

Building an OT Security Community

A Case Example from NZ

November 2020



Introducing Peter Jackson

- ❑ **Engineering Manager (Cyber)**
- ❑ **Senior Systems Engineer**
- ❑ **BE Hons; GICSP; GRID**
- ❑ **Industry Experience**
 - ❑ Control Systems (DCS/PLC)
 - ❑ Safety Systems (TÜV FSE 7040/13)
 - ❑ Industrial Networks (Ethernet/fibre)
 - ❑ Server Management (Windows)
 - ❑ Alarm Management
 - ❑ Conference presenter and member of ISA-99 (responsible for 62443 suite)
- ❑ **SANS Instructor (in dev) for ICS515 (GRID)**
- ❑ **Founder & facilitator of NZ ICS Cyber Technical Network (icscyber.org.nz)**



NZ approach

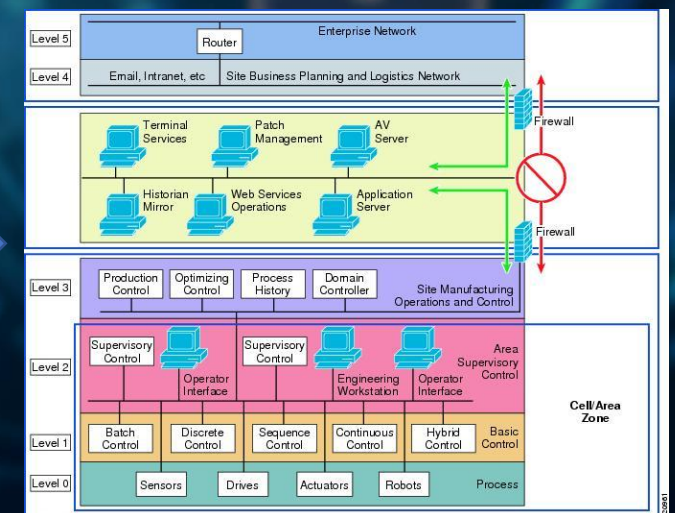
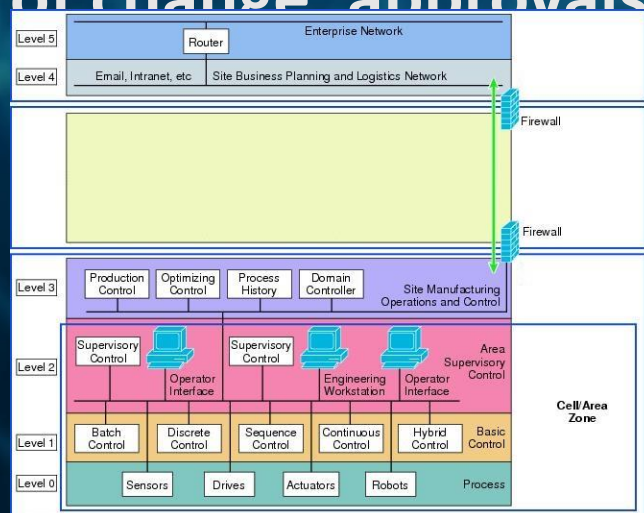
- ❑ **Based on control systems expertise**
 - ❑ **Working with ICS and IT stakeholders**
 - ❑ **Develop best-practice, defence-in-depth, appropriate solutions**
 - ❑ **Our OT-security tools, tactics, procedures need to be OT-specific**
 - ❑ Informed by the IT-security controls that work for our environments
-
1. **Case Studies – some examples**
 2. **NZ ICS Cyber TN – building a community**
 3. **VCSS-CSO – tool to support the community**

Case Study 1: Fast-tracking Defence-in-Depth in a NZ industrial facility

- ❑ IT compromise for global parent lead to IT/OT security audit
- ❑ Audit completed by IT-security and ICS-vendor auditors
- ❑ 5 months to full site shutdown. Short timeline for design, purchase, implement, commission, handover.
- ❑ Next full site shutdown >5 years

Case Study 1: Fast-tracking Defence-in-Depth in a NZ industrial facility

- ❑ OT assessments from IT and ICS vendors – different focus, priorities, background, standards
- ❑ ECL team collated results and fast-tracked design
- ❑ Top priority: quality
- ❑ Management of change approvals
- ❑ The results:



