Type here]

IISRI
Independent Information Security Rating Institute

Cyber Security Rating Report

[XXXXX]

Date: xx.xx.2022

xxxxxx
CISSP, CISM, PCI-DSS QSA, ISO27001 LA, ISO27701 LI, PECB MSA

DISCLAIMER

IISRI® DO NOT GUARANTEE THE ACCURACY, COMPLETENESS, TIMELINESS OR AVAILABILITY OF ANY INFORMATION OR CONTENT OF OUR REPORTS, AND IS NOT RESPONSIBLE FOR ANY ERRORS OR OMISSIONS, REGARDLESS OF THE CAUSE, OR FOR THE RESULT OBTAINED FROM THE USE OF SUCH INFORMATION. IISRI® REPORTS ARE STATEMENTS OF OPINION, BASED ON INTERVIEWS, DOCUMENTATION ANALYSIS, EVIDENCE BASED ON SAMPLING METHODOLOGY. THEREFORE, IISRI® GIVES NO EXPRESS OR IMPLIED WARRANTIES TO YOU (OR ANY OTHER PERSON OR ENTITY) OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE OR USE. ANY INFORMATION OR MATERIAL ON IN THIS REPORT MAY INCLUDE INACCURACIES OR OTHER ERRORS. THIS REPORT IS BY NO MEANS A LEGAL ADVICE AND THEREFORE YOU SHOULD SEEK LEGAL ADVICE BEFORE TAKING ANY FURTHER ACTION

Executive Summary

The security posture of XXXXX has been assessed on XXXX 2022. Based on the audit collateral provided, interviews and observations, the level of information security assurance to protect corporate and customer data is considered to be '**Moderate'**.

Several domains, including Compliance, are well managed and the controls were effective. The security controls in the domains of Network Security, Business Continuity and Disaster Recovery (Resilience) and Supplier Security were ineffective and improvements to manage the risks are recommended.

Based on the IISRI® rating scale (in the appendix), the overall information security rating of XXXXX is:

1. Assessed domains and results

Domain	Rating	Justification
Compliance	A	• XXXXX complies with local regulations (including NZ Privacy Act 2020) as well as with ISO27001. • The performed audit on the effectiveness of controls is limited to a subset of the Annex controls of the standard.
Risk management	BBB	• Risk management practice is in place and a risk register is maintained. • XXX some very high- level risks have not been acted on for a long period of time. • Assessing security risks in projects is done in an inconsistent way and not according to XXX's risk management framework.
Human resources	B	• Background checks and credit checks are performed for permanent staff; not for contractors. • There is no additional vetting process for critical staff members, such as a Ministry of Justice criminal check. • The HR policy hasn't been reviewed since 2019. • Security and privacy awareness training is done ad hoc and not for all staff.
Security testing	CCC	• Penetration testing is conducted once a year, but it is limited to XXX web portals. • Vulnerability scanning is performed monthly, but it also doesn't cover XXXXX internal servers and corporate network.
Endpoint security	BB	• All endpoints have anti-malware software installed. • Bitlocker is only on some devices enabled. • Ports on the endpoints are not disabled, allowing staff to use flash drives and transfer files unauthorised.
Network security	CC	• A Web Application Firewall is used but in passive mode and not actively monitored. • There are no DLP solutions in place, allowing confidential information to leave the organisation. • IDS/IPS systems are turned on, but only on the ingress/egress firewalls. • DDOS protection is in place, but limited to protocol based DDOS attacks.
Access management	C	• There is no defined provisioning and deprovisioning process. • Accounts of former employees have still not been removed from some systems. • User access reviews are performed (error-prone) manually, ad hoc and are limited to XXX systems.
Resilience	C	• XXXXX are not resilient to major interruptions: the implemented redundancy mechanism for XXXX sites have not functioned properly during lockdowns. • BCP has not been tested for the XXX site and backup recovery tests were not performed since 2020.
Supplier security	C	• There is no requirement or process to assess suppliers before engaging with them. • There is no periodic review performed on existing suppliers.
Security incident management	AA	• Logging of all servers is turned on • There is a SIEM solution in place to centrally monitor security events. • There is a practice but not a defined process to manage security incidents effectively.
Asset management	CC	• Various spreadsheets are used with different owners. • Not all assets are recorded in the asset register • There is a classification standard, but assets are not classified.

2. Recommendations

Domain	Rating	Recommendations
Compliance	A	
Risk management	BBB	
Human resources	B	
Security testing	CCC	
Endpoint security	BB	
Network security	CC	
Access management	C	
Resilience	C	
Supplier security	C	
Security incident management	AA	
Asset management	CC	

Appendix A. IISRI® Internal Rating Scale

Rating	Meaning	Mark	Risk
AAA	All information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met.	Excellent	None to minimal
AA	Almost all information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met.	Very good	Very low
A	Almost all information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met. A few specific control weaknesses have been noted. Minor additional work on information security or privacy is recommended.	Good	Low
BBB	Main information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met. A few specific control weaknesses have been noted. Minor additional work on information security or privacy is recommended.	Satisfactory	Low
BB	Main information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met. Some specific control weaknesses have been noted. Moderate additional work on information security or privacy is recommended.	Sufficient	Moderate
B	Some information security and privacy controls are adequate, appropriate, and effective enough to provide reasonable assurance that security and privacy risks are being managed and objectives are met. Many specific control weaknesses have been noted. Major additional work on information security or privacy is highly recommended.	Moderate	Moderate
CCC	Main information security and privacy controls are unlikely to provide reasonable assurance that security and privacy risks are being managed and objectives are met. Major work on information security or privacy is highly recommended.	Insufficient	High
CC	Almost all information security and privacy controls are unlikely to provide reasonable assurance that security and privacy risks are being managed and objectives are met. Major work on information security or privacy is highly recommended.	Very insufficient	High
C	Almost all information security and privacy controls are unlikely to provide reasonable assurance that security and privacy risks are being managed and objectives are met. Major work or complete new program on information security or privacy is required.	Poor	Very high
D	All information security and privacy controls are not providing any assurance that security and privacy risks are being managed and objectives are met. Complete new program on information security and privacy is required.	Very poor	Almost certain

The rating represents the level of information security or privacy assurance of an assessed organisation at a specific moment in time. **The risk score is given under the assumption of an imminent threat and significant impact on the (service of the) organisation.**

Appendix B. IISRI® domains mapped to security standards

Domain	ISO27001	NZISM	NIST CSF
Compliance			
Risk management			
Human resources			
Security testing			
Endpoint security			
Network security			
Access management			
Resilience			
Supplier security			
Security incident management			
Asset management			