NZ NCSC Standards

The Practitioner's Guide to Mastering the NZ NCSC Standards with Okta

From Compliance to Maturity

Primary Role
Okta is a primary solution for meeting the standard's requirements.

Supporting Role
Okta provides critical data, enforcement, or compensating controls that enable or strengthen other tools and processes.

What are the NCSC Minimum Cyber Security Standards?

The standards are a framework from New Zealand's National Cyber Security Centre (NCSC). Unlike a simple checklist, they are a maturity model. The goal isn't just to have a security control, but to prove it is effective, repeatable, and optimised. This is measured across Capability Maturity Model (CS-CMM) levels, with a target of Level 2 (Planned & Tracked) for mandated government agencies.

Who are these standards for?

These standards are intended for agencies mandated by the Government Chief Information Security Officer (GCISO). However, they represent best practices in cyber resilience that are highly relevant for any organisation, public or private, that is serious about building a mature and demonstrable security posture.

Why Identity is the Strategic Enabler

Achieving mature, trackable security processes is impossible without mastering identity. Identity is the common thread that runs through nearly every NCSC standard - from Risk Management and Patching to Least Privilege and Threat Detection. Okta provides the central identity and access control plane to enforce policies, automate processes, and audit activity, providing the evidence needed to demonstrate CMM Level 2 maturity and beyond.

How to Use This Guide

This document maps Okta's capabilities against the corresponding standard from the NCSC. Each section details how Okta's role as a 'Supporting' or 'Primary' contributor can help meet the requirements at each maturity level.

Risk Management

Okta's Role: Supporting

Okta transforms identity risk management from a subjective exercise into a data-driven, quantifiable process. By providing deep visibility into your identity security posture and mapping findings to recognised compliance frameworks, we empower you to prioritise your most critical risks, make informed investment decisions, and clearly demonstrate your security posture to auditors and stakeholders.

While Okta is not a risk management framework itself, it provides the critical data, context, and metrics that feed into and validate an organisation's risk management processes. Okta Identity Security Posture Management (ISPM) is the key capability that delivers this value.

CS-CMM2: Planned & Tracked

- **Discover and Quantify Identity Risks:** A foundational part of any risk framework is understanding your current state. ISPM provides this by connecting to your identity providers and critical applications to automatically uncover hidden identity risks. This includes visibility into misconfigurations, MFA bypass vulnerabilities, over-privileged accounts, and dormant identities - risks that are often invisible to traditional tools. This provides the foundational data needed to begin a planned and tracked risk assessment.
- **Track and Audit Access Risk:** To manage the risk of who has access to what, Okta Identity Governance (OIG) provides detailed reporting on governance processes. Dashboards and exportable reports provide clear metrics on the status and outcomes of access requests and certification campaigns, giving compliance teams and auditors the data needed to track and verify that access is being formally and regularly fulfilled and reviewed.

CS-CMM3: Standardised

- **Prioritise Risks Based on Impact:** A mature risk process requires a standardised way to prioritise remediation. ISPM contextualises and ranks discovered risks based on their potential impact. This allows security teams to move from a reactive state to a proactive

defence, focusing their limited resources on the vulnerabilities that pose the greatest threat to the organisation.

- **Map Risks to Compliance Frameworks:** ISPM's findings are mapped out-of-the-box to controls from common industry frameworks such as NIST, ISO 27001, SOC 2, and PCI DSS. This provides a standardised language to communicate identity risk and helps streamline compliance reporting and audit preparation.

CS-CMM4: Quantitatively Controlled

- **Enable Continuous Monitoring:** At the highest level of maturity, risk assessment is a continuous, quantitative process. ISPM is constantly assessing your identity posture and detecting configuration drift. This provides ongoing, near real-time visibility, moving beyond periodic, point-in-time assessments.
- **Automate Risk Response:** The detection of a new, high-priority risk can trigger an automated response. Through integration with Okta Workflows, if ISPM detects an account created out of band for example, it can create a high-priority ticket for investigation and assign it to the relevant team, creating a controlled and auditable response process.

