RiskNZ

WELCOME TO

RiskNZ Lunchtime Seminar: 28 March 2023

RiskNZ is proudly sponsored by:

Premier Sponsors

Camms.

AON

PROTECHT
Redefining Risk

LexisNexis®

Sponsors

F24

Insurance
BUSINESS NZ

Cyber Risk, Reg-Change & Operational Resilience: Forge Your Path to Compliance

Kieran Seed
Head of Content
LexisNexis Regulatory Compliance

Michael Nelson
Senior Product Specialist,
LexisNexis Regulatory Compliance

Kieran Seed, Head of Content - Global LexisNexis *Regulatory Compliance*

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

Kieran Seed is the Head of Content-Global for LexisNexis Regulatory Compliance, supervising and coordinating the development of complex compliance data sets locally and internationally. Kieran's expertise lies at the nexus of compliance, law and content, to help organisations understand and monitor their compliance requirements in an accelerating and ever-changing regulatory landscape. Kieran's team of subject matter experts manage a wide content set across the Pacific, and SEA, and also collaborate closely with content teams across the globe to bring the Regulatory Compliance solution to new markets and jurisdictions.

Scan to Connect on

Michael Nelson, Senior Product Specialist LexisNexis *Regulatory Compliance*

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

Michael Nelson has worked in a number of industries over the course of his professional career, including the performing arts, the Commonwealth Public Service, a decade with a boutique insolvency practice specialising in forensic accounting and litigation, and is now a Senior Product Specialist with international information provider, LexisNexis Regulatory Compliance. He is also chair of the renowned Australian Network for Art and Technology (http://www.anat.org.au/).

