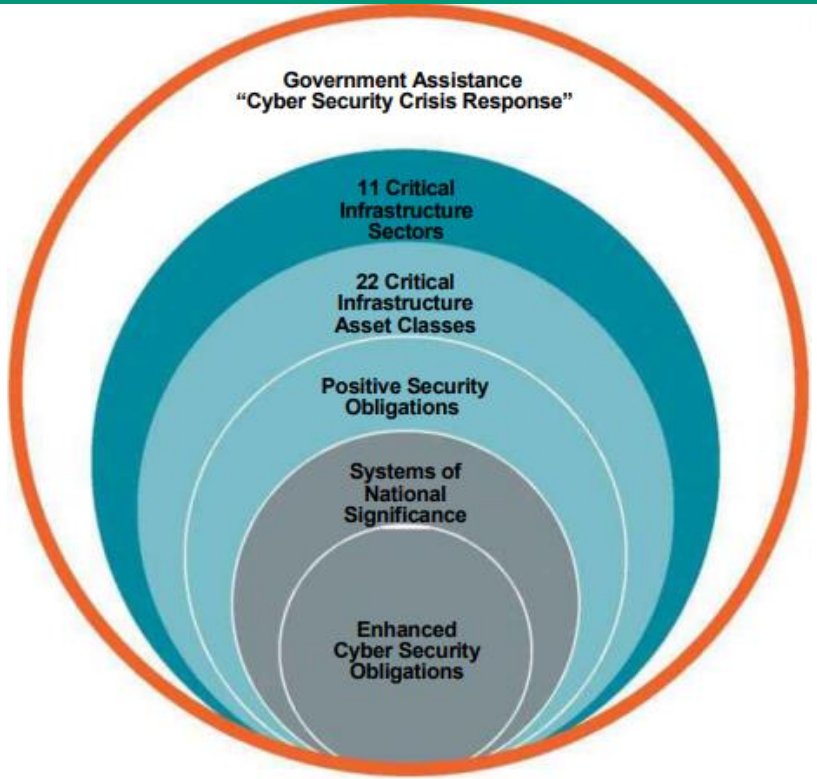
School of Science

Keeping your Critical Infrastructure secure

Professor Andrew Woodward

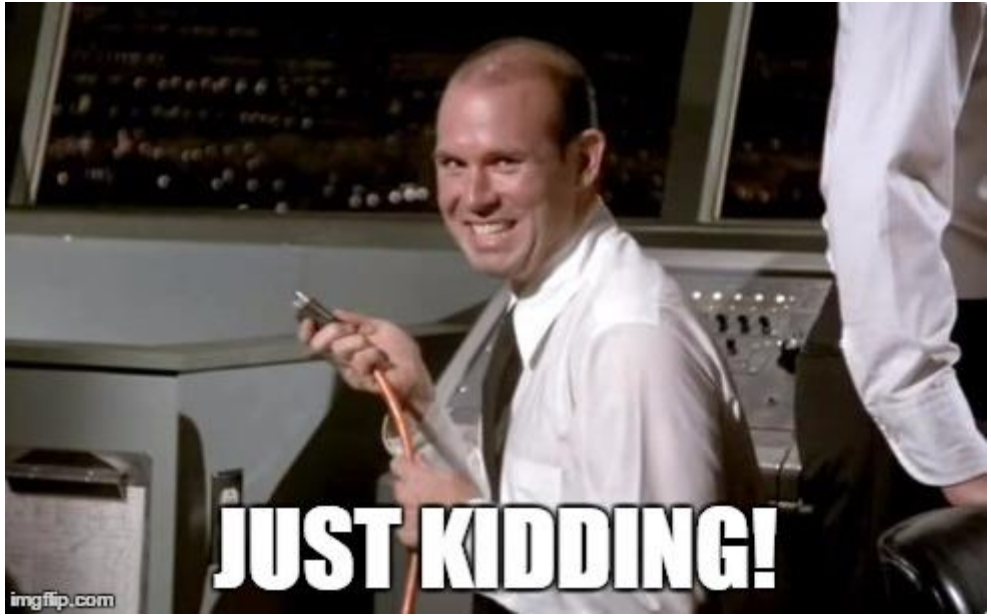
Executive Dean, School of Science
Edith Cowan University



Keeping your critical infrastructure secure

Problem solved!

Questions?



SOCI / SLACIP

- Security of Critical Infrastructure Act 2018
- Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
- Who does this apply to? More like, who *doesn't* this apply to…
- When does this apply?
- Umm… Now.

(Pauses to see if anyone gets up and leaves the room)

What is a ‘critical infrastructure asset’?

- Division 2 of the SOCI Act provides definitions for the 22 critical infrastructure asset classes.
- The Security of Critical Infrastructure (Definitions) Rules (LIN 21/039) 2021 (the Definition Rules) outline further parameters to these definitions where applicable.
- Critical infrastructure assets also include assets privately declared by the Minister for Home Affairs (the Minister) under section 51 of the SOCI Act; or, prescribed, by legislative instrument, by the Minister under section 9 of the SOCI Act. Those assets privately declared are kept confidential. Legislative instruments are published on the Federal Register of Legislation and are publicly available.

What is a ‘responsible entity’?

- A ‘responsible entity’ is an individual or organisation who owns or operates a critical infrastructure asset and may have obligations under the SOCI Act and associated Rules.
- The definition of ‘responsible entity’ differs for each asset class and can be found at section 12L of the SOCI Act.
- Just to clarify, I am *not* a responsible entity. Really. Ask anyone.

I don’t believe my asset is actually ‘critical’. How do I clarify my obligations?

