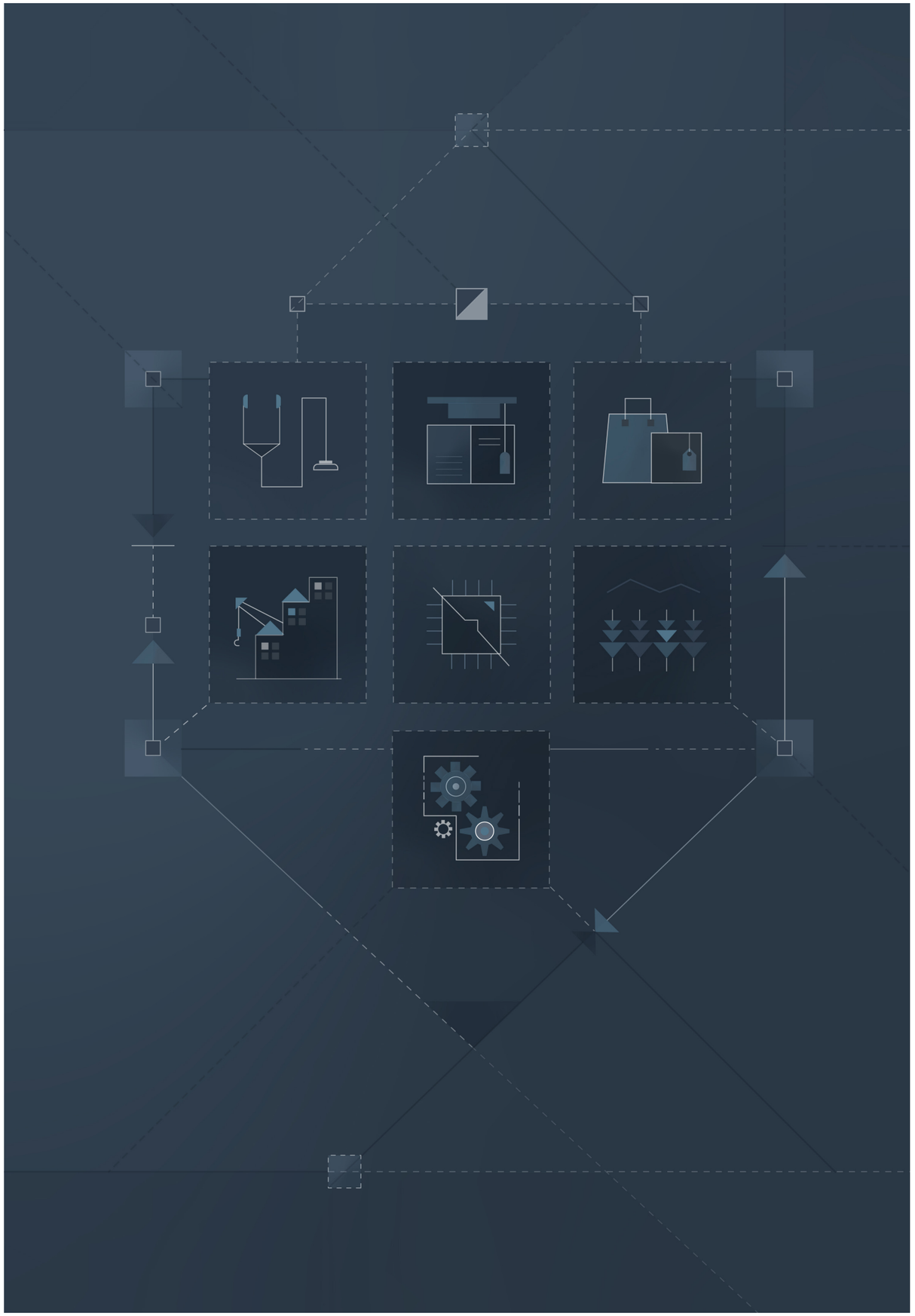
KordaMentha

Virtual CISO solutions

Retainer-based cybersecurity management

kordamentha.com



Retainer-based cyber risk management

We partner with our clients long-term, providing ongoing and on-demand access to independent and trusted cyber risk management and support.