Scan to Connect on

LexisNexis® | *Regulatory Compliance*

Cyber Risk, Reg-Change & Operational Resilience: Forge Your Path to Compliance

28 March 2023

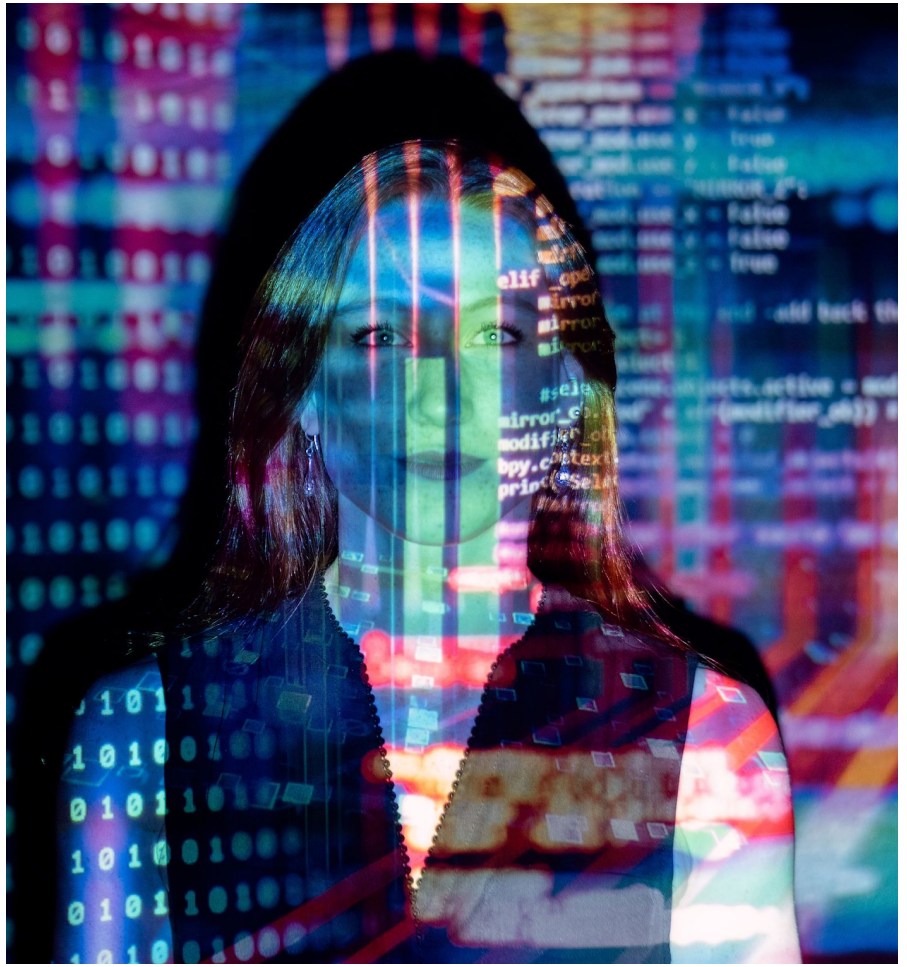
Michael Nelson and Kieran Seed

LEGALTECH BREAKTHROUGH AWARD 2021
OVERALL REGTECH SOLUTION OF THE YEAR

Today's Discussion

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

- NZ's current legislation and recent cyber breaches
- Three key focus areas in cybersecurity
- The local/global regulatory landscape and current compliance challenges
- The Regulatory Compliance difference
- Q&A



LexisNexis® | *Regulatory Compliance*

Around for **200** years

Part of RELX Group

Global provider of information and analytics

Compliance coverage in **8** jurisdictions

11,000+ Employees

20+ leading GRC platform partners

Over **250** Regulatory Compliance customers

Customers across **150+** countries

RiskNZ

Financial Services Federation

Governance New Zealand

Governance Institute of Australia

RMIA

GRC Institute

Proudly recognised for our support in the industry

LEGALTECH BREAKTHROUGH AWARD 2021 — OVERALL REGTECH SOLUTION OF THE YEAR

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.

POLLING QUESTION #1

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

What are the biggest compliance issues you are facing today?

A. AML/CFT and sanctions
B. Financial markets regulation
C. Cyber and security risks
D. Other

Current legislation and recent cyber breaches

Legislative Requirements

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

NZ Legislation

- Privacy Act 2020 (NZ)
- Harmful Digital Communications Act (NZ)
- Crimes Act 1961 (NZ)

International Legislation

- General Data Protection Regulation (EU)
- Federal Trade Commission Act 1914 (USA)
- Data Protection Act 2018 (UK)
- Privacy Act 1988 (AU)

Standards and guidelines

- New Zealand information security manual
- New Zealand Protective Security Requirements
- National Institute of Standards and Technology guidelines and tools
- Institute of Directors — Cyber-risk practice guide
- NCSC cyber resilience guidance

NZ Cyber Breaches

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

- The average number of incident reports per quarter is 2,124 and average direct financial loss is $4.6 million.
- $3.5 million in direct financial loss was reported in Q4. 26% of incidents reported financial loss.
- 1,757 incidents were responded to by CERT NZ in Q4 2022, down 15% from Q3 2022
- Ransomware reports increased 500% from Q3 2022.
- Between August and September 2022 Cisco 6700 business leaders in 27 countries, and found that in Aotearoa only 14 percent of organisations in New Zealand have a high level of readiness for the cybersecurity risks.

CERT NZ Quarter Four Cyber Security Insights 2022

Cybersecurity Readiness Index

NZ Cyber Breaches

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

- 6 December 2022 – the NZ Ministry of Justice announced that an external company that provided IT services to a third-party provider the Ministry has contracts with was subject to a cyber attack.
- The incident had affected access to approximately 14,500 coronial files relating to the transportation of deceased people, and approximately 4,000 post mortem reports.
- The MOJ sought and obtained orders from the High Court preventing people from accessing, sharing or publishing confidential and sensitive coronial and health information at the centre of a recent cyber security incident.
- On 18 January 2023, the MOJ advised that the people responsible for the wider incident have released information, not related to coronial, on the dark web.

