Using OT Cyber Security Programs to **amplify** your Impact

AusCERT Conference, May 2024

/whois @beLarge

- Chief Evangelist & Principal OT Cyber Security Architect at Secolve
- Worked in IT and OT in Network & System Engineering and Cyber Security roles for 15 years
- Chartered Engineer (CPEng) and Registered Professional Engineer of Queensland (RPEQ)
- Queensland President of the Professional Engineers a proud member of Professionals Australia (PA) – The Union for STEM Workers!
- Deputy Chair of the Queensland Branch of the Australian Information Security Association (AISA) and Lead of the AISA Security Architecture Special Interest Group (SecARCH SIG)
- Bach Eng (Telecomms) QUT and Master Business (Applied Finance) QUT

secolve

THE OT SECURITY SPECIALISTS

SABSA FOUNDATION LEVEL SCF

GIAC INDUSTRIAL CYBER SECURITY PROFESSIONAL GICSP

GIAC RESPONSE AND INDUSTRIAL DEFENSE GRID

GIAC SECURITY OPERATIONS MANAGER GSOM

ISA/IEC 62443 CYBERSECURITY EXPERT ISA

alc Cyber Security Foundation+Practitioner CERTIFIED

Why this presentation?

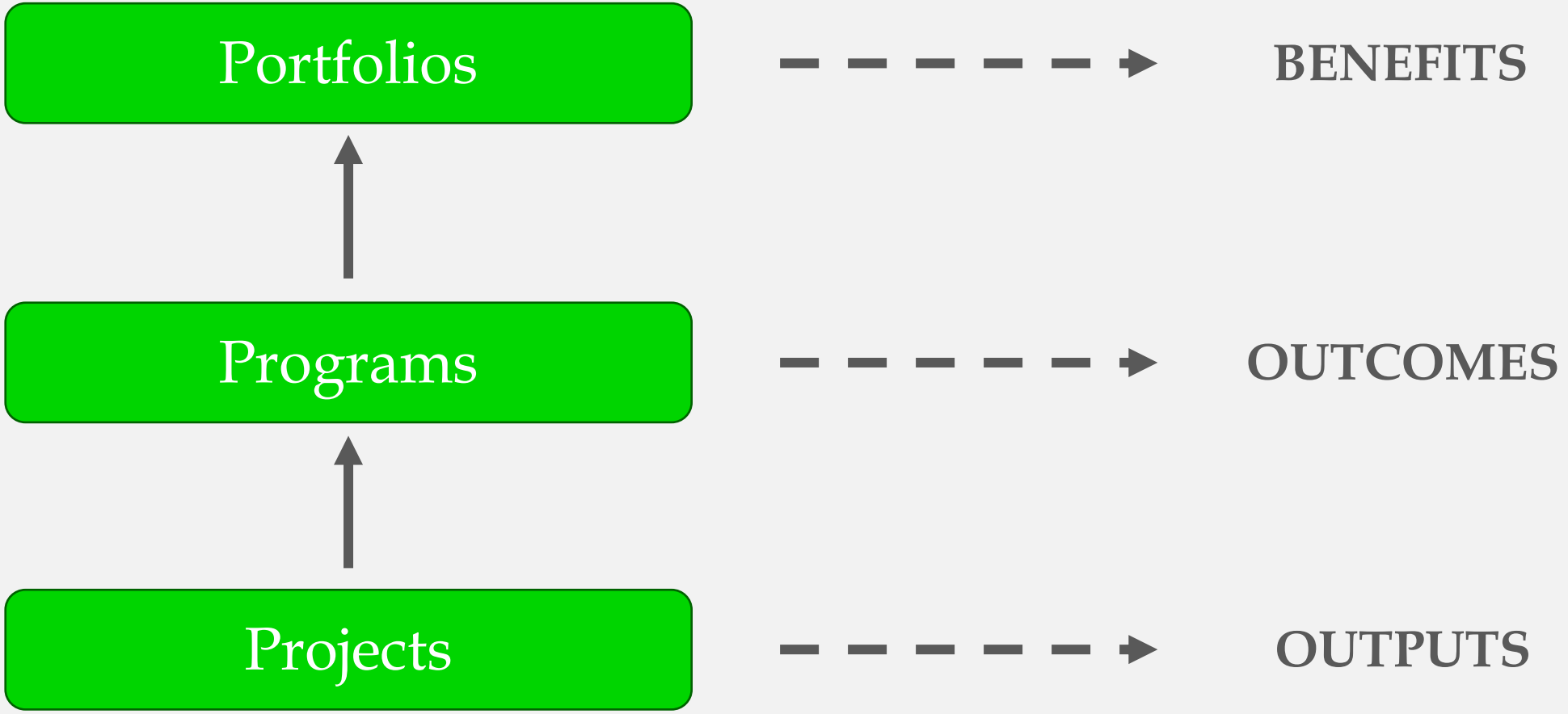
Source - https://tenor.com/en-AU/view/pirates-of-the-caribbean-explosion-ship-destroyed-captain-gif-3532311