Cybercrime poses a significant threat to business viability worldwide and ranks among organisations' key enterprise risks. Unknown risks can leave organisations vulnerable to cyber breaches and the impacts may be far reaching. From financial and intellectual property loss, reputational damage, and regulatory action, such incidents hinder client relationships and trust and dampen future growth potential whilst introducing a raft of additional operational risks, such as legal liability. With the increased regulatory scrutiny and shifting public sentiment around cybersecurity and data protection, business leaders need access to specialist cybersecurity expertise to navigate these issues, understand their obligations, mitigate risks, and minimise losses.

While cybercrime presents ongoing and evolving risks, many organisations lack the capacity, resourcing, or budget allocations to achieve a level of cybersecurity aligned to their risk appetite and compliance obligations. KordaMentha partners with boards, C-suite, and other senior executives to uplift their cybersecurity capability and enhance cyber resilience. With specialised knowledge and experience in cybersecurity governance, we help organisations achieve, and maintain, better practices in cybersecurity.

Through a retainer-based model, we assemble a dedicated, multi-disciplinary team of cybersecurity professionals to provide virtual Chief Information Security Officer ('vCISO') capabilities and on-demand expert advice and practical assistance. We leverage clients' existing resources to uplift capability and/or capacity to anticipate, innovate, and adapt as the risk and threat landscape evolves.

Virtual CISO solutions

KordaMentha delivers practical solutions to cyber advisory, consulting, and risk management.

Through our tailored vCISO offering, clients can customise the retainer-based service to suit their unique requirements. We provide organisations with timely, relevant, and impactful cybersecurity advisory and support services as and when they need them.

Our partnership model allows clients to attain a more sustainable level of cyber resilience while mitigating operational and business risks. We help clients understand their organisational cyber risk relating to information, people, processes, and technology. We then provide clients the support to determine their risk appetite and risk tolerance, consider the effectiveness of existing policies, procedures, and controls, and identify any gaps that could result in unacceptable cyber and business risk.

Our approach

KordaMentha's vCISO services provide a flexible, customisable approach to cyber risk governance and management to help our clients meet their operational and strategic goals.

Our dedicated team will schedule an initial briefing session to understand your specific requirements and work with you to devise a plan. We work collaboratively to understand your needs, priorities, and interests.

We then tailor, and agree on, your scope of works. Understanding that business needs evolve, our vCISO services are designed to adjust to changes as they arise.

Indicative parameters for a retainer agreement

Agreement term

Clients can select the agreement term that best suits their needs, from 12 months and above.

Service access

Our clients benefit from a prioritised access to our cybersecurity expertise. Over the course of our engagement, we will work with you on a retainer basis to provide cost certainty and peace of mind. Any unused credits at the end of each month can be carried over to the next period or can be used for additional cybersecurity related training or other services, as required.

How we can help you

We provide specialist cybersecurity services including high-level orchestration of essential tasks through to more comprehensive or extensive strategic and operational assistance. Our cybersecurity experts work with you to customise a service arrangement to your needs. This includes identifying any gaps in your current capabilities and incorporating the areas of focus and the depth or breadth of assistance you may need. We conduct regular review sessions with you to ensure the vCISO service agreement remains flexible and aligned with your needs and circumstances.

Cybersecurity governance

Diligent and effective cybersecurity begins with governance. We assist organisations with designing and implementing strong governance, operating models, and risk reporting frameworks. KordaMentha has extensive experience working with boards and C-suite professionals and partnering with internal teams to implement the best approach. We balance stakeholder management, time sensitivities, and cost. Our governance offering may include, but is not limited to:

- Participating in monthly audit and risk committee activities.
- Conducting independent reviews of relevant board papers, such as strategy and budgeting, and providing advice on the identification and management of relevant cyber risks.
- Reviewing, developing, and managing policy documents.
- Periodic cybersecurity governance reporting. This may include tracking of risks and adherence to compliance obligations and monitoring the alignment of performance to risk appetite.
- Cybersecurity governance mentorship, education, and exercises.