NZ Ministry of Justice

NZ Cyber Breaches

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

- 16 March 2023 – Latitude Financial (trading as GEM Finance in NZ) announced that it had been subject to a cyber attack.
- The attack apparently originated from a **major vendor** used by Latitude. Having obtained Latitude employee logins, the attacker appears to have used them credentials to steal personal information **held by two other service providers**.
- 7.9 million Australian and New Zealand driver licence numbers were stolen, of which approximately 3.2 million, or 40%, were provided to us in the last 10 years.
- In addition, approximately 53,000 passport numbers were stolen, **of which at least 1,300 belong to New Zealand citizens.**
- A further approximately 6.1 million records dating back to at least 2005 were also stolen, of which approximately 5.7 million, or 94%, were provided before 2013

Three Key Focus Areas in Cybersecurity

Cyber Resilience in Financial Services

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

FMA Cybersecurity & Operational Resilience

- Shortcomings in cyber resilience and operational systems - underinvestment in tech, legacy systems
- Must have adequate and effective systems, policies, processes and controls
- IT systems used to deliver service must be secure and reliable, perform efficiently and risks are managed

AU CPS 234 Information Security

- Applies to all APRA-regulated entities
- Obligations include defining information security-related roles/responsibilities, and implement appropriate protections of information assets

AU CPS 230 Operational Risk Management

- Consultation closed 21 October
- Designed to strength management of operational risk, including updated reqs for business continuity and service provider management

Security of Critical Infrastructure

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

NZ Voluntary Cyber Security Standards for Control System Operators

- Latest version released 2019
- Draw content from standards/guidelines of US bodies e.g. NIST
- Mandatory future cyber framework?

AU Security Legislation Amendment (Critical Infrastructure) Act 2021

- Effective December 2021
- Significantly expands sectors considered critical infrastructure
- New government assistance obligations
- Requirement to provide notice of any cybersecurity incident w impact on critical infrastructure assets

AU Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

- Effective April 2022
- Responsible entities to create/maintain critical infrastructure risk management program
- Enhanced cybersecurity obligations for operators of systems of national significance

Aligning to ISO Standards

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

- ISO 27001 – global standard for information security management systems (ISMS) and their requirements.
- Additional best practice in data protection and cyber resilience covered by more than a dozen standards in the ISO 27000 family
  - 27002:2022 – Reference set of generic information security controls
- Enables organisations to manage security of assets including financial information, intellectual property, employee details or third-party information
- Certification demonstrates a company's compliance with well-recognised standards and provides assurance on robustness of information security

