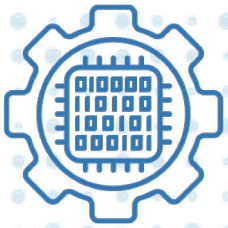


Cyber-Informed Engineering

Integrating Cyber-Informed Engineering into Enterprise Risk Management

September 30, 2024

Authors:

Andrew Ohrt
West Yost Associates

Amanda Jones
West Yost Associates

Jeremy Smith
West Yost Associates

Virginia Wright
Idaho National Laboratory

Benjamin Lampe
Idaho National Laboratory

Remy Stolworthy
Idaho National Laboratory

INL/MIS-24-81692-Rev000

Cyber-Informed Engineering (CIE) Program activities are sponsored by the U.S. Department of Energy's Office of Cybersecurity, Energy Security, and Emergency Response (DOE CESER) and performed by Idaho National Laboratory and the National Renewable Energy Laboratory.

INL/MIS-24-81692-Rev000

Contents

1. Introduction

Many critical infrastructure organizations have enterprise risk management (ERM) processes in place to help ensure their organization can address business risks and meet their established mission and deliver critical functions. Central to any ERM process is the evaluation of the criticality of systems, assets, and organizational components. Cyber-Informed Engineering (CIE) provides a new approach to addressing cyber-risk. This document aims to support organizations with the application of CIE within the context of ERM for their organization.

The approach presented can be implemented independent of formal ERM processes to support any organization's cyber-resilience. It provides a starting point and presents an approach by which any organization can begin the adoption of CIE in parallel with new or existing ERM practices. Both ERM and CIE are iterative processes. This approach also illustrates how CIE and ERM align to provide continuous improvement and support to the engineering and operations cultures of an organization.

1.1. Background on Cyber-Informed Engineering

The CIE Implementation Guide describes CIE as an extension of "secure-by-design" concepts beyond the digital realm to include the engineering of cyber-physical systems. CIE introduces cybersecurity considerations at the earliest stages of system design, long before the incorporation of software and security controls or mitigations. It calls on engineers to identify engineering controls and design choices that could eliminate attack vectors for cyber actors or minimize the damage they could inflict. [1]

CIE expands cybersecurity and cyber-resilience decision making into engineering teams, not by asking engineers to become cyber experts, but by calling on engineers to apply engineering tools and make engineering decisions that improve cybersecurity outcomes. CIE examines the engineering consequences that a sophisticated cyber attacker could achieve and drives engineering changes that may provide deterministic mitigations to limit or eliminate those consequences.

1.2. Background on Enterprise Risk Management

ERM is an approach to identifying, assessing, and managing risks across all business units and functions of an entire organization. ERM aims to provide a structured and consistent framework for managing risks that could impact an organization's objectives and operations. This comprehensive strategy helps organizations anticipate and evaluate the current and future threat environments, mitigate risks, and seize opportunities, to enhance overall resilience and decision-making. By adopting ERM, organizations can better align their risk appetite with their strategic goals, ensuring a proactive and coordinated response to both internal and external challenges.

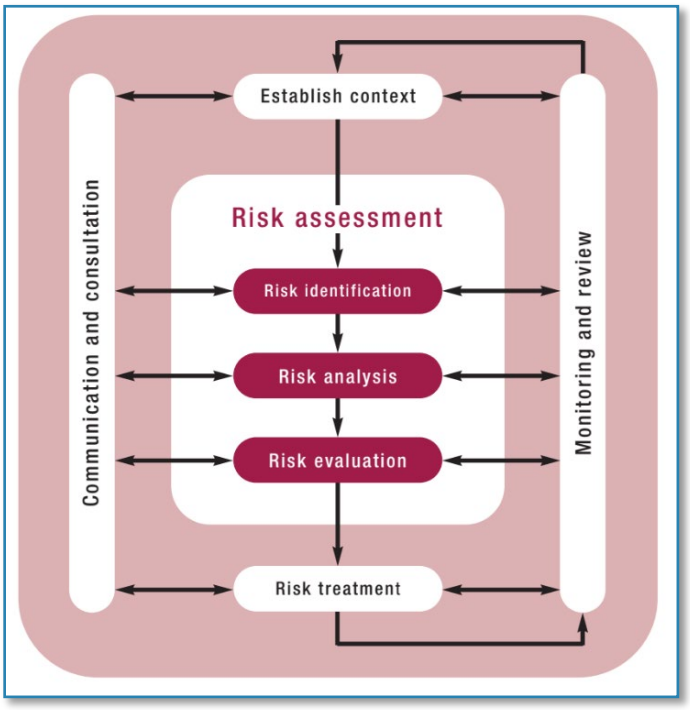
ERM is guided by standards such as the International Organization for Standardization (ISO) 31000 – Risk Management standard, which provides guidelines for effective implementation of risk management.

[1] Wright, Virginia L, et. al., 2023. "Cyber-Informed Engineering Implementation Guide." United States. https://www.osti.gov/servlets/purl/1995796.

The risk management process, as recognized by ISO 31000, is shown below in Figure 1. ISO 31000 Risk Management Process.

The ISO 31000 risk management process recognizes the importance of feedback and review of performance and communication and consultation. Monitoring and review ensure that the organization monitors risk performance and learns from experience. Communication and consultation are presented in ISO 31000 as part of the risk management process, but it may also be part of the supporting framework.[2]

Figure 1. ISO 31000 Risk Management Process



Risk identification helps an organization understand its exposure to risks and uncertainties. This requires a deep understanding of the organization, its mission and critical functions, its market, and the legal, social, political, and cultural environment it operates in, as well as its strategic and operational goals. It involves knowing the key success factors and the threats and opportunities related to achieving these goals. A methodical approach ensures that all important activities are evaluated, and their associated risks identified.

The outcome of this analysis is a risk profile that rates the significance of each risk, helping to prioritize risk management efforts. This process maps risks to the affected business areas, describes existing control measures, and indicates where investment in controls might need to be adjusted. Risk analysis supports efficient operations by highlighting risks that need management's attention, allowing for prioritized risk control actions. Available risk responses include tolerating, treating, transferring, or terminating the risk.

[2] International Organization for Standardization. *A Structured Approach to Enterprise Risk Management (ERM) and the Requirements of ISO 31000*. ISO, 2018.

Risk treatment is the identification and selection of measures to mitigate risks. In addition to mitigation, this could include risk avoidance, risk transfer, and risk financing. The cost of any risk treatments should be justified by the benefits of risk reduction. Any risk treatment must be done within the context of compliance with laws, regulations, and contractual obligations. Risk financing, such as insurance, can provide financial protection against risks, but some consequences, like damage to reputation, may be uninsurable.[3]

DEFINITIONS

Building on the prior section, select ERM-related terminology and definitions are provided for context. Common ERM terms and definitions[4] include:

Risk – the effect of uncertainty on objectives.

Risk Attitude – an organization's approach to assess and eventually pursue, retain, take or turn away from risk.

Risk Management Plan – a scheme within the risk management framework specifying the approach, the management components and resources to be applied to the management of risk.

Risk Owner – a person or entity with the accountability and authority to manage a risk.

Establishing the context – defining the external and internal parameters to be considered when managing risk and setting the scope and risk criteria for the risk management policy.

Communication and Consultation – continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

Risk Assessment – the overall process of risk identification, risk analysis and risk evaluation.

Risk Identification – the process of finding, recognizing and describing risks.

Risk Analysis – a process to comprehend the nature of risk and to determine the level of risk.