Assets and their Importance

Okta's Role: Supporting

Okta provides the foundational layer of ownership and business context for your digital assets. By assigning clear owners and classifying applications based on risk, you can allow your most critical resources to receive the highest level of protection and governance, directly aligning your security posture with business priorities.

To effectively manage and protect assets, you must first understand their importance and who is responsible for them. Okta helps establish this critical foundation of ownership and classification.

CS-CMM2: Planned & Tracked

- **Establishing Ownership:** The first step in managing assets is assigning clear accountability. Okta Identity Governance (OIG) allows you to assign specific business owners to digital resources, including applications and entitlements, creating a clear and auditable record of responsibility. Assigning owners is the prerequisite for the automated certification campaigns mentioned in the 'Least Privilege' Standard.

CS-CMM3: Standardised

- **Classifying by Business Risk:** Once owners are assigned, assets can be classified based on their importance. OIG allows you to apply descriptive labels - such as 'mission critical' or 'privileged' - to any managed resource. This enables you to proactively apply standardised security policies based on risk and criticality.

CS-CMM4: Quantitatively Controlled

- **Driving Data-Driven Governance:** The true value of asset classification is realised when it drives automated governance. Within Okta Identity Governance (OIG), these asset labels can

be used to power a dynamic, data-driven governance model. For instance, you can create a policy that automatically enrolls any application labeled ‘mission critical’ into a quarterly access review campaign, while less critical applications are reviewed semi-annually or annually. This helps ensure that the highest-risk assets receive the most frequent oversight, automating a risk-based approach to governance and focusing your review efforts where they matter most.

Secure Configuration of Software

Okta's Role: Supporting

Okta allows you to treat your identity and access policies like infrastructure - as auditable, version-controlled code. This transforms security configuration from a manual, error-prone task into a consistent, automated, and continuously monitored process, enabling your security posture to remain resilient against configuration drift.

Okta provides a clear maturity path for secure configuration, moving from centralised manual control to fully automated policy-as-code. While basic configuration is managed manually, Okta’s value comes into play at Level 4 by enabling Configuration-as-Code and Continuous Monitoring and Drift Detection.

CS-CMM4: Quantitatively Controlled

- **Enabling Configuration-as-Code:** Okta's Terraform provider allows your organisation to define, manage, and version-control all identity and access policies and configurations as code. This enables a fully automated CI/CD pipeline for security configuration.

- **Continuous Monitoring and Drift Detection:** By managing configurations as code, any deviation from the approved baseline can be automatically detected and alerted on. Furthermore, Okta Identity Security Posture Management (ISPM) continuously scans for configuration risks, providing an additional layer of assurance that policies remain in their intended secure state.

Patching

Okta's Role: Supporting

Okta acts as a critical compensating control that enforces your patching policy at the point of access. By preventing unpatched and non-compliant devices from accessing sensitive data, Okta reduces the immediate risk posed by vulnerabilities and gives your teams the time needed to safely test and deploy updates.

While Okta does not deploy patches to endpoints, it plays a vital supporting role by enforcing the outcomes of an organisation's device patching strategy at the point of authentication. Okta's value comes into play at Level 3, by providing a mechanism to proactively identify that specific patch levels are in place, effectively turning patch identification into an enforcement gate when accessing resources.

CS-CMM3: Standardised

- **Enforce Access Policies Based on Patch Level:** Okta Device Assurance provides the core enforcement capability. You can create precise assurance policies that evaluate the operating system version of a device at the point of login. This allows you to block devices that are not patched to your organisation's required level, confirming your standard is consistently applied for both corporate-managed and BYOD endpoints.

- **Automate User-Centric Remediation:** For a more advanced and user-friendly approach, Okta can orchestrate a self-remediation workflow. When an unpatched device is detected, Okta can display inline remediation instructions directly on the user's sign-in page. You can also configure a grace period, allowing the user a set amount of time (e.g. 7 days) to update their device themselves before access is fully blocked. This empowers users to resolve compliance issues independent of IT or service desk involvement.