Agenda

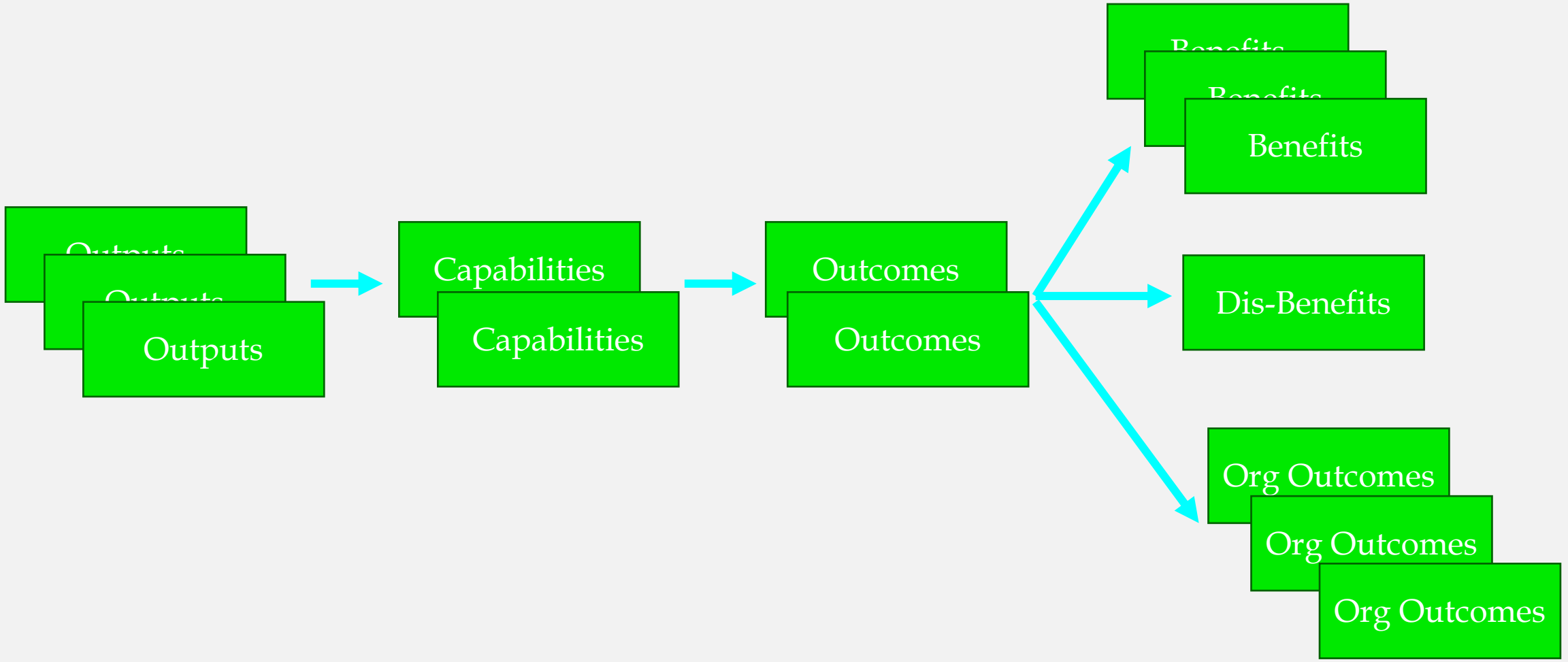
1. Program methodologies and what works
2. Sponsors, how to work with them
3. Stakeholder management with OT teams
4. Comparison of OT security frameworks and how to use them
5. Change management
6. Knowledge management
7. Q&A