Risk Evaluation – the process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.

Risk Treatment – a process to modify risk.

Monitoring – continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected.

Review – an activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives.

Risk Appetite – the magnitude and type of risk that an organization is willing to accept in pursuit of its objectives.

[3] International Organization for Standardization. ISO 31000:2009 Risk Management — Principles and Guidelines. ISO, 2009.
[4] Ibid.

1.3. Integration of Cyber-Informed Engineering and Enterprise Risk Management

CIE and ERM are complementary processes that, when integrated, provide an even more robust framework for integration of OT cyber-risk into ERM. CIE's proactive approach to embedding cyber-resilience across the engineering lifecycle phases aligns with ERM's holistic view of risk management across an organization. By incorporating CIE into an ERM process, organizations can ensure that OT cybersecurity risks are characterized and mitigated alongside other strategic, operational, and financial risks. The continuous improvement cycle that ERM fosters within an organization supports the iterative implementation of both CIE and adaptation to evolving threats. The approach presented below provides a way to integrate CIE into ERM.

2. Evaluation Process

To streamline integration of CIE into an organization's ERM framework, a flow chart process, illustrated in Appendix A, was developed. The flow chart provides an approach to integrate CIE into existing ERM processes and indicated in the chart. The flow chart illustrates a step-by-step process and considerations for each phase. The following sections, provide descriptions of and considerations for each step.

2.1. Step A.1 – Mission and Function Definition

Define the organization's mission and/or critical functions and the systems that support the mission and/or critical functions. For each mission and/or critical function of the organization, continue with the following approach.

Given that each organization's mission and/or critical functions can differ significantly, each assessment should be approached individually. This ensures that the unique aspects of the organization, such as operational requirements and current capabilities, are considered and accounted for. By doing so, risks are better characterized. This leads to improved strategies and solutions to reduce risk to the mission and critical functions, thereby improving the overall ERM of the enterprise.

NEXT STEPS

Move to Step B.1 to define how dependent the organization is upon digital automation.

2.2. Step B.1 – Digital Awareness

Is the organization dependent upon digital automation (i.e., computers, programmable logic controllers, Supervisory Control and Data Acquisition (SCADA) software) to achieve its mission and/or critical functions?

At this step, determine whether the organization depends on automation technologies, such as computers, programmable logic controllers (PLCs), and SCADA software, to fulfill its mission and critical functions. Understanding the extent of this reliance helps in identifying the specific operational needs and potential vulnerabilities associated with these systems. By fully understanding an organization's dependence on automation, it is expected that the ERM and CIE outcomes will best support the mission and critical functions.

NEXT STEPS

Potential answers and next steps include:

- YES, CERTAINLY – The organization DOES rely on automation to achieve its missions and/or critical functions. Go to Step B.2.
- NO, CERTAINLY – The organization DOES NOT rely on automation to achieve its missions and/or critical functions. Go to Step B.3.
- DON'T KNOW – The organization is uncertain if they are dependent or to what extent with which they are dependent. Go to Step B.4.

2.3. Step B.2 – Automation Engineering Analysis

Are the systems engineered with the capabilities to achieve its mission and/or critical functions for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation?

At this step, the organization assesses whether its engineered systems are designed to sustain their missions and critical functions for an extended period (weeks or more) without relying on automation. This includes situations where automation may be unreliable. Depending on factors such as the industry and historical engineering design decisions that have been made, this may not be practical. For example, a highly hazardous process environment may not be conducive to any operational scenario without automation. For engineered systems where this is possible, it could include current capabilities for safe and reliable operations under local, manual control or alternative methods.

NEXT STEPS

Potential answers and next steps include:

- YES – The organization's systems are engineered in a manner that allows for the mission and/or critical functions to be delivered for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation. Go to Step C.1
- NO – The organization's systems are not engineered in a manner that allows for the mission and/or critical functions to be delivered for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation. Go to Step B.3.

2.4. Step B.3 – Engineering Control Awareness

Does the organization have Engineered Controls for systems and assets that directly support critical functions?

The organization should evaluate the engineered controls currently in place to protect systems and assets that directly support critical functions. Engineered controls, as defined by CIE, are controls and processes used to eliminate or significantly reduce the consequences that a cyber attacker could achieve within the system. By evaluating whether engineered controls are present and protecting systems and assets that directly support critical functions aids the building of context and is a key input into understanding the types of consequences an organization may experience from an OT cyberattack.

NEXT STEPS

Potential answers and next steps include:

- YES – Engineered controls are in place for systems and assets that directly support critical functions. Go to Step C.2.
- NO or UNSURE – Engineered controls are either not in place for systems and assets that directly support critical functions, or the organization is unsure what is already in place. Achieving a high level of definition of engineered controls is an important input into understanding potential consequences. Go to Step C.3.

2.5. Step B.4 – Day Without Automation (DWoA) Exercise

To determine any uncertainties, assess the organization's current capabilities to operate in the absence of, or lack of reliable, automation by conducting an A Day without Automation Exercise and reassess.

When there is uncertainty about the organization's ability to operate without automation or without reliable automation, the next step is to evaluate the current capabilities by conducting workshops and exercises of varying complexity. This may include an exercise such as "A Day without Automation." This involves simulating a scenario where automation systems are unavailable or unreliable, allowing the organization to identify strengths in and potential improvements to the capability to operate without automation or reliable automation. By assessing how well the organization can maintain its mission and critical functions under these conditions, it can identify areas that require improvement and develop strategies to enhance resilience. This reassessment is crucial for ensuring that the organization is prepared to handle disruptions and maintain operational continuity.

NEXT STEPS

Return back to Step B.1 and reevaluate the organization's dependence upon digital automation (i.e., computers, programmable logic controllers, SCADA software) to achieve its mission and/or critical functions.

2.6. Step C.1 – Active Defense Analysis

Does the organization have the staff, staff training, and procedures in place to achieve the mission and/or critical functions for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation?

While the engineered systems may be designed to support operation in the absence of automation or lack of reliable automation, having the necessary staff, training, and procedures in place to sustain its missions and critical functions for an extended period (weeks or more) under these conditions is another story. This step focuses on the understanding, the readiness, and the capability of the organization's personnel to operate in the absence of automation.

NEXT STEPS

Potential answers and next steps include:

- YES – There are sufficient staff with the correct training and procedures to ensure the mission and/or critical functions can be achieved for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation. Go to Step B.3.
- NO – There are not sufficient staff with the correct training and procedures to ensure the mission and/or critical functions can be achieved for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation. Go to Step D.1.

2.7. Step C.2 – Consequence Analysis

In the case of an OT cyberattack, characterize the consequences to the organization according to the identified potential types of impacts. Are these consequences acceptable?

The organization should evaluate what types of consequences might be realized if an OT cyberattack occurs. By thoroughly assessing these consequences, the organization can determine if they are acceptable and/or which mitigation strategies are necessary and most appropriate.

NEXT STEPS

Building on the types of consequences described below in the Potential Impacts section,

- YES – The estimated consequences are acceptable to the organization. From an ERM perspective, they are within the risk tolerance of the organization. Go to Step E.1.
- NO or UNSURE – The estimated consequences are not acceptable to the organization. Based on the types of unacceptable consequences, determine how to reapply those Principles already addressed in this process and apply additional CIE Principles to address the specific types of consequences as noted in the CIE Principle Application section, below. Go to Step D.2.

2.8. Step C.3 – Engineered Controls Exercise

Evaluate and implement Engineered Controls to protect systems and assets that directly support critical functions.

