

Better OT Cyber Security Risk Assessments



Introduction

This guide aims to help you do your OT Cyber Security risk management better.

This guide outlines applicable cyber security frameworks, useful tips for running your cyber security assessments and how to self assess your OT Cyber Security Risk Management capability using the C2M2 Risk Domain.

This document also refers to the Crawl, Walk and Run maturity model framework to help you pick the right framework for where you are.

Table of Contents

[3. Use ISO 31000 as your base](#)

[4. Useful Cyber Security Frameworks](#)

[8. Tips for your next cyber security risk assessment](#)

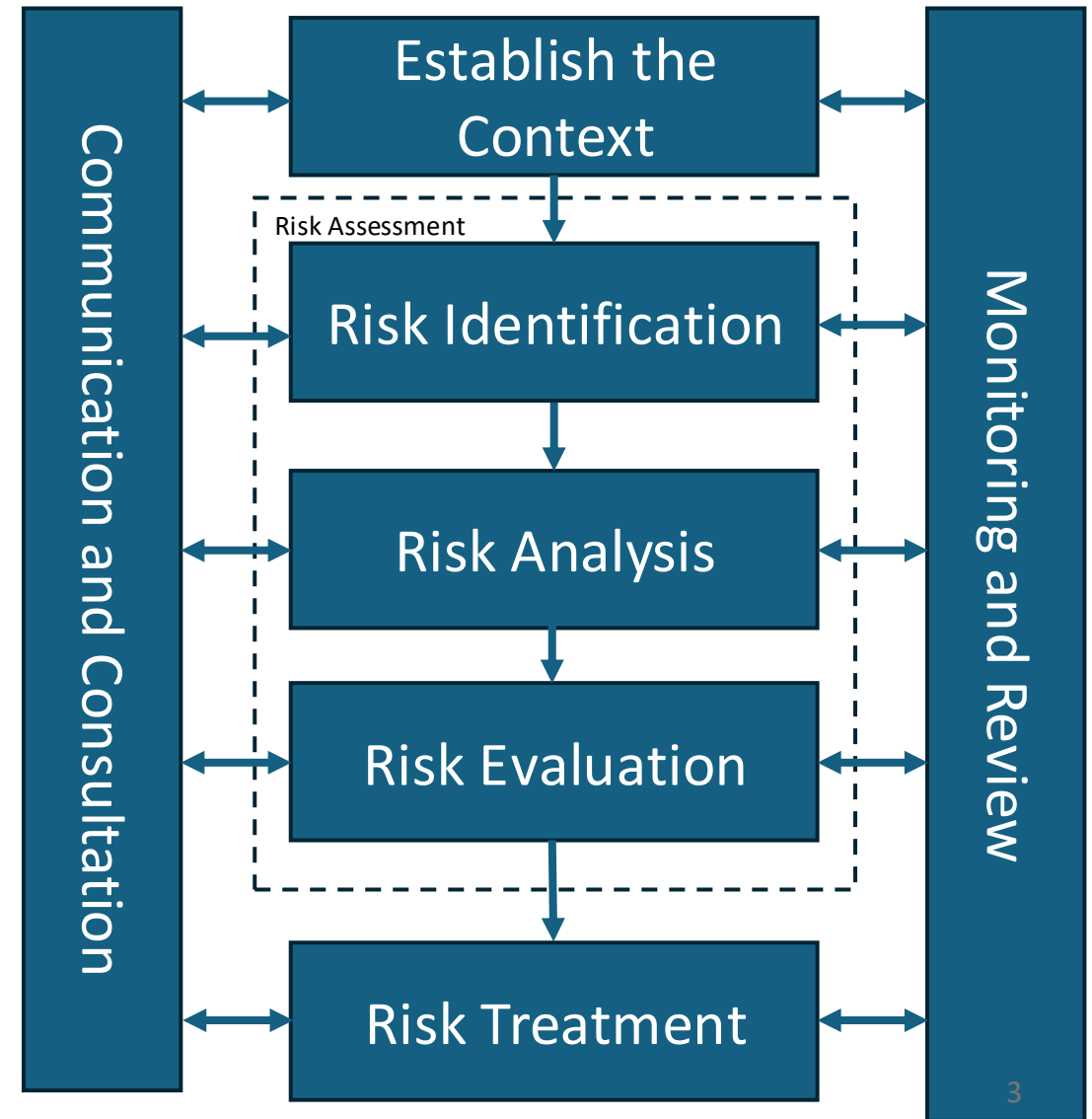
[10. Self Assess your OT Cyber Security Risk Management capabi...](#)

