REPORT

SECURITY ASSESSMENT

Defend with Confidence

PREPARED FOR
<Company name>
<Date>

nsp.co.nz

NSP
SECURE YOUR FUTURE

TABLE OF CONTENTS

Executive Summary 3

Methodology 4

Frameworks 5

Tools 6

Scope 7

Results 8

- CIS 8

Results 9

- Vulnerability Assessment 9

Recommendations 10

Conclusion 11

Executive Summary

The purpose of a security assessment is to evaluate the effectiveness of security controls and identify potential vulnerabilities that could compromise the confidentiality, integrity, and availability of systems and data.

A security assessment report serves as a valuable resource for stakeholders, offering insights into the current security state and guiding effective decision-making for risk mitigation through actionable recommendations. It is important to note that a security assessment provides a snapshot of the security landscape only for the time of assessment and is subject to change as new vulnerabilities emerge or security controls are modified. To ensure ongoing protection against evolving threats, regular assessments and implementation of proactive security measures are advised.

Company Name findings and recommendations around IT network and security include

KEY FINDINGS

1. Network assessment reveals firewall and network configuration concerns, indicating vulnerabilities.
2. Complexity on vendor management shows lack of accountability and over-reliance.

RECOMMENDATIONS

1. Improve network design to ensure the AOR network remains operational, during AT network incidents and to strengthen overall security posture.
2. Implement monitoring solutions and processes to detect network and security anomalies.
3. Improve service management and implement change management processes with your partners.

Methodology

At NSP, we use a four phase approach for strengthening our customer's security postures. The model that drives this approach is called the **Security Maturity Lifecycle 4A Model** and consists of Assess, Analyse, Advise and Activate.

We will start this journey to a secure future with a security assessment conducted by our Chief Information Officer (CISO). Our CISO can oversee and tie together your organisational security requirements and help define your information security posture.

Key activities carried out in the report:

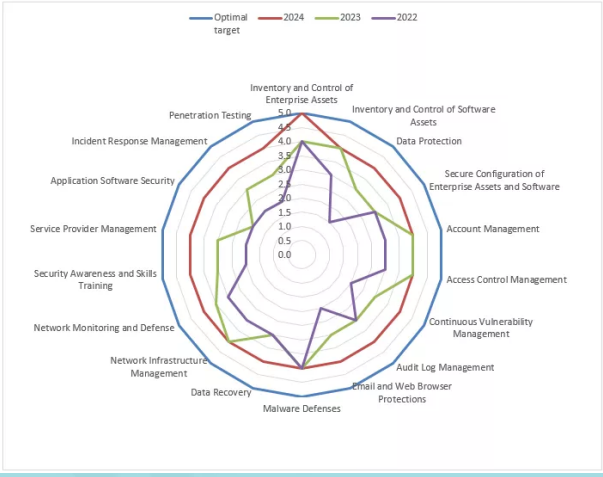
- Understanding what the current security position is and what the risks are. Determining where you want to be by considering your internal business goals and and risk appetite, along with any applicable laws, regulations, standards and best practices you need to follow.
- Assessments carried out by our CISO using cybersecurity frameworks such as Centre for Information Security (CIS) and NIST.

Frameworks

NSP security assessments involve the use of the following industry standard frameworks and activities

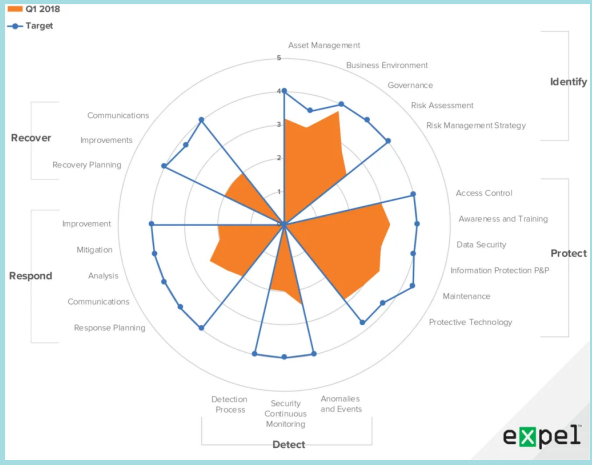
CIS

Developed by SANS with the goal of facilitating solutions for information security. CIS is a straightforward framework viewed by many as being the most practical or prescriptive approach. CIS is perhaps more technical focused than the NIST or ISO, yet no less reliable. Categories in lude basic, foundational and organisational.