At this step, for organizations that previously answered that they either do not have engineered controls in place, or they are unsure, it is necessary to perform an evaluation of engineered controls. Engineered Controls involve integrating engineering considerations and resilience strategies into the design and operation of systems from the outset. This proactive approach ensures that potential high-consequence scenarios are addressed early, enhancing the overall resilience and reliability of critical functions. By systematically assessing the current controls and identifying areas for improvement, the organization can develop and implement robust solutions that mitigate risks and safeguard essential operations. This step is vital for maintaining the integrity and continuity of the critical functions in the face of potential threats.

Some actions an organization may take are to review engineering documentation and identify engineered controls and the consequences that those controls mitigate.

NEXT STEPS

Return to Step B.2.

2.9. Step D.1 – Mission Assurance Planning

Develop staff training, education, and exercises as well as policies and procedures to enable the staff's ability to achieve the organization's mission and/or critical functions in the absence of automation.

This provides the organization with an opportunity to take action to improve operational capabilities. Actionable items associated with this step include creating targeted training sessions that equip staff with the necessary skills and knowledge to operate manually. Additionally, regular exercises and drills should be conducted to reinforce these skills and identify any gaps. Establishing clear policies and procedures will provide a structured framework for reliable operations in the absence of automation. These actions should be completed before conducting a reassessment.

NEXT STEPS

Go to Step B.4 and reevaluate the organization's ability to operate in the absence of automation or lack of reliable automation.

2.10. Step D.2 – Mitigation Analysis

According to Table 1 – CIE Principles by Impact, continue application of CIE Principles associated with the identified impacts.

Based on the impacts, apply CIE principles to identify potential improvements to reduce the consequences and thus risk to the mission and/or critical functions. The CIE principles associated with each type of consequence are discussed in the CIE Principle Application section, below. For example, the CIE Principle Engineered Controls directly addresses the identified operational impact by protecting assets from potential damage and/or ensuring assets continue operations in a normal or degraded state. This step ensures that the organization adopts a proactive and structured approach to mitigating consequences and risks, thereby strengthening resilience and reliability of operations.

NEXT STEPS

Return to Step B.1 to reevaluate risks to the mission and/or critical functions.

2.11. Step E.1 – Continuous Consequence Monitoring

The consequences of a successful cyberattack may be acceptable. Reassess periodically, as appropriate.

After determining the consequences of a potential OT cyberattack are acceptable, the organization must periodically reassess the potential consequences. This could be on the same schedule as the ERM monitoring and review schedule. In addition, if there are changes to the organization (e.g., people, process, or technologies) or threat environment (e.g., new threat actor capabilities) an additional review should be completed. This involves regularly reviewing and evaluating the identified impacts and the effectiveness of the implemented controls and strategies. Periodic reassessment allows for continuous

improvement and adaptation, ensuring that the measures in place continue to effectively support the organization's missions and critical functions.

NEXT STEPS

Return to Step B.1

3. Potential Impacts

Understanding the potential impacts of an OT cyberattack can be challenging due to the complexity of these systems and their interdependencies. As suggested by ERM best practices and the CIE Implementation Guide, it takes a team of professionals with diverse technical expertise to fully assess risks to an organization. As noted in Step C.2, above, the organization should assess the different types of consequences that could result from an OT cyberattack. These impacts provide context to allow for prioritization of CIE-driven improvements.

For the purposes of this document, potential types of impacts from an OT cyberattack that should be considered are presented below. These are neither entirely mutually exclusive from one another nor are they a comprehensive list of potential impacts. The order of the types of consequences is informed by engineering ethics established by the National Society of Professional Engineers.[5] This is the ethical code all licensed professional engineers in the United States are bound to. It begins with establishing that engineers shall "…Hold paramount the safety, health, and welfare of the public."

The following sections provide an introduction of each of the types of potential consequences an organization should consider. These impacts provide an initial framework for assessing and mitigating potential consequences. These are listed in the typical prioritization established by most engineering design criteria. Each organization or mission should validate these impacts and priority per utility, facility, and project.

3.1. Health and Safety Impacts

Health and safety impacts refer to the consequences arising from conditions or events that affect the well-being, physical health, and safety of individuals within a specific environment or context. The magnitudes of these potential impacts include measures and protocols designed to prevent accidents, injuries, illnesses, or other adverse health outcomes.

For each critical function, assess the potential for acute injuries, deaths, and chronic health impacts in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

3.2. Asset Damage or Loss

The impact of asset damage or loss encompasses the consequences arising from the destruction or deterioration of physical or digital assets owned or used by an organization. This impact may extend beyond the immediate loss of the asset itself, including the cascading effects on other assets or

[5] "Code of Ethics." Code of Ethics | National Society of Professional Engineers. Accessed September 26, 2024. https://www.nspe.org/resources/ethics/code-ethics.

functions that depend on it for operation or support. These cascading effects can amplify the overall impact, potentially leading to operational disruptions, increased costs, decreased productivity, or compromised safety.

For each critical function, assess the potential level of Asset Damage or Loss in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

3.3. Financial Losses

Financial losses encompass the consequences of a decrease in revenue, profit, or financial resources due to operational disruptions. This can occur due to various factors such as decreased sales or delivery of goods, increased expenses, response and recovery costs, or regulatory fines. Losses could result from the failure or lack of reliability of a system or infrastructure leading to disruptions to production processes, service delivery, or other critical functions that are dependent on the functioning of the system.

For each critical function, assess the potential level of Financial Impact in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

3.4. Environmental Impact

Environmental impacts may result from the failure of a system or infrastructure that results in environmental damage or degradation. This could include failures in industrial processes, waste management systems, or energy production facilities, that lead to environmental pollution, contamination, or ecological damage.

For each critical function, assess the potential level of Environmental Impact in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

3.5. Economic Impact

Economic impacts can result from disruption of the supply chain including the flow of goods, services, or resources to customers. Supply chain disruptions affect the procurement, production, distribution, or maintenance of the components, materials, or services of downstream or customer organizations. These can result in reductions in indirect (business to business transactions within the supply chain) or induced (spending by employees within the customers' supply chains) economic activity.[6]

For each critical function, assess the potential level of Economic Impact in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

[6] Demski, Joe. "Understanding Implan: Direct, Indirect, and Induced Effects." Understanding IMPLAN: Direct, Indirect, and Induced Effects. Accessed September 26, 2024. https://blog.implan.com/understanding-implan-effects.

3.6. Public/Customer Confidence Impact

Public and/or customer confidence impacts can be realized through degradation of the perception, image, and public opinion surrounding an organization's identity, values, products, services, and behavior. This includes the trust, credibility, loyalty, and goodwill that the organization has built with its customers, the communities it serves, and other stakeholders.

For each critical function, assess the potential level of Public/Customer Confidence Impact in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

3.7. Loss of Company Information

The impact of lost company information refers to the severity of unintentional or unauthorized disappearance, destruction, or compromise of data owned or managed by a company. This loss can occur due to various factors, including data breaches, cyberattacks, insider threats, hardware failure, software glitches, or natural disasters, and it can manifest in various ways, including financial losses, damage to reputation, legal liabilities, operational disruptions, regulatory penalties, and loss of competitive advantage.

For each critical function, assess the potential level of Loss of Company Information in the event of a worst-case OT cyber-attack on the organization. Refer to the example impact scale in Appendix B to evaluate the potential impact on the organization.