Multi-factor Authentication

Okta's Role: Primary

Okta delivers a clear maturity pathway for authentication, moving your organisation from baseline MFA compliance to an advanced, phishing-resistant, and risk-based security posture. We make it simple to protect your most critical assets today while providing the tools to build a truly passwordless and Zero Trust future.

CS-CMM2: Planned & Tracked

- **Broad Application and Service Coverage:** Okta's Adaptive MFA (AMFA) makes it simple to enforce MFA across business-critical systems, external-facing applications, and third-party services. The flexible policy engine allows for targeting MFA based on application context, user groups, and network location.
- **Centralised Auditing and Review:** To support analysis and oversight, all successful and unsuccessful MFA events are centrally and immutably logged in the Okta System Log.

CS-CMM3: Standardised

- **Extending MFA to Infrastructure:** Okta extends MFA beyond modern applications to protect core network access via RADIUS integrations and legacy web applications through Okta Access Gateway (OAG).
- **Securing the Endpoint:** Okta Device Access (ODA) enforces MFA directly at the desktop login for both Windows and macOS, securing the first point of entry.
- **Protecting Privileged Access:** Okta Privileged Access (OPA) secures just-in-time server and credential access with strong MFA, helping ensure that even the most sensitive administrative accounts are protected.

CS-CMM4: Quantitatively Controlled

- **Enforcing Phishing-Resistance:** The policy engine can be configured to enforce the use of high-assurance, phishing-resistant authenticators like Okta Verify FastPass and FIDO2/WebAuthn (passkeys) for the most sensitive applications, moving beyond traditional MFA.
- **Intelligent Risk-Based Authentication:** Authentication policies move beyond static rules to become dynamic and risk-based, automatically triggering step-up challenges in response to changes in user behavior or detected threats.
- **Achieving Universal Coverage:** The Okta platform is designed to scale and apply MFA policies across all systems and for all users, establishing the universal coverage required at this advanced stage.

Detect Unusual Behaviour

Okta's Role: Primary

Okta transforms threat detection from a reactive, manual process into a proactive, automated capability. By centralising identity security signals and enabling automated responses, Okta shortens the time to detect and contain threats, directly reducing the potential impact of a breach.

Okta provides a multi-layered approach to detecting and responding to unusual activity, helping agencies mature from manual log analysis to automated, intelligence-driven remediation.

CS-CMM2: Planned & Tracked

- **Centralised Logging:** As the central identity authority, Okta captures detailed, immutable logs for every authentication and access event. These can be streamed to a Security Information and Event Management (SIEM) system for centralised analysis.
- **Built-in Indicators:** Okta's Adaptive MFA includes out-of-the-box risk and behavior detection, such as "impossible travel" and new device sign-ons, providing the pre-built indicators needed for review and alerting.

CS-CMM3: Standardised

- **Threat Intelligence Enrichment:** Okta Identity Threat Protection (ITP) elevates detection by automatically identifying high-risk signals like breached credentials, brute-force attacks, logins from malicious IPs and other detections from Okta Threat Intelligence.
- **Privileged Account Discovery:** Okta Privileged Access (OPA) can discover unauthorised local accounts created on servers - a common persistence technique - providing a critical signal of unusual behavior that standard logs might miss.

CS-CMM4: Quantitatively Controlled

- **Continuous Posture Monitoring:** Okta Identity Security Posture Management (ISPM) delivers continuous, automated analysis of identity configurations to discover risks like MFA bypass or over-provisioned users.
- **Discovering and Controlling AI Risks:** The rapid adoption of AI introduces significant visibility blind spots. Extending this continuous monitoring into your SaaS and browser environments allows you to detect unmanaged Agentic AI and unauthorised OAuth grants. This enables you to automatically discover "Shadow AI" usage, identify risky authorisations, and highlight autonomous agents operating outside your control.
- **Automated Remediation:** Through Okta Workflows, discoveries from ISPM or threat detections from ITP can trigger immediate, automated actions. For example, a high-risk login can automatically suspend a user's account, while the detection of a Shadow AI authorisation can instantly trigger a workflow to onboard that AI agent into Okta. This automatically closes the loop from detection to response without human intervention.