Program Methodologies and what works

The difference between Projects, Programs and Portfolios

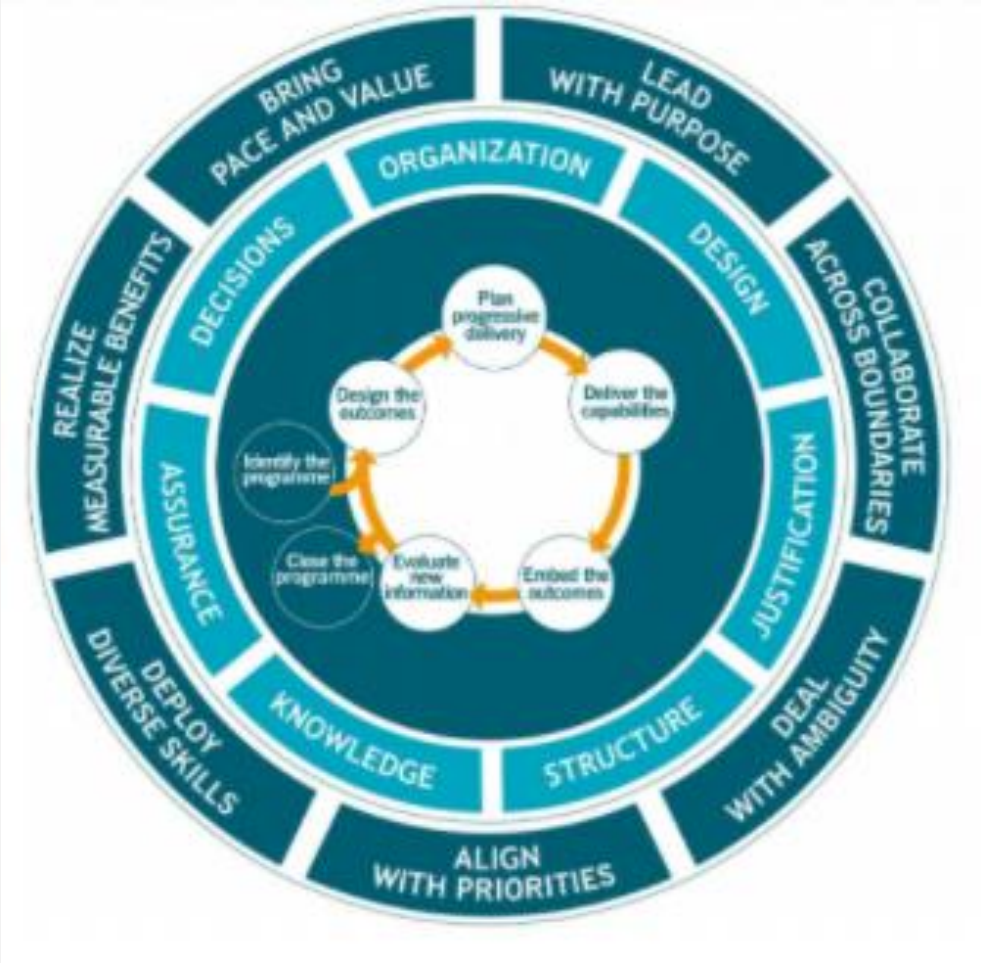


Another way to look at it …



Source - MSP

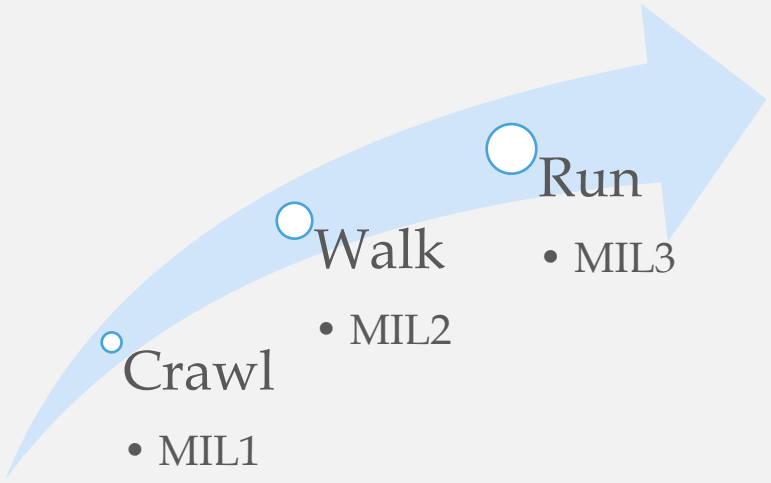
Managing Successful Programs



Source - https://www.qrpinternational.ch/en/qrp-news/msp-guide-5th-edition/

C2M2 – PROGRAM Domain

- A great place to start is the C2M2 PROGRAM Domain



1. Establish Cybersecurity Program Strategy

MIL1	a.	The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner
MIL2	b.	The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities
	c.	The cybersecurity program strategy and priorities are documented and aligned with the organization's mission, strategic objectives, and risk to critical infrastructure
	d.	The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities
	e.	The cybersecurity program strategy defines the structure and organization of the cybersecurity program
	f.	The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program

2. Establish and Maintain Cybersecurity Program

MIL1	a.	Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner
MIL2	b.	The cybersecurity program is established according to the cybersecurity program strategy
	c.	Senior management sponsorship for the cybersecurity program is visible and active
	d.	Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies
	e.	Responsibility for the cybersecurity program is assigned to a role with sufficient authority
	f.	Stakeholders for cybersecurity program management activities are identified and involved
MIL3	g.	Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy
	h.	Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes
	i.	The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate
	j.	The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies

Source – https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

Sponsors,
how to work with them

The Role of the Sponsor

- The Sponsor is a critical and challenging role
- Has the accountability for the success of the program, consequences for failure!!
- There must be a partnership between the Sponsor and the Program Manager
- The sponsor must be visible and engaged

Understand your sponsor's communication style

- Are they a Visual Communicator?
- Or, are they Conversational?
- Or, do they prefer to stick to the facts and are detail orientated??
- Ask if they have a DISC profile?

