INDUSTRIAL CYBER RISK MANAGEMENT

A GUIDELINE FOR OPERATIONAL TECHNOLOGY

AUTHOR

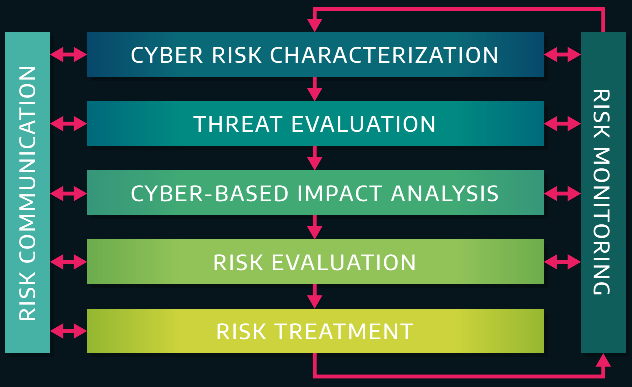
Jason D. Christopher

PRINCIPAL CYBER RISK ADVISOR
DRAGOS, INC.

MARCH, 2021

Executive Summary

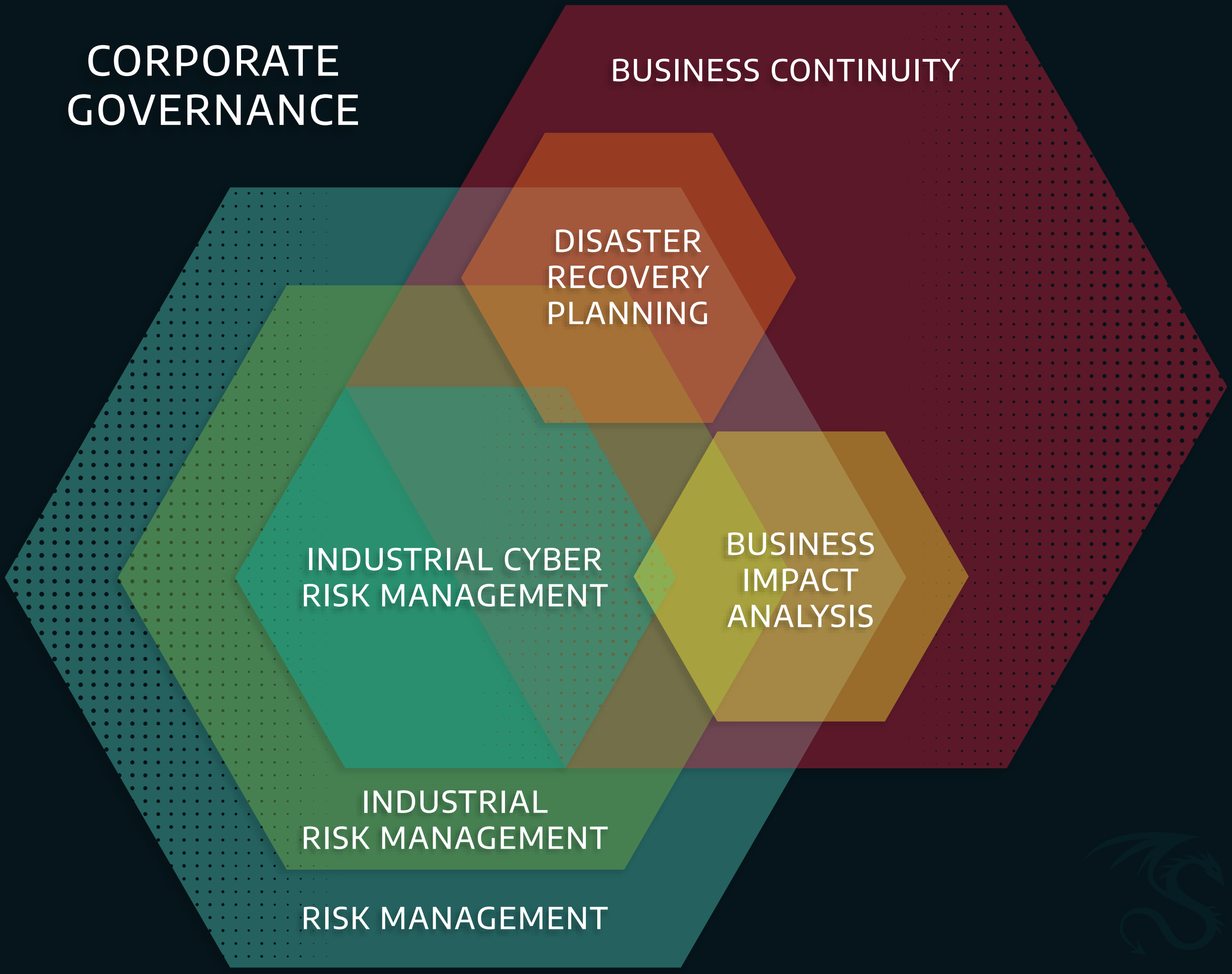
Critical infrastructure owners and operators have managed industrial risk for hundreds of years. This risk is usually measured in impact to health, safety, and reliability. As these industrial systems become increasingly digitized, so does the risk. What were once seen as isolated, manual processes have become reliant on communication networks and digital devices. As a result, a new category of industrial risk was created: industrial cyber risk.



