibility of the provider vs. the customer under a shared responsibility model?
- Are there clear definitions of liabilities, remedies, and indemnifications in the contract?

11.4. Breach Notification

- In the event of a data breach, what is the defined timeline for notifying customers?
- What information will be provided in a breach notification (scope, impacted data, remediation steps)?

12. Security Awareness & Personnel

12.1. Employee Screening & Onboarding

- Do you conduct background checks for employees with access to customer data or systems?
- How do you manage role-based access for new hires?

12.2. Security Awareness Training

- Do you conduct regular security awareness training for all employees?
- Are specialized training provided for staff with privileged or technical responsibilities?

12.3. Contractor & Third-Party Access

- How do you ensure contractors or third parties adhere to the same security standards?
- Are NDAs or security clauses part of the engagement contract?

12.4. Employee Offboarding

- What is the process for disabling accounts, retrieving access tokens, and recovering assets when an employee leaves?

13. Ongoing Governance & Reporting

13.1. Security Governance Meetings

- How often do you hold security governance or oversight meetings?
- Do customers have access to governance reports or dashboards?

13.2. Reporting & Metrics

- What key security metrics (KPIs/KRIs) do you track (e.g., mean time to detect, mean time to respond)?
- Do you provide regular security or compliance reports to customers?

13.3. Continuous Improvement

- How are post-incident reviews conducted, and do they feed into updated processes or technology investments?
- Do you have a roadmap for future security enhancements?

13.4. Customer Security Assessments

- Can customers or their auditors schedule on-site or virtual security assessments of your controls?
- What artifacts are you willing to share (policies, procedures, network diagrams)?

14. Final Considerations & Sign-Off

14.1. References & Documentation

- Can you provide references or case studies of customers with similar security or compliance needs?
- Are detailed architectural diagrams and control mappings (e.g., CCM from Cloud Security Alliance) available?

14.2. Clarifications & Exceptions

- Are there any known exceptions to the security policies or deviations from recommended controls?
- How do you track, approve, and periodically review these exceptions?

14.3. Contractual & SLA Review

- Has legal counsel reviewed the Master Service Agreement (MSA), Service Level Agreement (SLA), and Data Processing Agreement (DPA)?
- Do you agree to security and compliance audits as stipulated by the contract?

13.4. Sign-Off & Next Steps

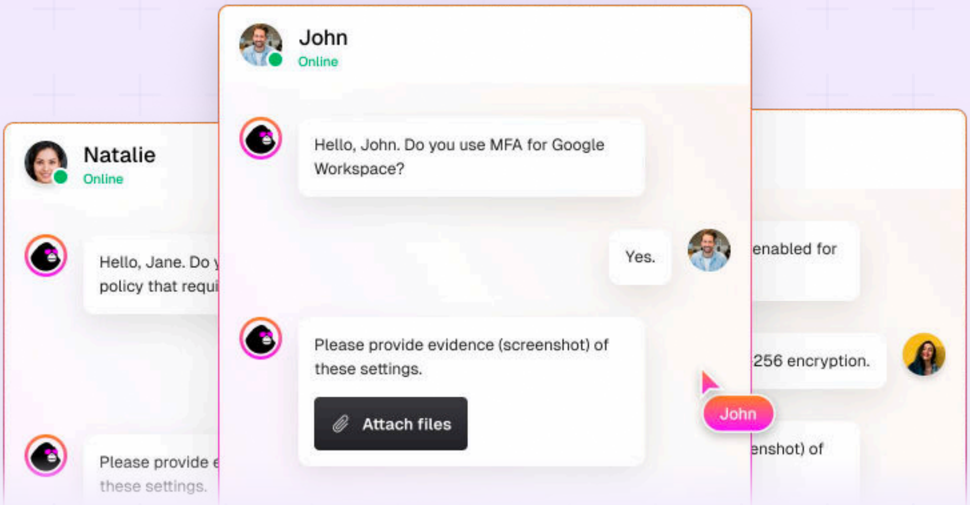
- Confirm that all questions have been answered accurately.
- Provide a timeline for any outstanding items or follow-up actions.

Additional resources

Checklist for key documents

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

Document / Certification	Document / Certification	Checked
Information Security Policy	Outlines the organization’s security goals, scope, and responsibilities.	□
Cloud Architecture Diagram(s)	High-level view of network layout, data flows, and segmentation.	□
Risk Management & Governance Policy	Defines risk identification, assessment, and treatment processes.	□
Data Classification & Handling Guidelines	Specifies classification levels and handling rules (e.g., encryption, retention).	□
Incident Response Plan	Provides detection, escalation, containment, and recovery procedures.	□
IAM Policy & Procedures	Covers user/privileged account management, MFA requirements, deprovisioning.	□
Vulnerability & Patch Management Policy	Outlines scanning frequency, patch rollout process, and remediation timelines.	□
Business Continuity & Disaster Recovery Plan	Documents RTO/RPO, failover strategies, and backup/restore processes.	□
Vendor Management & Third-Party Agreements	Describes requirements and SLAs for external providers and subcontractors.	□
Compliance / Audit Reports	Examples: ISO 27001 certificate, SOC 2 Type II, PCI DSS AoC.	□



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