ANCHORAM CONSULTING

Critical Infrastructure Services Summary

Ensuring the resilience and security of this infrastructure is paramount to prevent economic instability and safeguard public health and safety

Our capabilities

Meeting your needs

Highly Experienced Assurance Specialists

The Anchoram Consulting Integrated Assurance team have an individual average of 15 years of experience providing risk management, governance advisory, internal audit and cyber assurance advice to clients throughout Australia. All associates at Anchoram Consulting are appropriately tertiary qualified, and have up-to-date, current industry certifications, which include:

- Certified Internal Auditor (CIA)
- Certified Information Systems Auditor (CISA)
- Certified Information Systems Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Industry certifications where applicable such as IEC 62443

Customer Focused Approach

We work closely with our clients to provide the best approach to suit their needs. We are proud to be flexible and pragmatic. Our team have practical work experience, combined with strong skills and appropriate qualifications. We approach each project in partnership with our clients, by working together in a co-sourced model or independently as required. Our team have a positive philosophy – we approach each project with professional scepticism and an open mind to improvement and opportunity. We are capable, innovative, adaptable and responsive to the needs of our clients.

We focus on examining our clients' needs from different perspectives, in order to master what we believe is the most important step – clearly defining the actual problem. We can then provide meaningful, and professional advice, along with strategic solutions that assists our clients to achieve successful outcomes.

Security Cleared

All Anchoram consultants hold an Australian Government Security Vetting Agency (AGSVA) Baseline clearance at a minimum, but most hold Negative Vetting 1 or higher. This is an important requirement when dealing with public service entities, government information and critical infrastructure within Australia.

Our differentiators

Meeting your needs

Our People – We're successful due to our people, when you engage Anchoram you leverage decades of experience with staff who have deep understanding of the problems that organisations have, this is because we've had them too. Our experienced staff have held C-Suite and senior roles across Commonwealth and private sector clients and in the critical infrastructure sector have led the development of strategies to address the same problems that organisations faces today.

Select Credentials – We've performed diverse work for multiple clients within the utilities sector across water, rail, energy and mining which provides us a detailed understanding of the different types of cyber challenges these organisations face. Our deliveries range from technical, strategic, risk and regulatory compliance assisting organisations to have clear focus on their goals.

Cutting-Edge Research – Our team are interested in what they do!, they actively participate in the cyber security and critical infrastructure sectors which includes developing academic works which all of industry can benefit from. This research and submission to the community mean that we're actively working to understand the problems of our potential customers.

Partnerships – Security and compliance requirements within the critical infrastructure sector are complex and broad. We have partnered with a range of companies to augment our offerings in the areas of legal support, cyber threat intelligence, physical security, training, staff security vetting and certification services.

We provide strategic advice not products – We remain vendor agnostic and do not have agreements with hardware, software and service suppliers. When a customer seeks a solution to a problem we work to develop specific requirements, review the offerings using known sources of authority and then provide the customer a pragmatic recommendation that is accurate and meets their requirements.

Breadth of Services – Effective security is multi-dimensional and requires a deep understanding of the interconnected nature of risk, we cover off protective security, data, technology and risk throughout our other service lines.

Past engagements

Anchoram Consulting is pleased to have worked with a range of customers, including:

- Aboriginal Housing Limited
- ACT Audit Office
- ACT Chief Minister, Treasury and Economic Development Directorate
- ACT Health
- Australian Financial Services Authority
- Australian Radiation Protection and Nuclear Science Authority
- Batchelor Institute of Indigenous Tertiary Education
- Civil Aviation Safety Authority
- Department of Education
- Department of Home Affairs
- Department of Human Services / Services Australia
- Department of Innovation, Industry, Science and Research
- Department of Social Services
- Department of the Prime Minister and Cabinet
- Essential Energy
- Family First Bank
- Hymba Yumba Indigenous School
- Inspector-General of Taxation and the Taxation Ombudsman
- National Insurance Disability Agency
- Queensland Department of Regional Development, Manufacturing and Water
- Queensland Department of Resources
- Queensland Rail
- Shared Services ACT
- State Insurance Regulatory Authority, New South Wales
- Transport Canberra and City Services
- TRILITY Group