- The definitions for each critical infrastructure asset were developed through extensive consultation with industry and experts within and outside of government with the intent to capture all assets critical to the secure operation of Australia’s key sectors.
- You should contact the Cyber and Infrastructure Security Centre if your asset is captured under the SOCI Act and associated Rules, and you do not believe it should be considered a critical infrastructure asset.
- While the Cyber and Infrastructure Security Centre will take into consideration submissions from industry that an asset is non-critical, only the Minister is empowered to make a determination that an asset is non-critical.
- Section 9(2) of the SOCI Act allows the Minister, via a rule, to prescribe that a specified asset is not a critical infrastructure asset.

Will entities that operate critical infrastructure assets need to inform third party holders of data that they are affected by the SOCI Act?

- Yes, in accordance with SOCI Act section 12F(3), if you are a responsible entity and you use a data storage or processing service provider for your commercially-provided business critical data, you must take reasonable steps to tell them that you are operating a critical infrastructure asset.
- A reasonable step might be for the responsible entity to discuss why the data is considered business critical with third party data holders in order to explain the associated risk that disclosure of this information could entail.

The risk management program obligation

Who needs to do this?

- Broadcasting, DNS, data storage or processing, Electricity, energy market operator, gas, liquid fuels, payment systems, food and grocery, hospitals, freight infrastructure and services, water.
- What are the rules?
  - Rule #1 – Cyber and information security hazards
  - Rule #2 – Personnel hazards
  - Rule #3 – Supply chain hazards
  - Rule #4 – Physical and natural hazards

Rule #1

Cyber and information security hazards

1. Responsible entities for critical infrastructure assets must, within 6 months of the commencement of this rule, ensure that their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.

2. Responsible entities for critical infrastructure assets must, within 18 months of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:

   a) The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;

   b) AS ISO/IEC 27001:2015;

   c) The National Institute of Standards and Technology (NIST) Cybersecurity Framework;

   d) The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;

   e) Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or

   f) an equivalent standard.

Frameworks – which one?

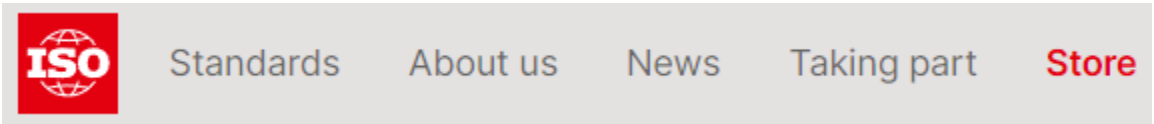
- Depends…
- What sector?
- What assets?
- Organisation size
- Budget
- Pick one you like?
- Toss a coin?

Frameworks

- ACSC E8 MM L1
  - relatively straight forward,
  - focusses heavily on technical controls,
  - VS is ok but can only find knowns,
  - Not risk based,
  - Scalability?

Frameworks

- AS ISO/IEC 27001:2015
  - very risk management focussed.
  - It is an info sec framework, not cyber security
  - Guidance only?
  - Many resources available
  - Certification available $$$$$$
  - Suitable for smaller entities?



Frameworks

- The National Institute of Standards and Technology (NIST) Cybersecurity Framework
  - comprehensive,
  - many associated guides and frameworks (eg NIST 800-61)
  - Currently v1.1, V2.0 soon™
  - Appropriate for small through to enterprise
  - Is US created and owned

Frameworks

- The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1
  - Developed for energy sector but applies to IT and OT
  - Adopted globally, is free to use
  - Is a tool and has useful guides to run workshops and training
  - Comprehensive, includes risk and other components

Level	Name	Description
MIL1	Initiated	• Initial practices are performed, but may be ad hoc
MIL2	Performed	• Practices are documented • Adequate resources are provided to support domain activities • Practices are more complete or advanced than at MIL1

Frameworks

- The 2020-21 AESCSF Framework Core published by Australian Energy Market Operator Limited (ACN 072 010 327)
  - Its all the things
  - The AESCSF leverages recognised industry frameworks such as the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF), and references global best-practice control standards (e.g. ISO/IEC 27001, NIST SP 800-53, COBIT, etc.). The AESCSF also incorporates Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles (APPs), and the Notifiable Data Breaches (NDB) scheme.
  - BUT specifically for the energy sector
  - Comprehensive (complex?) and granular

Frameworks

- “Other”…

What is an equivalent framework?

Entities should consider their risk management methodology and the cyber and information security hazards that are most relevant to their asset when considering implementing cyber security frameworks not listed in the Rules.

If an alternative framework better addresses the risk vectors threatening an entities critical assets then the CISC would consider this a valid equivalent framework.

The CISC is wanting to proactively engage with entities considering implementing alternative frameworks. Please contact enquiries@CISC.gov.au if your organisation is looking to explore alternative cyber security frameworks.

VA vs Pen test vs VS

- Pen test – limited value (IMO), very specific use case
- Pen test != organisational security
- VS – if you have implemented a framework, little value, technical controls only
- VS – great if you are starting from nothing, periodic review, spend little
- VA – IMO the best option
    - Risk integrated

Insource or outsource? (or BBQ sauce!)

What are you outsourcing? SIEM, SOC, firewall, monitoring etc

Again, depends on your environment

If you are in an OT world, caution (based on my experience in this sector)

Go for it, but read those SLAs REALLY carefully…

You can outsource risk, but not all of it and not reputation

Trust, but verify

Don’t forget!

- You still have to comply with everything else -
  - Data privacy regulations locally and potentially globally (GDPR etc)
  - The law(s)
  - WHS

My advice?

- Assume this applies to you, even in the unlikely event that it doesn’t

- Understand your obligations
- Ensure C-suite understand (they probably do)
- Choose the most appropriate framework for your sector / organisation size / resource availability - I like NIST (personal opinion)

Thanks for listening