

NZISM v3.6

NZISM 3.6 provides security controls and guidance to protect government information and manage cyber risk across public sector systems.



What it is

New Zealand Information Security Manual (NZISM) 3.6 is a national cybersecurity framework that helps organizations safeguard government information and manage security risks across digital systems. The framework establishes comprehensive guidelines for implementing effective security controls and aligning information security practices with New Zealand government requirements.

Published by the New Zealand Government Communications Security Bureau (GCSB), NZISM is primarily used by government agencies, contractors, and organizations working with sensitive public sector data. It covers key areas including cybersecurity controls, risk management, data protection, incident response, and compliance with national security policies.

At a glance

PUBLISHER National Cyber Security Centre (NCSC)	TYPE Framework	VERSION NZISM Version 3.6
EFFECTIVE 2023	DOMAIN Cybersecurity	FAMILY Other
REGION New Zealand	INDUSTRY Government & Public Sector	ADOPTION MODEL Regulatory Compliance
IMPLEMENTATION COMPLEXITY High		

Source: <https://nzism.gcsb.govt.nz/>

Why it matters

- Strengthen information security governance** Support consistent accountability and oversight for information security practices within governmental and contractor environments.
- Enhance national compliance alignment** Ensure information security polices comply with New Zealand government standards and relevant national regulatory requirements.
- Improve risk management effectiveness** Enable organizations to systematically identify, assess, and mitigate cybersecurity risks associated with sensitive government data.
- Support incident detection and response** Strengthen preparedness for security incidents through clearly defined processes for identifying and responding to security events.

How SmartSuite supports NZISM 3.6

Government Security Control Framework Structure NZISM controls with ownership, scope, and implementation tracking across systems.	System Classification and Security Baselines Classify systems and apply appropriate baseline security controls based on sensitivity.	Authentication and Access Governance Manage authentication, authorization, and user access aligned to NZISM requirements.
Network Security and System Hardening Track secure configurations, network protections, and system hardening practices.	System Activity Monitoring and Incident Response Monitor system activity and manage incident response workflows and escalation processes.	NZISM Compliance and Government Reporting Provide dashboards showing control coverage, system compliance status, and NZISM readiness.

Common framework mappings

ASD ISM

CIS Controls v8.1

ISO 27001:2022

ISO 27002:2022

ISO 27017

ISO 27701

NIST CSF 2.0

NIST 800-53 Rev.5

Official resources

New Zealand Information Security Manual (NZISM) 3.6 Defines comprehensive guidelines for cybersecurity controls within New Zealand's government agencies. nzism.gcsb.govt.nz	NZISM Implementation Guidance Provides detailed implementation insights for integrating NZISM controls into organizational policies. nzism.gcsb.govt.nz
NZISM Risk Management Framework Outlines risk management practices aligned with NZISM for effective information assurance. nzism.gcsb.govt.nz	NZISM Compliance and Security Requirements Describes compliance requirements to meet NZISM security standards in public sector organizations. nzism.gcsb.govt.nz

Frequently asked questions

- What is NZISM used for?**

NZISM is used to provide comprehensive information security requirements and guidance for New Zealand government agencies and related organizations. It sets standards for managing security risks, implementing cybersecurity controls, and safeguarding sensitive government data across digital systems.
- Is NZISM compliance mandatory for organizations?**

NZISM compliance is mandatory for New Zealand government agencies and organizations handling sensitive government information. Compliance is enforced through government policy and oversight by the Government Communications Security Bureau (GCSB).
- Who must comply with NZISM and what does its scope cover?**

NZISM applies to all New Zealand government departments, agencies, and any contractors or third parties managing official or classified government information. Its scope includes the protection of information, systems, infrastructure, and supporting services that process or store government data.

How should organizations implement NZISM requirements?

Organizations should integrate NZISM requirements into their risk management processes, security policies, and operational procedures. This typically involves conducting risk assessments, performing security control gap analyses, and regularly reviewing operational practices for alignment with NZISM controls.

How does NZISM relate to other cybersecurity frameworks?

NZISM aligns with international standards such as ISO 27001 and NIST, providing a national context tailored for New Zealand government needs. It often references or complements controls from these frameworks, allowing organizations to leverage existing best practices when achieving NZISM compliance.

What are the ongoing compliance and audit requirements for NZISM?

Ongoing compliance with NZISM requires continuous risk assessments, regular reviews of security controls, incident reporting, and maintaining records of compliance activities. Agencies are subject to periodic internal and external audits to validate adherence to NZISM standards.

How would SmartSuite support NZISM 3.6?

SmartSuite can help organizations operationalize NZISM by centralizing management of cybersecurity policies, tracking risk assessments, and documenting control implementation. It enables efficient collection of compliance evidence, facilitates audit readiness through automated reporting, and helps security teams monitor and maintain NZISM requirements across the organization.

License included / downloadable: Yes The NZISM is publicly available through the New Zealand National Cyber Security Centre.

Full framework page and mappings: smartsuite.com/frameworks/new-zealand-nzism-3-6-new-zealand-information-security-manual