Cybersecurity self-assessment questionnaire template

- 1. Who is responsible for cybersecurity in your organisation?
- 2. Do you have a chief information security officer (CISO)?
- 3. Do you regularly meet, across company departments, to discuss and monitor cybersecurity issues?
- 4. How do you protect customer information? Please be specific.
- 5. How are cybersecurity incidents reported?
- 6. Have you ever experienced a significant cybersecurity incident? Please define and describe the incident.
- 7. When was last time you had a cybersecurity assessment performed by a third-party organisation? What were the results?
- 8. What were the results of your most recent vulnerability assessment or penetration test?
- 9. Do you outsource any IT or IT security functions to third-party service providers? If so, who are they, what do they do, and what type of access do they have?
- 10. What types of cybersecurity policies do you have in place in your organisation today?
- 11. How frequently are your employees trained on your IT security policies, and do you use automated assessments?

Need help answering a cybersecurity self-assessment?

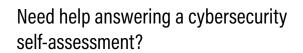
Get in touch for guidance

CONTACT US





- 12. Have you developed secure configurations for hardware and software?
- 13. How do you continuously assess and remediate your organisation's cyber vulnerabilities?
- 14. How do you assess the security of the software that you develop and acquire?
- 15. Do you have a data recovery capability? Including recovery from ransomware/ crypto locking. Please provide specific details.
- 16. Do you have automated tools that continuously monitor to ensure malicious software is not deployed?
- 17. Describe the processes and tools you use to reduce and control administrative privileges.
- 18. Do you blacklist or whitelist communications?
- 19. What processes do you have in place to prevent the exfiltration of sensitive data, particularly sensitive customer data?
- 20. What types of physical protection do you have in place to prevent unauthorised access to data or infrastructure assets?
- 21. How do you manage remote access to your corporate network?
- 22. How do you monitor for unauthorized personnel, connections, devices, and software?
- 23. Describe the process you have in place to communicate to us security incidents affecting our data.



Get in touch for guidance

CONTACT US



