KINETICS GROUP
making IT work for you

SMB1001 WHITEPAPER
Q2 2026

Can You Prove You're Secure to CLIENTS, INSURERS & REGULATORS?

Cybersecurity is no longer a trust-me issue. Clients want evidence. Insurers want controls. Regulators want accountability.

This paper explains why SMB1001 is gaining traction, how the framework works in practice, and what New Zealand businesses can do to strengthen trust, reduce risk and build a more credible security posture.

inside this guide

- Why cybersecurity is now a board-level business issue, not just an IT concern
- What clients, insurers and regulators increasingly expect from SMBs
- How the five SMB1001 certification tiers work in practice
- What usually stops businesses from getting certified
- How to build a practical roadmap with the right IT partner

THE NEW ZEALAND THREAT LANDSCAPE

Why 2026 is a Turning Point for Cybersecurity in New Zealand

New Zealand businesses are facing a cyber threat environment that has fundamentally changed. Three major incidents in the first three months of 2026 alone have exposed hundreds of thousands of New Zealanders' most sensitive data — and triggered calls for regulatory reform at the highest levels of government.

In February 2026, the New Zealand Government released its Cyber Security Strategy 2026–2030, declaring that the era of geographic isolation as a natural defence is over. The strategy frames cybersecurity as a matter of national security and economic resilience — not an IT concern. The cost of cybercrime to New Zealand is now estimated at $1.6 billion annually.

High-Profile NZ Breaches January – March 2026

Organisation	Date	Attack Type	Impact	Sector
ManageMyHealth	Jan 2026	Ransomware / Data Exfiltration	126,000 patients' records stolen (108 GB). $60,000 ransom demanded. Government review ordered. High Court injunction sought. Health Minister intervened.	Health
MediMap	Feb 2026	Unauthorised Access	Patient records tampered with. Portal serving aged-care homes, hospices and disability providers taken offline. Triggered Privacy Act reform calls.	Health
MediaWorks	Mar 2026	Data Exfiltration / Extortion	Data of 2.4M competition entrants allegedly stolen (names, addresses, DOB, contact details). Individual victims directly extorted via email.	Media

These are not isolated failures. They point to a broader pattern seen across many organisations: weak control environments, poor visibility, and limited evidence of a formal security posture.

$1.6B

Annual cost of cybercrime to NZ

$173K

Avg. breach cost for a Kiwi SMB

61%

Of businesses face major disruption after a breach

42%

Of ransomware victims paid the ransom

What Your Stakeholders Are Already Asking

Cybersecurity is no longer a conversation between IT managers. Across every industry sector, different stakeholders are asking pointed questions — and they want answers backed by evidence, not reassurance.

YOUR BOARD & LEADERSHIP	YOUR CLIENTS & PARTNERS	YOUR INSURER
"Are we exposed? What would a breach cost us — financially and reputationally?"	"Before we share client data with you, what security controls do you have in place?"	"What security controls do you have? Have they been independently verified?"
"Do we have any way to demonstrate our security posture to auditors or regulators?"	"Our contract requires suppliers to meet a minimum security standard. Can you evidence that?"	"Your premium renewal depends on evidence of MFA, EDR and an incident response plan."
"How do we know our cyber insurance will actually pay out after an incident?"	"We were affected by a breach at a partner recently. How do we know you're secure?"	"We're requiring certified evidence of your cybersecurity posture for your next renewal."

SMB1001 was created specifically to answer these questions — with a structured, evidence-based framework that any organisation can implement, regardless of size or resources.

THE SMB1001 FRAMEWORK

What Is SMB1001?

SMB1001 is a practical, multi-tiered cybersecurity framework designed specifically for small and medium businesses. Developed by Dynamic Standards International, it was created in direct response to a gap identified by MSPs and SMBs worldwide: existing frameworks like Australia's Essential Eight were too technical, too complex, and poorly aligned with the real-world risks and resources of smaller organisations.

Unlike compliance frameworks that treat cybersecurity as a single pass/fail test, SMB1001 is a journey. It allows organisations to start at a level appropriate to their current posture and progress over time — building genuine capability rather than ticking boxes.

SMB1001 is updated annually, ensuring it stays current with the evolving threat landscape. It is already recognised by leading cyber insurers, professional associations and supply chain procurement programmes.



The Five Levels of SMB1001 Certification

Each level builds on the last. Bronze establishes the foundation; Diamond represents the highest level of maturity, aligned with international standards like ISO 27001.