Case Study 1: The Design

- ❑ **IDMZ (Industrial DMZ)**
 - ❑ Replaced existing OT firewall with upgrade redundant firewall
 - ❑ Added IDMZ components into network architecture – VM Host pair
 - ❑ VM Guests – DC (primary/backup); WSUS; AV; Future (services)
- ❑ **Network hardening**
 - ❑ Physical segregation to firewall; VLANs; Firewall routing
- ❑ **Network segmentation**
 - ❑ Tight controls on Safety Networks (19)
 - ❑ Implementing segregation on Miscellaneous Networks (5)



Case Study 1: The Design

- ❑ **Logging and Monitoring (including display)**
- ❑ **Access and Asset Controls**
- ❑ **Training**
 - ❑ VM operation and maintenance
 - ❑ Use of Windows, Firewall, Logging and Monitoring tools
 - ❑ Industrial Cyber Awareness/Advanced training
- ❑ **Governance**
 - ❑ Policies, procedures – specific to site requirements for OT environment

Case Study 1: The good, the bad and the ugly

❑ The good

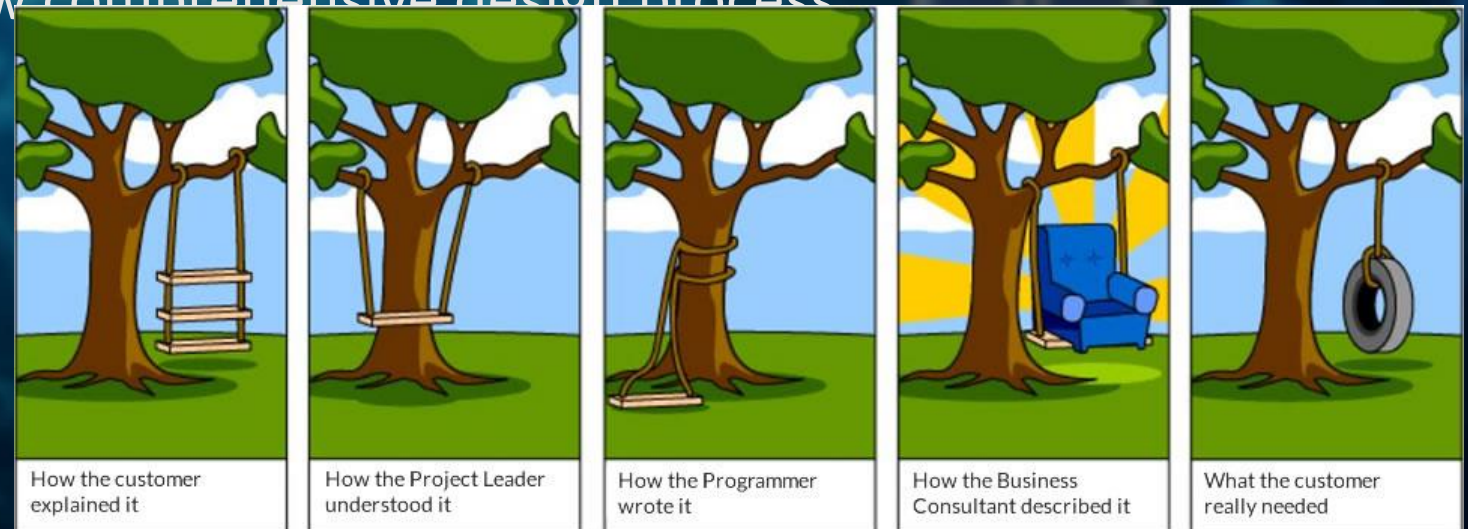
- ❑ Collaboration and cooperation with client, service providers (2) and other stakeholders (∞)

❑ The bad

- ❑ Fast-tracking does not allow comprehensive design process

❑ The ugly

- ❑ Understanding what the client asked for vs wanted vs needed



Case Study 2: Remote Access

- ❑ **Project required collaboration from many engineers:**
 - ❑ Germany – specialist vendor expert
 - ❑ USA – specialist vendor software developer
 - ❑ Australia – experienced project team
 - ❑ NZ – client & local support (ECL)
- ❑ **Too expensive to complete the project in NZ – would not happen**
- ❑ **But the project was important**
- ❑ **Solution: secure remote access**

Case Study 2: Remote Access

- ❑ **Working with client IT, developed secure remote access:**
 - ❑ Requirements Controls Security Design Architecture
- ❑ **ECL project management and local engineering support**
- ❑ **Project was completed successfully with remote specialists contributing well**
- ❑ **Small change in code or configuration could be done online, remotely, securely**

Case Study 2: The good, the bad and the ugly

❑ The good

- ❑ Collaboration and cooperation with client, service providers (2) and developers (2). Cost effective implementation of highly-specialist work

❑ The bad

- ❑ Challenges with time-zones (especially meetings or related requirements)

❑ The ugly

- ❑ None – successful project!