Client	Scope	Delivery
Sydney Metro Trains	Ongoing cyber security assurance activities for Sydney Metro Trains Systems Operations and Maintenance (TSOM)	Detailed risk assessments reports, cyber standard assessments IEC 62443, for Power Control Systems, Train Control Systems, including technical reporting and advisory
TRILITY Group	Foreign Investment Review Board (FIRB) audit and assessment activities (multi-year) and Technical Standards Gap analysis	Detailed assessment against FIRB requirements onsite/remote using defined audit framework and process and IEC 62443 Gap Analysis
Family First Bank	CPS 232 and CPS 234 Business Continuity and IT Security reviews	Conducted assessment of progress to implement APRA endorsed recommendations for compliance and performed multiple business continuity and disaster recovery scenario tests
Essential Energy	Conduct operational risk management workshops and risk assessment and subsequent development of bow tie risk registers for ICT risks for annual iPART audit compliance	Bow tie risk registers and tool for ongoing development and maintenance of the risk activities, sufficient for iPART audit requirements
Hymba Yumba Independent School	Perform internal audit and risk management services in a fully outsourced environment for HYIS over several years	Established the risk framework, assurance map and strategic internal audit program, and conduct audits and assurance engagements of the control environment.

ANCHORAM CONSULTING

Industry Specific Services - Rail

- Modern rail systems have become reliant on technologies for system control and safety functions such as authorisations, scheduling and recovery.

  These technologies aim to improve operational efficiencies and leverage data to understand the performance and condition of assets but require a new approach to ensuring these remain secure.

- Operators are competing to implement automated systems across Passenger, Freight and Light Rail with digital systems adding another layer of security complexity not seen in traditional rail control systems.

- As your trusted partner and expert advisor, Anchoram can help your organisation navigate the complexities of rail systems security, ensuring your operations remain resilient to external threats.

Technology Footprint	Example Services
Low (e.g. manual train orders, driver/guard rail operations, limited or no signalling)	Compliance & Auditing Regulatory Response Support Trusted Insider Risk Management
Medium (digital train orders, asset management systems, power control system, electronic interlockings and signalling)	Maturity Assessments Cyber & OT Security Risk Assessments Security Architecture Design and Reviews
High (GOA4 automation, CBTC signalling, central control system, wireless and passenger information technologies)	Security Hardening Penetration Testing Cyber Incident Simulation Exercises Cyber Incident Response Plans Regulatory Response Support Cyber & OT Security Risk Assessments