[11. About BLARGE](#)



Use ISO 31000 as your base

- ISO 31000 as the base for your OT Cyber Security Risk Management Capability



Useful Cyber Security Frameworks



Crawl – ISO 27005 & NIST 800-37, 800-39

ISO 27005

- ISO 27005 is the application of ISO 31000 for Information Security
- Learn more at [Information security, cybersecurity and privacy protection — Guidance on managing information security risks](#)

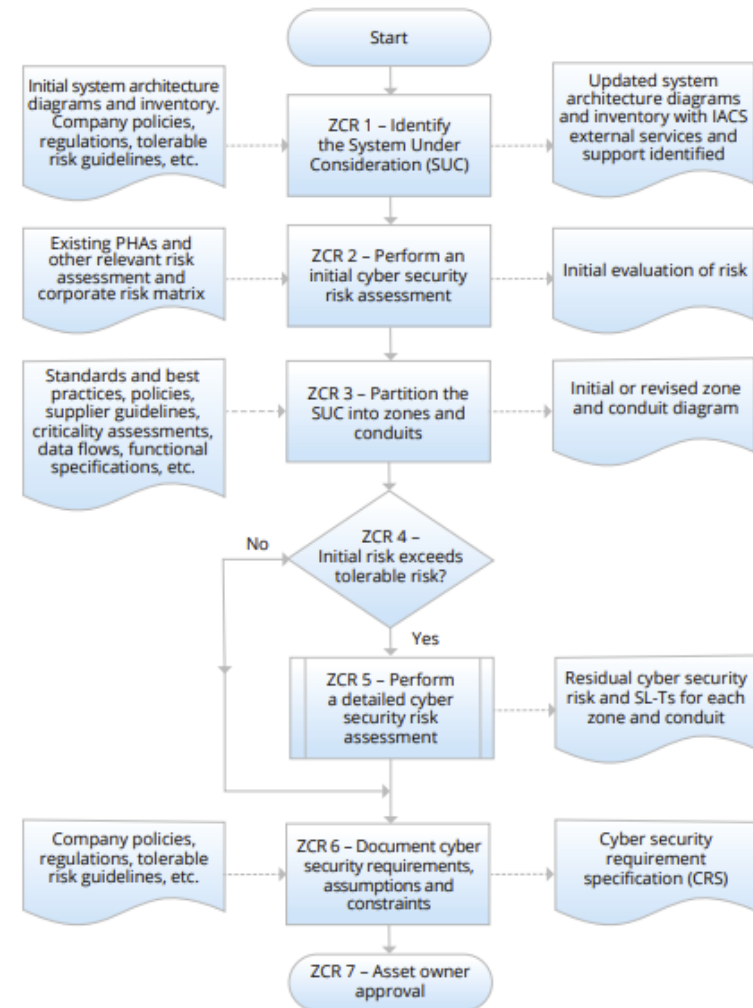
NIST 800-37 & 800-39

- These NIST Standards outline how to manage your cyber security risk management program learn more at:
 - [NIST SP 800-37 Rev. 2](#)
 - [NIST SP 800-39](#)



Walk – ISA/IEC 62443

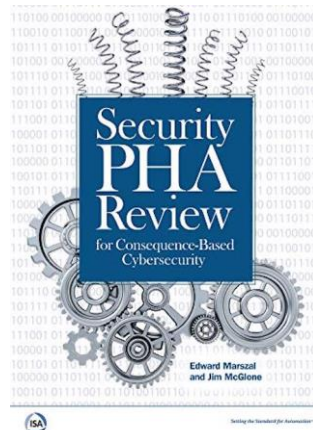
- The ISA/IEC 62443 Standard Series considers how Cyber Security is managed for Industrial Automation and Control Systems (IACS)
- It has 14 Publications and 62443 Part 3-2 considers how to assess cyber risk for IACS
 - 3-2 outlines the Zone and Conduit Requirements (ZCR)
- Learn more at [Leveraging ISA 62443-3-2 for IACS Risk Assessment and Risk Related Strategies](#)



