Module	**CYBERSECURITY**
Jurisdictions	**NEW ZEALAND**
Legal Expert	**TANIA GOATLEY** Partner at Bell Gully https://www.bellgully.com/our-people/tania-goatley/ https://www.linkedin.com/in/tania-goatley-0310119a/

Module Scope

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

Does the organisation have systems and procedures in place to manage and maintain software, devices and external system inventories, and does it implement security measures designed to protect the confidentiality, integrity and availability of data, digital services and information systems?

Does the organisation conduct a risk assessment to determine its digital security risks and identify available responses, and does it develop a risk management strategy to address identified risks?

Does the organisation have processes in place to ensure and protect data security and digital assets, and does it have processes in place to control access to information systems?

Does the organisation provide its workers with training on digital security and the organisation's processes and procedures?

Does the organisation have procedures in place to ensure the security of information systems undergoing maintenance or repair, and does it monitor information system assets, network traffic and the activities of personnel to detect potential cybersecurity events?

Does the organisation have incident response measures in place to effectively respond to and manage any cybersecurity incidents, and does it effectively communicate with all relevant stakeholders and affected parties?

Module Application

The NEW ZEALAND CYBERSECURITY module can assist organisations to create an effective and appropriate digital security framework on any scale. Organisations should consider the following questions:

- Does your organisation transact with New Zealand residents online?

- Does your organisation store information collected from New Zealand residents on local hardware, using third party storage provider, or in the cloud?
- Does your organisation rely upon digital systems to conduct operations or possess commercially sensitive data?

If the organisation answers 'yes' to the above, then the NEW ZEALAND CYBERSECURITY module is relevant to them.

The NEW ZEALAND CYBERSECURITY module is divided into 21 topics. These topics reflect the format of the National Institute of Standards and Technology (NIST) in the United States. The module follows the format of the NIST Framework for Improving Critical Infrastructure Cybersecurity and provides a sequential process for constructing a risk-management-based framework of cybersecurity measures.

The 21 topics are:

1. Asset Management
2. Business Environment
3. Governance
4. Risk Assessment
5. Risk Management Strategy
6. Supply Chain Risk Management
7. Identity Management, Authentication and Access Control
8. Awareness and Training
9. Data Security
10. Information Protection Processes
11. Maintenance
12. Protective Technologies
13. Anomalies and Events
14. Security Continuous Monitoring
15. Detection Processes
16. Response Planning
17. Communication
18. Mitigation
19. Improvements
20. Recovery Planning
21. Recovery Communications

The New Zealand Government Communications Security Bureau (GCSB) has published the following resources:

- The Protective Security Requirements, a policy framework that outlines the New Zealand government's expectations for security governance, personnel security, information security and physical security
- The New Zealand Information Security Manual, a manual that complements the Protective Security Requirements framework and provides current best practice guidance on the subject of information security to both agencies and organisations

Organisations with digital operations in New Zealand should select and adopt a suite of governance measures and security controls from these resources to demonstrate compliance with their obligation to implement reasonable digital security measures.

The NEW ZEALAND CYBERSECURITY module also covers legal requirements from New Zealand as well as international sources, including:

- Privacy Act 2020
- Harmful Digital Communications Act 2015
- Crimes Act 1961
- Telecommunications (Interception Capability and Security) Act 2013
- Federal Trade Commission Act 1914 (USA)
- National Institute of Standards and Technology Special Publication 800-53 (Rev. 5) (USA)
- Centre for Information Security Controls (USA)
- Data Protection Act 2018 (UK)
- General Data Protection Regulation (EU)
- Regulation (EU) 2016/679 (General Data Protection Regulation)
- Privacy Act 1988 (Cth)

The digital environment is transnational by nature. Organisations that intend to offer digital services in New Zealand should maintain awareness of their obligations under international laws, particularly in relation to the following:

- The General Data Protection Regulation of the European Union
- The Federal Trade Commission Act of 1914 of the United States
- The Data Protection Act 2018 (UK) of the United Kingdom
- The Privacy Act 1988 (Cth) of Australia

The module also covers the possible consequences to organisations that fail to comply with their relevant obligations, which include:

- National and international penalties
- Monetary penalties
- Compensation and damages
- Investigations by the Privacy Commissioner

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.