The Dragos Industrial Cyber Risk Management Process

As with other areas of industrial risk, cyber risk requires specific processes tailored to operations and reliability. Unfortunately, due to the variety of stakeholders involved, ownership of cyber risk is rarely defined in most organizations, which causes increased confusion and lack of action.

This guidance document is based on a collection of standards, best practices, and applied knowledge from industrial system owners and operators in critical infrastructure. This industrial cyber risk management guideline is designed for scalability and can be adapted to any operational environment—from large multinational corporations to small municipal utilities. The methodology includes concepts, artifacts, and processes that can be added to any existing risk management program—regardless of overall maturity or resources.


CORPORATE GOVERNANCE
BUSINESS CONTINUITY
DISASTER RECOVERY PLANNING
INDUSTRIAL CYBER RISK MANAGEMENT
BUSINESS IMPACT ANALYSIS
INDUSTRIAL RISK MANAGEMENT
RISK MANAGEMENT

Dragos Industrial Cyber Risk Governance

Unlike traditional information-centric cyber risk programs, the Dragos risk management process leverages operational technology concepts and builds on safety and reliability artifacts, like Process Hazard Analysis (PHA) and engineering -controls that may be leveraged in treating industrial cyber risk. Industrial organizations already have readily available information regarding failure modes, safety implementation levels, and possible physical impacts due to equipment damage—all of which should be leveraged in a cyber risk program. All of which are part of the Dragos Industrial Cyber Risk Management process.

Many industrial organizations already manage certain risks. This guideline is designed to further refine existing processes to include a cybersecurity perspective for existing risks, such as safety and reliability. A cyber risk program should not “reinvent the wheel” or create undue overhead. By leveraging strengths across engineering, IT, OT security, finance, compliance, and other risk departments, industrial organizations can go beyond understanding cyber risk—they will finally feel confident that they can effectively manage it.

INDUSTRIAL CYBER RISK "QUICK CHECK"

The Dragos industrial cyber risk management process is designed to be flexible and can easily be added to any existing risk program.

While this document provides detailed examples and guidance, some organizations need a "quick check" for easier use. The following table provides an easy maturity model (crawl, walk, run) for the process used throughout this guideline.[i]

	PRACTICE	CRAWL	WALK	RUN
1	The organization has an inventory of industrial assets and systems.	X		
2	The inventory includes criticality of the system, associated Process Hazard Analysis (or other safety and engineering analysis), business impact analysis, and other important characteristics. (See Cyber Risk Characterization)		X	
3	OT-specific threat information is gathered within the organization.	X		
4	Relevant threats for the organization are monitored.	X		
5	Cyber threat profiles are established. (See Threat Evaluation)		X	
6	OT-specific vulnerability information is gathered within the organization.	X		
7	The organization has defined impact criteria for risk management. (See Cyber-Based Impact Analysis)			X
8	An OT-specific cybersecurity architecture is established.		X	
9	Industrial cyber risks evaluations, both qualitative and quantitative, are performed and leverage IT and OT architecture. (See Risk Evaluation).		X	
10	Industrial cyber risks are treated. (See Risk Treatment)	X		
11	Industrial cyber risks are tracked with a risk register. (See Risk Monitoring)			X
12	A common language, or risk taxonomy, is used when discussing organization-wide risks, including industrial cyber risk. (See Risk Communication).			X
13	Stakeholders for industrial cyber risk, including OT, IT, legal, safety, and human resources, are involved in the risk management process.		X	
14	Responsibility and authority for the performance of industrial cyber risk management activities are assigned to personnel.			X
15	Personnel performing industrial cyber risk management activities are trained and they have the necessary skills and knowledge required for each task.			X

