

New Zealand Cybersecurity Compliance Checklist



About the New Zealand Cybersecurity Compliance Register

The New Zealand Cybersecurity compliance register provides organisations the information and strategies they need to secure digital information and systems in accordance with all of their legal obligations. Divided into 21 topics that affect the format of the NIST Framework for Improving Critical Infrastructure Cybersecurity and provide a sequential process for constructing a risk-management-based framework of cybersecurity measures.

About the Expert

Tania Goatley

Partner, Bell Gully



Tania has assisted with cyber security breaches across multiple jurisdictions and has advised on the first mandatory reportable privacy breach under the Privacy Act. Regularly advises clients on privacy and cyber security issues, including advising:

- » a client operating in the telecommunications sector as to how to deal with a breach that involved the public disclosure of phone numbers that were designated as 'unlisted'.
- » the receivers of a New Zealand retailer that went into liquidation on how to deal with, use and protect databases containing customer information across multiple jurisdictions.
- » a multinational media company about its privacy and cyber security practices, including assisting in managing data security incidents and corresponding with official agencies to mitigate any fallout.

She has a strong media law background, advising on defamation claims, appearing in Court on name suppression issues, and providing media law training to journalists. She advises on all aspects of intellectual property law, including copyright, passing off and trademark infringement disputes and litigation.

In addition to her particular areas of expertise, Tania provides general advice on commercial and contractual disputes and litigation with successful outcomes for her clients.

Chambers Asia Pacific 2023 ranks Tania as a leading lawyer for intellectual property and technology, media and telecommunications. The Legal 500 Asia Pacific 2023 recommends Tania for data protection, intellectual property and technology, media and telecommunications.

Tania is recognised as a media and entertainment lawyer of the year and trademark lawyer of the year in the Women in Business Law Awards APAC 2023 shortlists.

Tania is an active member of the International Association for the Protection of Intellectual Property (AIPPI) and the Intellectual Property Society of Australia and New Zealand (IPSANZ).

Expertise

Media and communications, Consumer law, Intellectual property, Litigation and dispute resolution, Privacy and data protection, Information, communications and technology, Cyber security

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Overview

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the organisation implement cybersecurity measures to protect digital systems and information?

Asset Management

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the organisation maintain device, software and external system inventories, map data flow to determine the boundaries of networks, assess the sensitivity of each resource, and assign cybersecurity roles and responsibilities to staff?

Does the organisation maintain an inventory of all physical devices and systems that store or transmit information on the organisation's network?

Does the organisation maintain a software inventory and implement controls designed to ensure that only trusted software may run on its network?

Does the organisation maintain a current map of the boundaries of its data flow and digital communications network?

Does the organisation maintain a catalogue of external information systems that represent potential threats to digital security, and does it also employ controls for the management of mobile devices?

Does the organisation assess and categorise the sensitivity of all digital resources?

Does the organisation assign digital security roles and responsibilities to every member of staff and (where applicable) third-party stakeholders?

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Business Environment

Requirement	Needs work	Don't know	Meets requirement
Does the organisation identify and record a range of data in order to document the organisation's business environment for risk management purposes?			
Does the organisation identify and document its role in supply chains?			
Does the organisation identify and document its role in critical infrastructure and the organisation's industry sector?			
Does the organisation define, prioritise and document its mission and objectives?			
Does the organisation identify and document the services and functions critical to its business activities?			
Does the organisation identify and document resilience requirements to protect its ability to conduct business activities in a range of operational states?			

Governance

Requirement	Needs work	Don't know	Meets requirement
Does the organisation incorporate digital security into governance processes by establishing a cybersecurity policy, coordinating personnel responsibilities and assessing legal liabilities?			
Does the organisation create, publish and implement a policy to govern its digital security activities?			
Does the organisation coordinate the digital security roles and responsibilities of internal personnel and external service providers to implement security controls?			
Does the organisation maintain an understanding of the potential legal consequences of digital security breaches?			
Does the organisation integrate digital security considerations into governance, budgetary and risk management processes?			
Does the organisation make the required cyber resilience reports to the Reserve Bank of New Zealand by the relevant due dates?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Risk Assessment

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the organisation conduct a risk assessment process to determine its digital security risks and identify available responses?