NIST

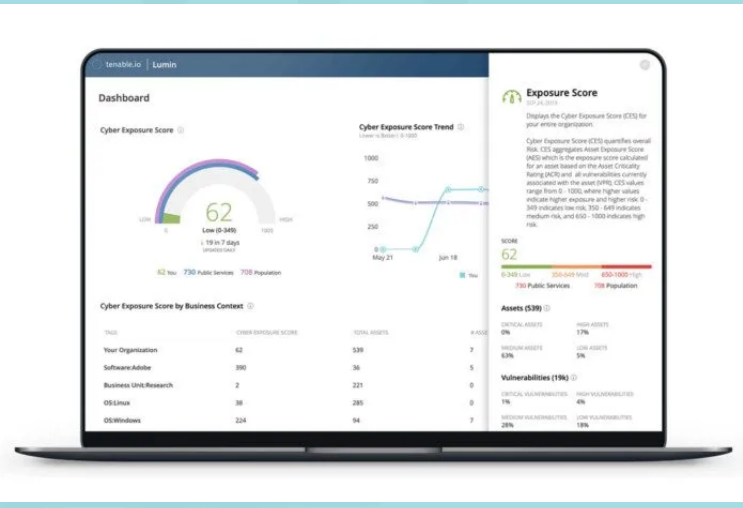
Designed by the U.S. federal government but most widely used by American companies, NIST is considered the gold standard. Small and modest-sized organisations may also find it intimidating in scope, and resource-intensive to keep up. Categories include identify, protect, detect, respond and recover.



Tools

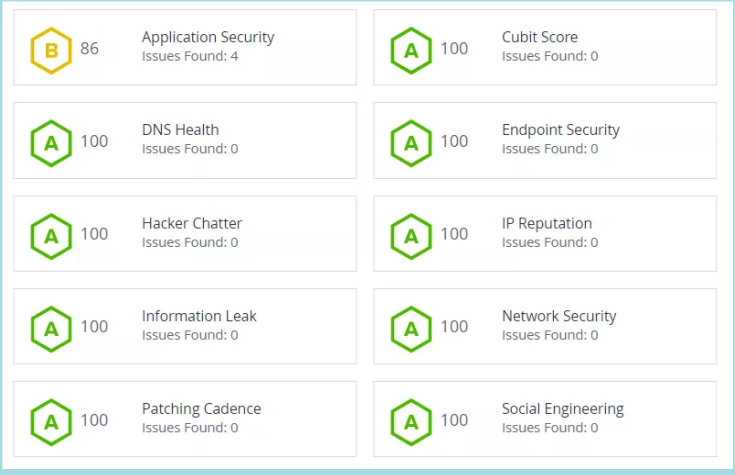
VULNERABILITY SCANNING

Vulnerability scanning is crucial for cybersecurity, identifying weaknesses in IT infrastructure. This datasheet outlines its benefits: reducing the attack surface, enhancing security posture, and ensuring compliance. With automated tools and detailed insights, organizations can strengthen defenses against threats.



MATURITY SCORECARD

The NSP 5 security pillars categorize CIS and NIST controls into key areas: people security, data security, infrastructure security, crisis management, and physical security. They work together to mitigate vulnerabilities, protect data, and respond effectively to crises, providing a holistic approach.



Scope

The security assessment for Company Name aimed to identify potential threats and vulnerabilities within your existing IT infrastructure environment with the aim of prioritising effective mitigation efforts based on likelihood and impact. Ongoing monitoring and regular risk assessments are recommended to ensure continued effectiveness. Please note that the risk assessment provides a snapshot of risks at the time of assessment and may require periodic updates to address emerging threats.