Case Study 3: Intruder

- ❑ Maintenance personnel attend substation for routine maintenance activities
- ❑ Find unauthorised, unidentified person
 - ❑ Laptops, proprietary cables
 - ❑ Cushion, blanket
- ❑ Person calmly packs up and leaves substations



Case Study 3: Intruder

- ❑ **The good**

- ❑ Kick-started their security program – finally some support from management

- ❑ **The bad**

- ❑ Kick-started security program was ineffective – focus on governance/compliance not fit-for-purpose/risk-based security controls


- ❑ **The ugly**

- ❑ To this day, unknown person, unknown activities, unknown duration


NZ ICS Cyber Technical Network

- ❑ 2017 'Seminar'
 - ❑ 3 talks
- ❑ 2018 'Summit'
 - ❑ 5 talks + Q&A
- ❑ 2019 'NZ ICS Cyber TN'
 - ❑ 8 events... and counting
- ❑ 2019 'Summit'
 - ❑ 5 talks + Q&A
 - ❑ ... + drinks


2019 NZ ICS CYBER SECURITY SUMMIT			
12:30 PM	DOORS OPEN	2:30 PM	AFTERNOON TEA
12:50 PM	OPENING ADDRESS <i>MC: Peter Jackson from ECL Cyber</i>	3:00 PM	SPEAKER 4 RESPOND: Do Your Homework Before It's Duel <i>Rob Caldwell from Mandiant (US)</i> It's been said that no one plans to fail, people only fail to plan, and this is exactly the case when dealing with Incident Response. The middle of a crisis is no time to create an Incident Response plan, especially when dealing with the nuances of ICS IR. We will look at the components of planning for IR, as well as the special considerations needed for effective IR with ICS.
1:00 PM	SPEAKER 1 IDENTIFY: Getting the Foundations Right! <i>Wenzel Huettner from Defend</i> Building cyber resilience without understanding your business environment, knowing your assets and establishing effective governance is impossible. What's the point in adding more security tools when your risks sit in the supply chain? Why would you build a bigger wall when the gates are always open? IDENTIFY is about getting your foundations right and making the journey not only easier but also more effective and efficient.	3:30 PM	SPEAKER 5 RECOVER: The Need for Intel-Driven Defense for Proper Root Cause Analysis and Recovery <i>Robert M Lee from SANS/Dracos (US)</i> This presentation will examine multiple high profile ICS cyber attacks including the Ukraine attacks and the TRISIS attack and look at where there were challenges in recovery due to failure to properly identify root cause analysis of the attack. This presentation will look at the cyber threat landscape for ICS and note challenges to the community with focus areas to reduce this area of concern.
1:30 PM	SPEAKER 2 PROTECT: Building on strengths <i>Bhraj Palmar from Vector</i> ICS owners need to identify their strengths in safety and protection of critical assets to implement learnings in order to fortify their networks and processes. This presentation will shed light on some of the existing strengths in our industries and discuss how these can be leveraged to build and operate defendable ICS environments.	4:00 PM	Q&A PANEL <i>Facilitator: Peter Jackson from ECL Cyber</i> For our final session, we bring together several experts to answer any questions the attendees may have regarding ICS Cyber Security in NZ. <ul style="list-style-type: none">• Rob Lee from SANS/Dracos (US)• NCSC Incident Responders (x2)• James Blair (Todd Energy)• Malcolm Baillie (Nozomi)
2:00 PM	SPEAKER 3 DETECT: Malware Free Networks – scaling cyber threat detection and disruption. <i>NCSC</i> Malware Free Networks (MFN) uses STIX/TAXII to deliver a cyber threat intelligence feed that involves taking cyber threat information from a range of sources, and sharing it with customers – either directly or via their network operator. Recipients will be able to use MFN to detect and disrupt a broad range of malicious activity, and provide telemetry back to the NCSC. This presentation provides a look under the hood at how the NCSC proposes to deliver scalable, future-proof threat intelligence to New Zealand organisations of national significance.	4:30 PM	CLOSING DRINKS An opportunity for attendees to socialise with experts and industry peers.
		POST EVENT	Informal gathering at BREW, 1103 Tutanekei Street




TLP: WHITE (UNRESTRICTED)
Information may be distributed publicly without restriction.