Does the organisation identify and document digital security vulnerabilities across all assets?

Does the organisation implement and document a threat awareness programme?

Does the organisation document its internal and external digital security threats?

Does the organisation identify and document the impact and likelihood of harm that may result from any digital security threats?

Does the organisation determine, document and review its digital security risks?

Does the organisation identify and document its digital security risk responses?

Risk Management Strategy

Requirement	Needs work	Don't know	Meets requirement
-------------	------------	------------	-------------------

Does the organisation establish a risk management strategy that outlines processes for addressing digital security risks and specifies the organisation's risk tolerance?

Does the organisation develop, communicate and implement a risk management strategy?

Does the organisation establish and document its risk tolerance?

Does the organisation update its risk tolerance in response to changes in the organisation's critical dependencies?

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Supply Chain Risk Management

Requirement	Needs work	Don't know	Meets requirement
Does the organisation perform risk assessments, design contract provisions, conduct audits and create response and contingency plans to manage cyber supply chain risks?			
Does the organisation establish processes for managing risks associated with cyber supply chains?			
Does the organisation identify and assess the risks associated with third-party suppliers of ICT equipment and digital services?			
Does the organisation incorporate provisions into contracts with third-party suppliers designed to implement security controls in accordance with a supply chain risk management plan?			
Does the organisation audit third-party suppliers to ensure they are meeting their contractual digital security obligations?			
Does the organisation establish incident response and contingency plans, and test these plans in collaboration with third-party suppliers?			

Identity Management, Authentication and Access Control

Requirement	Needs work	Don't know	Meets requirement
Does the organisation implement authentication processes and security measures designed to control access to information systems?			
Does the organisation issue, manage, verify and revoke identities and credentials in accordance with an identification and authorisation policy?			
Does the organisation implement controls designed to restrict and monitor physical access to information system assets?			
Does the organisation implement controls designed to prevent unauthorised remote access to its information systems?			
Does the organisation manage access permission and authorisations in accordance with an access control policy?			
Does the organisation segment and segregate its network to improve security?			
Does the organisation obtain proof of the identity of a user before issuing the user an account and providing the user with access to higher-value digital assets?			
Does the organisation adopt multi-factor authentication to address security risks associated with users and devices?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Awareness and Training

Requirement	Needs work	Don't know	Meets requirement
Does the organisation provide digital security training to all personnel and implement measures designed to maintain awareness of digital security responsibilities among staff and other stakeholders?			
Does the organisation provide digital security training to all users?			
Does the organisation take steps to ensure privileged users maintain awareness of their digital security responsibilities?			
Does the organisation take steps to ensure external stakeholders maintain awareness of their digital security responsibilities?			
Does the organisation take steps to ensure senior executives maintain awareness of their digital security responsibilities?			
Does the organisation take steps to ensure security personnel maintain awareness of their digital security responsibilities?			

Data Security

Requirement	Needs work	Don't know	Meets requirement
Does the organisation implement security measures designed to protect the confidentiality, integrity and availability of data, digital services and information systems?			
Does the organisation implement digital security controls designed to protect data at rest?			
Does the organisation implement digital security controls designed to protect data in transit?			
Does the organisation sanitise digital assets before removing the asset from service, transferring the asset to a new business area or disposing of the asset entirely?			
Does the organisation implement digital security controls and create contingency plans designed to maintain critical business functions during a denial of service attack?			
Does the organisation implement digital security controls designed to prevent data leakage?			
Does the organisation deploy integrity-checking mechanisms to verify the integrity of software, firmware and data?			
Does the organisation separate its development and testing environments from its production environment?			
Does the organisation deploy integrity-checking mechanisms to verify the integrity of system hardware?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Information Protection Processes