Source - https://medium.com/innovators-gargage-ig/disc-assessment-and-personality-test-7259cef09b4

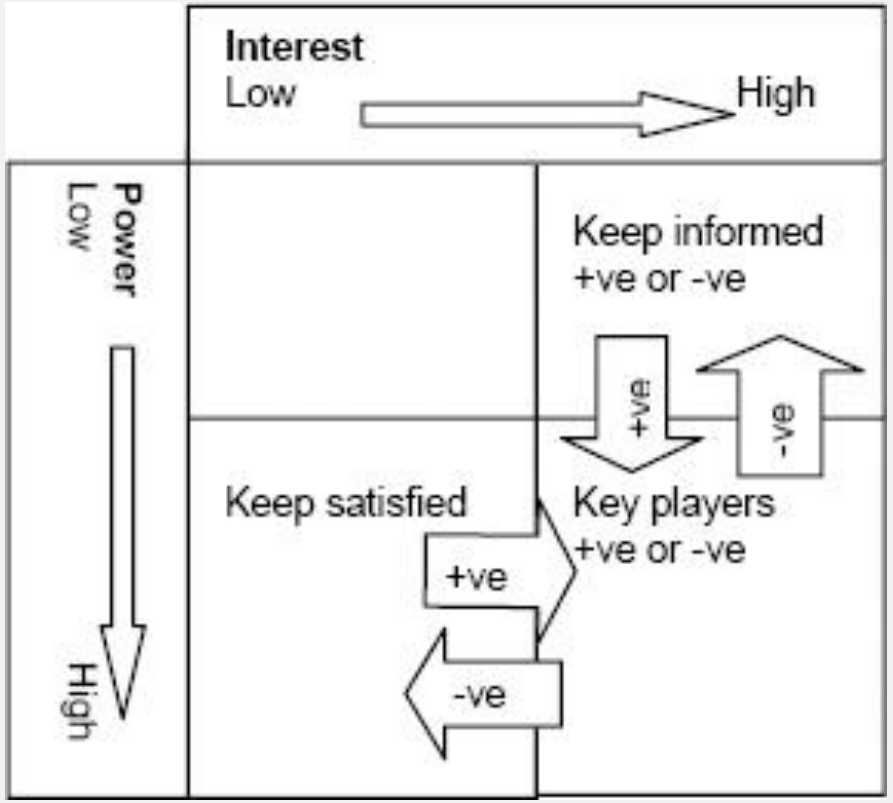
The Courageous Sponsor

- Defines the role expectations of the Sponsor, Project manager and project terminology
- Defines Sponsor Personas
  - Peacock
  - Magpie
  - Ostrich
  - Duck
  - Eagle
  - Owl
- Helps sponsors understand how they can ask for help & structure their projects

Stakeholder management with OT Teams

Stakeholder Management is Vital for Program Success

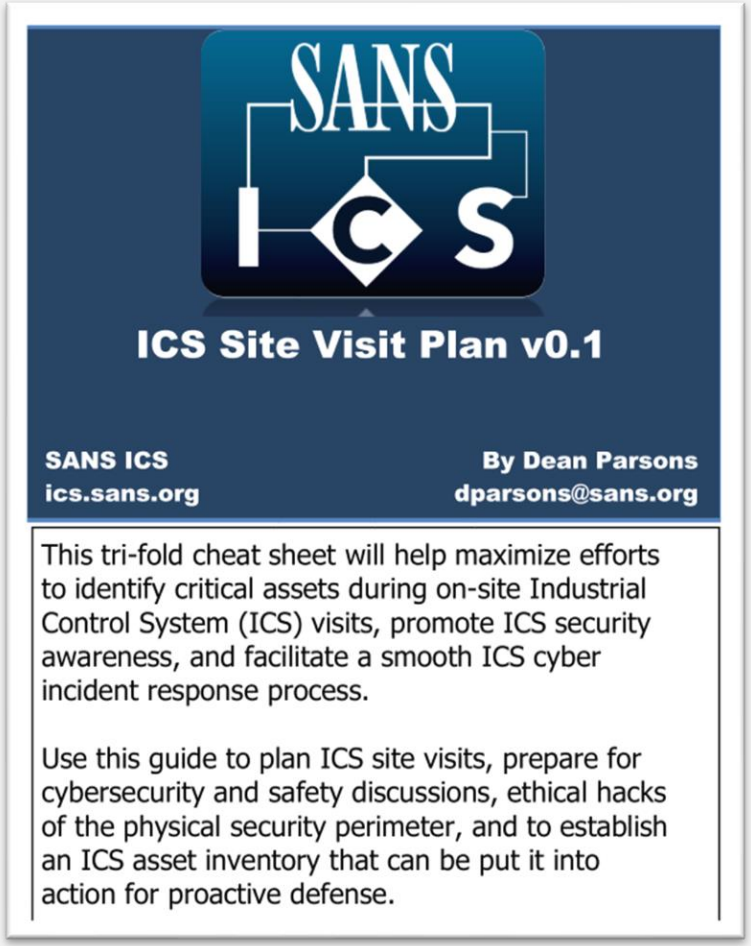
- Build a stakeholder analysis matrix
- Use this analysis to build a communications plan
  - High Interest and High Power – in person updates, understand their communication preference
  - Low Power and Low Interest – general mailing list updates