IN ASSOCIATION WITH:
SANS ICS



ECL Cyber



ECL

Overview

□ NZ ICS Cyber Technical Network

□ Representatives from owners, operator and service provider organisations with an interest in ICS Cyber Security in NZ.

□ An industry-led organisation established to promote the sharing and understanding of Industrial Control Systems (ICS) Cyber Security ideas in order to foster learning, development and improve cyber security maturity for NZ industrial companies.

□ <https://icscyber.org.nz>



TLP: WHITE (UNRESTRICTED)

NEXT EVENT:

Thursday 28th May 2020, 12:00-1400

Michael Lagana, ICS Cybersecurity Consultant, Clarity on 'Secure Remote Access for OT (under the hood)'

Glen Willoughby, Digital Innovation Advisor, NASA JPL on 'Utilising Emerging Technologies to Secure Critical Infrastructure'

Jim Scott, ICS Security Consultant on 'Cloud computing business methodology for OT'

Register at <https://icscyber.org.nz> for remote access instructions. Note: No physical location for May 2020 forum

NZ ICS CYBER TECHNICAL NETWORK

PURPOSE/AIM:

An industry-led organisation established to promote the sharing and understanding of Industrial Control Systems (ICS) Cyber Security ideas in order to foster learning, development and improve cyber security maturity for NZ industrial companies.

AUDIENCE:

Representatives from owners, operator and service provider organisations with an interest in ICS Cyber Security in NZ.

GROUND RULES:

- NCSC Traffic Light Protocol to be used for all information transfer (primarily TLP: GREEN)
- Specific company standards and practices will not be shared unless approved in writing by the company.
- No commercially or contractually sensitive information will be exchanged or discussed (although vendors may be invited to attend and describe their solutions and approaches to ICS Cyber Security).
- The information shared is intended to educate and promote learning. The steering committee will accept no liability resulting as a use of the information or offer any guarantee of the accuracy of the information.

2019 Forum Talks included:

- Fast-Tracking Defence-in-Depth
- A Tale of Two Hats
- Control Systems in the Cloud
- The Value of ICS Visibility Within a SOC
- NCSC – Thinking Ahead. Being Prepared
- The TTPs of Hard Hat Incident Response
- VCSS–CSO Analysis and My Journey
- Cyber Security Strategy for ICS Systems
- Risk Based Approach to Security

2019 NZ ICS Cyber Summit Talks:

IDENTIFY: Getting the Foundations Right!

PROTECT: Building on strengths

DETECT: Malware Free Networks – scaling cyber threat detection and disruption. NCSC

RESPOND: Do Your Homework Before It's Due!

RECOVER: The Need for Intel-Driven Defense for Proper Root Cause Analysis and Recovery

Register at <https://icscyber.org.nz> or email info@icscyber.org.nz for more information

v14.1



TLP: WHITE (UNRESTRICTED)
Information may be distributed publicly without restriction.



IN ASSOCIATION WITH:



NZ ICS Cyber TN – Ground Rules

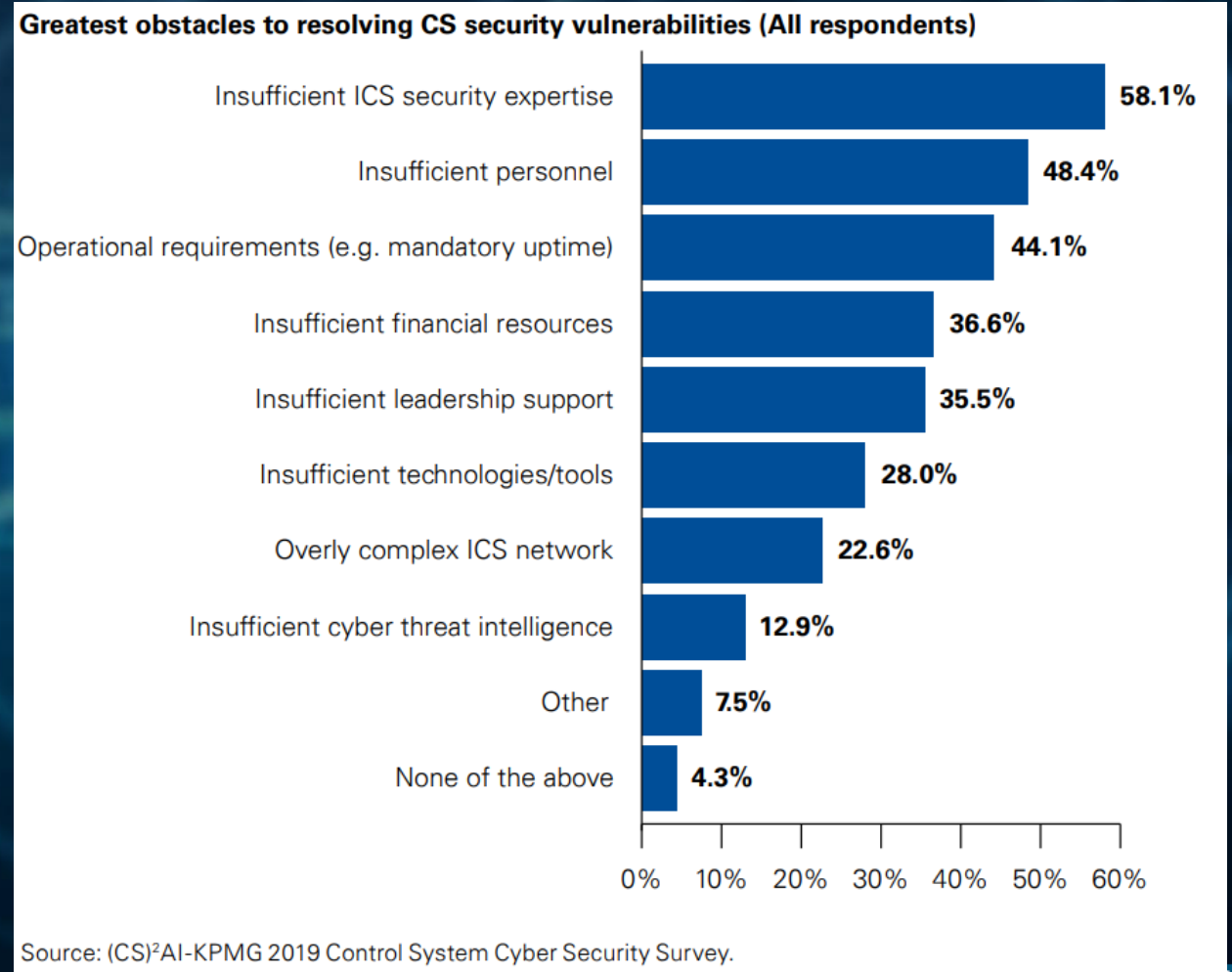
1. NCSC Traffic Light Protocol to be used for all information transfer
 - ❑ Assume TLP: GREEN – Share within sector; Not public
2. Specific company standards and practices will not be shared unless approved in writing by the company.
3. No commercially or contractually sensitive information will be exchanged or discussed (although vendors may be invited to attend and describe their solutions and approaches to ICS Cyber Security).
4. The information shared is intended to educate and promote learning. The steering committee will accept no liability resulting as a use of the information or offer any guarantee of the accuracy of the information.

NZ ICS Cyber TN

- ❑ **The good**
 - ❑ Building a community of 'OT practitioners'
- ❑ **The bad**
 - ❑ Driving forces can be a challenge
- ❑ **The ugly**
 - ❑ Letting the 'right' people in

NZ ICS Cyber TN

- ❑ **By the numbers**
- ❑ **Self-identify:**
 - ❑ 32% as 'IT'
 - ❑ 30% as 'OT'
 - ❑ 38% as 'IT, OT'
- ❑ **Growth**
 - ❑ Up to 208 since last year
- ❑ **(CS)²AI-KPMG 2020 Survey**
 - ❑ Trying to address #1 & #2



NZ Cyber Security Standard for ICS

❑ NCSC VCSS-CSO

1. Asset Identification
2. Security Management
3. Security Controls
4. Security Perimeter
5. Physical Security
6. Incident Reporting
7. Incident Response
8. Recovery Plans
9. Personnel & Training
10. Managing Confidentiality ^{new 2019}
11. Connected Devices & IoT ^{new 2019}