Cyber risk management

Beyond managing your risks related to systems and data, effective cyber risk management also helps with mitigating and minimising both financial and reputational losses. Our vCISO offering includes proactive and ongoing cyber risk identification and management, including periodic incident response planning and testing.
This may include:

- Guidance on the identification and definition of the organisation's cyber risk appetite.
- Cyber risk diagnostics, compliance assessments aligned to standards such as ISO/IEC 27001, and gap assessments aligned to regulatory requirements such as APRA CPS-234 and CPS-230.
- Maturity assessments against the Australian Cyber Security Centre Essential Eight, the NIST Cybersecurity Framework ('NIST CSF'), and other relevant standards and guidelines.
- Third-party risk identification, assessment, and management.
- Incident response preparedness project management.

Cybersecurity strategy

Cybersecurity is a critical enterprise risk for all organisations that goes well beyond technology platforms and systems. For modern organisations, cyber risk is a central element of their strategic and operational ambitions. Maximising both security and resilience requires an action plan for how an organisation will protect itself from cyber threats. Focusing on security principles and resource allocation, our experts help to ensure your cybersecurity strategy is appropriately planned and aligned with your specific organisational goals. We review and advise on security awareness, risk prevention, data management, network security and access control, and security monitoring and review.

Our strategic advisory services include, but are not limited to:

- Developing and reviewing cybersecurity strategies.
- Developing prioritised roadmaps of strategic and tactical initiatives to improve cybersecurity and resilience.
- Advice and guidance on implementing a formal security program and security architecture, including Information Security Management Strategies ('ISMS'), policies, procedures, and baselines.

> "... the vCISO service agreement remains flexible and aligned with your needs and circumstances."

Cybersecurity compliance management

Incorporating security compliance requirements into our vCISO offering helps you to enhance your consumer and business partner confidence. Our experts help organisations to understand and meet their legal, regulatory, and supply chain compliance obligations. We consider matters of data protection, activity monitoring, network infrastructure security, and cybersecurity policies and procedures and their alignment with established standards.
This may include:

- Identifying your organisation's compliance obligations aligned with relevant legislation and regulations, such as the Privacy Act, Corporations Act, Security of Critical Infrastructure ('SOCI') obligations, and APRA regulations.
- Performing compliance-based cyber risk assessments.
- Specifying, operationalising, and providing assurance on compliance improvement programs.

Cybersecurity culture

We help manage insider risks that can stem from accidental or even deliberate harm by assessing your cybersecurity culture – the underlying values and attitudes that can drive behaviours and risk appetite regardless of procedural rules. We review policies, procedures, and cyber awareness amongst key personnel to identify what the organisation is doing well and potential vulnerabilities. We may help you with:

- Conducting cybersecurity incident response and crisis management simulation exercises with boards and senior management.
- Developing incident response playbooks for common cyber risk scenarios.
- Organisational cybersecurity awareness assessments and exercises.
- Developing and implementing ongoing cybersecurity training.
- Understanding, developing, and implementing whistleblower policies and procedures for the reporting of critical cyber risks and cultural issues.