ANCHORAM CONSULTING

Industry Specific Services - Energy

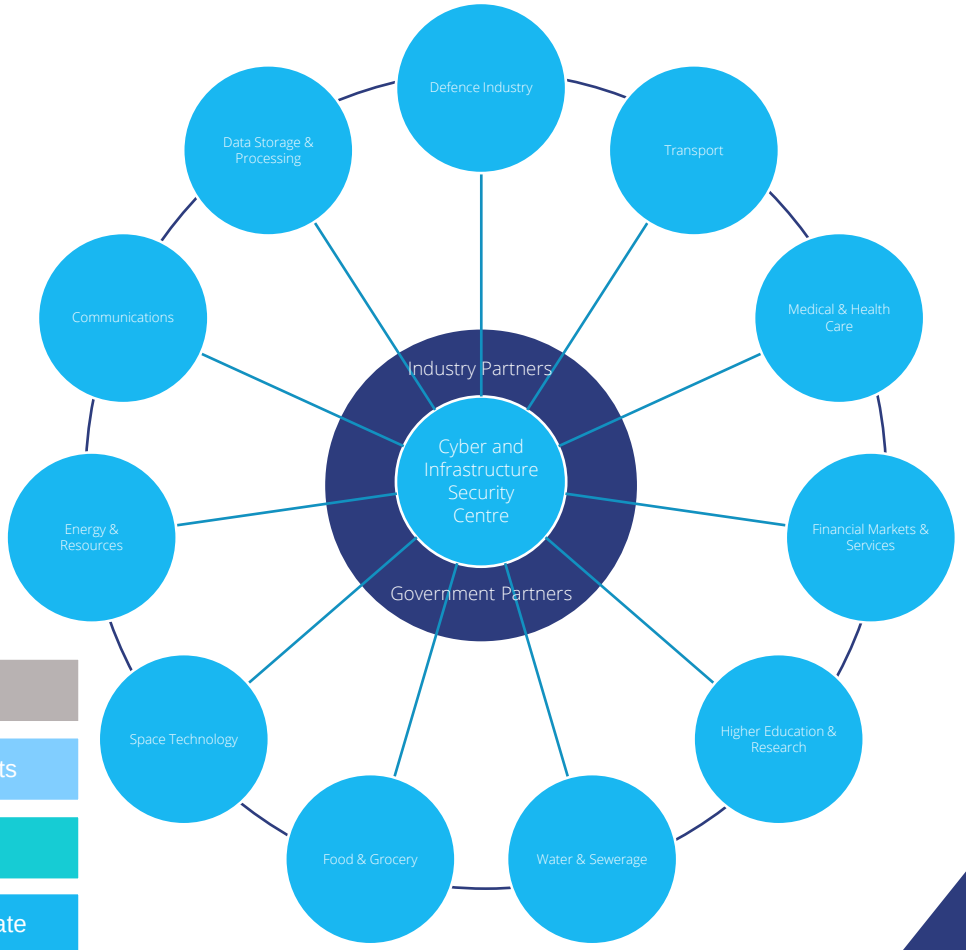
Standards Assessments	Power Systems Resilience	OT/IT Convergence Strategies	Security Testing, Intelligence and Response
Understanding security postures against known sources of authority is a guaranteed method providing traceability to reinforce both investment proposals and maturity across various cyber security domains. Anchoram has deep experience providing analysis against industry standards. We can provide strategic views for organisations seeking to adopt a standards-based approach to applying the controls and countermeasures represented in the standards Standards such as: • IEC 62443 • IEC 62446 • National Energy Rules • NIST 800-52 • CLC/TS 50701 • ASD ISM • AEMO AESCSF • NERC CIP C2M2	Finding an organisation who fundamentally understands the cyber inputs to the operational imperative is challenging, Anchoram is in the enviable position to have a team who spent the time analysing and defining core concepts and taxonomies with notable published works on power systems resilience. This deep understanding can be readily leveraged by utilities who may not have the dedicated resources to ensure compliance and address the potential cyber threats to the power system. Resiliency Assessment & Planning: • System resiliency workshops • Power system security architecture assessment • Security response planning for control centres • Security assurance plans threat modelling for resilience	Understanding the interactions between OT/IT systems is a key part of ensuring the security of an asset heavy organisation. Anchoram understands how systems with operational technology control system assets such as SCADA, ADMS, DMS etc. need to integrate with ICT systems for planning, asset inventory and enterprise resource planning and can readily develop secure methods of achieving this whilst supporting both business and operational stakeholder goals. Convergence Strategies: • Technical design services • Secure integration strategies • Development of convergence models	Anchoram provides strategic intelligence on threats and actors as part of understanding the Energy Sector threat landscape. This approach encourages security teams in IT and OT move beyond reactive measures and take a forward- looking approach to security integrating the security function into critical decisions. This is further supported by our team that understands how to securely test Energy Sector technologies that cross the OT/IT boundary. Testing and intelligence services: • Threat landscape briefings red/blue/purple teaming • Cyber incident simulation exercises incident response plans and assessments • Cyber forensics support • Regulatory response support (AEMO, OAIC, State and Commonwealth)

ANCHORAM CONSULTING

Critical Infrastructure

When supporting clients in the critical infrastructure arena, we adopt the Australian Government Cyber Security Strategy model, applying it to assure any of the 11 designated critical infrastructure sectors defined in the strategy.

These principles help clients to ensure they adequately manage their risks through generally-accepted models and methods. Our assurance method assesses clients' ability across the six spheres of: anticipate, react, survive, sustain, recover and adapt to ensure their resilience and ability to maintain services throughout periods of instability or loss of continuity.



Anticipate ✓maintain situational awareness and proactively detect potential threats

React ✓avoid, deter, or neutralise detected threats and respond to adverse events

Survive ✓mitigate, absorb, or withstand the impacts of an adverse event

Sustain ✓retain control and preserve core functions and services in a degraded state

Recover ✓respond, restore operations, and 'bounce back' from adverse events

Adapt ✓evolve based on threat intelligence and lessons learned

ANCHORAM CONSULTING

Thought Leadership

Our blogs and articles provide us a platform to engage with customers and establish authority in our industry. By consistently publishing informative and relevant content Anchoram shares insights on industry trends and positions ourselves as thought leaders.

We've collated a selection of relevant articles which may provide some clarity as to specific challenges and provides additional information to assist with clarifying topics in the critical infrastructure sector.