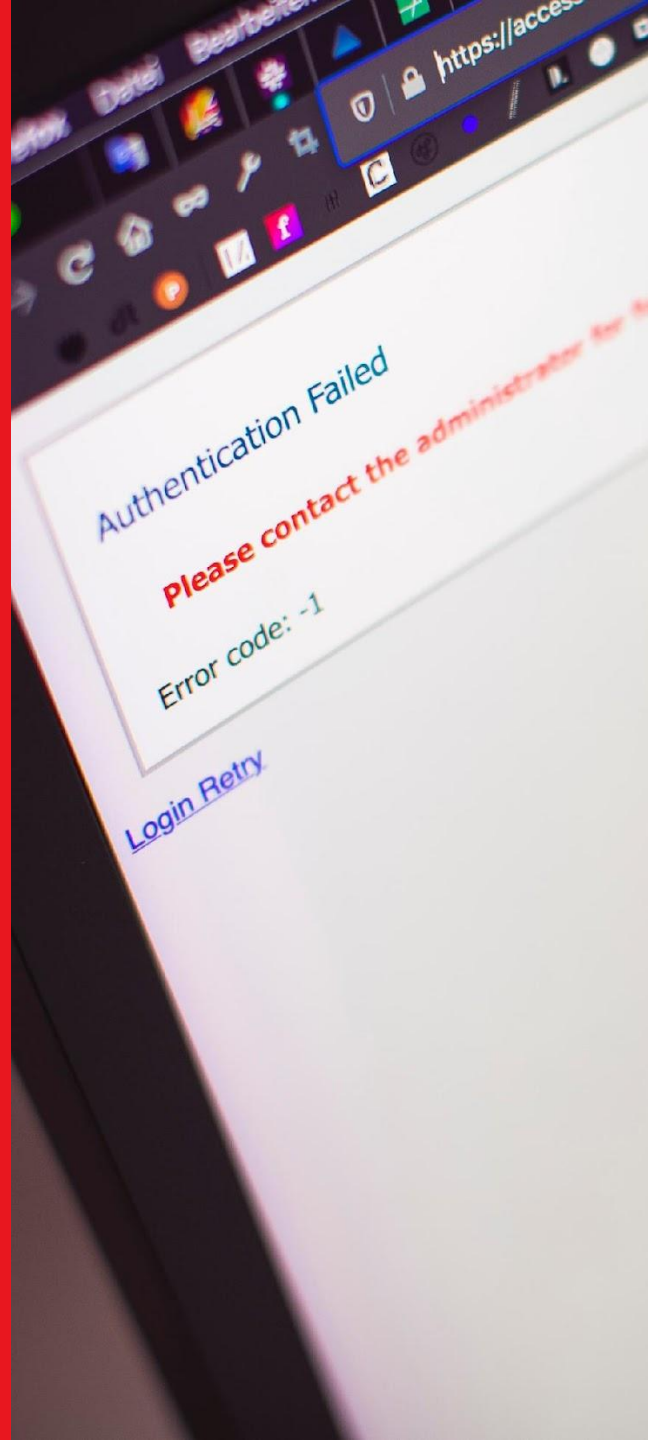
POLLING QUESTION #2

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

Which of the following focus areas has been your biggest priority?

A. Cyber security and operational resilience
B. Alignment to national/international frameworks
C. Horizon scanning and forecasting regulatory change
D. Other

Regulatory Landscape & Compliance Challenges



NZ Change Context: A Refresher

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

Privacy Act 2020

- New privacy breach notification framework
- Expanded enforcement powers for Privacy Commissioner
- Stronger cross-border protections
- New offences, with fines of up to $10k

Consumer Data Rights

- Orgs to share data held about consumers with 3rd party data recipients
- Exposure draft of framework to be issued for consultation 2023
- Banking the first designated sector

Further privacy reform?

- Consultation on biometric technologies
- Changes to Privacy Act 2020 to address indirect collection

2022–23 Action Plan for the Digital Strategy for Aotearoa

Flagship Initiatives include:

- Digital Identity Services Trust Framework
- Christchurch call
- Rollout of Cyber Security Strategy
- Māori Data Governance

AU Privacy Act Review Report (submissions close 31 March 2023)

Includes expansion of personal information, strengthening consent reqs, including a 'right to erasure'

Fines increased to $50 million / 3 times value of benefit obtained from info misuse / 30% adjusted annual turnover (which higher)

LexisNexis®
Regulatory Compliance

Important Changes from the Privacy Act 2020

Scan the QR code to download the infographic

Privacy Act 2020
Repeals and replaces the Privacy Act 1993

Here are the key changes that businesses and organisations should expect and prepare for ▸▸

Notifiable Privacy Breaches
If a breach causes serious harm to someone (or is likely to), the Office of the Privacy Commissioner and the affected people must be notified as soon as possible.

Privacy Commissioner Increased Powers
- Publishing compliance notices
- Making binding decisions on access requests
- Strengthened information gathering powers

Cross Border Disclosures
New controls ensure that personal information being sent offshore will be subject to comparable privacy safeguards as those that apply in New Zealand.

Increased Powers of the Privacy Commissioner

PUBLISHING COMPLIANCE NOTICES: Requiring a business or organisation to do, or stop doing something, if they are not meeting their Privacy Act obligations.

