sonatype

NZISM Compliance with Sonatype Solutions

Introduction

In today's digital landscape, government agencies face increasing pressure to secure their data and systems while adhering to stringent standards. The **New Zealand Information Security Manual (NZISM)** provides a comprehensive framework to guide organisations in managing cybersecurity risks. It offers best practices for software security, data transfers, and secure software development, ensuring systems remain resilient to modern cyber threats.

This document outlines how Sonatype's solutions—**Sonatype Nexus Repository, Sonatype Lifecycle, Sonatype Repository Firewall, and Sonatype SBOM Manager**—align with NZISM's guidelines. Through automated governance, component management, and continuous monitoring, Sonatype helps organisations achieve compliance, enhance security, and build a robust software supply chain.

NZISM Section	NZISM Control Requirement	Control Description	Sonatype Capabilities
Standard Operating Environments (SOE)	14.1.3 - Characterisation	Baseline system configurations must be recorded to verify system integrity.	Nexus Repository stores software artifacts securely, ensuring consistent baselines and integrity.
Standard Operating Environments (SOE)	14.1.8.C.01	Agencies must develop hardened SOEs by disabling unused services and setting access controls.	Repository Firewall blocks unapproved components and enforces security policies for hardened environments.
Standard Operating Environments (SOE)	14.1.9.C.01	Continuous software patching is required to prevent degradation of SOE security.	Sonatype Lifecycle provides continuous monitoring and alerts to ensure up-to-date patching and vulnerability remediation.
Secure Software Development	14.4.4.C.01	Development, testing, and production environments must be separated with limited access.	Sonatype Nexus Repository creates isolated repositories for each environment to ensure proper segregation.

NZISM Section	NZISM Control Requirement	Control Description	Sonatype Capabilities
Secure Software Development	14.4.6.C.01	Code must be reviewed or tested for vulnerabilities before deployment.	Sonatype Lifecycle integrates with CI/CD pipelines to provide continuous vulnerability scanning during development.
Data Transfers	20.1.6.C.01	Agencies must establish policies for secure data transfers and hold users accountable.	Sonatype Lifecycle and Sonatype Repository Firewall enforce secure transfer policies, tracking software components involved.
Data Transfers	20.1.10.C.01	Data must be scanned for malicious content before being imported.	Sonatype Repository Firewall ensures that all imported artifacts are scanned and verified for security risks.
Data Transfer Authorisation	20.1.8.C.01	Transfers to less secure systems must be approved by a trusted source.	Sonatype Lifecycle tracks workflows to ensure that only approved data transfers occur.
Data Transfer Authorisation	20.1.9.C.01	Trusted sources must assess and approve all data transfers.	Sonatype Nexus Repository maintains records of all data transfers and approvals for auditing purposes.
Monitoring Data Transfers	20.1.15.C.01	Protective marking checks must be used for data exports.	Sonatype SBOM Manager applies protective marks to track software components during transfers.
Monitoring Data Transfers	20.1.15.C.02	Agencies must conduct monthly audits of data transfer logs.	Sonatype Lifecycle automates audit processes, providing detailed reports on transfer activities.

Conclusion

The NZISM outlines essential measures for securing data and software environments. Compliance with these guidelines ensures that government agencies can protect their systems against evolving threats. Sonatype's platform provides the tools needed to meet these requirements, from component management and continuous monitoring to secure data transfers and application controls.

With **Sonatype Nexus Repository**, **Sonatype Lifecycle**, **Sonatype Repository Firewall**, and **Sonatype SBOM Manager**, Sonatype delivers a complete solution to automate governance, manage artifacts, and enforce security policies. By aligning with NZISM controls, Sonatype helps organisations build a secure software supply chain and maintain compliance with New Zealand's cybersecurity framework.

Our team is here to help you achieve compliance, strengthen your cybersecurity posture, and safeguard your systems. For further assistance with Sonatype's solutions and to discuss your organisation's specific requirements, visit **sonatype.com/contactus**.

Sonatype is the leader in software supply chain optimization. Sonatype's platform empowers enterprises to create safer software faster and to protect against the inherent risk from free open source components used to develop modern software applications. As founders of Nexus Repository and stewards of Maven Central, the largest public repository of Java, Sonatype pioneered software supply management and maintains the world's leading knowledge base of open source intelligence for software composition analysis and dependency management.

Sonatype's platform integrates this intelligence with customers' Software Development Life Cycle and delivers reliable automated identification and remediation of vulnerable and malicious open source code while also enabling customers to generate and continuously monitor SBOMs (Software Bill of Materials) to increase their security posture and be prepared for the next zero-day threat or software supply chain attack.

More than 2,000 organizations, including 70% of the Fortune 100, fifteen million software developers and hundreds of government customers rely on Sonatype to set and enforce policies for open source governance, and "shift left" to deliver software applications that are secure by design and secure by default. For more information, please visit **Sonatype.com**, or connect with us on **Facebook**, **Twitter**, or **LinkedIn**.

Headquarters
8161 Maple Lawn Blvd,
Suite 250
Fulton, MD 20759
USA • 1.877.866.2836

European Office
168 Shoreditch High
St, 5th Fl
London E1 6JE
United Kingdom

APAC Office
60 Martin Place,
Level 1
Sydney 2000, NSW
Australia

Sonatype Inc.
www.sonatype.com