Title	Link
Can't Protect What You Can't See - Asset Identification in OT	Link
The Purdue Model: Old friends are the best friends	Link
TSA Release New Cybersecurity Requirements for the Rail Sector	Link
Are railways lost in a sea of cyber security standards?	Link
Australian Cyber Security 2023-2030: Key actions and takeaways	Link
Cloud Security for Industrial Automation and Control Systems	Link
NIST 800-82: the quiet achiever	Link
The Purdue Model: Old friends are the best friends	Link
Australian Energy Sector Cyber Security Framework version 2	Link

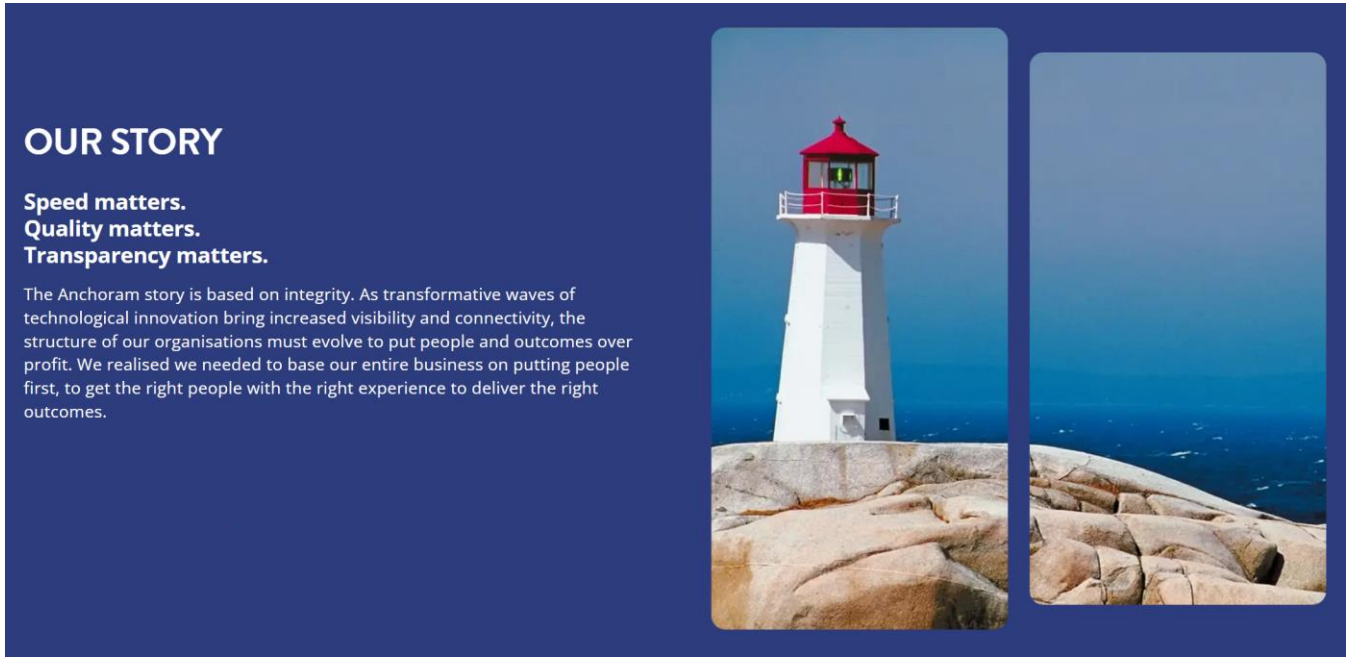
ANCHORAM CONSULTING

Available Panel Arrangements

Our services are available as direct procurement, or through the following panels that we have been pre-approved:

- SON3921486 – Australian National Audit Office Provision of Professional and Associated Services
- SON3520191 – Department of Defence Information Communication Technology Provider Arrangement
- Department of Education and Workplace Relations Cyber Panel
- SON3413842 – Digital Transformation Agency - Digital Marketplace Panel 1.0
- New South Wales Treasury Performance and Management Services Scheme
- New South Wales SCM002 – ICT Services Scheme

This list is continually expanding as we are successful in our panel applications. Please contact us to discuss the best procurement method for your organisation.



ANCHORAM CONSULTING

ANCHORAM CONSULTING

Anchoram Headquarters

Level 1, Suite 3
16 Napier Close
Deakin, ACT 2600
Australia

Phone: 1300 042 833
Email: contact@anchoramconsulting.com.au