[i] Maturity Indicator Levels (MILs) in terms of "crawl, walk, run" are based on the US Department of Energy's Cybersecurity Capability Maturity Model (C2M2), specifically designed for industrial control system considerations: https://www.energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

Contents

Risky Business: Industrial Cyber

"Cyber risk" is a difficult term used within industrial security.

For engineers, the concept of cyber risk invokes the idea of endless assessments in operational environments. Meanwhile, IT security professionals lack tools and processes to effectively measure cyber risk for industrial control systems. And, despite these challenges, executives—who may interpret everything in terms of business risk—want to see repeatable methods to communicate the state of cybersecurity internally. These different stakeholders, with their unique perspectives of "cyber" and "risk," need to somehow communicate, coordinate, and manage a complicated set of issues to ensure reliable operation for critical infrastructure. And it is not getting easier.

Enter the Dragos *Industrial Cyber Risk Management* process.

This guidance document is based on a collection of standards, best practices, and applied knowledge from real industrial system owners and operators. The Dragos Industrial Cyber Risk Management guidance was designed for scalability and can be adapted to any environment—from large multinational corporations to small municipal utilities, regardless of the sector or operations. The methodology includes concepts, artifacts, and processes that can be added to any existing risk management program—regardless of overall maturity or resources.

This guideline includes a lightweight process that will complement any existing program. Even if "risk management" is a foreign concept, the guideline builds on something industrial organizations know all too well: disaster recovery and business continuity. Leveraging a practical approach to evaluating, treating, and consistently communicating cyber risk, organizations will be able to build sustainable security programs based on threats and impacts.

DEFINING INDUSTRIAL CYBER RISK

With the variety of stakeholders involved in managing cybersecurity, it is critical to use common definitions when describing risk. Unfortunately, "cyber risk" has historically been defined as an information-centric concept, where the primary concern centers on data breaches. While industrial organizations certainly need to understand information cyber risk, it is even more critical to define operational technology specific, or industrial, cyber risk.

According to the National Institute of Standards and Technology, "cyber" is defined as "refer[ing] to both information and communication networks."[1] For critical infrastructure and industrial organizations, however, a more appropriate definition would be:

CYBER

CY·BER / ˈSĪBƏR/

REFERRING TO DIGITAL TECHNOLOGIES AND COMMUNICATION NETWORKS USED FOR INFORMATIONAL AND/OR OPERATIONAL CAPABILITIES

Similarly, "risk" is defined as "the level of impact on organizational operations, assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring."[2] This again is, unfortunately, information-centric.

Since operational technology (OT) translates digital commands into real-world, physical impacts, it makes more sense for the risks discussed in industrial organizations to be linked to those impacts. Fortunately, owners and operators of OT systems are well-versed in disaster recovery and business continuity, which are uniquely tied to physical impacts. Industrial organizations may already leverage process hazard analysis, safety evaluations, and other business impact tools to evaluate "disaster risk." These same tools can be used to discuss the impacts of cyber risk across industrial control systems.

Disaster risk benefits from decades of study and multiple models, with significantly more structure than cyber risk. The United Nations Office for Disaster Risk Reduction defines disaster risk as "the potential loss of life, injury, destroyed or damaged assets which could occur to a system, society or a community in a specific period of time, determined probabilistically as a function of hazard, exposure, vulnerability and capacity."[3]

Recognizing the complexity of industrial organizations, this guideline combines IT and OT cyber risk with specific concepts in disaster recovery. The subsequent definition of cyber risk must align with other forms of business risk within industrial organizations, such as legal, financial, and reliability risks. Therefore, throughout this guidance document, cyber risk is defined as:

INDUSTRIAL CYBER RISK

IN·DUS·TRI·AL CY·BER RISK / INˈDƏSTRĒƏL ˈSĪBƏR RISK/

THE POTENTIAL LOSS OF LIFE, INJURY, DAMAGED ASSETS, FINANCIAL LOSS, AND OTHER HARM FROM THE FAILURE OR MIS-OPERATION OF DIGITAL TECHNOLOGIES AND COMMUNICATION NETWORKS USED FOR OPERATIONAL CAPABILITIES.