Ref https://www.pmi.org/learning/library/stakeholder-management-task-project-success-7736

Tips for working with OT Stakeholders

- Meet with OT Stakeholders on site and 'walk the line'
- Prepare for the conversations before the meeting – find previous risk assessments, reports and other internal references
- Many more great tips on the SANS ICS Site Visit Plan:
  - OSINT for ICS Defenders
  - Coordinate with Safety and Security Teams
  - Ethically Hack the Physical Security Perimeter
  - Plant Floor Cyber Security Discussions
  - Spreadsheet, Laptop Stand & Network Diagrams
  - Follow up with Traffic Analysis
  - Storing Asset Inventory Back at the Office



Source - https://www.sans.org/posters/ics-site-visit-plan/

Comparison of OT Security Frameworks

And how to use them

NIST Cyber Security Framework (CSF)

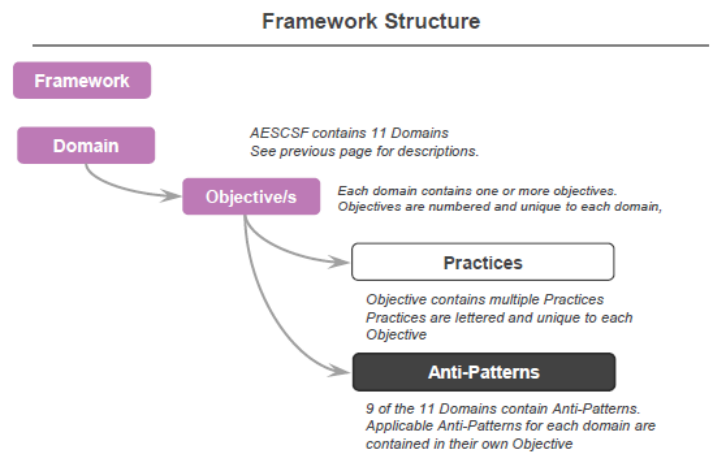
- The NIST CSF is the most well known framework for management (e.g. Boards)
- Version 2 defines 6 Functions, the new "GOVERN" function
- Has the concept of "Implementation Examples"
- Has a mapping to ISA/IEC 62443 Security for Industrial Automation and Control Systems

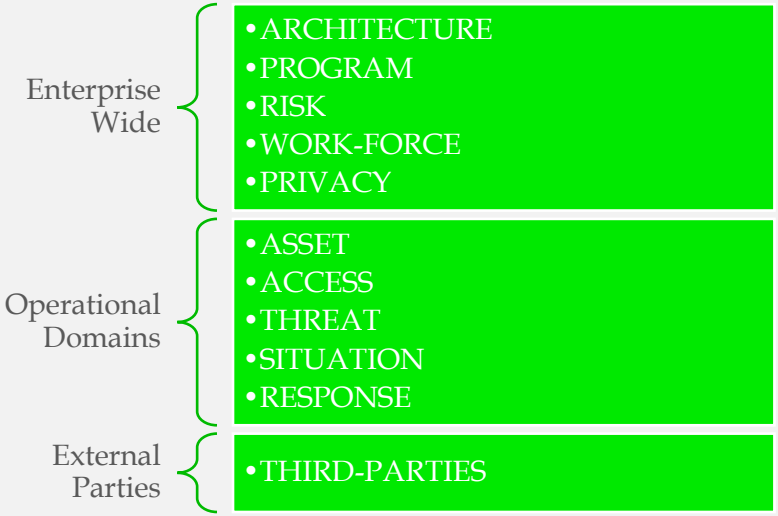
Category	Subcategory	Implementation Examples
Organizational Context (GV.OC): The circumstances — mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements — surrounding the organization's cybersecurity risk management decisions are understood		
	GV.OC-01: The organizational mission is understood and informs cybersecurity risk management	**Ex1:** Share the organization's mission (e.g., through vision and mission statements, marketing, and service strategies) to provide a basis for identifying risks that may impede that mission
	GV.OC-02: Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered	**Ex1:** Identify relevant internal stakeholders and their cybersecurity-related expectations (e.g., performance and risk expectations of officers, directors, and advisors; cultural expectations of employees) **Ex2:** Identify relevant external stakeholders and their cybersecurity-related expectations (e.g., privacy expectations of customers, business expectations of partnerships, compliance expectations of regulators, ethics expectations of society)
	GV.OC-03: Legal, regulatory, and contractual requirements regarding cybersecurity — including privacy and civil liberties obligations — are understood and managed	**Ex1:** Determine a process to track and manage legal and regulatory requirements regarding protection of individuals' information (e.g., Health Insurance Portability and Accountability Act, California Consumer Privacy Act, General Data Protection Regulation) **Ex2:** Determine a process to track and manage contractual requirements for cybersecurity management of supplier, customer, and partner information **Ex3:** Align the organization's cybersecurity strategy with legal, regulatory, and contractual requirements

