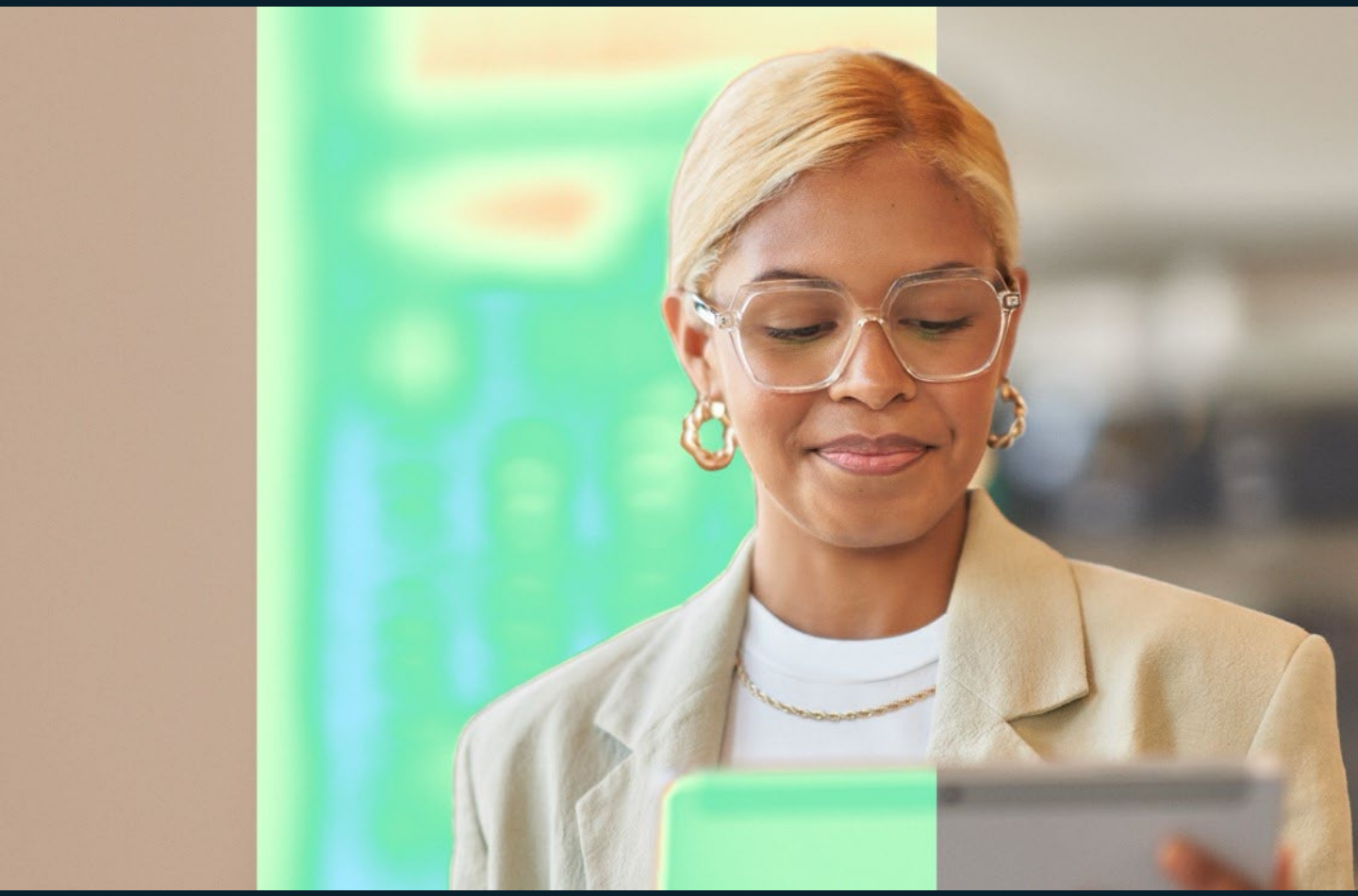
# SMB Security Regulatory Changes: What your business needs to know



From 2025, businesses in New Zealand need to be aware of key regulatory changes that will impact small and medium businesses (SMBs):

a. New Zealand Privacy Act 2020 compliance requirements
b. Cross-border implications of Australian Privacy Act amendments
c. The rise of industry-led cybersecurity frameworks like SMB1001

With millions of SMBs potentially impacted, businesses must take proactive steps to comply. Failure to do so could lead to significant penalties if there is a breach.

Additionally, these security controls align closely with requirements for responsible AI adoption, turning compliance investments into strategic assets for future business growth.

# New Zealand Privacy Act 2020: Key requirements for SMBs

The Privacy Act 2020 is New Zealand's primary privacy legislation, governing how personal information is collected, used, and disclosed by businesses of all sizes. The Act includes several key provisions that directly impact SMBs:

## Requirements for all businesses

To comply with the Privacy Act 2020, all businesses need to:

1. **Understand and implement the Information Privacy Principles (IPPs)** which outline requirements for: A. Collection, storage, and disclosure of personal information B. Ensuring data accuracy and providing access rights C. Limiting use of personal information to stated purposes D. Implementing reasonable safeguards against loss, misuse, or disclosure.
2. **Establish mandatory data breach reporting processes to:** A. Notify the Privacy Commissioner and affected individuals when breaches occur B. Respond promptly when a data breach is likely to cause serious harm.
3. **Prepare for compliance notices** which can be issued by the Privacy Commissioner requiring businesses to take corrective actions.
4. **Increase transparency** in how personal information is collected and used, especially when collected indirectly.

