

TRAINING & DEVELOPMENT

Cyber Risk & Information Security Management



 **PROTECHT**

 **RiskNZ**



RiskNZ

RiskNZ is the leading non-profit association for risk professionals in New Zealand. The Society brings together people and organisations managing risk under the guiding vision that New Zealand prospers when risk is well managed. Our focus is to organise regular opportunities for members to meet and experience a wide variety of professional development and networking opportunities.

The society supports special interests groups, encourages research, informs public thinking, influences government, and conducts other activities to achieve risk management best practice in the private and public sectors.

Training & Development

RiskNZ is proud to partner with Protecht to bring the latest in training and development opportunities.

www.risknz.org.nz



Protecht helps create the risk leaders of tomorrow by providing risk training that meets people where they are in their risk management journey.

It is an online learning platform that enables delivery of Protecht's risk methodology training to individuals or organisations that is backed by decades of industry experience, an understanding of risk management challenges learned through ongoing engagement with Protecht customers and the risk community, and a commitment to high quality training materials.

Protecht Academy courses are broken down into two Catalogs:

Organisational Risk Excellence

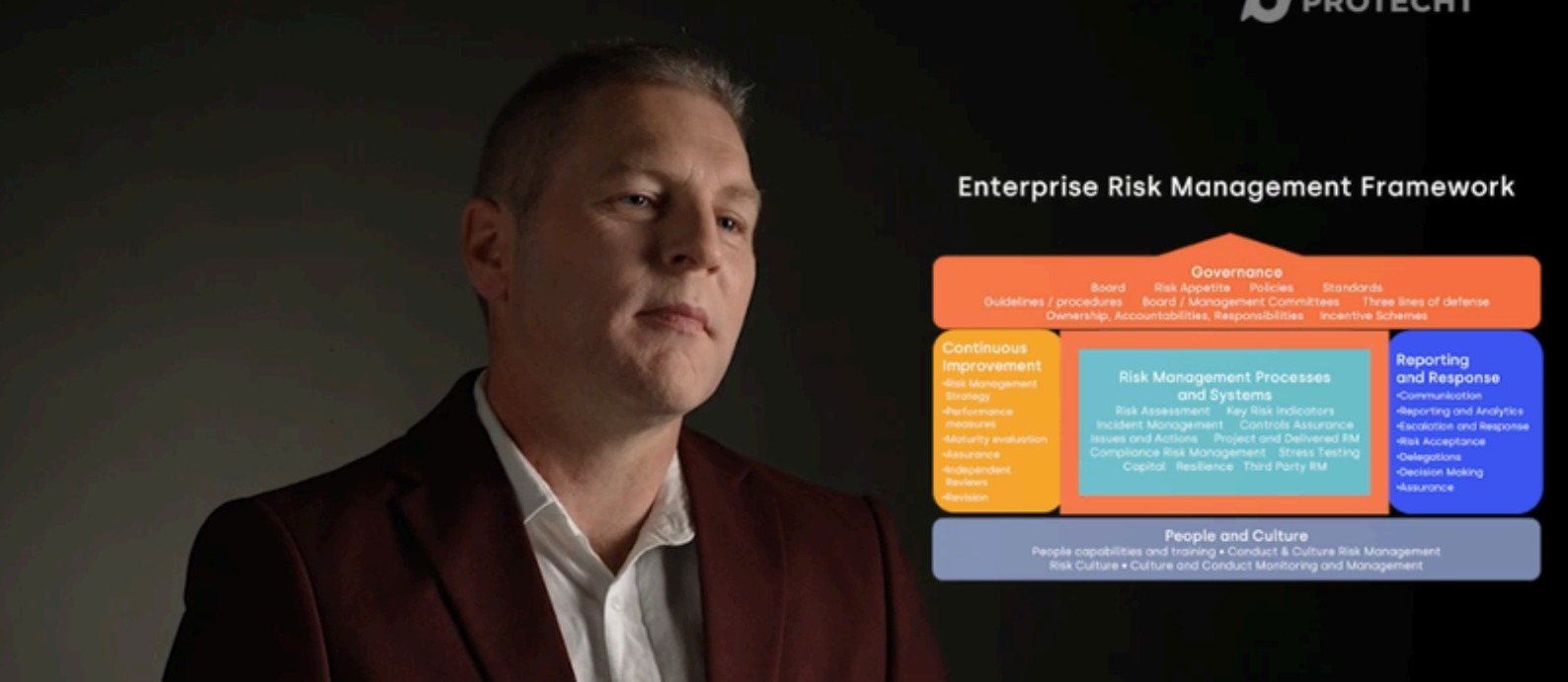
Primarily intended for groups and organisations

Risk Management Mastery

Aimed at individuals or for teams looking to up-skill in a specific area.

See all courses available [here](#):

Note: By completing and submitting a course application form (online, emailed request or in any other form that was used to make a training booking), you are agreeing to [Protecht Academy User Terms & Conditions](#) and [RiskNZ's Training Terms and Conditions](#).



Enterprise Risk Management Framework



Cyber Risk & Information Security Management

Course Overview

Cyber and information security are no longer just technical issues, they are critical business risks that demand enterprise-wide management. This course bridges the gap between cybersecurity frameworks and enterprise risk management, helping you connect your cyber controls, assurance, and governance practices to your broader organisational risk objectives. Whether you're a cyber leader seeking to align with risk frameworks, or a risk professional expanding into the cyber domain, this course will give you the clarity and confidence to bring the two worlds together.