Our experience

Cyber risk management for a financial services provider

Background and approach

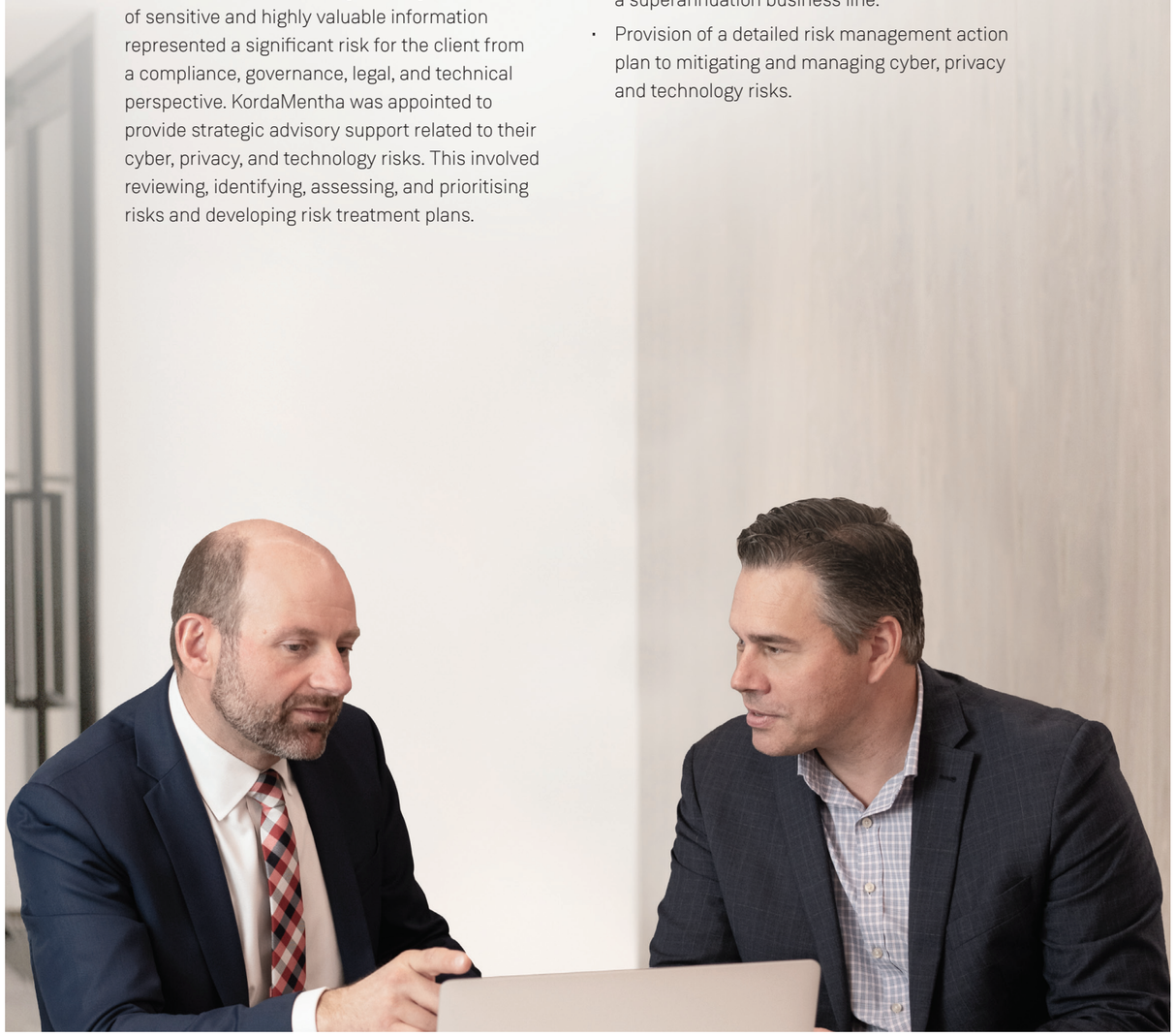
A leading multi-national financial services provider in the investment and superannuation sector acquired an organisation divested from a major ‘Big 4’ banking group in Australia. This ambitious M&A program involved the acquisition of staff members, technologies, client records, and superannuation accounts.

This import and processing of a large volume of sensitive and highly valuable information represented a significant risk for the client from a compliance, governance, legal, and technical perspective. KordaMentha was appointed to provide strategic advisory support related to their cyber, privacy, and technology risks. This involved reviewing, identifying, assessing, and prioritising risks and developing risk treatment plans.

With crucial support provided by the KordaMentha cybersecurity team, the client successfully and securely onboarded service line operations for the acquired superannuation business, avoiding business and customer service disruption.