MAKING BINDING DECISIONS ON ACCESS REQUESTS: In investigating complaints about businesses organisations failing to give people access to their personal information, the Commissioner can now make binding decisions on these complaints and issue an access direction.

STRENGTHENED INFORMATION GATHERING POWERS: The Commissioner can shorten the time-frame for agencies to comply with investigations.

Class Actions
Now permitted for privacy breaches.

New Criminal Offences with Penalties
- To mislead a business or organisation by impersonating someone, or pretending to act with that person's authority, to gain access to their personal information or to have it altered or destroyed.
- To destroy a document containing personal information, knowing that a request has been made for that information.

Increased Fines for Organisations that Don't Comply

UP TO $10k **Notifiable Privacy Breaches**
Failure to notify Commissioner of notifiable privacy breach

UP TO $10k **Increased Powers of the Privacy Commissioner:**
A failure to comply with access orders without reasonable excuse

How to Prepare for These Changes

Updating privacy policies to reflect these changes

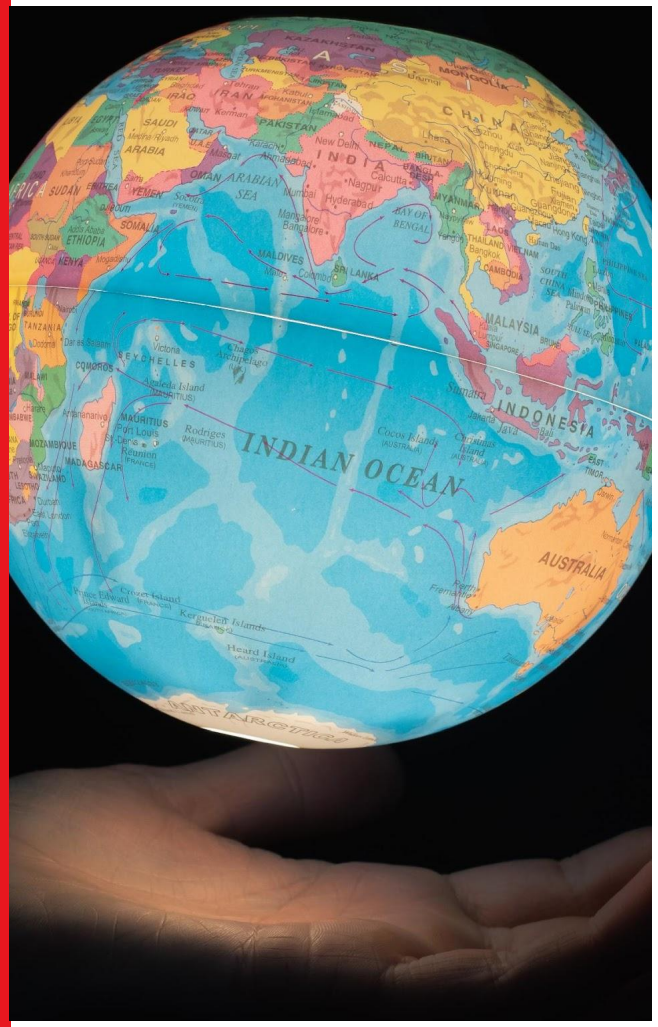
Educating key staff of these changes to the Act through training

Reviewing your current processes and management of information

Processes are clearly defined for personal data breaches

Global Legislative Landscape

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance



Australia

- CDR scheme in banking & energy – telecom next
- Online Safety Act & the Basic Online Safety Expectations

European Union

- Schrems II and the EU/US Privacy Shield (Schrems III?)
- e-Privacy Regulation – position adopted by EU Council
- Agreement on NIS 2 Directive and Data Governance Act

United Kingdom

- Brexit and the UK-GDPR
- Data Protection and Digital Information Bill 2022

United States

- California Consumer Privacy Act - Comparative laws in Colorado, Connecticut, Virginia, Utah from 2023
- New York SHIELD Act
- Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) from March 2022 - protections and guidance to entities in critical infrastructure sectors