Through relatable stories, real-world examples, and practical tools, you'll learn how to design and implement cyber risk management processes that integrate seamlessly with your enterprise risk management framework. We'll cover the key components of cyber and information security management—from frameworks and governance, to metrics, incident response, and risk appetite—equipping you to provide meaningful assurance and insight to executives and boards.

Our trainers David Tattam – Chief Research & Content Officer, Michael Howell – Head of Risk Research & Knowledge, and Michael Franklin – Cyber Security Lead guide you through Protecht's approach to managing cyber risk within an enterprise context. You'll finish with a complete, ready-to-use toolkit to embed effective cyber risk management, align with standards such as ISO 31000 and NIST, and drive a culture of informed risk-taking—not risk avoidance—across your organisation.



Cyber Risk & Information Security Management

In this course, you'll learn:

1. The Need for Cyber Risk Management

- Introductory definitions
- Business drivers
- Social drivers
- Dynamic drivers
- Regulatory drivers

2. Defining Cyber Risk

- Definitions of risk
- Definitions of cyber risk and information security
- Components of risk
- Introduction to risk bow ties
- How cyber overlaps with privacy, technology and data risks
- Integrating cyber into an enterprise risk taxonomy

3. Defining Cyber Risk Controls

- Definition of controls
- 7 treatment methods to manage cyber risk
- How to map controls to components of risk
- The use of cyber-related control frameworks and standards
- Contrasting compliance and risk, and handling controls that aren't controls

4. Cyber Risk Management Frameworks & Processes

- Applying ISO 31000 steps to cyber risk management
- Applying an Enterprise Risk Management Framework to cyber risk management
- Aligning cyber-specific frameworks to Enterprise Risk Management frameworks
- Common risk management processes applied to cyber

5. Cyber Risk Appetite

- Setting appetite for objectives and risks
- Setting risk appetite for cyber
- How to use risk appetite

6. Cyber Risk Assessment

- Stages of a risk assessment
- An overview of risk assessment techniques
- Scoping the risk assessment – enterprise, process or asset
- Understanding risk and controls using bow ties
- Considering inherent risk, residual risk, and the effect of controls
- Evaluating risk assessment against risk appetite
- Writing risk scenarios
- Aligning cyber specific methodologies with enterprise risk assessment

7. Measuring Cyber Risk

- Why we measure risk
- The common measures of risk
- Main types of risk measurement
- Qualitative measurement
 - Risk matrices and subjective approaches
 - Challenges with the risk matrix
- Semi-quantitative methods
 - Scoring models for risk
 - Scoring models for controls
 - Challenges and assumptions in scoring models
- Quantitative measures
 - Risk as a distribution
 - Types of quantitative measures
 - Challenges of risk quantification
 - A simplified linear quantification approach
- Data sources to measure components of cyber risk
 - Internal sources of data
 - External sources of data

8. Cyber Risk Metrics

- The purpose of risk metrics
- The types of risk metrics
- Characteristics of good metrics and pitfalls to avoid
- Defining zones and thresholds
- How to use metrics for escalation, reporting and response
- Metrics for risk versus information security capability

9. Cyber Controls Management

- The need for controls assurance
- Distinction between internal assurance and external assurance
- Difference between governance controls and technical controls
- Documenting controls information
- Mapping control frameworks
 - Mapping controls you apply to external frameworks and standards
 - Challenges and approaches to mapping multiple frameworks
- Control testing versus controls assessment
- A control testing process
 - Importance of control objectives
 - Assessing design effectiveness
 - Assessing operating effectiveness
- Controls assessment over a group of controls
- Considering automated controls
- Applying outcomes of controls management activities
- A Control library and testing template

10. Cyber Incident & Crisis Management

- Defining cyber incidents
- An enterprise approach to incident management
- Distinctions for cyber incident management

11. Issues and Action Management

- Raising issues
- Common ways that issues arise or are identified
- Ownership and tracking
- Linking to other components of risk management
- Action management
- Tracking actions and reporting
- Alignment between systems or reporting mechanisms
- Dangers when actions are ignored

12. Reporting & Communication

- The purpose of reporting
- Main types of reports
- What to report
- Considering stakeholders
- Collecting data for reporting
- Report examples

13. Integrating with Enterprise Risk Management

- Benefits of integration
- Integrating cyber risk processes within the ERMF 'House'
- Managing shifting cyber exposure during Risk In Change
- Cyber Compliance Management
- Alignment with Operational Resilience framework
- Alignment with Third Party Risk Management
- 14. Responsibilities for Cyber Risk Management
- Everyone as a risk manager
- The Three Lines Model
- Roles related to cyber risk management
- Key behaviours that support strong risk culture

Course expectations

- Watch 14 videos
- 7 Interactive examples
- Access 14 downloadable materials
- Answer 10 quiz questions

Timings

- 5.5 hours of video content
- Approximately 6.5 hours for the whole course

Register, Receive Invoice, Payment, Set-up with Log In To Course

Cost: RiskNZ Members: \$875+GST | Non-member: \$1000+GST

Next steps

Register now via: adminofficer@risknz.org.nz Please contact RiskNZ directly if you would like to discuss packages to implement this training across your organisation. Bulk discounts are available.