4. CIE Principle Application

The identified impacts from the previous step can be mitigated through the implementation of CIE principles. **Table 1** is an example matrix that allows the organization under evaluation to organize potential mitigations by the related CIE principles. To support the mitigation of cyber-risk, the questions in the CIE Implementation Guide may be used. For a minimal approach, the CIE Scoping Questions may be used by the organization.[7]

Once potential mitigations have been identified, the potential costs and benefits should be evaluated. Section 5 provides a formula to evaluate the Benefit-Cost Ratio.

[7] Lampe, Benjamin. On the Application of Cyber-Informed Engineering (CIE). 2024 IEEE Workshop on Security and Resiliency of Critical Infrastructure and Space Technologies (SR-CIST). 2024.

Table 1. CIE Mitigations by Principle

Identified Impacts	1 – Consequence-focused Design	2 – Engineered Controls	3 – Secure Information Architecture	4 – Design Simplification	5 – Layered Defense	6 – Active Defense	7 – Interdependency Evaluation	8 – Digital Asset Awareness	9 – Cyber-Secure Supply Chain Controls	10 – Planned Resilience	11 – Engineering Information Control	12 – Organizational Culture
Health and Safety Impact												
Asset Damage or Loss												
Financial Impact												
Environmental Impact												
Economic Impact												
Public/ Customer Confidence Impact												
Loss of Company Information												

5. Benefit Cost Analysis

The formula for the Benefit-Cost Ratio (BCR) is:

$$BCR = \frac{Present\ Value\ of\ Benefits}{Present\ Value\ of\ Costs}$$

A Benefit-Cost Ratio (BCR) greater than one indicates that a project should be implemented. This means that the present value of benefits exceeds the present value of costs, suggesting that the project is expected to generate a net positive value.

- **BCR > 1:** Benefits outweigh costs (project is viable).
- **BCR = 1:** Benefits equal costs (project breaks even).
- **BCR < 1:** Costs outweigh benefits (project is not viable).

6. Case Study

The water and wastewater utility described in Appendix C of the CIE Implementation Guide[8] has decided to integrate CIE into its regulatorily required ERM process. The utility must go through this process every five years, at a minimum. The fictional water and wastewater utility serves approximately 500,000 people and has numerous facilities including water treatment plants, a large central water pump station, and a wastewater treatment plant.

To integrate CIE within the ERM process, the utility went through the evaluation process described above. Previously, the utility had evaluated the risks to the SCADA systems. However, rather than start with previous risk assumptions, the utility followed the evaluation process from the beginning.

Step A.1 – Define the organization's mission critical functions and the systems that support those mission critical functions. For each mission and/or critical function of the organization, continue with the following approach.

The utility's critical functions include:

1. Providing drinking water at sufficient quality and quantity.
2. Collecting wastewater safely and discharging treated water to the environment.

The physical assets and digital assets support these functions with limited redundancy.

[8] Wright, Virginia L, et. al., 2023. "Cyber-Informed Engineering Implementation Guide." United States. https://www.osti.gov/servlets/purl/1995796.

These conditions were unchanged, but by following the process the utility was able to accomplish the following:

A. Integrate recent changes to the CIE evaluation process and recommendations.

B. No new utilities or critical functions have been adopted that would require expansion of the internal CIE process.

C. Confirm that no new significant regulations were in effect that would change prioritization or risk factors.

Step B.1 – Is the organization dependent upon digital automation (i.e., computers, programmable logic controllers, SCADA software) to achieve its mission and/or critical functions?

Yes, the utility is dependent upon multiple SCADA systems to deliver its critical functions.

Step B.2 – Are the systems engineered with the capabilities to achieve its mission and/or critical functions for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation?

Yes, the infrastructure is engineered with the capabilities to achieve its critical functions indefinitely.

Step C.1 – Does the organization have the staff, staff training, and procedures in place to achieve the mission and/or critical functions for an extended period of time (weeks or more) in the absence (or lack of reliability) of that automation?

Due to staff turnover, the utility is uncertain whether operations staff are currently capable to achieve the state critical functions in the absence of automation.

Step D.1 – Develop staff training, education, and exercises as well as policies and procedures to enable the staff's ability to achieve the organization's mission and/or critical functions in the absence of automation.

To ensure operations staff can operate the systems to achieve the utility's critical functions without automation, the utility took the following measures:

1. Reviewed and updated existing standard operating procedures (SOPs) based on how the systems are operated on a day-to-day basis. This included daily procedures to detect automation outage or disruption.
2. Developed SOPs on how to safely shut facilities down and start facilities back up.
3. Developed strategies on how to stabilize operations and respond to demand fluctuations without automation.
4. Conducted training exercises to help staff build the knowledge, skills, and abilities to operate individual processes, facilities, and the system without automation. These exercises are now regularly scheduled and include after-action reports to identify vulnerabilities and new responses or improvements. These are reviewed with the engineering team to update any applicable design standards, design details, or standard bills of material.

5. Developed quickly deployable backup communications capabilities with backup networking and communications devices to allow for backup monitoring at the most remote facilities.
6. As part of regular SOP reviews, staff job descriptions, staffing plans, and succession plans are also reviewed and updated.

Step B.4 – To determine any uncertainties, assess the organization's current capabilities to operate in the absence of, or lack of reliable, automation by conducting an A Day without Automation Exercise and reassess.

Culminating from the activities completed as part of Step D.1, the utility completed a functional exercise at the most critical facilities to ensure that staff could operate the systems in the absence of automation.

Following this the utility returned to Step B.1 and revisited and revised answers to arrive at Step B.3.

Step B.3 – Does the organization have Engineered Controls for systems and assets that directly support critical functions?

Utility staff generally agreed that engineered controls were present for many of the assets. However, documentation had not been maintained and institutional knowledge had been lost due to retirements and staff turnover. Therefore, immediately following this step a detailed review of engineered controls was completed as part of Step C.3.

Step C.3 – Evaluate and implement Engineered Controls to protect systems and assets that directly support critical functions.

Staff reviews of workshops revealed that several of the newer groundwater well pumps were installed without physical backspin timer relays that would prevent someone from accidentally or intentionally turning the down-well groundwater pumps on and off too quickly. If this were to happen, the pump could have the impellor sheered off the pump shaft. For the newer pumps, a software-backspin timer in the PLC program was substituted for the physical hardwired time delay relay. The risk is that an adversary could defeat the software control, leading to the retrofitting hardwired relays at the newer wells.