Run – SPR & CCE

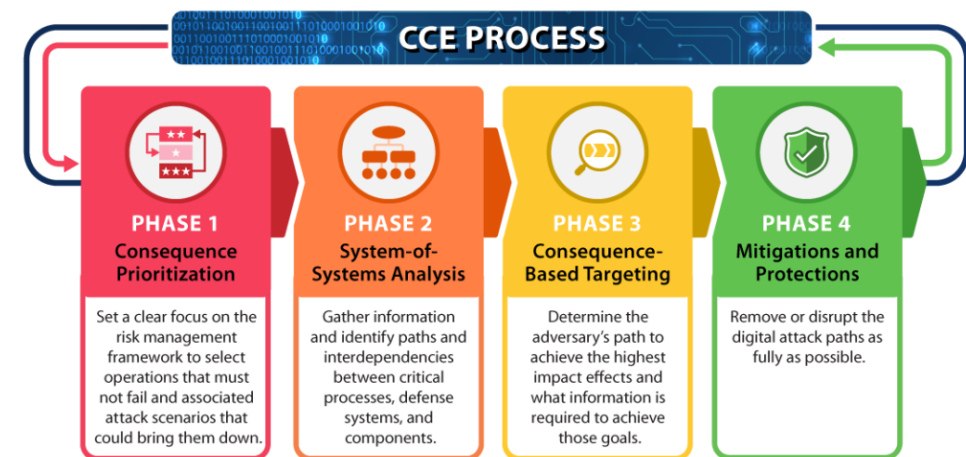
Security PHA Review (SPR)

- A Security PHA Review takes a PHA and asks if it could be initiated by a cyber event and if the controls could be Cyber compromised
- Learn more at this [ISA Intech Article](#)



Consequence-Driven Cyber-Informed Engineering (CCE)

- Learn more at <https://inl.gov/national-security/cce/>



Tips for your next cyber security risk assessment



Practical Tips for running your next Assessment

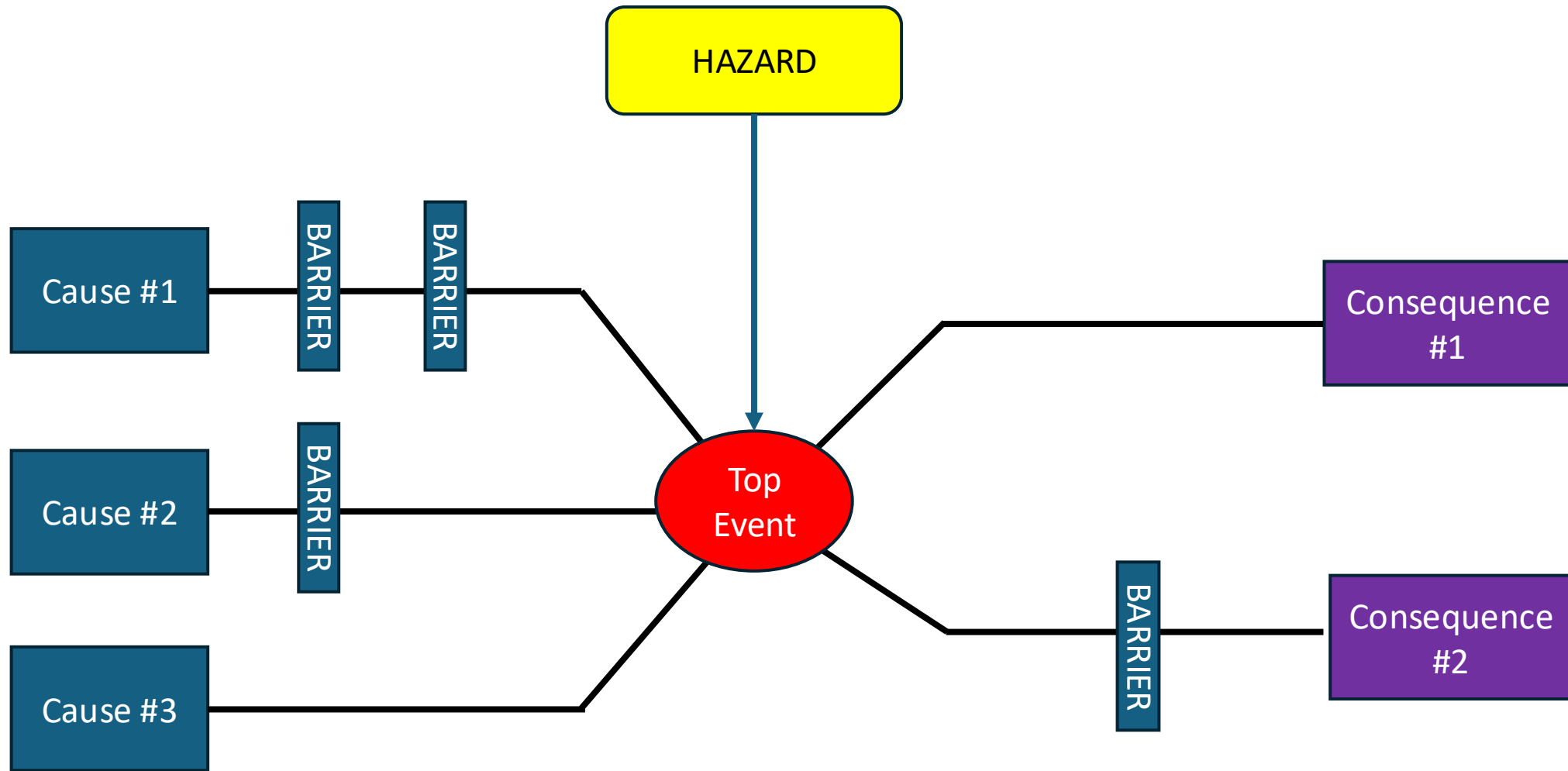
1. Have an experienced Risk Facilitator
 - A great facilitator is able to constructively challenge assumptions and assertions
2. Clear Scope and agreed System under Consideration
 - Use the System Under Consideration (SUC)
3. Make sure you have the right people in your assessment
 - Cyber Risk often lives in the intersection of systems and responsibilities