LEVEL	WHAT IT MEANS	KEY CONTROLS INTRODUCED
DIAMOND	Highest maturity. Aligns to ISO 27001. External audit required. Demonstrates global-level cyber resilience.	All Platinum controls + ISO 27001 alignment, continuous external auditing, advanced threat intelligence
PLATINUM	Advanced GRC posture. External independent audit required. Suitable for regulated industries and supply chain compliance.	All Gold controls + External audit, ISMS documentation, risk register, business continuity plans
GOLD	Comprehensive protection. Demonstrates rigorous security to enterprise partners and insurers.	EDR/MDR, MFA on all apps, cyber insurance, incident response plan, digital asset register, AI use policy, RDP restrictions
SILVER	Strong foundations. Shows clients and insurers you practice good cybersecurity. Meets most insurer requirements.	TLS certificates, MFA on email, password managers, anti-spoofing, invoice fraud controls, confidentiality agreements
BRONZE	Entry-level certification. Establishes core controls. A credible starting point for SMBs.	Technical specialist engaged, firewalls, antivirus, patching, strong passwords, backups, security awareness training

Key differentiator: From Bronze through Gold, organisations self-attest their compliance — but a director or owner must personally sign off, creating executive accountability. Platinum and Diamond require independent external audits.

Introducing GRC Governance, Risk and Compliance

SMB1001 doesn't just address technical controls — it introduces the concept of GRC (Governance, Risk and Compliance) to SMB-scale organisations. For many business owners, this is a new idea. Here's what it means in practice:

G GOVERNANCE

Who is accountable for cybersecurity in your organisation? SMB1001 requires a director to personally attest to your compliance posture — placing cyber firmly at board level. It establishes clear policies: acceptable use, incident response, AI use, and data handling.

R RISK

What are the risks to your business, and how are you managing them? SMB1001 moves organisations from reactive problem-solving to proactive risk identification. Higher tiers require a documented risk register, business continuity planning, and regular review.

C COMPLIANCE

Can you demonstrate, with evidence, that your security controls are in place and working? Certification gives you a structured, auditable record of your cybersecurity posture — what you can show to clients, insurers, and regulators when asked.

GRC is not just for large enterprises. The 2026 NZ Cybersecurity Strategy explicitly calls for cybersecurity to be treated as a core governance priority across all sectors. SMB1001 provides the practical path for SMBs to get there.

HOW KINETICS HELPS YOU GET CERTIFIED

Your MSP as Your Certification Partner

Getting certified isn't something you need to do alone. A strategic Managed Services Provider (MSP) like Kinetics has the expertise, tools and processes to assess your current posture, identify gaps, implement the required controls, and guide you through the certification process — at the right pace for your business.

Kinetics KARE Foundation service is structured to align with SMB1001 requirements. Many of our clients are already meeting Bronze and Silver requirements as part of their day-to-day managed service — without realising it. Our role is to make that posture visible, documented and certifiable.

SMB1001 LEVEL	KINETICS SERVICE ALIGNMENT	WHAT WE PROVIDE	WHO IT'S FOR
SILVER / BRONZE	KARE Foundation Basic & SME	Firewall, AV, patching, backups, MFA on email, security awareness training	SMBs establishing a credible security baseline
GOLD	KARE Foundation Complete	EDR/MDR, MFA across all apps, incident response plan, cyber insurance guidance, digital asset register	Organisations responding to insurer or client requirements
PLATINUM / DIAMOND	KARE Foundation + GRC Advisory	External audit coordination, risk register, ISMS documentation, BCM planning, ISO 27001 pathway	Professional firms, regulated sectors, enterprise supply chains

The Kinetics Approach: Strategy-First Certification

For most organisations, SMB1001 should not be treated as a stand-alone compliance project. Done properly, it becomes part of a broader operating model - helping strengthen governance, support insurance conversations, and provide clearer evidence of cybersecurity maturity. Our approach starts with your business goals, then builds the technology and policy controls to support them.

STEP 01

Closer Look Assessment

We map your current controls against the SMB1001 framework and identify exactly where you sit today and what's needed to reach your target level.

STEP 02

FlightPlan Roadmap

We build a prioritised plan to close gaps, aligned with your budget and timeline. Certification becomes a milestone in your broader IT strategy, not an add-on.

STEP 03

KARE Foundation Delivery

We implement and manage the technical and policy controls required for your target tier — including MDR, MFA, patching, backups, security training and GRC documentation.

STEP 04

Certification & Ongoing Maintenance

We support your attestation process, maintain your documentation through annual updates, and provide quarterly reviews to keep your posture current as threats evolve.

KINETICS GROUP
making IT work for you

" The real shift is this: cybersecurity is no longer just something you say you take seriously. More and more, organisations are being asked to prove it. "

NEED A CLEARER VIEW OF YOUR CURRENT POSTURE?

Book a complimentary SMB1001 Readiness Review. We'll help you understand where you likely sit today, where the gaps are, and what a realistic path forward could look like.



0800 546 384



kinetics.co.nz



Auckland & Christchurch

Since 1996, Kinetics has been helping New Zealand businesses transform functional IT into strategic competitive advantage.
New Zealand's most awarded Microsoft partner. No fixed-term contracts. All documentation belongs to you.