Least Privilege

Okta's Role: Primary

Okta provides the automated governance to manage the entire access lifecycle, from scheduled reviews to just-in-time elevation. This approach replaces high-risk standing privileges with an on-demand model, helping ensure access is appropriate and temporary, which eliminates privilege creep and significantly shrinks your attack surface.

Okta offers a unified identity platform to enforce the principle of least privilege, moving agencies from ad-hoc manual processes to a state of automated, just-in-time access.

CS-CMM2: Planned & Tracked

- **Formal Granting of Access:** Okta Identity Governance (OIG) provides a request and approval workflow through its Access Requests capability. Integrated with the Okta Dashboard, it allows users to formally request access to applications and entitlements, replacing informal systems with a structured process and creating a clear audit trail of every grant.
- **Dynamic and Scheduled Reviews:** To automate the process of re-validating user access, OIG uses Access Certification Campaigns. These can be configured to run at scheduled intervals for regular assurance, or triggered dynamically by specific events, such as when a user has been inactive in an application for a set period (e.g. 90 days). This verifies privileges are justified at critical moments and automatically cleans up unused access to reduce entitlement creep
- **Automated Lifecycle Management:** Okta Lifecycle Management (LCM) automates the entire user journey by integrating with a source of truth, like an HR system. It handles both provisioning - helping ensure users have the correct, role-based access on day one - and deprovisioning. When a user changes roles or leaves the organisation, their access is automatically modified or revoked, enabling a consistent and timely process that prevents accumulation of privileges.

CS-CMM3: Standardised

- **Just-in-Time Application Access:** With Okta Identity Governance, organisations can implement a just-in-time (JIT) model where users request temporary access to applications for a limited time. This helps ensure privileges are granted only when needed and are automatically revoked after a specified period of time.
- **Securing Privileged Infrastructure:** Okta Privileged Access (OPA) extends the JIT model to critical infrastructure across both Windows and Linux environments. It secures access by issuing ephemeral credentials for server sessions, effectively eliminating standarding privileges. For Active Directory privileged accounts, OPA vaults credentials and enforces automated password rotation on schedule or usage, helping ensure that even standing accounts remain secure and under policy control.
- **Controlling Non-Human Identities:** Often overlooked and undermanaged, non-human identities - such as Active Directory service accounts, default 'built-in' administrator profiles, and critical 'break-glass' accounts within SaaS applications - are a frequent source of compromise. OPA brings these accounts under control by discovering them, vaulting their credentials, and enforcing automated rotation on schedule and usage. This verifies that these powerful, silent accounts are securely managed and monitored, preventing them from being exploited as backdoors.
- **Governing Agentic AI:** As organisations deploy AI agents to automate tasks, these entities act as distinct, autonomous identities operating at machine speed. Okta enforces strict boundaries for Agentic AI by helping ensure it can only access data on behalf of a human user - and strictly within that user's existing permissions - using advanced token exchange capabilities. Furthermore, Okta Privileged Access (OPA) secures the underlying secrets these agents rely on, while Okta Identity Governance (OIG) subjects AI access to the same rigorous, automated review cycles as human employees, preventing autonomous privilege creep.

CS-CMM4: Quantitatively Controlled

- **Continuous Monitoring and Automated Remediation:** Okta Identity Security Posture Management (ISPM) continuously scans connected environments to discover identity-related risks, such as over-privileged users or dormant admin accounts. Through its native integration with Okta Workflows, these discoveries can trigger immediate, automated remediation actions. For example, if ISPM detects a rogue privileged account, a workflow can be initiated to automatically onboard the privileged account to OPA, rotate its password, and notify the security team, closing the loop from detection to response in near real-time.
- **Making Temporary the Default:** By combining OPA with the JIT capabilities in OIG, an organisation can make temporary, expiring access the default for all sensitive systems. This approach establishes temporary access as the default operational model, verifying privileged sessions are deliberate, approved, and automatically time-bound.