Requirement	Needs work	Don't know	Meets requirement
Does the organisation establish the security policies, procedures and systems necessary to protect digital assets?			
Does the organisation maintain a baseline configuration for each information system?			
Does the organisation incorporate digital security controls into its system development life cycle?			
Does the organisation establish configuration change control processes to manage the adjustment of digital asset configurations?			
Does the organisation backup system and user information routinely and verify the integrity of backup data?			
Does the organisation locate information system components in a secure physical environment?			
Does the organisation destroy digital information in accordance with device sanitisation processes?			
Does the organisation operate a continuous monitoring program designed to generate data the organisation may use to improve digital security plans and processes?			
Does the organisation communicate the effectiveness of its digital security controls with the digital security community of practice?			
Does the organisation create contingency plans and have a digital security incident response plan?			
Does the organisation test digital security incident response plans and contingency plans routinely to ensure they remain effective?			
Does the organisation implement human resources procedures designed to maximise the security of sensitive information and digital services?			
Does the organisation detect and address digital asset vulnerabilities in accordance with a vulnerability management plan?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Maintenance

Requirement	Needs work	Don't know	Meets requirement
Does the organisation establish processes designed to ensure the security of information systems undergoing maintenance or repair?			
Does the organisation maintain and repair information systems in accordance with an information system maintenance program?			
Does the organisation approve, log and control all remote maintenance activities?			

Protective Technologies

Requirement	Needs work	Don't know	Meets requirement
Does the organisation deploy technological security measures and controls designed to protect stored data, network integrity and critical digital services?			
Does the organisation retain and review a log of audit events?			
Does the organisation store and transport digital media securely and restrict the use of digital media in essential business functions?			
Does the organisation configure all information system components to provide only essential capabilities?			
Does the organisation deploy security controls designed to protect its communications network from surveillance, disruption and interference?			
Does the organisation implement resilience mechanisms designed to ensure the reliability of systems that provide critical services?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Anomalies and Events

Requirement	Needs work	Don't know	Meets requirement
Does the organisation detect network anomalies, identify the events causing the anomalies, assess the harm caused by anomalous events, and trigger incident response measures when appropriate?			
Does the organisation maintain a network operation and data flow baseline and monitor network activity for events that deviate from this baseline?			
Does the organisation analyse detected anomalies to determine the method and targets of digital attacks?			
Does the organisation collect data about anomalous network events from a range of sources?			
Does the organisation investigate unexplained events to determine their impact upon information systems and digital security?			
Does the organisation establish impact thresholds to determine when an anomalous event will trigger incident response measures?			

Security Continuous Monitoring

Requirement	Needs work	Don't know	Meets requirement
Does the organisation monitor information system assets, network traffic and the activities of personnel to detect potential cybersecurity events?			
Does the organisation monitor network activity to detect potential cybersecurity events?			
Does the organisation monitor the physical environment of information systems to detect potential cybersecurity threats?			
Does the organisation monitor the activities of personnel to detect potential cybersecurity threats?			
Does the organisation configure network devices and perform scans of information systems to detect malicious code?			
Does the organisation establish a mobile code policy and scan all emails, web content, documents and external devices to detect unauthorised mobile code?			
Does the organisation monitor the activities of external service providers to detect potential cybersecurity events?			
Does the organisation monitor the configurations of information systems to detect potential cybersecurity events?			
Does the organisation scan digital assets to detect new vulnerabilities?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Detection Processes

Requirement	Needs work	Don't know	Meets requirement
Does the organisation implement processes to assist in detecting any potential cybersecurity events that could occur within the organisation?			
Does the organisation define all incident detection roles and responsibilities clearly so that potential cybersecurity events can be detected effectively?			
Does the organisation ensure that its activities for detecting potential cybersecurity events meet all applicable requirements?			
Does the organisation undertake adequate and effective testing of its processes that are used to detect potential cybersecurity events?			
Does the organisation communicate all necessary information relating to the detection of a potential cybersecurity event to relevant personnel and authorities?			
Does the organisation review and adjust detection processes routinely to achieve continuous improvement?			