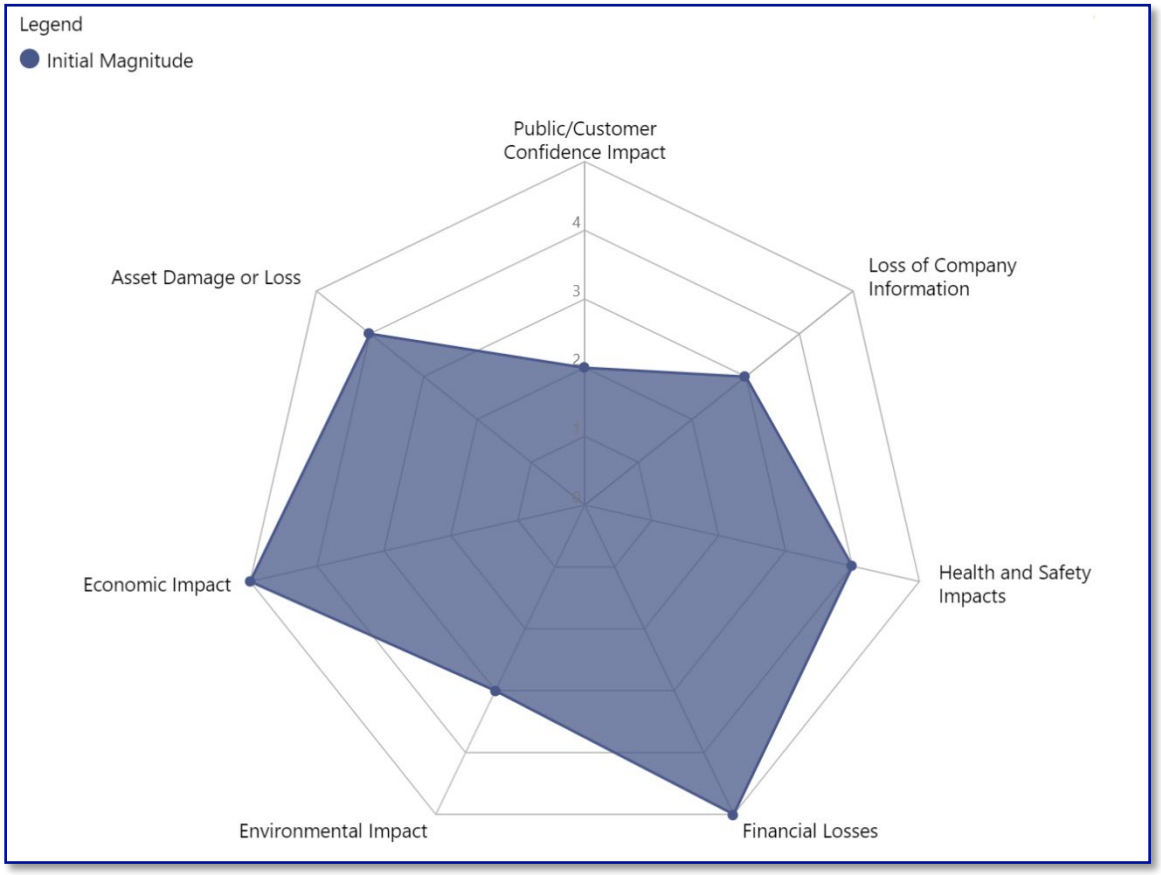
By addressing this step and implementing additional engineered controls, the utility returned to Step B.3, answered yes and moved on to Step C.2.

Step C.2 – In the case of an OT cyberattack, characterize the consequences to the organization according to the identified potential types of impacts. Are these consequences acceptable?

Staff completed a detailed evaluation of the potential impacts of an OT cyberattack. They chose to use the types of impacts described above which are consistent with industry-best ERM practices.

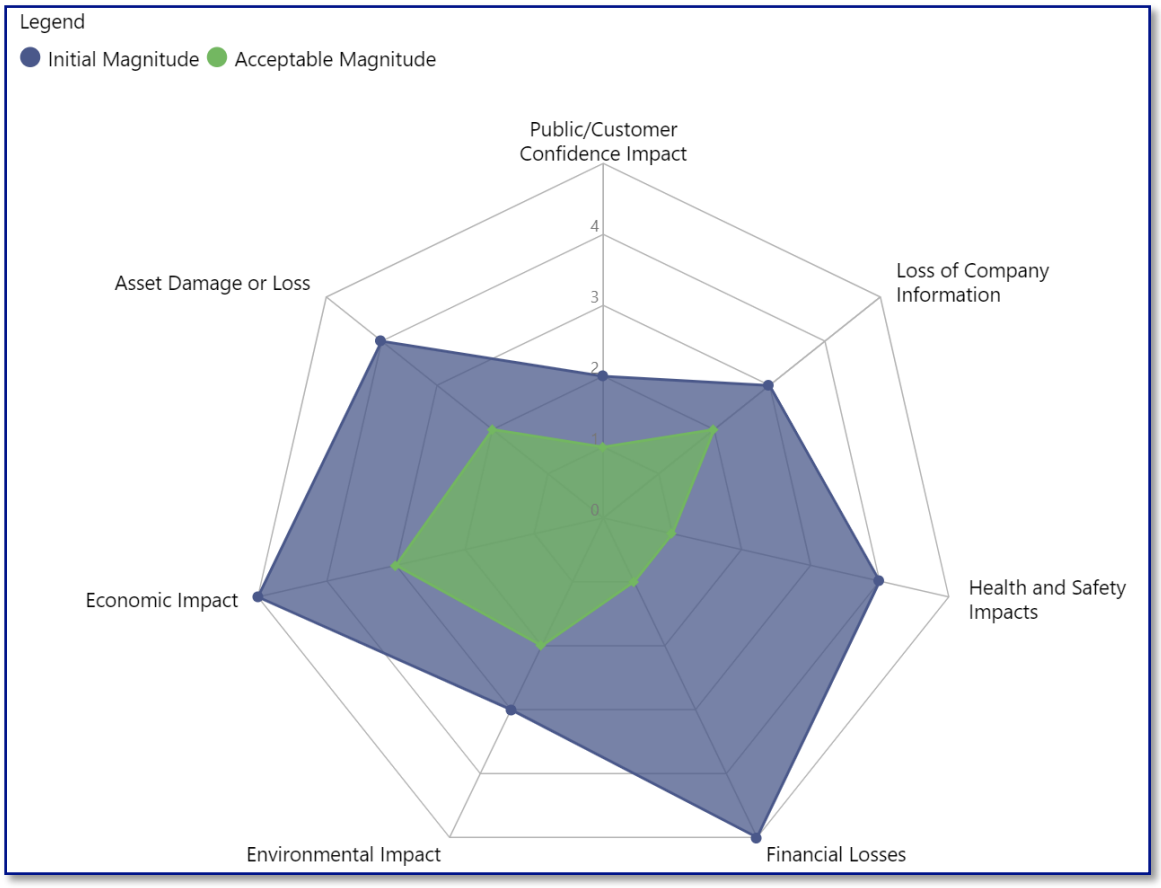
Figure 2 shows the initial magnitude for each impact category as estimated by the utility staff.

Figure 2. Initial Impact Magnitude by Impact Category



Upon estimating the impacts, utility staff determined the acceptable magnitudes of potential impacts. These are shown on Figure 3 along with the initial qualitative magnitudes previously determined.

Figure 3. Initial Magnitude and Acceptable Magnitude by Impact Category



Staff understood that they could not remove all potential impacts, and the organization would have some residual risk associated with a potential OT cyberattack. They determined that they could reduce the impact of an OT cyberattack sufficiently through applying CIE-driven mitigations. After determining the initial impact estimates and the acceptable potential impacts, staff determined their risk appetite.

Risk can be defined via various methodologies. A common formula for risk is risk equals consequences multiplied by threat likelihood. Given the current threat environment and the high certainty of a cyberattack, utility staff decided that consequences are equal to risk.

Table 2 summarizes select CIE mitigations identified, informed by the principles, to reduce OT cyberattack risk by impact type.