Industrial organizations and critical infrastructure operators must manage risks with significant potential impacts. Before addressing how to manage cyber risks, it is vital that leaders define what is a cyber risk. These definitions require understanding cyber risk from an operational, business impact, legal, financial, and security perspective—no one stakeholder group can define and manage cyber risk in a silo.

WHO OWNS THE RISK?

If a company's employee records are kept on paper, who is responsible for locking them in a cabinet every night? Is it the HR department or the security department? Is the security guard expected to walk through the office and put away any sensitive document found during the walk-through? Of course not. The HR department, ultimately, owns the risk of documents being stolen. It is their responsibility to secure those documents.

This risk does not change just because the documents may be electronic. In both cases, the HR department needs training, tools, and support to secure the document properly. However, they are neither inventing those tools nor are they relying on someone else to lock up the documents.

This example is similar for industrial control systems. The safety, security, and reliability of OT systems has always been the responsibility of engineers and operators. Now that these systems have undergone digitalization, that does not mean the cyber risk magically shifts elsewhere. Those OT teams will need training, tools, and support—but risk ownership is still the same.

Industrial Cyber Risk Elements

As discussed in the Dragos approach to consequence-driven ICS security scoping, the traditional information security risk equation does not account for the functional, real-world physical outputs of industrial processes.[4] For reference, we state that a more OT-centric risk equation should be:

$$\textit{Cyber Risk} = \textit{Consequence} \times \textit{Threat} \times \textit{Vulnerability}$$

By focusing on a more consequence-driven approach, cyber risk and its associated impacts can benefit from engineering and reliability inputs, such as PHA (process hazard analysis) and FMEA (failure mode and effects analysis). These evaluations, which may exist already in industrial organizations, provide detailed information on conditions that may result in unreliable, unsafe, and possibly destructive states for control systems—something that does not exist in IT-centric cyber risk models.

Because of the link to physical impacts and reliability, industrial cyber risk should include additional concepts from disaster recovery and business continuity. Disaster risk has an extremely similar equation to cyber risk:

$$\textit{Disaster Risk} = \textit{Hazard} \times \textit{Exposure} \times \textit{Vulnerability}$$

Where,

A "hazard" is the adverse event causing the loss,

An "exposure" is the property, people, plant, or environment that are threatened by the event, and

A "vulnerability" is how the exposure at risk is vulnerable to an adverse event of that kind.

However, within disaster risk, there is also a concept for "capacity to cope" or manageability during a disaster. This fourth element defines the ability of a system to respond after the event to mitigate the loss.[5] This then redefines the disaster risk equation as:

$$\textit{Disaster Risk} = \textit{Hazard} \times \textit{Exposure} \times \frac{\textit{Vulnerability}}{\textit{Capacity}}$$

The Dragos Industrial Cyber Risk Management process combines best practices across both consequence-driven ICS security principles and business recovery concepts. Within OT security, it is important to understand the various impacts that may occur from a cybersecurity incident (physical damage, health and human safety, financial losses, reputation, etc.) which may already be assessed as part of hazard analysis, property insurance studies, and other data-rich conversations around the engineering processes. The analysis of "consequence" is, in fact, more aligned to disaster risk than traditional information-centric cybersecurity models. On the other side of that same coin, however, cyber threats are uniquely positioned to compromise "exposed" assets. As such, the industrial cyber risk equation must ingest threat information to examine the activity groups for specific consequences. [ii]

The last element of the industrial cyber risk equation borrows heavily from the disaster recovery concepts surrounding "capacity." Vulnerabilities, in the traditional cybersecurity sense, are ubiquitous in industrial environments from a digital perspective. However, there are many methods available to OT security professionals to leverage manual recovery or strengthen mitigations and perimeters to prevent vulnerabilities from being exploitable. These capabilities decrease the overall severity associated with a specific vulnerability through mitigation and recovery techniques. Since this must combine both engineering and network security, the industrial cyber risk equation is a mix of both the classic IT-centric cyber risk equation, augmented with business continuity concepts:

$$\textit{Industrial Cyber Risk} = \textit{Consequence} \times \frac{(\textit{Threat} \times \textit{Vulnerability})}{\textit{Resilience}}$$