China

- 2021 Data Security Law
- 2021 Personal Information Protection Law

Hong Kong

- Personal Data (Privacy) (Amendment) Ordinance 2021 (anti-doxxing legislation)
- Proposed PDPO Reforms – back on 2023 agenda

Japan

- Amended Act on Protection of Personal Information (effective April 2022)

Singapore

- Personal Data Protection (Amendment) Act 2020 – increase to financial penalties from October 2022

Current Compliance Challenges

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

Increasing complexity of regulatory regimes

- Multiple, disparate, pieces of legislation feed into regulatory obligations; ~400-700 instruments per organisation
- Increased use of extraterritorial powers (e.g. UK Modern Slavery Act, US FCPA)

Larger and broader penalties and enforcement action

- Privacy breaches - Facebook $5bn (US), Amazon €746 million (GDPR)
- Reputational harm from negative media reporting and perception

Accelerating regulatory changes

- Thousands upon thousands of legislative changes each year
- 3-5 times more regulatory activity during pandemic – 'COVID normal' is a higher pace of regulatory change

The challenge of achieving continuous compliance in an evolving regulatory landscape

POLLING QUESTION #3

RiskNZ Lunchtime Session | Cyber Risk, Reg Change & Operational Resilience: Forge Your Path to Compliance

What is the main driver of your regulatory compliance program?

A. Improving enterprise risk management
B. Aligning to regulations
C. Meeting the requirements and expectations of stakeholders
D. Fear of non-compliance and associated penalties

Responding to the Challenges

- Breaking down barriers between IT, legal, risk & compliance systems/teams – allow all levels to engage
- Scope the primary and secondary legal landscape of your privacy, cybersecurity, and other compliance reqs – identify liability across roles
- Continually monitor latest legal/regulatory developments to stay compliant in relevant jurisdictions
- Conduct ongoing horizon scanning on the changing global compliance landscape
- Ensure accountability is delegated/dispersed effectively and ensure ongoing, transparent reporting

LexisNexis *Regulatory Compliance*
DELIVERS A CLEAR PATH TO COMPLIANCE

The LexisNexis Regulatory Compliance Difference

- Legal obligations register and alerting solution that combines regulatory content with technology to empower customers to take control of their compliance obligations
- Practical, **plain language** interpretation of all relevant legislative and regulatory materials
- **Ongoing notifications** and content updates and
- **Expert authorship** across the entire content development process
- Supporting content with **flexible technology** options

THE RESULT

Turning **4 hours** of compliance research
into **10 minutes** of clarity

Your clear path to compliance | LexisNexis Regulatory Compliance

Legislation Change
[NZPV41] PCI Security Standards Council: Updated PCI DSS v4.0 validation documents