IDENTIFY	RATE	RECOMMEND	PRIORTISE
Evaluate security controls in terms of effectiveness, highlighting weaknesses / gaps. (CIS / NIST) Secure Scorecard Vulnerability Scan	Rate risks in terms of likelihood of occurring, operational impact, affect on reputation, and impact on compliance requirements.	Recommend mitigations for all risks.	Prioritise risk mitigations based on severity, exploitability, impact, data confidentiality concerns, system integrity and system availability.

Note: Since a security assessment is based on a snapshot of risks at the time of assessment, it is recommended that ongoing monitoring and assessment be put in place to address future emerging threats.

Results

CIS

The Company Name external security posture is xxx

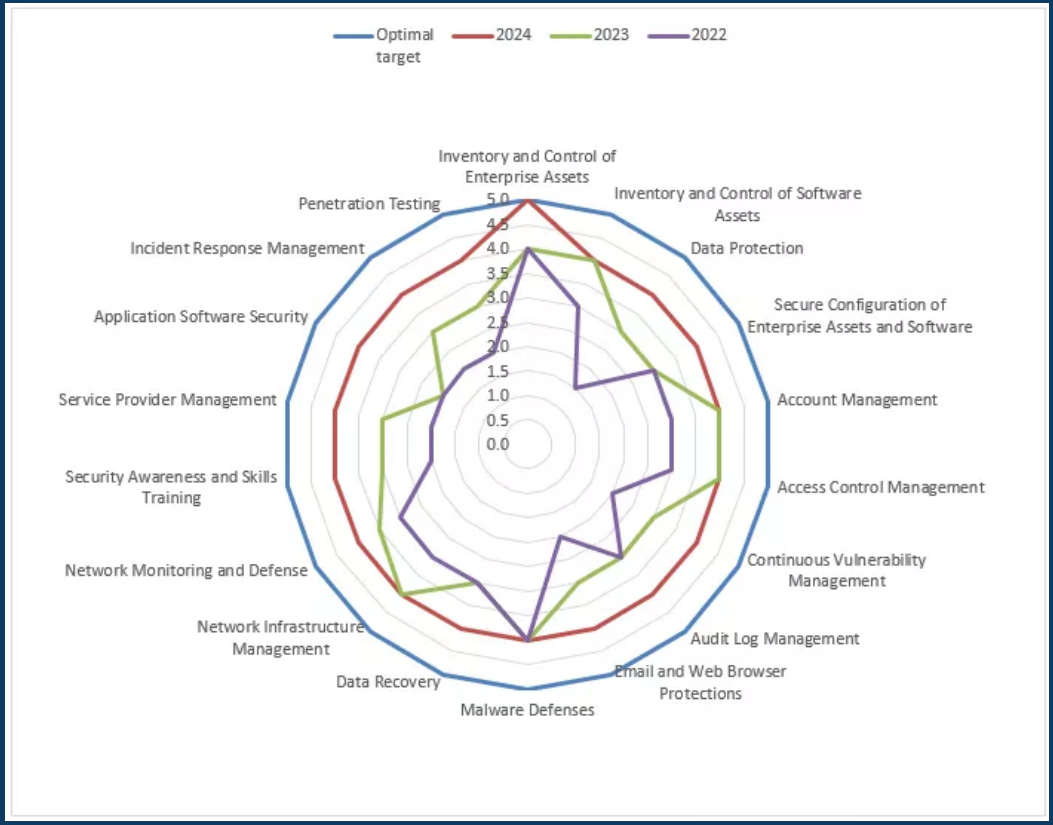


Fig: 1: CIS Spider Chart

Results

Vulnerability Assessment

The Company Name external security posture is excellent for your industry. The score is based on your grades across ten major security categories:

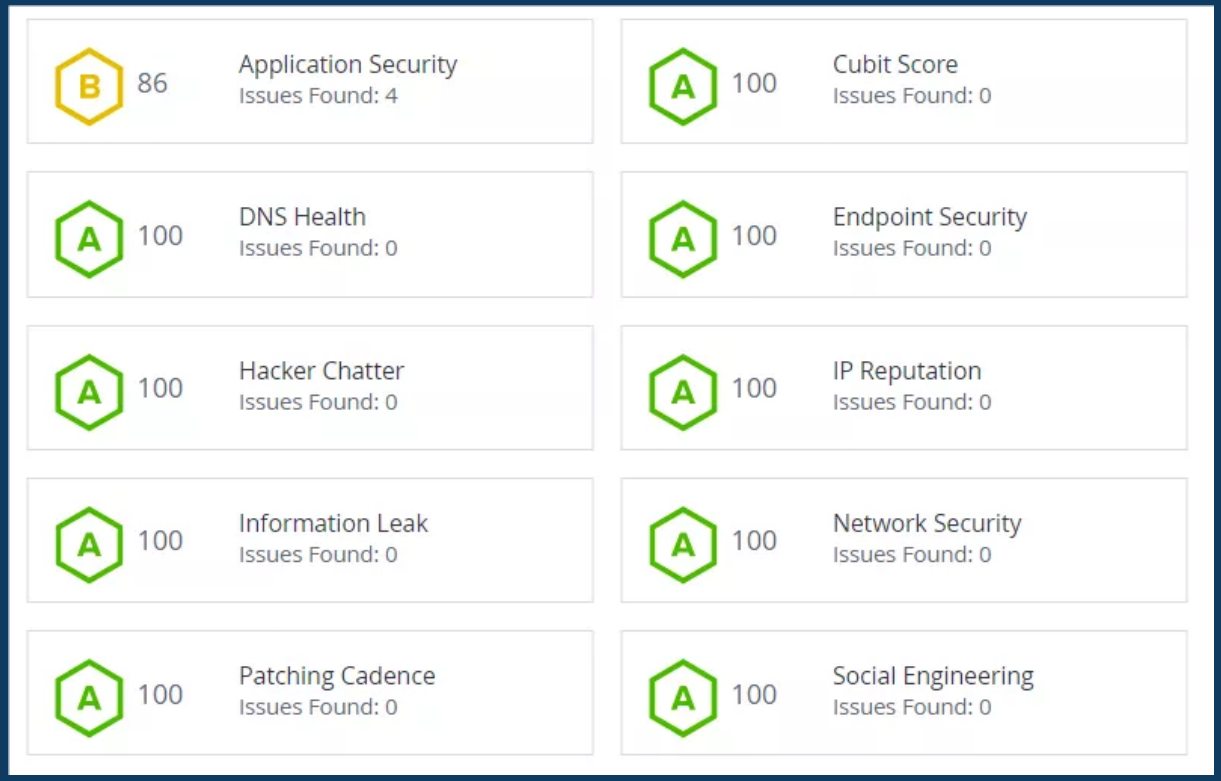


Fig: 2: Vulnerability Assessment

Recommendations

Domain	Action	CIS Control	Priority	Timing
People Security	Identity and Access Management (IAM) should be further automated	5,6	High/Medium/Low	
	Disable dormant accounts	5		
	Review permissions regularly	6		
	Implement security awareness training	14		
	Review yearly third-party supplier access	15		
Data Security	Create a data classification standard and utilise Microsoft 365 to classify and control data	3		
	Look at improving security on the databases, particularly around encryption	3		
Infrastructure Security	Improve visibility and reporting around application usage (Shadow IT)	2		
	Establish and maintain a vulnerability management process	7		
	Use DNS filtering services	9		
	Improve email security via DMARC	9		
	Implement account management for BOYD per user	12		

Domain	Action	CIS Control	Priority	Timing
Crises Management	Increase policy hardening across all firewalls	13		
	Document incident response plan. Too informal process in place.	17		
	Plan next BCP/DR test.	17		
	Perform annual penetration testing	18		

Conclusion

xxxxxxxxxxx

Let's Talk

We'd love to discuss your project in more depth

sales@nsp.co.nz

NSP
SECURE YOUR FUTURE