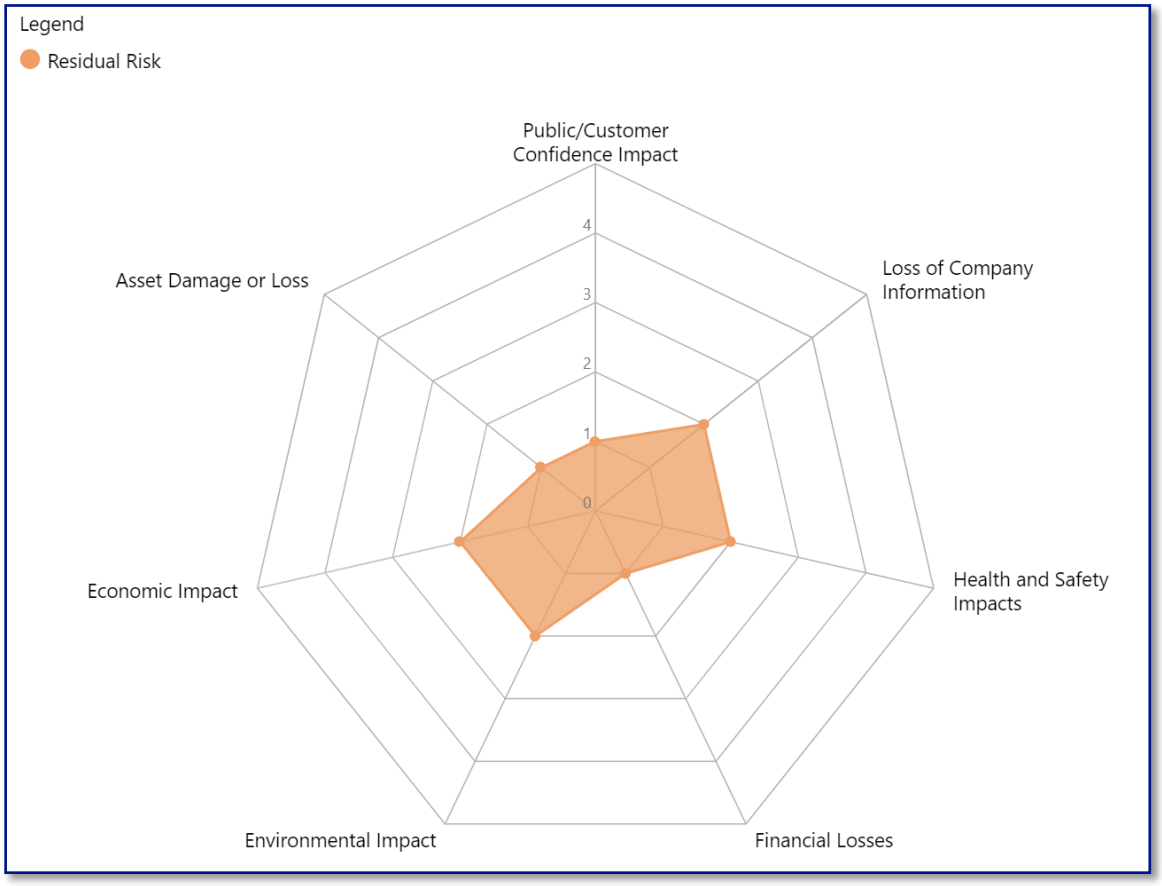
Table 2. Select CIE Mitigations Identified to Reduce OT Cyber Attack Risk

Identified Impacts	1 – Consequence-Focused Design	5 – Layered Defense	10 – Planned Resilience	12 – Organizational Culture
Health and Safety Impact	Deploy a hardwired relay for each chemical dosing system at groundwater well sites. This relay removes the ability to turn the chemical feed pump on/off through SCADA. This avoids giving attackers the ability to overdose/underdose chemicals in finished water.	N/A	N/A	N/A
Asset Damage or Loss	N/A	Lift Station pumps with unreliable level indicator transmitters (LITs) that require software-based control that can be compromised. Hardwired low level interlock from low level float. This helps to avoid running pumps dry or overrunning the pumps when the LITs are not reliable.	Maintain a reliable intertie with a neighboring system that provide operational redundancy.	N/A
Financial Impact	N/A	N/A	Create backups for the control system database and PLC programs. This improves incident response capabilities. Backups are completed periodically and kept offline. Staff test their ability to load programs new devices to confirm restoration capabilities.	N/A

Identified Impacts	1 – Consequence-Focused Design	5 – Layered Defense	10 – Planned Resilience	12 – Organizational Culture
Environmental Impact	N/A	N/A	N/A	N/A
Economic Impact	N/A	N/A	N/A	N/A
Public/ Customer Confidence Impact	N/A	N/A	N/A	Be prepared to communicate effectively with customers should an OT cyberattack occur. This would include pre-written statements and plans to issue those statements across different types of media (e.g. social media channels).
Loss of Company Information	N/A	N/A	N/A	N/A

It is estimated that with these improvements, the residual risks become acceptable to the utility. The estimated residual risks are shown in Figure 4.

Figure 4. Residual Risk by Impact Category

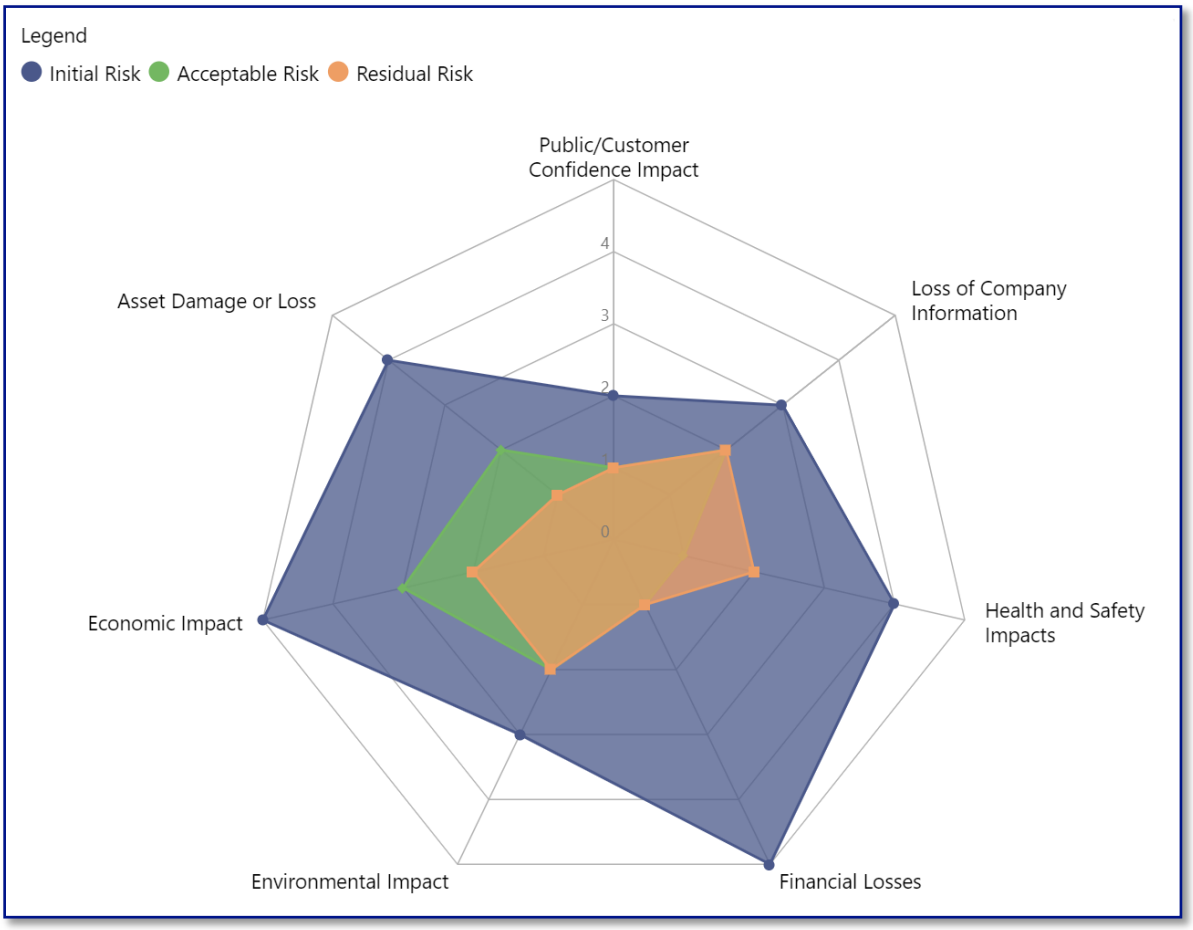


It is important to note that improvements to address engineered controls have already been addressed in prior steps. In addition, the staff have improved the operations team's capabilities and can now successfully be operated in the absence of automation. However, there are additional CIE-driven improvements that can be made.

