Cyber Security Risk Survey (CSRS)

CyberRiskPMC

Wednesday, October 25, 2023

Cyber Security Risk Survey (CSRS)

This is the Cyber Security Risk Survey (CSRS) conducted by Cyber Risk PMC, a division of Peter Moore Consulting. It is designed to identify the level of understanding and management of cyber risk in your company. It is aligned with the international standard, "ISO/IEC 27001:2022 Information technology, cybersecurity and privacy protection - Information security management systems - Requirements" (the Standard). It addresses the knowledge of cyber in your organization and assists in the improvement of the governance of your company, as well as integrating cyber risk into your enterprise risk management framework. The survey will take approximately 20 minutes to complete, following which you can submit the form and it will be received by Peter Moore Consulting who will provide feedback directly to you.

SECURITY

THIS FORM IS SECURE AS IT IS OPENED USING SSL SECURITY (HTTPS IN YOUR BROWSER). ADDITIONALLY, THE FORM IS ENCRYPTED USING AN ENCRYPTION KEY ONLY AVAILABLE TO PETER MOORE CONSULTING. THIS MULTI-LAYER SECURITY ENSURES THE INFORMATION YOU PROVIDE REMAINS SECURE AND CONFIDENTIAL.

Terms and Conditions of Use

This Cyber Security Risk Survey (CSRS) is designed to identify level of knowledge, understanding and management of cyber risk in your company or organization, and assist in the improvement of your Information Management Security System (ISMS). It will also assist in identifying your current level of cyber resilience and areas for improvement in the governance of your company regarding cyber risks and the potential impact to your business.

It has been designed against industry best practice and the international standard for information security, cybersecurity and privacy protection, ISO/IEC 27001:2022 (the Standard). This evaluation does not provide a complete assessment of all the risks in your company. To meet ISO 27001 standards, you will need a detailed risk assessment.

This is not an audit.

Detailed technical auditing is carried out by our technology partner, Netlink Group Pty Ltd.

Peter Moore Consulting
September 2023

Company/ Organization	ABC Corporation Ltd
Your Name	John Smith
Role	Chief Executive Officer
Email	ceo@abc.com

A. Policy and Governance

Commence (Click on the button to start the survey)

1. Does your company have a Cyber Security Policy?

Yes

2. If the answer to the above question is Yes, how often is it reviewed and updated?

Annually

3. Is your Cyber Security Policy integrated into your Information Security Management System (ISMS)?

Not sure

4. If the answer to the above question is Yes, how often is your ISMS reviewed and updated?

5. Does your Cyber Security Policy address; email management, online information sharing, management of sensitive data, handling of technology, standards for social media and internet access, incident management, and staff training and education ?

Not sure

6. Does your company have a policy for the use of Artificial Intelligence (AI) software tools (i.e., ChatGPT)?

No

7. If the answer to the above question is Yes, how often does your company review its AI Usage Policy?

8. Does your company have external third party reviews and audits on your Information Security Management System (ISMS) and cyber risk exposure?

Yes

9. If the answer to the above question is Yes, how often do external reviews occur?

10. Does your company have a Ransomware Negotiation Strategy?

Not sure

11. If the answer to the above question is Yes, have you considered engaging an external Ransomware Negotiator ?

Page Break

B. Cyber risk knowledge and experience	**Click on the button to commence this section of the survey.**
12. Is the Board and Executive fully aware of the implications of information breaches and theft through cyber attacks (i.e., breach of the law, litigation, financial impact, operational disruption, reputation impact)?	Yes
13. If the answer to the above question is Yes, how often does the Board review its internal knowledge base and skill level around cyber security?	Annually
14. Is there an awareness and training process in place for educating Board members and the Executive on cyber risk ?	Not sure
15. If the answer to the above question is Yes, how often is training carried out ?	
16. Is the Board and Executive fully aware of the implications of potential information breaches, loss of intellectual property, and breaches of law through the use of AI tools and software in the company?	Not sure
17. If the answer to the above question is Yes, how often is the Board and Executive kept up to date and informed on the use of AI software tools in the company?	
18. Do employees in the company currently use AI tools?	No
19. If the answer to the above question is No or Not sure, does your company plan to formally use AI tools in the business?	Undecided

20. If your staff currently use AI do they have guidance and training on the use of AI through policies, procedures and guidelines?	Not sure
21. If the answer to the above question is No or Not sure, does your company plan to train staff on the use of AI in the business?	
22. Has your company experienced a cyber attack?	No
23. If the answer to the above question is Yes, how recent was the attack?	
24. If the answer to question 22 is Yes, how long did it take to fully recover from the attack (operationally and financially)?	