Outcomes and benefits delivered

- Comprehensive cyber risk management analysis and treatment related to a strategic acquisition of a superannuation business line.
- Provision of a detailed risk management action plan to mitigating and managing cyber, privacy and technology risks.



vCISO services for a public sector client

Background and approach

A leading state-government appointed container deposit scheme provider engaged KordaMentha to assess its cybersecurity posture across its core business services, IT systems, and third parties. The client’s cybersecurity posture was assessed against the globally recognised NIST Cybersecurity Framework (‘NIST CSF’). The NIST CSF considers people, processes, and technology elements to assess the current efficacy of the organisation’s information security risk management approach and identify areas for improvement.

Parallel to this engagement, KordaMentha helped the client undertake a third-party cyber risk assessment of key IT managed services providers. We developed a process and methodology for the client to assess additional third parties.

Following this work, KordaMentha was engaged by the client to provide retainer-based vCISO services. The service agreement included:

- Development of a cybersecurity roadmap based on the NIST CSF findings.
- Information security policy review and development.
- A privacy impact assessment.
- An incident response plan.
- Incident response simulation testing.
- Regular reporting of progress to the board, senior management, and audit and risk committee.
- 12 hours of additional support per month.

Outcomes and benefits delivered

- Comprehensive cyber risk assessment based on international standards. This allowed the client to define a prioritised security strategy that reduced its cyber risk in line with its risk appetite.
- A detailed plan of action on mitigating and managing identified cyber risks.
- Strategy and policy development to ensure that policies and procedures are compliant with statutory requirements and fit for purpose.
- Increased organisational resilience through development and testing of cybersecurity incident response plans.

“Managing cyber risk is at the forefront of our minds. KordaMentha went over and above in their work to review risk and provide us with a roadmap to further mitigate risk.”

CEO, Not-for-profit organisation

Key contacts

Tony Vizza | Executive Director

Tony has over 20 years’ experience helping organisations manage information technology and cyber risk. Having worked with global government, industry, and academia stakeholders, he brings extensive expertise in IT, cybersecurity, privacy, risk governance, and the law. With board and senior management experience, Tony helps organisations optimise cyber risk management strategies, helping convert their challenges and concerns into strengths and devising strategies to reduce risk, optimise operations, and promote cyber resilience.

+61 2 8257 3032 | tvizza@kordamentha.com

Guillaume (Gui) Noé | Executive Director

Gui is passionate about technology, security, and privacy, and assisting organisations thrive in competitive, disrupted, and threatened environments. He has over 20 years’ experience in cybersecurity advisory, technology development, solutions delivery, and leading and growing cybersecurity practices. Gui advises organisations on improving cyber risk management and regulatory compliance, and driving effective digital transformations.

+61 7 3338 0269 | guillaume.noe@kordamentha.com

Ian Simpson | Director

Ian has 23 years’ experience in information technology, including security related roles. He helps clients implement security controls and frameworks in a pragmatic fashion, contextually aligned to the organisation’s strategy, operating model, and threat environment. Ian is a member of the Information Systems Audit and Control Association and holds certification in the Governance of Enterprise IT, as an Information Security Manager, and as a Lead Auditor in ISO/IEC 27001:2013.

+61 7 3338 0257 | ian.simpson@kordamentha.com

Luke Scerri | Director

Luke is a seasoned advisor, business leader, and consultant in cybersecurity, privacy, and technology. He is a respected leader with over two decades of experience in the development, implementation, and management of information security and risk strategies. Luke helps clients navigate an increasingly volatile cybersecurity landscape. He aligns information, business, operational, risk, and compliance strategies, bringing significant value to clients. Before joining KordaMentha, Luke held Chief Technical Officer roles, spearheading IT infrastructure and security projects for local and federal agencies, and global renewable energy companies.

+61 2 8934 3184 | luke.scerri@kordamentha.com

KordaMentha

Contact us

Auckland
+64 9976 4747

Brisbane
+61 7 3338 0222

Canberra
+61 2 6188 9222

Jakarta
+62 21 3972 7000

Melbourne
+61 3 8623 3333

Perth
+61 8 9220 9333

Singapore
+65 6593 9333

Sydney
+61 2 8257 3000

Townsville
+61 7 4724 9888

For more information visit
kordamentha.com