## Cross-border implications: Australian Privacy Act changes

Amendments to Australia's Privacy Act 1988 have expanded its extraterritorial scope, requiring New Zealand businesses operating in Australia to comply with stricter privacy regulations. This includes:

- Preemptive compliance assessments for NZ businesses with Australian operations
- Higher penalties for breaches affecting Australian residents
- Potential removal of the small business exemption (for businesses with annual turnover less than AU$3 million)

While New Zealand's privacy laws are evolving incrementally, SMBs should remain vigilant about both local requirements and international impacts from neighboring countries like Australia.

## Penalties for non-compliance

If there is a breach, the potential maximum penalties for Privacy Act violations could include:

- Up to $50 million for serious or repeated privacy breaches
- Three times the value of any benefit obtained through the misuse of information
- 30% of a company's adjusted turnover during the relevant period

# SMB1001 Cybersecurity Compliance Framework

SMB1001 is a cybersecurity framework specifically designed for small and medium businesses. Published in 2024, this framework provides a structured approach to achieving cybersecurity certification.

It introduces a tiered certification model (Bronze, Silver, Gold) to help SMBs strengthen their cybersecurity posture. Bronze establishes essential foundations, Silver adds comprehensive controls, and Gold represents advanced security maturity for handling sensitive data.

While not government-mandated, SMB1001 is an industry-led framework that incorporates elements from established standards like the Essential Eight and ISO 27001, but is specifically designed to be more accessible and practical for smaller businesses.

## Key components of the framework

### Governance Controls

a. Establishing security roles and responsibilities
b. Implementing security policies and procedures
c. Regular security risk assessments
d. Incident response planning

### Technical Controls

a. Identity and access management requirements
b. Data protection and encryption standards
c. Network security and monitoring
d. Endpoint protection requirements
e. Backup and recovery protocols

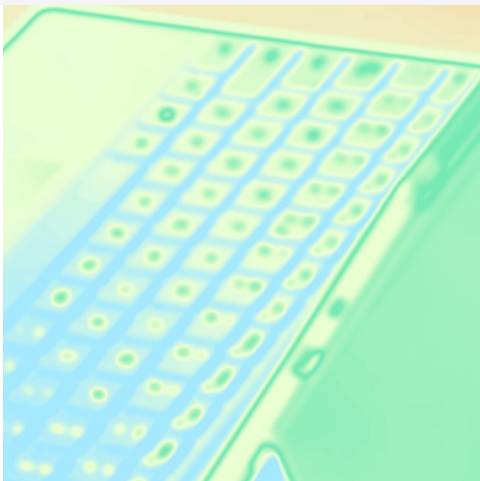
### Operational Controls

a. Security awareness training for all staff
b. Third-party vendor risk management
c. Change management procedures
d. Regular security testing and validation

## Compliance timeline and approach

While full details of the certification process are still being finalised, businesses should prepare by:

- **Conducting a gap assessment** against the framework requirements
- **Developing a remediation roadmap** to address identified gaps
- **Implementing required controls** in a prioritised manner
- **Documenting evidence of compliance** for certification purposes
- **Preparing for regular reassessment** as the framework evolves



# Business impact and strategic considerations

These regulatory changes represent both a challenge and an opportunity for small and medium businesses:

## Business challenges

- Additional compliance costs and resource requirements
- Need for specialised security and privacy expertise
- Potential operational changes to meet new requirements

## Strategic opportunities

- Enhanced trust with customers and partners through demonstrated compliance
- Reduced risk of costly security incidents and data breaches
- Competitive advantage in an increasingly security-conscious market
- Better positioning for contracts with larger organisations and government entities

# Getting prepared: A practical approach

Rather than viewing these changes as purely compliance hurdles, forward-thinking businesses are using them as catalysts to improve their overall security posture:

- **Start early:** Begin compliance efforts now to avoid a last-minute rush
- **Take a risk-based approach:** Focus first on your most sensitive data and critical systems
- **Leverage integrated solutions:** Use platforms like Microsoft 365 that address multiple compliance requirements
- **Document everything:** Maintain precise records of your compliance efforts and security controls
- **Seek expert guidance:** Work with a qualified technology partner who understands both the regulatory requirements and practical implementation

By proactively addressing these upcoming regulatory changes, your business can not only meet compliance requirements but also build a stronger security foundation that protects your most valuable assets and supports sustainable growth.

DICKER DATA | Microsoft

# Let's work together to supercharge your security

Our Microsoft security experts will help you navigate the complex threat landscape and build a security foundation that protects your business now and in the future.

## About Dicker Data

As ANZ's largest owned and operated technology distributor, we represent over 8,000 technology providers. With 30 years of New Zealand experience, we're committed to building a network of specialist cyber security partners who help local healthcare organisations mitigate risks and defend against increasing threats.

## Meet our proven healthcare security partners

daraco I.T. SERVICES

Daraco IT, a leader in technology services and Cyber Security, exceling in safeguarding digital landscapes. With a mission to empower healthcare providers through cutting-edge technologies and expert strategies, we provide robust protection against cyber threats, fostering secure and resilient environments for our clients. Learn more at www.daraco.com.au/health-solutions or call 1300 327 226

NTT DATA

NTT DATA is a $30B+ global leader in business and tech services. With experts in 50+ countries and a strong partner ecosystem, we help clients innovate, optimize, and transform through consulting, data & AI, and industry solutions. Learn more at www.services.global.ntt

inde

Inde is a New Zealand-based, employee-owned IT consultancy delivering cloud-first enterprise solutions. With deep expertise and a customer-first approach, Inde empowers businesses through tailored consulting, innovative technology, and managed services. Learn more at www.inde.nz

**Connect with a proven healthcare security specialist:**
Visit www.dickerdata.co.nz/microsoft/healthcare-security