Vendor Risk Assessment Questionnaire

40-question security assessment for third-party suppliers

Use this questionnaire to evaluate the security posture of third-party vendors and suppliers. It covers organisational security, data protection, access controls, incident management, business continuity, and compliance. Adapt questions based on vendor risk tier.

Prepared by: Nuvencia — Information Security Advisory

Author: Jaouhar Mosbahi, CISSP, CCSP, ISO 27001 LI/LA

Version: 1.0 — February 2026

Classification: Template — Customise for your organisation

This template is provided by Nuvencia for guidance purposes. Organisations should customise it to reflect their specific context, risk appetite, and regulatory requirements.

© 2026 Nuvencia. All rights reserved.

A. Organisation and Governance

Q1. Does your organisation have a dedicated information security function or officer?

Response:

Q2. Do you maintain documented information security policies that are reviewed at least annually?

Response:

Q3. Is your organisation certified to ISO 27001, SOC 2, or equivalent security standard?

Response:

Q4. Do you conduct regular risk assessments of your information assets and systems?

Response:

Q5. Do you maintain cyber liability insurance? If yes, what is the coverage amount?

Response:

B. Data Protection and Privacy

Q6. How do you classify and handle data based on sensitivity levels?

Response:

Q7. Is data encrypted at rest and in transit? Specify encryption standards used.

Response:

Q8. Where is our data stored geographically? Do you use sub-processors?

Response:

Q9. What is your data retention and secure deletion policy?

Response:

Q10. How do you ensure compliance with GDPR and other applicable data protection regulations?

Response:

© 2026 Nuvencia. All rights reserved.

Q11. Can you provide a Data Processing Agreement (DPA) if required?

Response:

C. Access Control

Q12. Do you enforce multi-factor authentication (MFA) for all system access?

Response:

Q13. How do you manage user provisioning and de-provisioning?

Response:

Q14. Do you conduct regular access reviews? How frequently?

Response:

Q15. Do you enforce the principle of least privilege?

Response:

Q16. How do you manage privileged access accounts?

Response:

D. Network and Infrastructure Security

Q17. Do you perform regular vulnerability scanning and penetration testing?

Response:

Q18. How do you manage patching and remediation of vulnerabilities?

Response:

Q19. Do you use intrusion detection/prevention systems (IDS/IPS)?

Response:

© 2026 Nuvencia. All rights reserved.

Q20. How do you segment your network to isolate client environments?

Response:

Q21. Do you use endpoint detection and response (EDR) solutions?

Response:

E. Security Operations

Q22. Do you have a Security Operations Centre (SOC) or equivalent monitoring capability?

Response:

Q23. What logging and monitoring tools do you use?

Response:

Q24. How long do you retain security logs?

Response:

Q25. Do you perform regular security awareness training for employees?

Response:

Q26. How frequently do you conduct phishing simulations?

Response:

F. Incident Management

Q27. Do you have a documented incident response plan?

Response:

Q28. What is your process for notifying clients of security incidents?

Response:

Q29. What is your committed notification timeline for data breaches?

© 2026 Nuvencia. All rights reserved.

Response:

Q30. Have you experienced any security breaches in the past 24 months? If yes, describe.

Response:

Q31. Do you conduct post-incident reviews and implement corrective actions?

Response:

G. Business Continuity

Q32. Do you have a documented business continuity and disaster recovery plan?

Response:

Q33. What are your Recovery Time Objective (RTO) and Recovery Point Objective (RPO)?

Response:

Q34. How frequently do you test your DR plan?

Response:

Q35. Do you maintain geographically separated backups?

Response:

H. Compliance and Audit

Q36. What security certifications or attestations do you hold?

Response:

Q37. Can you provide your most recent SOC 2 Type II report or ISO 27001 certificate?

Response:

Q38. Do you allow client-initiated security assessments or audits?

Response:

© 2026 Nuvencia. All rights reserved.

Q39. How do you manage compliance with regulatory requirements applicable to our data?

Response:

Q40. Do you have a process for tracking and remediating audit findings?

Response:

© 2026 Nuvencia. All rights reserved.