Leveraging this new equation, industrial organizations must consider building risk management programs that establish the following key concepts:

- Establish clear communications—and roles and responsibilities—for cyber risk across IT and OT capabilities, including how cyber risk and disaster risk are related.
- Create a repeatable process to evaluate impacts, leveraging business continuity and/or safety impact analysis where possible.
- Use common terminology across each business unit to describe risk.
- Evaluate relevant threats, particularly noting capabilities that may impact industrial processes, which can be tied to consequence-driven analysis.
- Maintain consistent methods to evaluate cyber risks.
- Leverage the expertise across engineering, IT, and OT teams to establish "risk ownership" and criteria for successful evaluation.
- Treat evaluated cyber risks using every method available to industrial organizations, including technical and procedural controls, monitoring, and insurance.
- Understand that OT systems will always have an element of residual risk that will never be eliminated but can be managed with engineering and financial controls.

A traditional IT-only cyber risk program will not satisfy the discussions required to establish an OT cyber risk management program. Protecting industrial processes requires a multidisciplinary approach, rooted in engineering and based on physical-world impacts. IT plays a critical role in protecting the enterprise, but the operational technology requires its own consideration of cyber risk based on unique threats, consequences, vulnerabilities—and their capacity for resilient operations.

[ii] To learn more about Threat Activity Groups, visit https://www.dragos.com/threat-activity-groups/

This guidance document is built on unifying different disciplines to create a cohesive cyber risk management program for industrial organizations. Leveraging the key concepts above, this guideline can be adapted to any risk management program (including a traditional cybersecurity or disaster recovery program) to provide clear communication, monitoring, and treatment of OT cyber risk.

Dragos Industrial Cyber Risk Management

Risk management has existed throughout human history. Risk, being potential harm or danger, is constantly being "managed" in one way or another.

Risk management, as a discipline, is a critical part of our daily lives, though most of us may not recognize it. There are risks associated with mundane tasks, like driving a car or making an online purchase, that humans automatically "solve" in a matter of seconds. These risks are either accepted, mitigated, or ignored near real-time.

As a business practice, risk management predates cybersecurity by hundreds of years. Risks have been associated with every aspect of corporations, municipalities, cooperatives, and nonprofits. These risks are often managed in varying levels of maturity based on corporate governance and processes. Other business risks include financial risk, reputation risk, environmental risk, competition risk, safety risk, and operational risk. Leaders that understand these risks will follow a consistent process to evaluate and communicate risks across the organization.

The same is true of industrial cyber risk. Organizations that invest in cyber risk management will have a similar governance structure as financial risk or safety risk. As a matter of fact, any generic risk management process can be adapted to include industrial cyber risk, as outlined in Appendix: Risk Management Approaches.

As risk management is a significantly more mature business practice, it would make sense for cyber risk practitioners to leverage existing standards and bodies of knowledge where applicable. Industrial cyber risk should augment existing risk discussions based on data and robust communication.

The Dragos Industrial Cyber Risk Management process is designed to:

- Fit any existing risk management process;
  - If a risk management process does not exist, this guideline can be used to build one from scratch;
- Leverage international risk management (and cybersecurity) standards;
- Approach cyber risk management with discrete processes;
  - Organizations can adopt the entire Dragos Industrial Cyber Risk Management workflow or specific parts, depending on their unique capabilities or maturity.

The DRAGOS Industrial Cyber Risk Management Process

RISK MANAGEMENT PROCESSES ARE UNIVERSAL, AS DEMONSTRATED BY THE SIMILARITY BETWEEN INDUSTRY STANDARDS.

Where implementations deviate is on industry-specific concerns. Our recommended process builds on the concepts from these standards and specifically focuses on operations, business continuity, resilience, and security. These disciplines, collectively, manage industrial cyber risk.

The Dragos approach is modular and may be tailored for any organization, regardless of industry or size. Specific implementations may vary, but a general process is outlined here in Figure 1.