❑ Developed by NCSC (GCSB) and industry

❑ Alignment with best-practice advice from ICS vendors

❑ Alignment with international standards for ICS Security

❑ IEC-62443 Suite

❑ ISA-TR84.00.09 – SIS

❑ Updated 2019



VCSS High Level Overview

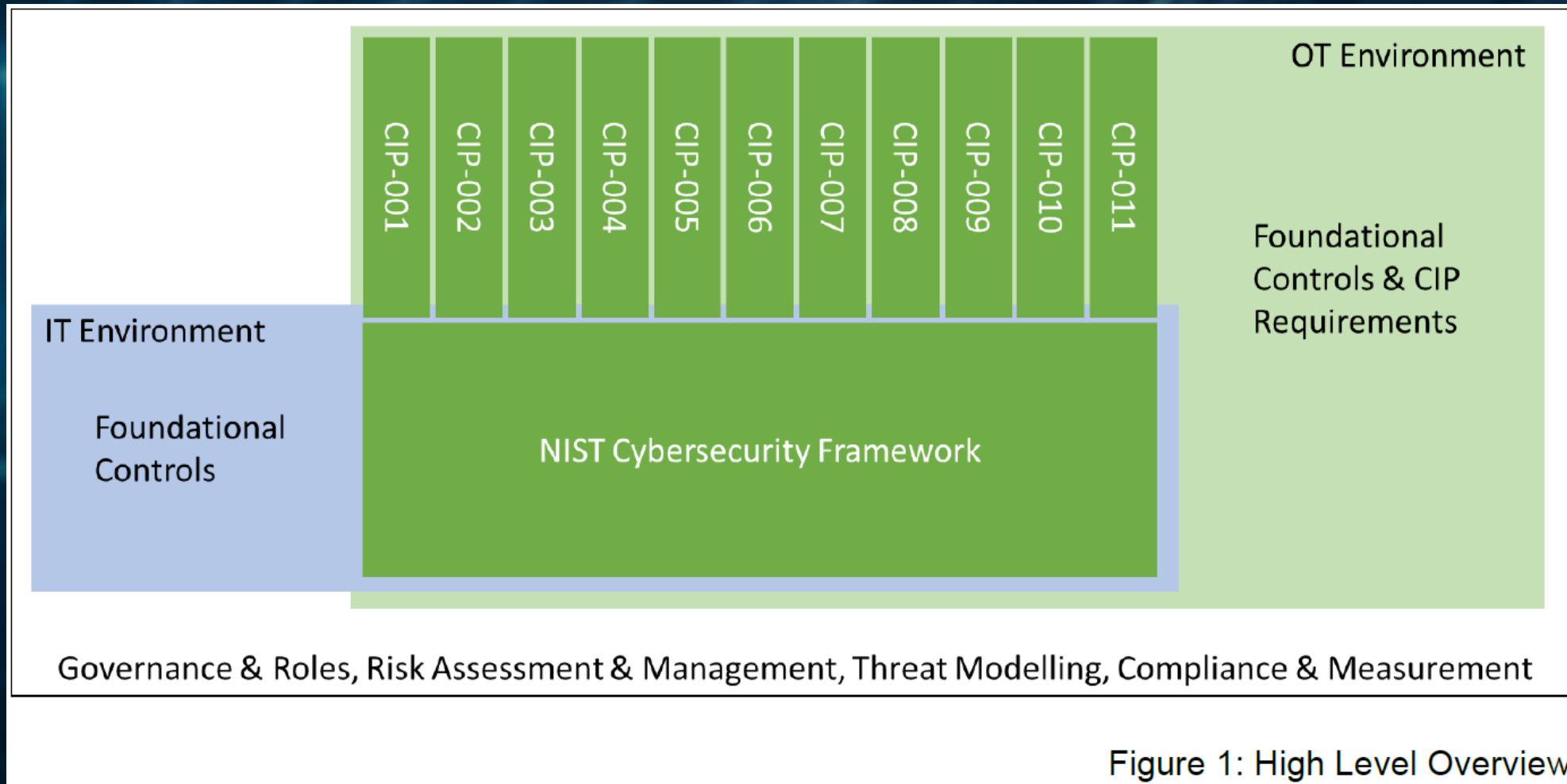


Figure 1: High Level Overview

VCSS Overview

- ❑ **Governance and Roles**
 - ❑ Roles and responsibilities; key stakeholders, senior leadership and third-party
- ❑ **Risk Assessment and Management**
 - ❑ Business integration; continuous assessment and reporting; management framework
- ❑ **Threat Modelling**
 - ❑ **Threats** abuse **vulnerabilities** of **assets** to generate **harm** for the **organisation (27005)**
 - ❑ Threat (Adversary, Likelihood); Asset (Vulnerabilities, Controls); Impact (Consequence).
- ❑ **Framework and Foundational Controls**
 - ❑ Identify; Protect; Detect; Respond; Recover
- ❑ **CIP Requirements**
- ❑ **Assurance**
 - ❑ Assessments; Audits; Testing

Thank You!
#hallway-peter-jackson