Source - https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Australian Energy Sector Cyber Security Framework

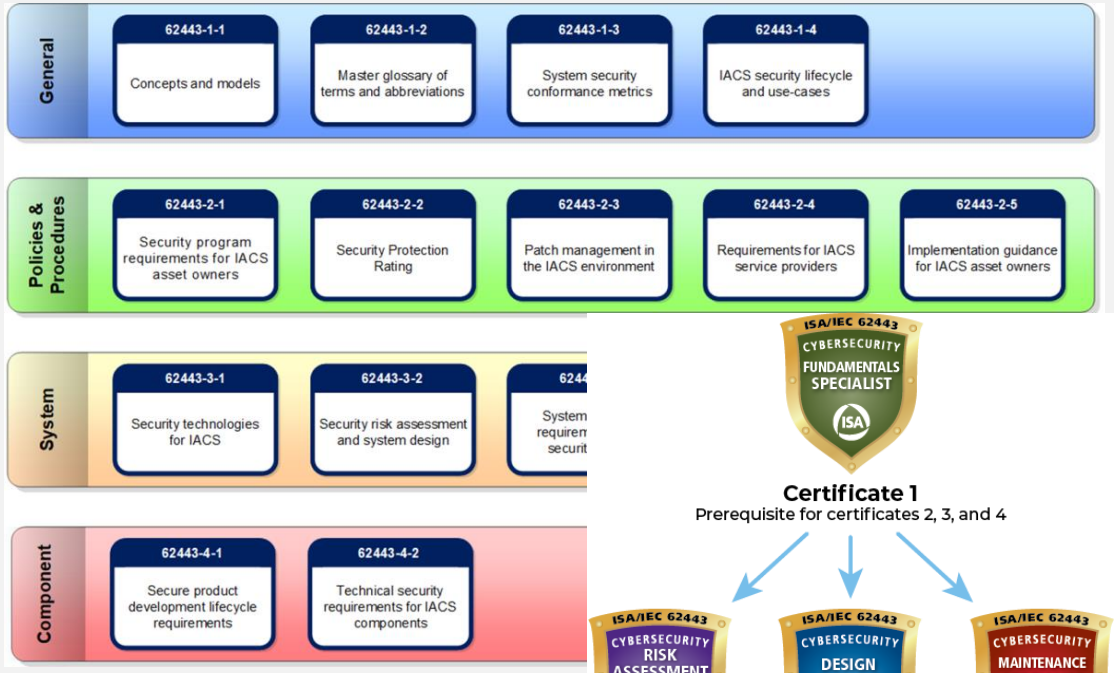
- Originally developed by the CSIWG, led by the AEMO in 2018 and version 2 released in 2021
- A modification of the US C2M2, Addition of the PRIVACY Domain and the addition of Anti Patterns
- 11 Domain, 354 Practices including 42 Anti Patterns in Version 2
- Practices are mapped to Maturity Indicator Level and Security Profiles





ISA/IEC 62443 Standard Series

- Framework of Cyber Security Publications for Industrial Automation and Control Systems (IACS)
- ISA 99 is the Working group and the standards were now published in partnership with the IEC and are designated ISA/IEC 62443
- NIST Cyber Security Framework references Part 2-1 and Part 3-3
- Has a certification program for Process, Systems and Components
- Has a training & certification program for people
- Key concepts of a Cyber Security Management System and Cyber Security Requirements Specification



Ref - https://www.isa.org/certification/certificate-programs/isa-iec-62443-cybersecurity-certificate-program

How to use them?