ALERT → MONTHLY SUMMARY → OBLIGATION → MODULE

Advanced and ongoing notifications of regulatory change

Timely notifications guiding you to actionable items

Customers receive monthly summary on Privacy

Continuous improvement of content portfolio

Obligation: Payment Card Industry Data Security Standard

Practical content developed across ALL modules

Up-to-date Privacy Module from LexisNexis

Comprehensive & simplified view of your obligations register

LexisNexis® | *Regulatory Compliance*

Global Cybersecurity Checklist

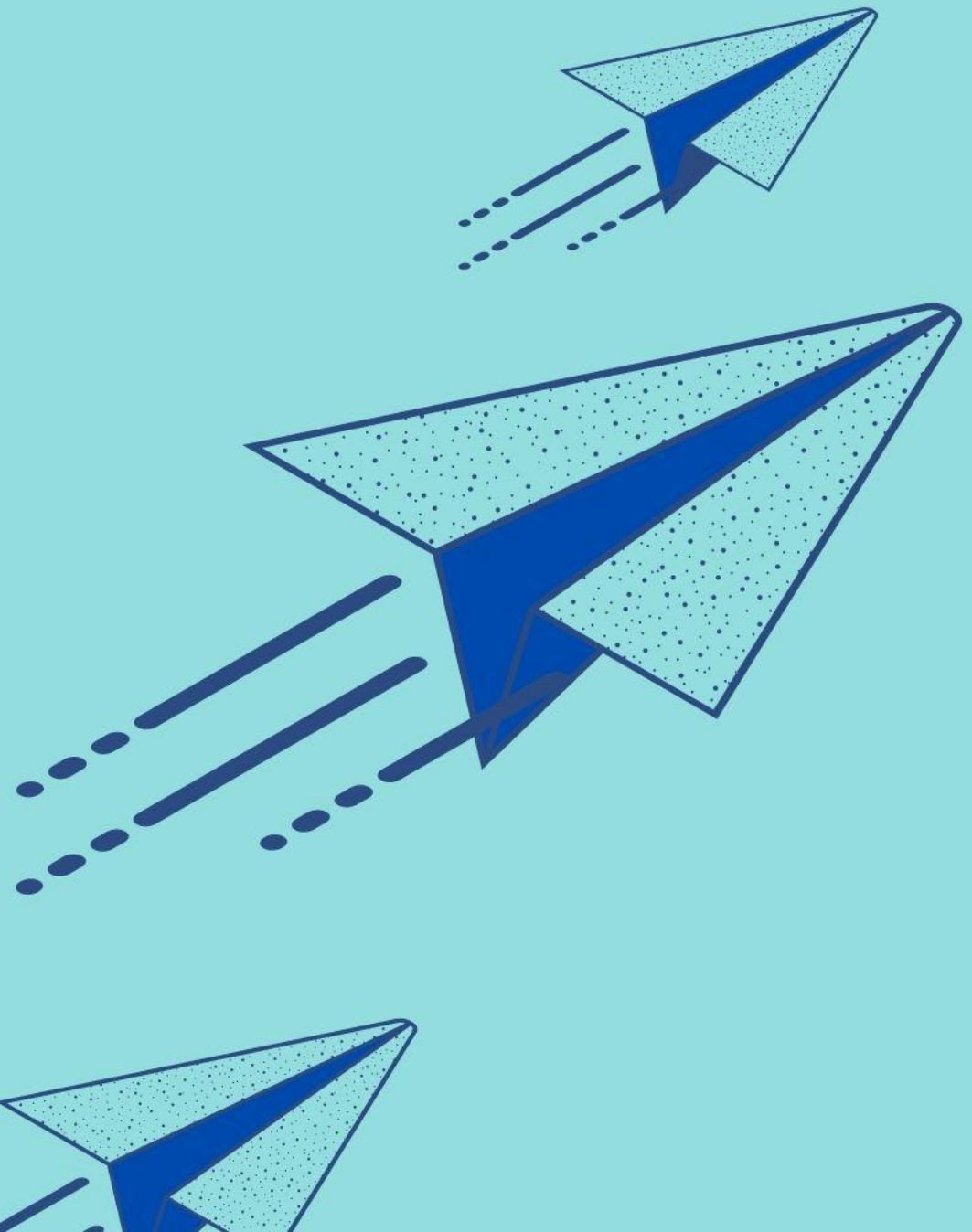
Does your organisation understand how to navigate the legislative and compliance requirements that surround the cybersecurity framework when using data locally and internationally? As cybersecurity and data breaches continue to make the news, is your organisation prepared to meet its cybersecurity compliance obligations?

This checklist guides you to identify your global cybersecurity compliance requirements. It covers Risk Management Strategy, Supply Chain Risk Management, Data Security, Recovery Planning and more.

Gain clarity on your cybersecurity obligations, scan the QR code and download the checklist today!

Do you have any questions?

Type them into the Q&A platform



RiskNZ

Thank you for joining us today