Response Planning

Requirement	Needs work	Don't know	Meets requirement
Does the organisation develop and execute effective response mechanisms to be used in the event of a cybersecurity incident?			
Does the organisation execute incident response plans and contingency plans when response thresholds are met?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Communication

Requirement	Needs work	Don't know	Meets requirement
Does the organisation establish avenues of communication with all stakeholders to manage cybersecurity incidents and prevent future cybersecurity events?			
Does the organisation explain the roles and the order of operations within the organisation to all personnel, so that they can respond appropriately to any cybersecurity incidents?			
Does the organisation establish criteria and procedures for reporting cybersecurity incidents?			
Does the organisation share cybersecurity incident information with stakeholders according to its response plans?			
Does the organisation coordinate incident response activities with those of internal and external stakeholders, consistent with its incident response plan?			
Does the organisation share information about incident response activities with the digital security community of practice?			

Mitigation

Requirement	Needs work	Don't know	Meets requirement
Does the organisation undertake activities to contain and mitigate the effects of digital security incidents and document any new vulnerabilities?			
Does the organisation contain any cybersecurity incidents so as to limit their expansion and their effects?			
Does the organisation mitigate the effects of cybersecurity incidents to facilitate their resolution?			
Does the organisation identify, document and address any new vulnerabilities that could result in a cybersecurity incident?			

NEW ZEALAND CYBERSECURITY CHECKLIST

This checklist has been designed to help you identify your requirements.

Improvements

Requirement	Needs work	Don't know	Meets requirement
Does the organisation improve response activities by incorporating lessons learned from current and previous detection and response activities?			

Does the organisation update digital security incident response plans routinely to incorporate lessons learned?

Recovery Planning

Requirement	Needs work	Don't know	Meets requirement
Does the organisation execute documented recovery processes designed to ensure restoration of systems and assets affected by cybersecurity incidents?			

Does the organisation execute its recovery plan during or after a digital security incident?

Recovery Communications

Requirement	Needs work	Don't know	Meets requirement
Does the organisation communicate with internal and external parties during recovery activities in accordance with a communications strategy?			

Does the organisation manage public relations following a digital security incident in accordance with a documented communications strategy?

Does the organisation evaluate its digital security compliance, adjust policies and practices, and communicate these changes with stakeholders to protect its reputation following a digital security incident?			
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--	--

Does the organisation communicate recovery activities to internal and external stakeholders?

Your No-Obligations Demonstration

If you would like a demonstration of the New Zealand Cybersecurity register, click or scan the QR code. →



About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance helps you forge a clear path to compliance.

With LexisNexis content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.

- Find relevant obligations faster with jargon-free registers that are aligned with your business processes.
- Stay up to date with near real-time alerts delivered straight to your inbox when you may be impacted by regulatory change.
- Explore your compliance obligations under a particular regulator, or a particular compliance source, with SourceData.
- Engage with the wider compliance community and LexisNexis experts through the Community Portal, our self-support platform.
- Access comprehensive, current LexisNexis content that meets your unique needs, with key core modules relevant to all businesses, and a rapidly accelerating roadmap of industry-specific modules that guide your path to compliance.

Authored by leading legal, attorney and industry experts, and supported by flexible technology that works the way you do, LexisNexis Regulatory Compliance gives you peace of mind while saving time and money.

Call 0800 800 986

Email compliance@lexisnexis.co.nz

Visit www.lexisnexis.co.nz/compliance

About LexisNexis

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 175 countries, across six continents, with over 10,000 employees.