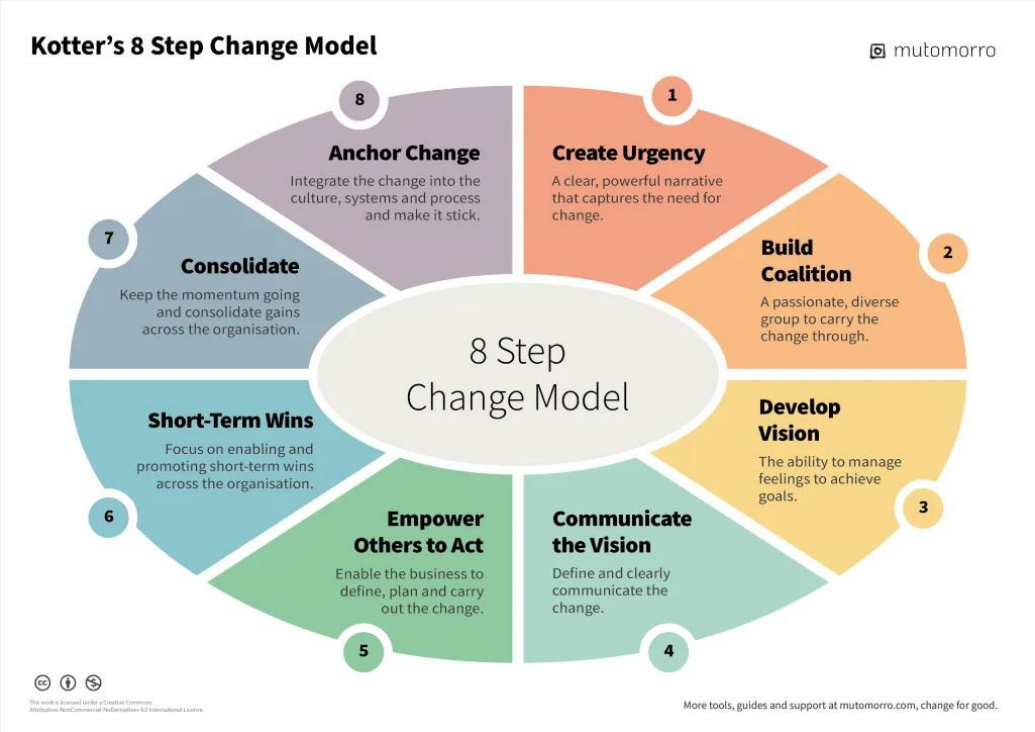
- Use the framework your organisation is most familiar with initially
- Consider regulatory requirements such as SOCI CIRMP Cyber Security Frameworks
  - ISO 27001
  - Essential 8 Maturity Model - Maturity Model Level 1
  - NIST CSF
  - C2M2 - MIL-1
  - AESCSF (2020-2021) – SP-1
- If you don’t know where to start, start with the NIST CSF!

Change Management

“Everyone loves progress,
but nobody loves change”

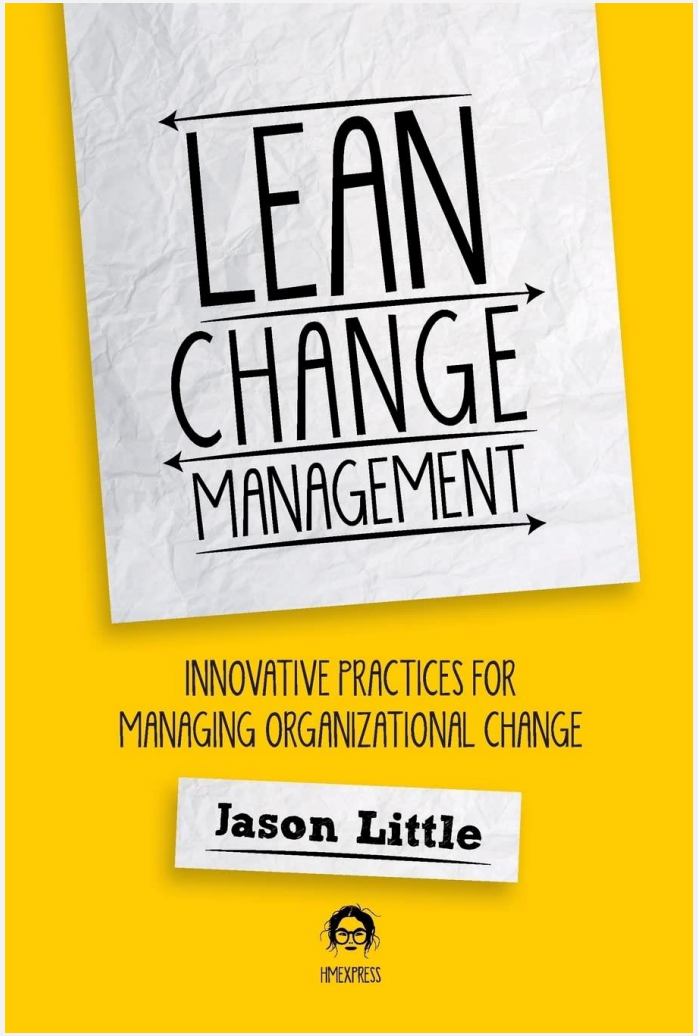
Change Management

- Use frameworks like
  - ADKAR
  - Kotter's Change
- Understand the Change Appetite of impacted people
- Communicate, Communicate, Communicate



