Module	**INFRASTRUCTURE RESILIENCE AND SECURITY**
Jurisdictions	**CTH, NSW, VIC, SA, TAS, WA, NT, QLD, ACT**
Legal Expert	**SCOTT ALDEN** Partner at HWL Ebsworth https://hwlebsworth.com.au/people/scott-alden/ https://www.linkedin.com/in/scott-alden-5884432b/?originalSubdomain=au

Module Scope

What are the responsibilities of your organisation under the Australian critical infrastructure protection regime?

Does your organisation understand and meet its routine registration and reporting obligations?

Are you required to meet enhanced cyber security obligations or prepare a critical infrastructure risk management plan?

What interventions are government authorities likely to deploy to close resilience gaps or respond to cyber security incidents? How do those interventions affect your organisation?

Does the Telecommunications Sector Security Reforms (TSSR) regime apply to your organisation? What are your organisation's TSSR obligations?

Are any assets controlled by your organisation subject to the rules that govern financial market infrastructure (FMI)? What are your obligations under the FMI regime?

Module Application

The Infrastructure Resilience and Security Module explains the obligations of relevant entities under the Australian critical infrastructure protection regime.

The module addresses the obligations of each category of relevant entity. These obligations vary according to whether the entity is a:

- **Responsible entity**, which is an organisation that has a prescribed relationship with the asset and carries the greatest legal responsibility for its protection
- **Direct interest holder**, which is an organisation that holds an interest of at least 10% of the asset or holds enough interest to exert influence or control over the asset
- **Asset operator**, which is an organisation that operates the asset or part of the asset, or
- **Managed service provider**, which is an organisation that manages, manages an aspect, or manages an aspect of the operation of all or part of an asset

In addition, the module addresses industry-specific infrastructure resilience obligations applicable to relevant entities and other organisations operating in the telecommunications and financial services sectors.

1. Register of Critical Infrastructure
Each organisation must recognise critical infrastructure assets and its role (or roles) as a relevant entity in relation to those assets.

The responsible entity and direct interest holders for each critical infrastructure asset must register the asset with the Cyber and Infrastructure Security Centre (CISC) unless an exemption applies. Having registered a critical infrastructure asset, the organisation must notify CISC of changes to any registered information.

2. Reporting and Information
The responsible entity for a critical infrastructure asset must notify the Australian Cyber Security Centre (ACSC) of any cyber security incident that affects the asset and meets prescribed impact thresholds.

Each relevant entity for a system of national significance must report information about the nature, operation, security and other qualities of computer systems to the Australian Signals Directorate.

The SOCI Act applies protections to information collected or communicated in compliance with the Act. Each organisation that possesses protected information must only use or disclose that information under authorised circumstances.

3. Cyber Security
The responsible entity for a system of national significance must meet enhanced cyber security obligations. These include a requirement to prepare an incident response plan that will govern the entity's activities when a cyber security incident occurs.

In addition, the responsible entity for a system of national significance must conduct cyber security exercises and vulnerability assessments as directed by the Secretary.

4. Risk Management
The responsible entity for a designated asset must prepare a critical infrastructure risk management program (CIRMP). The CIRMP must govern how the entity will mitigate and minimise the risks that arise from hazards affecting that asset.

Having adopted a CIRMP, the responsible entity must review and update the program routinely. The entity must submit annual reports of the state of the program to the Secretary.

5. Government Powers
The SOCI Act empowers the Minister and the Secretary to issue directions to relevant entities to achieve national security objectives. Compliance with directions is compulsory.

Each relevant entity must act in accordance with risk reduction directions and information requests. Relevant entities must also install monitoring software on computer systems in accordance with system information software notices.

The SOCI Act also establishes a regime designed to enable the government authorities to respond to serious cyber security incidents. When this regime is activated, the Minister and Secretary may issue directions designed to mitigate the impacts of recent, ongoing or imminent cyber security threats.

6. Telecommunications Sector
The Telecommunications Sector Security Reforms (TSSR) creates a regulatory framework to manage the security of Australia's telecommunications industry. Administration of TSSR is performed by CISC and the Office of the Communications Access Coordinator (CAC).

Carriers, carriage service providers (CSPs), carriage service intermediaries (CSPIs), and nominated carriage service providers (NCSPs) each have obligations under the TSSR. These obligations exist in parallel with an organisation's responsibilities as a relevant entity.

All organisations subject to the TSSR must take every reasonable step to secure their networks from unauthorised access and interference. Depending on their role under the TSSR, an organisation may also be required to notify authorities of planned network changes and comply with ministerial directions.

7. Financial Services Sector
Financial market infrastructures (FMIs) are the mechanisms and entities that enable trading in Australian capital markets. FMIs include important payment systems, central counterparties, trade repositories, and clearing and settlement facilities.

Relevant entities and other organisations that control an FMI must comply with resilience and security standards created by the Reserve Bank of Australia (RBA). FMI controllers must also notify the Australian Prudential Regulation Authority (APRA) or the Australian Securities and Investments Commission (ASIC) of significant security breaches.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.