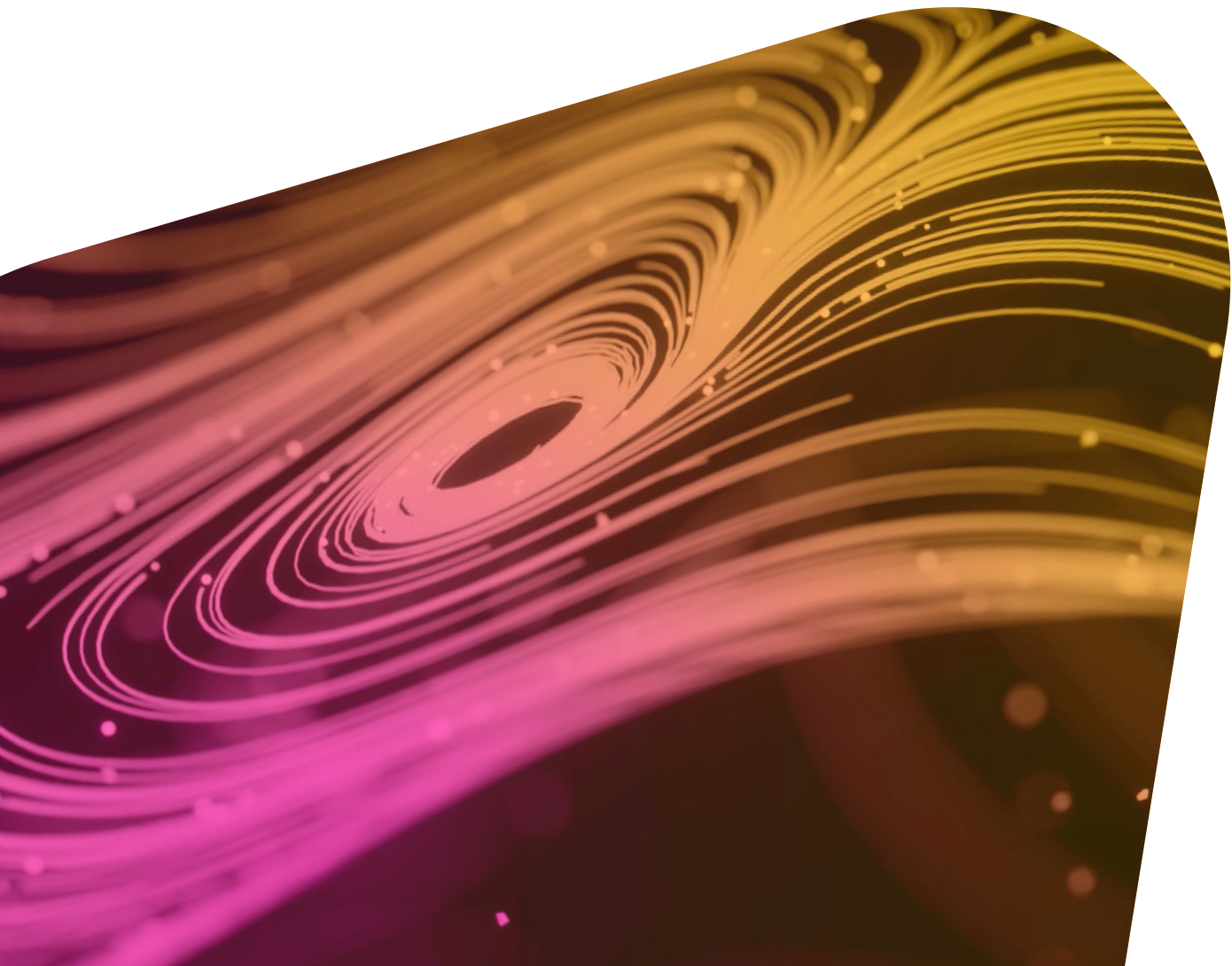




Governance, Risk & Compliance

Align your IT and strategic objectives while managing risk and meeting government and industry regulations for cyber security.



Securely Connected Everything™

With increased cyber threats to business continuity, revenue and customer relationships, your governance, risk and compliance (GRC) approach is a critical component of cyber security.

A GRC framework allows you to identify and assess IT-related risks and establish strategies and processes to mitigate organisational risks and threats.

GRC helps you understand your most effective strategy to address obligations around compliance and regulations, as well as your current data storage security, data privacy and protection risks.

An integrated GRC strategy will clearly outline the shared policies, procedures and tools needed to educate your business, reduce non-compliance risk and share information with stakeholders and customers effectively.

Key benefits of governance, risk and compliance.

-  Understand your risk and align risk management with key business objectives.
-  Improve cyber security with an integrated GRC approach that uses standards and frameworks to protect company and customer data.
-  Comply with regulations, including data privacy and industry frameworks, to build customer trust and protect your organisation from penalties.
-  Streamline operations around a common culture that promotes a cyber-first business strategy.
-  Unify your team and make better decisions with shared policies, decisions and actions for compliance and security.

How we help you.

> Governance

GRC reports provide insights that help organisations make informed decisions and create a strong governance framework. This includes an annual cyber security assessment and performance report based on specific roles, responsibilities and accountability across the organisation.

> Compliance

Depending on your industry, there may be specific cyber security regulations and certifications required for your organisation in order to remain compliant. We align to a range of industry specific frameworks to audit your compliance and report any variance requiring remediation.

> NIST Cybersecurity Framework

The NIST framework contains more than 100 best practice security actions across five critical cyber security functions to identify, protect, detect, respond, and recover from a cyber attack. Our NIST assessment report will enable your organisation to apply a common language and strategy for managing cyber security risk, which will help in prioritising and achieving your cyber security objectives.

> Risk assessment

A risk assessment identifies risk in your environment, aligned to your specific business, industry and cyber security requirements. We will share a comprehensive and actionable list of recommendations to mitigate risks and close security gaps.

> ISO 27001 compliance

ISO 27001 is a robust assessment that uses a collection of international standards to guide organisations to establish strong cyber security. This assessment details requirements for implementing, maintaining and improving an information security management system (ISMS) to increase security across information assets. Organisations that meet the standard's requirements can be audited and certified by an accredited certification body.

> CPS 234

CPS 234 is an information security law designed to ensure that regulated entities can withstand a cyber attack. The key objective is to reduce the risk of an attack while also securing information assets, including those managed by third parties. The regulation makes it clear that the Board is ultimately responsible for data security and requires timely reporting of any data breach or security incident.

Revolutionary thinking, evolutionary evaluation.

We are a multi-disciplinary team of innovative thinkers who use a no-nonsense approach to always find the right network security solution for your business, which means playing chess, not checkers to achieve the right outcomes.

> Technology & People

Our strong customer relationships stem from a commitment to always advise on fit for purpose technology, and doing right by our customers.

> Accurate & Proactive

We deliver real-time alerts and reports to help you achieve proactive transformation and monitoring to mitigate issues in alignment with attack surface management to maintain business-as-usual across your digital environment.

> Strategic Partnerships

Through our strong business and vendor partnerships, we have the breadth of knowledge and expertise to help you deal with any scenario as soon as it happens. We provide you with the expertise and flexibility to get the results you need through a strategic approach.

Mitigate risk with intelligently secure services.

To learn more about our governance, risk and compliance service or discuss your technology and business needs, reach out to the Orro team today.

1300 900 000
sales.enquiries@orro.group

Sydney | Melbourne | Brisbane | Perth | UK | Philippines