Page Break

C. Cyber Risk Management

Click on the button to commence this section of the survey.

25. Does your company currently adopt and follow international standards such as ISO 27001:2018 (Information security ISMS) and ISO 27001:2022 (Information security, cybersecurity and information privacy)?

Yes

26. If the answer to the above question is Yes, what role in your company is responsible for their implementation, adherence to, and review?

Other

27. What role in your company is responsible for cyber security and information management security?

Other

28. If the answer to the above question was Other, what role is currently responsible for cyber security and information security management in your company?

Chief Financial Officer

29. When conducting information management security management system (ISMS) risk assessments and reviews are the scope, context and criteria established and/ or reviewed?

Not sure

30. How often are ISMS risk assessments and risk reviews carried out?

As and when required

31. During the risk assessment process (risk analysis and evaluation) does the company use a Risk Appetite and Risk Tolerance Statement as guidance regarding what actions to take in managing risks?

Not sure

32. During the risk evaluation process (after identification and assessment), is risk transfer used as part of the risk treatment process?

Not sure

33. Does your company have cyber insurance in place to manage cyber risks in the event of a cyber attack?

Yes

34. If the answer to the above question is Yes, how often is the risk coverage in your cyber insurance policy reviewed?

35. If the answer to question 33 Yes, are you aware of the specific exclusions in the policy such as the exclusion of ransom payments?

Not sure

36. Does your company have a policy of using Multi Factor Authentication (MFA) as part of the control framework for managing authentication theft?

Yes

37. Does your company have a Password Management Policy as part of the suite of controls to manage information and cyber risk?

Not sure

38. Does your company have controls in place for remote working and end point point device management (such as VPN's, anti virus/ anti malware software, MFA login to the corporate network?)

Yes

39. Does your company utilise internal or external services for data backup and data security?

Combination of both

40. Following cyber and ISMS risk assessments, are the outcomes reported to the Board for consideration regarding adherence and compliance to the company's policies?

Sometimes

41. Following cyber and ISMS risk assessments are the outcomes communicated to relevant stakeholders such as staff within the company?

Mostly

42. Is the company's cyber risk profile monitored and reviewed?

Not sure

43. If the answer to the above question is Yes, how often is the cyber risk profile reviewed?

44. Is the ISMS and cyber risk assessment and management process integrated into the company's Enterprise Risk Management Framework and systems?

Partially

45. If the answer to the above question is Not Sure or No, do you intend to integrate cyber security risk management into your Enterprise Risk Management framework and system?

Page Break

D. Confidentiality of sensitive data

Click on the button to commence this section of the survey.

46. Does your company have a policy and process for the management of confidential and sensitive data such as Personally Identifiable Information (PII)?	Yes
47. If the answer to the above question is Yes, how often are these documents reviewed and updated?	Annually
48. Does your company have a process of categorising data such as; secret, confidential, business use only and public?	Not sure
49. If the answer to the above question is Yes, what role in your company is responsible for the categorisation of data?	
50. Does your company encrypt secret or confidential data during the transmission of documents across the internet?	Yes
51. If the answer to the above question is Yes, is this done internally or through a Managed Service Provider (MSP)?	Managed by external MSP
52. If the answer to the above question is Yes, what is the name of your MSP?	XYZ IT Services Pty Ltd

Page Break

E. Cyber compliance

Click on the button to commence this section of the survey.

53. Is the Board aware of its obligations with regard to the governance and protection of Personally Identifiable Information (PII) and other private information under Australia's Privacy Protection Act 1988 (Act)?

Partially

54. If the answer to the above question is Yes (fully or partially), does the Board review its obligations of managing, securing, and maintaining PII and other private information within its obligations under the Act ?

Not sure

55. If the answer to the above question is yes, how often does the Board review its obligations under the Privacy Act, 1988?

56. Is cyber security incorporated into the company's Corporate Governance Framework?

Partially

57. If the answer to the above question is Yes fully or Partially, how frequently is the Corporate Governance Framework reviewed?

Annually

58. Does your company have procedures for the collection of evidence in the event of a cyber attack and data breach?

Not sure

59. Does your company have a formal and documented process to report material cyber attacks resulting in data breaches to the authorities such as; the Australian Cyber Security Centre (ACSC), the Australian Federal Police (AFP), and the Office of the Australian Information Commissioner (OAIC) ?