Response Planning

Okta's Role: Supporting

Response planning relies heavily on business processes, but those processes are only as effective as the data available to support them. Okta acts as the source of truth for identity activities, confirming that when an incident occurs, your team has the critical data needed to execute the plan.

Whilst Levels 2 and 3 focus on defining and testing the response plans themselves, Okta's value comes into play at Level 4, by providing the immutable data foundation required for adequate oversight and monitoring.

CS-CMM4: Quantitatively Controlled

- **Centralised Identity Visibility:** Okta provides this essential visibility through the **System Log**, which captures all authentication events, privilege changes, and potential indicators of compromise. By logging every interaction- both normal and abnormal - Okta helps ensure that the complete dataset required for forensic analysis is preserved, while allowing you to pinpoint specific exceptions based on risk, behaviour, or other contextual and threat-based indicators.

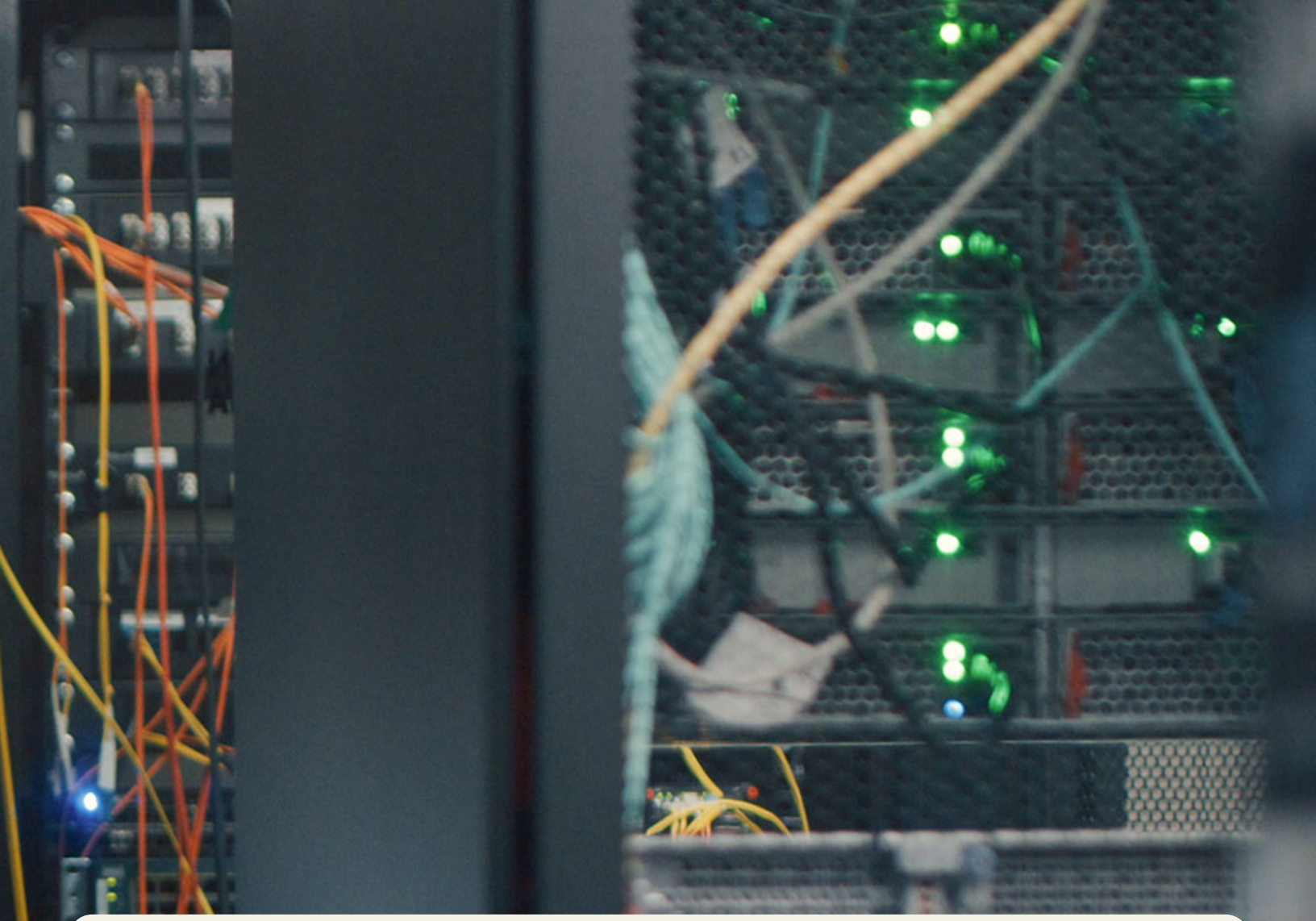
Standards Not Addressed by Okta Identity