Risk Scenario Structure

[There is a risk that a]
[THREAT]
does an
[ACTION or EXPLOIT VULNERABILITY]
against an **[ASSET]**



Communicate Cyber Risk using Bowtie diagrams



Self Assess your OT Cyber
Security Risk Management
capability using the C2M2
RISK domain



An overview of the C2M2 RISK Domain

1. Establish and
Maintain Cyber Risk
Management
Strategy and Program

2. Identify Cyber Risk

3. Analyze Cyber Risk

4. Respond to Cyber
Risk

5. Management
Activities for the RISK
domain



1. Establish and Maintain Cyber Risk Management Strategy and Program

1. Establish and Maintain Cyber Risk Management Strategy and Program

MIL1	a. The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner
MIL2	b. A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture c. The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy d. Information from RISK domain activities is communicated to relevant stakeholders e. Governance for the cyber risk management program is established and maintained f. Senior management sponsorship for the cyber risk management program is visible and active
MIL3	g. The cyber risk management program aligns with the organization's mission and objectives h. The cyber risk management program is coordinated with the organization's enterprise-wide risk management program



2. Identify Cyber Risk

2. Identify Cyber Risk

MIL1	a. Cyber risks are identified, at least in an ad hoc manner
MIL2	b. A defined method is used to identify cyber risks c. Stakeholders from appropriate operations and business areas participate in the identification of cyber risks d. Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level e. Cyber risk categories and cyber risks are documented in a risk register or other artifact f. Cyber risk categories and cyber risks are assigned to risk owners g. Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events
MIL3	h. Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction i. Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities) j. Threat management information from THREAT domain activities is used to update cyber risks and identify new risks k. Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks l. Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks m. Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations



3. Analyze Cyber Risk

3. Analyze Cyber Risk

MIL1	a. Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner
MIL2	b. Defined criteria are used to prioritize cyber risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance) c. A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification) d. Defined methods are used to analyze higher priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility) e. Organizational stakeholders from appropriate operations and business functions participate in the analysis of higher priority cyber risks f. Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response
MIL3	g. Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains



4. Respond to Cyber Risk

4. Respond to Cyber Risk

- | | |
|-------------|--|
| MIL1 | a. Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner |
| MIL2 | b. A defined method is used to select and implement risk responses based on analysis and prioritization |
| MIL3 | <ul style="list-style-type: none">c. Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risksd. Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated, and risk tolerances are not exceedede. Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate |



5. Management Activities for the RISK domain

5. Management Activities for the RISK domain

MIL1 No practice at MIL1

- MIL2**
- a. Documented procedures are established, followed, and maintained for activities in the RISK domain
 - b. Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain
-

- MIL3**
- c. Up-to-date policies or other organizational directives define requirements for activities in the RISK domain
 - d. Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel
 - e. Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities
 - f. The effectiveness of activities in the RISK domain is evaluated and tracked
-



About BLARGE

MISSION CRITICAL CYBER SECURITY

BLARGE is a specialist Cyber Security Consultancy focusing on Australian Critical Infrastructure.

At BLARGE we reference world-class methodologies and frameworks and learn from the best to help you manage your cyber security risks.

Our services include:

1. Cyber Security Tabletops and Executive Education
2. Cyber Security Program and Project Advisory
3. Cyber Security Risk Assessments
4. Cyber Security Architecture Support and Development
5. OT Cyber Security Operations Advisory
6. OT Cyber Security Advisory Retainer



<https://blarge.io>



contact@blarge.io