

## CYBERSECURITY SERVICES

# Cybersecurity and Resilience Consulting Services

In today's digital landscape, where organisations are increasingly driven by complex, data-intensive operations, cybersecurity resilience is no longer optional—it is imperative. As cyber threats become more sophisticated and business operations rely on high-speed data, video, and other critical digital services, organisations must undergo a transformation to fortify their digital infrastructure.

Organisations are faced with the challenge of securing critical infrastructure while managing budget constraints and escalating operational demands. To meet these challenges head-on, many are turning to Managed Security Service Providers (MSSPs) or system integrators, outsourcing their cybersecurity operations partially or fully, and leveraging cutting-edge cloud infrastructure.

Only by taking this proactive, resilient approach can organisations ensure that their critical systems remain secure, operational, and impervious to both present and future cyber threats. The stakes are high, and the time to act is now—cybersecurity resilience is not just a requirement, it is the foundation of business survival in the digital age.

It is a complex procurement specification and operational process. Erkmar has the experience to guide you through this.



## About Erkmar

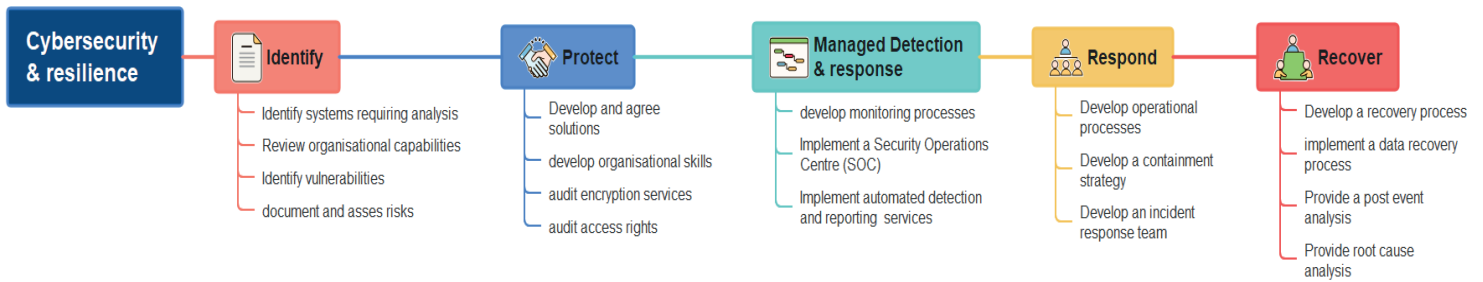
Erkmar is a UK-based global consultancy business with an Australian subsidiary. We specialise in supporting our global clients' telecom, spectrum and technology needs.

We have delivered assignments throughout the world for the last 14 years. Some examples of our services:-

- Technology strategy development
- Business case development
- Technical procurement specification creation
- Procurement process management
- Validation of vendor proposals against our client's requirement
- Project/program management of installations
- Post-implementation validation of project deliverables
- Wireless network coverage mapping and validation
- Quality of experience / Quality of coverage measurement and reporting
- Business process design and validation
- Economic evaluation

We have worked extensively with governments, regulators, public organisations and private companies in all the above areas.

Contact us:  
Email: [enquiry@erkmar.com](mailto:enquiry@erkmar.com)  
Telephone: +44 203 034 2459  
or +61 7 3473 1160



## Cybersecurity and resilience consulting

The five key cybersecurity functions aligned with the National Institute of Standards and Technology (NIST) can also be defined as managed services that organisations can leverage to strengthen their cybersecurity posture. These services encompass key security areas, helping businesses protect against, detect, respond to, and recover from cyber threats.

### Risk & Vulnerability Assessment Services

These services focus on identifying potential cybersecurity risks, threats and vulnerabilities across the organization. Managed security providers conduct asset discovery, risk assessments, and compliance audits to create a detailed understanding of the organisation’s cybersecurity risks. This service helps organisations prioritise security investments and understand critical areas of exposure.

### Threat Prevention & Security Control Services

These services provide the tools and processes to protect critical assets and data. This includes identity and access management (IAM), firewall and antivirus management, data encryption services, multi-factor authentication (MFA), endpoint protection, and security awareness training. The goal is to proactively prevent unauthorised access, data breaches, and other threats.

### Managed Detection & Response (MDR) Services

These services focus on continuously monitoring systems for suspicious activity and cybersecurity events. Managed Security Operations Centres (SOCs) provide real-time threat detection, event logging, and alerting. Advanced detection services leverage security information and event management (SIEM) platforms and machine learning to identify anomalous behaviour across networks, endpoints, and applications.

### Incident Response & Containment Services

When a cybersecurity incident occurs, these services are designed to quickly respond to and mitigate the impact. Managed incident response teams provide services like forensic analysis, threat eradication, communication, and remediation. They also deliver incident response planning and playbooks to ensure that the organisation is prepared to handle future incidents effectively.

### Business Continuity & Disaster Recovery Services

These services help organisations recover and restore normal operations after a cyber incident. This includes data backup and restoration, system recovery, and process improvement services. Providers offer post-incident analysis to identify root causes and recommend enhancements to prevent future attacks, ensuring that the organisation is resilient and operational as quickly as possible.

Erkmar is your trusted partner for resilience and cybersecurity advice