The NCSC standards for **Security Awareness** and **Data Recovery** are critical parts of a comprehensive cyber resilience program. These controls are outside the scope of an identity platform and are typically addressed by dedicated security awareness training platforms and backup and disaster recovery (DR) solutions respectively.

Okta Capabilities by Maturity Level

NCSC Standard	Okta's Role	CS-CMM 2	CS-CMM 3	CS-CMM 4
Risk Management	Supporting	Discover & quantify risks across IdPs & apps **(ISPM)** Track & audit access risk **(OIG)**	Prioritise risk remediation based on impact **(ISPM)** Map risks to compliance frameworks **(ISPM)**	Continuous risk monitoring **(ISPM)** Automate risk response and remediation **(ISPM, Workflows)**
Assets and their importance	Supporting	Establish ownership of digital resources **(OIG)**	Classify digital resources by criticality via labels **(OIG)**	Drive automated, data-driven governance campaigns **(OIG)**
Secure Configuration of Software	Supporting	N/A	N/A	Enable configuration-as-code **(Terraform)**
Patching	Supporting	N/A	Enforce access policies based on patch level and automate user-centric remediation **(AMFA)**	N/A
Multi-factor Authentication	Primary	Broad application and service coverage **(AMFA)** Centralised and immutable auditing **(System Log)**	Protect core network access & legacy apps **(RADIUS Agent & OAG)** Secure end user workstations **(ODA)** Protect infrastructure and credential access **(OPA)**	Enforce phishing-resistance **(FastPass, Passkeys)** Intelligent risk-based auth **(AMFA)**

NCSC Standard	Okta's Role	CS-CMM 2	CS-CMM 3	CS-CMM 4
Detect Unusual Behaviour	Primary	User behaviour and risk detection **(AMFA)**	Identification of high risk events and signals **(ITP)** Privileged account discovery **(OPA)**	Continuous identity security posture monitoring **(ISPM)** Discover & control AI risks **(ISPM, Okta for AI Agents)** Automated remediation of detections within ITP & ISPM **(Workflows)**
Least Privilege	Primary	Request & approval process **(OIG)** Scheduled & event based access reviews **(OIG)** Automated lifecycle management **(LCM)**	Just-in-time application access **(OIG)** Just-in-time infrastructure access **(OPA)** Control non-human & agentic AI identities **(OPA, Okta for AI Agents)**	Continuous monitoring & remediation **(ISPM, Workflows)** Default to temporary just-in-time access **(OPA, OIG)**
Response Planning	Supporting	N/A	N/A	Centralised identity security visibility **(System Log)**



Your Partner on the Maturity Journey

Bridging the gap between manual policy (Level 2) and automated enforcement (Level 3+) requires the right platform. Okta empowers you to make this leap by turning your security policies into active controls - from implementing phishing-resistant authentication to automating zero standing privilege for your resources.

Ready to turn your NCSC compliance goals into operational reality? Reach out to our team to see how Okta's Workforce Identity Cloud can secure your critical assets today.

The full framework

References

NCSC Minimum Cyber Security Standards: Read the full framework and official guidelines at https://www.ncsc.govt.nz/protect-your-organisation/minimum-standards/

NZ NCSC Standards

The Practitioner's Guide to Mastering the NZ NCSC Standards with Okta

okta

Okta Inc.
80 Pacific Hwy, Level 13
North Sydney, NSW 2060,
Australia
info_apac@okta.com
+61-2-8310-4484