6.1. Comparing Risk Estimates to Risk Appetite

Once risks and potential post-treatment risks are estimated, it is important to compare those to the risk appetite of the organization. Figure 5 illustrates the initial estimated risk and the risk appetite of the organization for each identified impact. CIE's methodology aligns with ERM principles by providing a structure to identify improvement projects to reduce risk across different the different types of impacts.

Figure 5. Initial Risk, Acceptable Risk, and Residual Risk by Impact



6.2. Case Study Conclusion

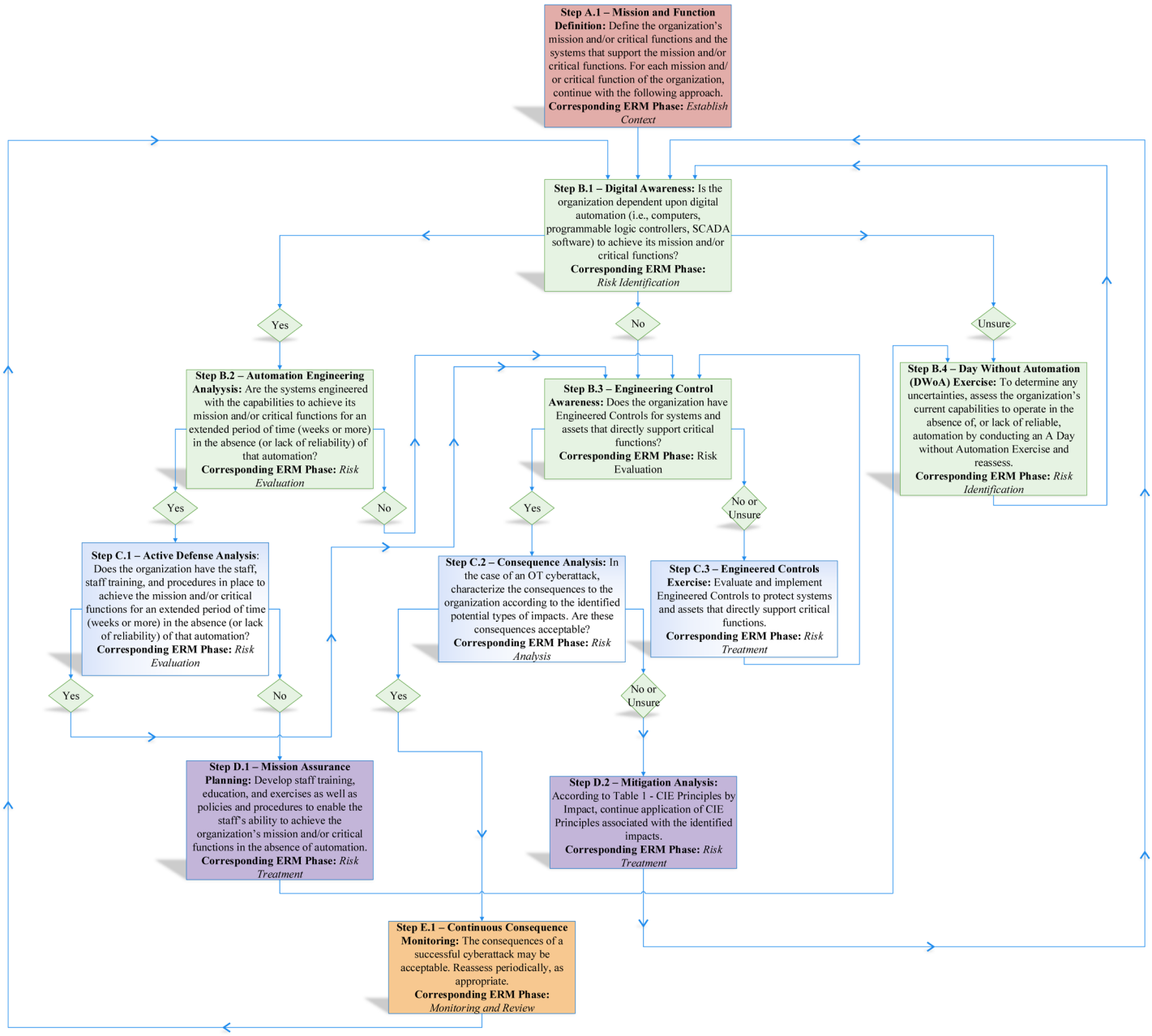
Based on the impact/risk reductions that are possible through the implementation of CIE mitigations, the utility decided to move forward with the projects. Staff recognize that making these improvements will take time and money. As noted in Step E.1, the staff will make improvements and iteratively review the potential impacts and risks as the system, people, and threat environment continue to evolve. Integrating CIE into the ERM process aims to create a holistic view of the risks the organization faces. CIE contributes to this by ensuring that cyber-risks are considered alongside other types of risks. This alignment helps organizations prioritize resources, improve decision-making, and enhance overall resilience.

7. Summary

ERM is critical to establish within organizations. While ERM helps to ensure the organization can address business risks and meet their established mission and deliver critical functions, incorporating CIE provides a new approach to addressing cyber-risk within an ERM process. This document provides organizations with a clearly defined process of evaluating the systems and capabilities, identifying the organization's needs, and providing the context to implement CIE where it provides the most benefit.

By following the evaluation process, organizations assess the qualitative magnitude for each impact category as well as the acceptable magnitudes of potential impacts. While an organization cannot eliminate all potential impacts, the organization can significantly reduce the impact of a successful OT cyberattack, or OT unreliability, through applying CIE-driven mitigations. Understanding both the initial impact estimates and the acceptable potential impacts leads an organization toward determining its risk appetite. With a well-defined risk appetite, the organization can better prioritize resources when applying CIE-driven mitigations and make more efficient decisions to enhance overall resilience.

Appendix A: Approach to Integrate CIE into Existing ERM Processes



Appendix B: Summary of Impacts

Table 3. Health and Safety Impacts.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
Health and safety measures are effectively implemented, resulting in minimal incidents or risks to individuals' well-being. Any issues that arise are quickly addressed and have little to no lasting consequences.	While health and safety measures are generally effective, there may be occasional incidents or minor risks that result in temporary disruptions or inconveniences. These incidents are manageable and do not pose a significant threat to individuals' health or safety.	Health and safety incidents occur periodically, leading to noticeable disruptions or risks to individuals' well-being. These incidents may result in injuries, illnesses, or property damage, requiring intervention to mitigate the impact and prevent future occurrences.	Health and safety incidents are frequent or severe, resulting in significant harm, injuries, or fatalities among individuals. These incidents disrupt operations, damage reputation, and may lead to legal liabilities or regulatory sanctions, necessitating urgent action to address underlying issues and improve safety protocols.	Health and safety incidents have catastrophic consequences, posing an existential threat to individuals' lives or well-being. This results in widespread harm, multiple fatalities, or long-term health consequences, with severe repercussions for the organization's reputation, financial standing, and legal liabilities. Urgent and comprehensive measures are needed to prevent further harm and rebuild trust with stakeholders.