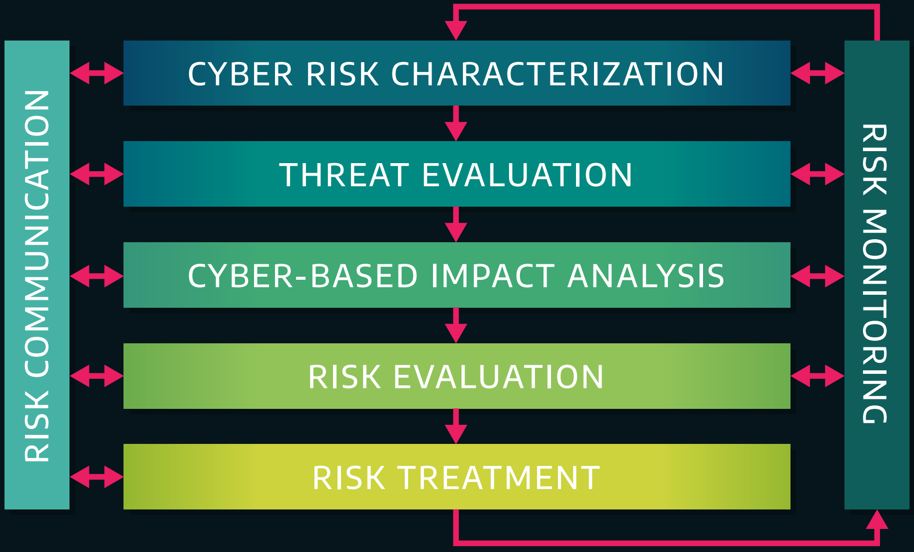


Figure 1. The Dragos Industrial Cyber Risk Management Process

This guideline is not intended to reinvent the wheel for risk management. It is designed to supplement existing risk management processes with expertise required to manage cyber risks specific to operational technology. Organizations that already have a risk management process in place will find the Dragos workflow complimentary to those efforts, while also supporting asset owners and operators that may need additional maturity in developing risk management capabilities.

THE FOLLOWING SECTIONS WILL ADDRESS EACH MODULE OF THE DRAGOS INDUSTRIAL CYBER RISK MANAGEMENT PROCESS.

STEP 01 | CYBER RISK CHARACTERIZATION

Characterizing cyber risk for critical infrastructure and other industrial organizations requires building a blend of OT security, process engineering, and business continuity knowledge. Since each business unit needs to be involved in the risk management process, each manager for those business units needs to define assets with an evaluation of what existing security controls already exist to protect those assets and systems. For each business unit, there is:

- List of critical assets and systems
- Associated internal and external dependencies and infrastructure
- Associated cybersecurity architecture or list of security controls
- Associated business impact analysis or disaster recovery plans
- Associated Process Hazard Analysis (PHA) and/or any safety-related analysis
- Identification of stakeholders for the assets and systems
    - Including roles and responsibilities (both internal and external)
- Owner of cyber risk for the assets and systems
    - Escalation paths for unmitigated and/or accepted risks

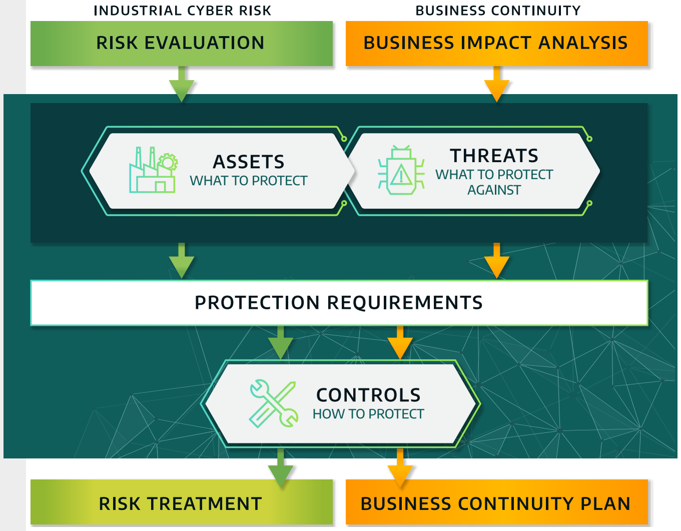


Figure 2. Risk Management and Business Continuity Management Functional Elements[iii]

[iii] The European Union Agency for Cybersecurity (ENISA) discusses business continuity and risk management interfaces as an overall approach to resilience, as found here: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces

Business continuity approaches serve as a valuable input for risk analysis, especially for critical infrastructure asset owners and operators, where uninterrupted processes have national importance. The Dragos Industrial Cyber Risk Management process applies business continuity where applicable in framing risk activities, noting the different objectives for risk management and business continuity management.