Ref - https://mutomorro.com/kotters-8-step-change-model/

Lean Change Management



Knowledge Management

What is Knowledge Management

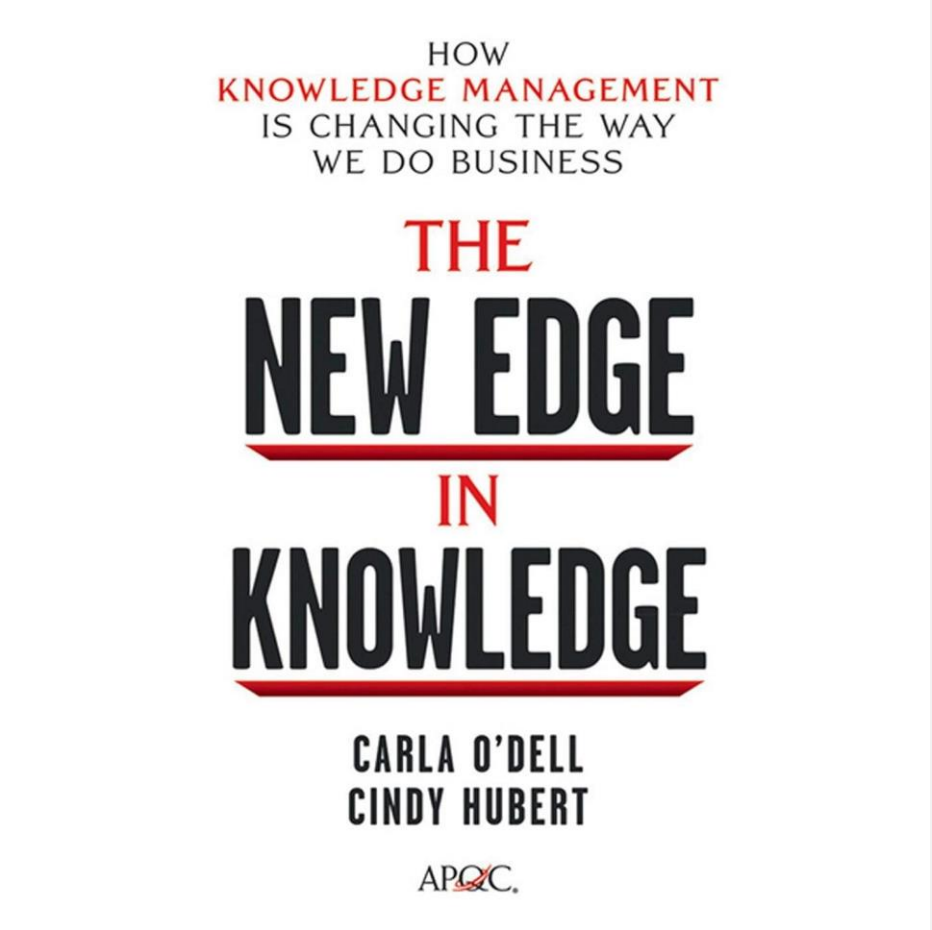
- "Knowledge management (KM) is the process of identifying, organising, storing and disseminating information within an organisation."

Companies with a knowledge management strategy achieve business outcomes more quickly as increased organisational learning and collaboration among team members facilitates faster decision-making across the business.

Source IBM

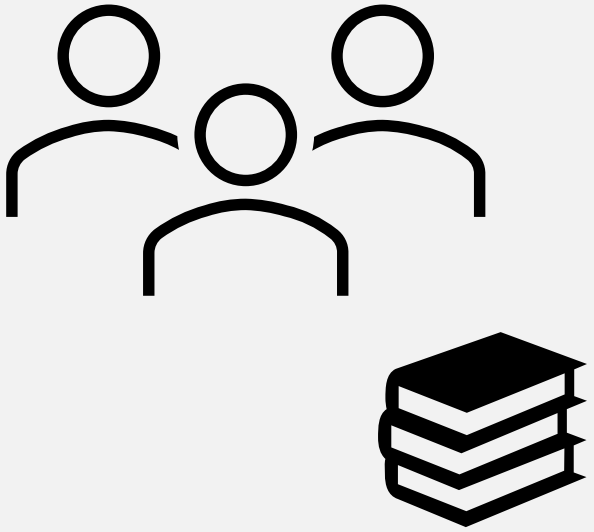
Tips for Knowledge Management

- Have Knowledge Management (KM) ready at the teachable moment
- Make the process easy to share and obtain knowledge – make it part of their normal working process
- Focus on connecting people, not just content
- KM Methods to consider:
  - Self Service
  - Lessons Learnt
  - Communities of Practice
  - Transfer of Best Practices



Communities of Practice

- Communities of Practice are a fantastic method to share knowledge
- Creates a space for people to connect and share information
- Ask people to present teach backs following training
- Don’t know where to start, make a Microsoft Teams Group!



Document Management

- Document who has been involved and engaged in the development of standards (TIP – Useful for AESCSF MIL 2 Practices)
- Use Meta Data tags to make the documents easily organised, managed and discoverable
- Share updates with Communities of Practice

Summary

Summary & Homework

1. Understand how to use Programs to deliver change
2. Your relationship with your sponsor is key, don't forget it's a partnership!
3. The right framework can help give structure and show progress, if you don't know where to start, use the NIST CSF
4. Change is hard, make sure you invest in your change management strategy
5. Your program is developing a lot of knowledge, manage it

Thank you!
Questions?


https://linkedin.com/in/blargeau


https://github.com/beLarge


@beLarge