Table 4. Asset Damage or Loss.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The asset damage or loss has minimal consequences on other assets or functions within the organization. Alternate resources or backup systems are readily available, and the disruption is quickly contained without significant repercussions.	The asset damage or loss leads to some disruptions or inefficiencies in other assets or functions that rely on it. While there may be some temporary setbacks or additional costs, the overall impact is manageable, and operations can resume relatively quickly with minimal lasting effects.	The asset damage or loss results in noticeable disruptions or challenges for other assets or functions that depend on it. This may require additional resources or temporary workarounds to maintain operations, leading to increased costs, decreased productivity, or delays in achieving organizational objectives.	The asset damage or loss causes significant disruptions or constraints for other assets or functions, amplifying the overall impact on the organization. This leads to prolonged downtime, increased expenses, or impaired ability to deliver products or services, resulting in tangible impacts on revenue, profitability, or stakeholder confidence.	The asset damage or loss has catastrophic consequences for the organization, triggering a domino effect that severely impairs its ability to function or survive. This leads to widespread disruptions, substantial financial losses, or irreversible damage to infrastructure, capabilities, or stakeholder relationships. Recovery efforts are complex and may require extensive resources, with long-term implications for the organization's viability and competitiveness.

Table 5. Financial Losses.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The financial loss is relatively small and does not significantly affect the organization's overall financial stability or ability to meet its financial obligations. The loss may be easily absorbed by the organization's financial reserves or mitigated through cost-saving measures without significant long-term consequences.	The financial loss leads to some reduction in profitability or financial resources, resulting in minor adjustments to operations or investments. While there may be some short-term challenges, the organization's financial position remains relatively stable, and recovery is feasible with moderate efforts.	The financial loss is significant enough to cause noticeable disruptions to the organization's operations, financial performance, or growth prospects. This may require substantial adjustments to budgets, strategies, or resource allocation to mitigate the impact and restore financial stability.	The financial loss has a severe impact on the organization's financial health, leading to substantial revenue declines, profit erosion, or liquidity constraints. This results in increased financial pressure, potential debt obligations, or stakeholder concerns, requiring urgent measures to address underlying issues and prevent further deterioration.	The financial loss has catastrophic consequences for the organization, posing an existential threat to its survival or long-term viability. This may result from insolvency, bankruptcy, or default on financial obligations, triggering legal proceedings, credit rating downgrades, or loss of investor confidence. Recovery efforts are complex and may involve restructuring, asset sales, or external interventions to stabilize the organization's financial position and prevent complete collapse.

Table 6. Environmental Impact.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The system failure results in minor environmental disturbances or localized pollution with limited consequences for ecosystems or human health. The incident is quickly contained and remediated without significant long-term effects.	The system failure causes some environmental damage or contamination, but the effects are manageable and confined to a specific area. Cleanup efforts are required, but the overall impact on ecosystems or human health is limited.	The system failure leads to moderate environmental degradation or pollution, affecting larger areas or populations. There may be disruptions to ecosystems, water sources, or air quality, requiring significant resources for cleanup and restoration.	The system failure results in significant environmental harm or pollution, with widespread effects on ecosystems, biodiversity, or public health. The incident attracts attention and concern from regulatory agencies, communities, and the media, necessitating urgent action to mitigate the damage and prevent further harm.	The system failure has catastrophic environmental consequences, causing extensive damage to ecosystems, natural resources, and human health. The incident poses a significant threat to public safety, economic stability, and environmental sustainability, requiring emergency response measures and long-term recovery efforts.

Table 7. Economic Impact.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The operations disruption causes minor disruptions to operations, with minimal consequences for productivity or service delivery. Alternate measures or backup systems are readily available, and the impact is quickly mitigated with little to no lasting effects.	The operations disruption leads to some disruptions in operations, resulting in minor delays or inconveniences for stakeholders. While there may be some temporary impact to customers, the overall impact on productivity or service quality is manageable, and operations can resume relatively quickly.	The operations disruption causes significant disruptions to operations, resulting in delays, downtime, or reduced efficiency. This leads to tangible impacts to customers, requiring concerted efforts to restore normalcy and address any resulting bottlenecks or backlogs.	The operations disruption has a severe impact on operations, causing prolonged downtime, widespread disruptions, or major setbacks in productivity and service delivery. This results in significant impacts to customers, requiring extensive resources and time to recover and rebuild trust with stakeholders.	The operations disruption leads to a complete breakdown of operations, posing an existential threat to the organization's viability. This results in catastrophic consequences to customers, such as bankruptcy, loss of market share, or irreparable damage to the organization's reputation and relationships with stakeholders. Recovery efforts are complex and challenging, with long-term implications for the organization's survival.

Table 8. Public/Customer Confidence Impact.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The organization's reputation and brand are strong, positive, and well-regarded by the public and customers, resulting in widespread trust, loyalty, and support. Any issues that arise have minimal impact on the organization's image or standing in the eyes of its stakeholders, and the organization quickly recovers with little to no lasting consequences.	While the organization's reputation and brand are generally positive, there may be occasional minor incidents or controversies that result in temporary setbacks or negative publicity. However, these issues are manageable and do not significantly erode stakeholder trust or confidence in the organization.	The organization experiences periodic challenges or controversies that have noticeable impacts on its reputation and brand. These incidents may result in negative media coverage, public scrutiny, or criticism from stakeholders, leading to reputational damage, loss of trust, or decreased consumer confidence.	The organization faces frequent or significant challenges that severely impact its reputation and brand. These incidents may involve scandals, crises, or ethical lapses that attract widespread negative attention, erode stakeholder trust, and damage the organization's credibility, resulting in financial losses, customer defections, or regulatory sanctions.	The organization experiences catastrophic consequences that pose an existential threat to its reputation and brand. This may result from severe crises, public scandals, or systemic failures that trigger widespread condemnation, boycotts, legal liabilities, or regulatory interventions, requiring urgent and comprehensive measures to rebuild trust, restore credibility, and salvage the organization's viability and competitive position.

Table 9. Loss of Company Information.

1	2	3	4	5
Insignificant	Minor	Moderate	Significant	Severe
The loss of company information has minimal consequences, with little to no financial losses or operational disruptions. The data may be of low importance or easily recoverable without significant effort or expense.	The loss of company information causes minor disruptions or inconveniences, with limited financial losses or reputational damage. While there may be some inconvenience or temporary setbacks, the overall impact is manageable and does not pose a significant threat to the company's viability.	The loss of company information results in noticeable financial losses, reputational damage, or operational disruptions. Recovery efforts are required, and there may be some lasting repercussions that affect the company's performance or competitive position.	The loss of company information leads to significant financial losses, reputational damage, or legal liabilities. Operational disruptions are severe, and the incident attracts negative attention from stakeholders, potentially eroding trust and confidence in the company.	The loss of company information has catastrophic consequences for the organization, potentially jeopardizing its survival. Financial losses are substantial, regulatory penalties may be severe, and the company's reputation may be irreparably damaged. Recovery efforts are complex and resource-intensive, with long-term implications for the company's viability and competitiveness.

Cyber-Informed Engineering

INL/MIS-24-81692-Rev000