Yes

60. If the answer to the above question is Yes, what role in your company is responsible for reporting material cyber attacks and data breaches where confidential information and PII is compromised or stolen?

Chief Executive Officer (CEO)

Page Break

F. Incidence response, business continuity, disaster recovery	**Click on the button to commence this section of the survey.**
61. Does your company have an Incident Response Plan (IRP) in the event of a cyber attack?	No
62. If the answer to the above question is Yes, how often is it reviewed, tested and updated?	
63. Does your company have Business Continuity Plan (BCP) in the event of a cyber attack?	Yes
64. If the answer to the above question is Yes, how often is it reviewed, tested and updated?	Annually
65. Does your company have Disaster Recovery Plan (DRP) in the event of a cyber attack?	Not sure
66. If the answer to the above question is Yes, how often is it reviewed, tested and updated?	
67. Who is responsible for the development of the IRP, BCP and DRP in your company?	

Page Break

G. Supply chain cyber risk management

Click on the button to commence this section of the survey.

68. Does your company utilise the services of a Managed Service Provider (MSP) to manage data management and cyber security?

Yes

69. If the answer to the above question is Yes, how often does your company review the Terms and Conditions (such as Service Level Agreements) in the contract with your MSP?

Annually

70. Has a risk assessment been carried out on third party providers of IT services such as cloud based software, cloud data storage providers, or your MSP (if utilising the services of one)?

Not sure

71. If the answer to the above question is Yes, how often does your company review information management and cyber risks associated with the use of third party IT service providers?

Page Break

H. Human resource management, cyber awareness, training and education

Click on the button to commence this section of the survey.

72. Does your company have a screening process for personal employed in managing sensitive, private and confidential data (i.e., Police background checks)?

Yes

73. Does your company have a process of induction and training for personnel managing information assets?

Yes

74. Does your company have Terms and Conditions of employment utilising acceptable use policies for the use of computers, internal corporate networks, data assets and the internet?

Not sure

75. Does your company have a process of segregation of duties regarding the handling and management of information assets?

Not sure

76. Does your company have non-disclosure agreements for personnel managing information assets?

Yes

77. Does your company maintain an inventory of information assets?

Not sure

78. Does your company have a process of "lessons learned" following cyber incidents?

Not sure

79. Does your company have a cyber awareness, training and education system in place for your staff?

Yes

80. If the answer to the above question is Yes, how often is carried out?

As and when required

Page Break

I. Cyber risk awareness, cyber vulnerability and cyber resilience

Click on the button to commence this section of the survey.

81. On a scale of 1-10, indicate your CURRENT level of cyber risk and threat KNOWLEDGE AND UNDERSTANDING (1 being the lowest and 10 being the highest).

6

82. On a scale of 1-10, indicate your DESIRED or PLANNED level of cyber risk and threat KNOWLEDGE AND UNDERSTANDING in twelve months time (1 being the lowest and 10 being the highest.

10

83. On a sliding scale from 0 - 100, with 100 being the highest level of potential threat (move the slider bar with cursor or finger), what is your CURRENT level of CYBER RISK EXPOSURE?

80

84. On a sliding scale from 0 - 100 with 0 being the lowest level of potential threat (move the slider bar with cursor or finger), what is your DESIRED or PLANNED level of CYBER RISK EXPOSURE in twelve months' time?

15

85. On a sliding scale from 0 - 100 with 0 being the lowest and 100 being the highest, what is your CURRENT level of CYBER RESILIENCE?

60

86. On a sliding scale from 0 - 100 with 0 being the lowest and 100 being the highest, what is your PLANNED level of CYBER RESILIENCE in twelve months' time?

90

Page Break

J. General

Click on the button to commence this section of the survey.

87. Specific questions or comments in relation to cyber risk security?

What is the best control framework to use when conducting cyber risk assessments?

88. Can we provide further assistance?

Yes, please provide a report on the outcome of this survey to assist us increase our cyber resilience.

Double click to edit...

How do you rate this survey regarding its ability to assist your company improve your cyber risk awareness and cyber risk management?

★★★★★

Double click to edit...

Completion

Click on the button to commence this section of the survey.

Double click to edit...

Please sign the form using mouse input from computer or touch pen/ finger for touch screen devices (for the purpose of non-repudiation).

Double click to edit...