By characterizing the risks with information across operations, security, and business continuity, the Dragos process ensures resources and communications are aligned internally. This is further exemplified below in Table 1.[iv]

	RISK MANAGEMENT	BUSINESS CONTINUITY
KEY METHOD	Risk Analysis	Business Impact Analysis
KEY PARAMETERS	Consequence, Threats, and Vulnerabilities	Availability and Consequence
TYPE OF INCIDENT	“All” types of events	Events causing significant business interruption
SIZE OF EVENTS	“All” events affecting the organization	Events threatening availability of the organization’s core processes
SCOPE	Focus primarily on management of risks to business objectives in order to prevent or reduce incidents	Focus primarily on incident management and recovery of critical business processes following an incident
SEVERITY	“All”	Sudden or rapid events

Table 1. Comparison of Risk Management and Business Continuity Management

> “ RISK MANAGEMENT, AS A DISCIPLINE, IS A CRITICAL PART OF OUR DAILY LIVES, THOUGH MOST OF US MAY NOT RECOGNIZE IT. THERE ARE RISKS ASSOCIATED WITH MUNDANE TASKS, LIKE DRIVING A CAR OR MAKING AN ONLINE PURCHASE, THAT HUMANS AUTOMATICALLY “SOLVE” IN A MATTER OF SECONDS. THESE RISKS ARE EITHER ACCEPTED, MITIGATED, OR IGNORED NEAR REAL-TIME.

[iv] Ibid. The ENISA document further walks through how business continuity and cybersecurity can complement one another, specifically in identifying more severe or potentially catastrophic cyber risks, like those seen in industrial sectors.

STEP 02 | THREAT EVALUATION

Once the assets and systems are characterized, asset owners and operators need to evaluate the threats that may impact those systems. A common approach to this is to have a tailored cybersecurity threat profile based on threats specific to the organization, operating region, industry, and other unique demographics that may impact critical infrastructure, such as vendor-specific threats.

Threat evaluations and threat profiles are valuable in harmonizing communications around external and internal threats that may initiate a cyber attack. For OT-specific threats, Dragos recommends leveraging the ICS Cyber Kill Chain[6] and MITRE ATT&CK for ICS Framework[7] for consistent language.

Table 2, below, is an example of a threat profile, but the concept can be applied for non-OT threats or Dragos Threat Activity Groups, including hacktivists and malicious insiders.[v]

XENOTIME

ID: D.AG.XT

Description: Dragos considers this the most dangerous cyber threat to ICS, active since at least 2014. The group is known for its disruptive attack behavior and the ability to build and execute ICS-specific malware to disrupt processes within the operations environment. This group was observed targeting several original equipment manufacturers and vendors and is considered a supply chain threat.

Relationship: External

Target Geography: North America, Europe, APAC, Middle East

Links: TEMP.Veles

Victimology: Oil and Gas, Petrochemical, Electric

ICS Capability: XENOTIME is capable of infiltrating and disrupting ICS and operations. XENOTIME created and deployed the TRISIS malware, which targeted Schneider Electric Triconex safety instrumented systems. Dragos has observed XENOTIME targeting safety systems beyond this product line.

Behavior: XENOTIME leverages IT compromise and credential theft for Valid Accounts [T859] to enable remote access to the ICS network via External Remote Services [T822]. The group developed custom tools and ICS-tailored malware called TRISIS [S0013] specifically targeting safety equipment and was able to inhibit the equipment's response function via Device Shutdown [T816]. Its activities have resulted in a Loss of Safety [T880] and Loss of Productivity and Revenue [T828]. The group has conducted Supply Chain Compromise [T862] via OEM and vendor targeting.

Additionally, XENOTIME inhibited response function via Modifying Control Logic [T833], System Firmware [T857], and Utilize/Change Operating Mode [T858]. XENOTIME impaired processes via Change Program State [T875] via the TriStation protocol, Masquerading [T849] as the Triconex software, Program Download [T843] on the SIS, and Change Operating Mode [T858] on the controller. TRISIS was able to cause a Loss of Safety [T880].

Capabilities: The group developed ICS-targeting malware, TRISIS [S0013] which shutdown safety system operations. XENOTIME uses Mimikatz [T1003] for credential harvesting and custom-developed tools with similar functionality.

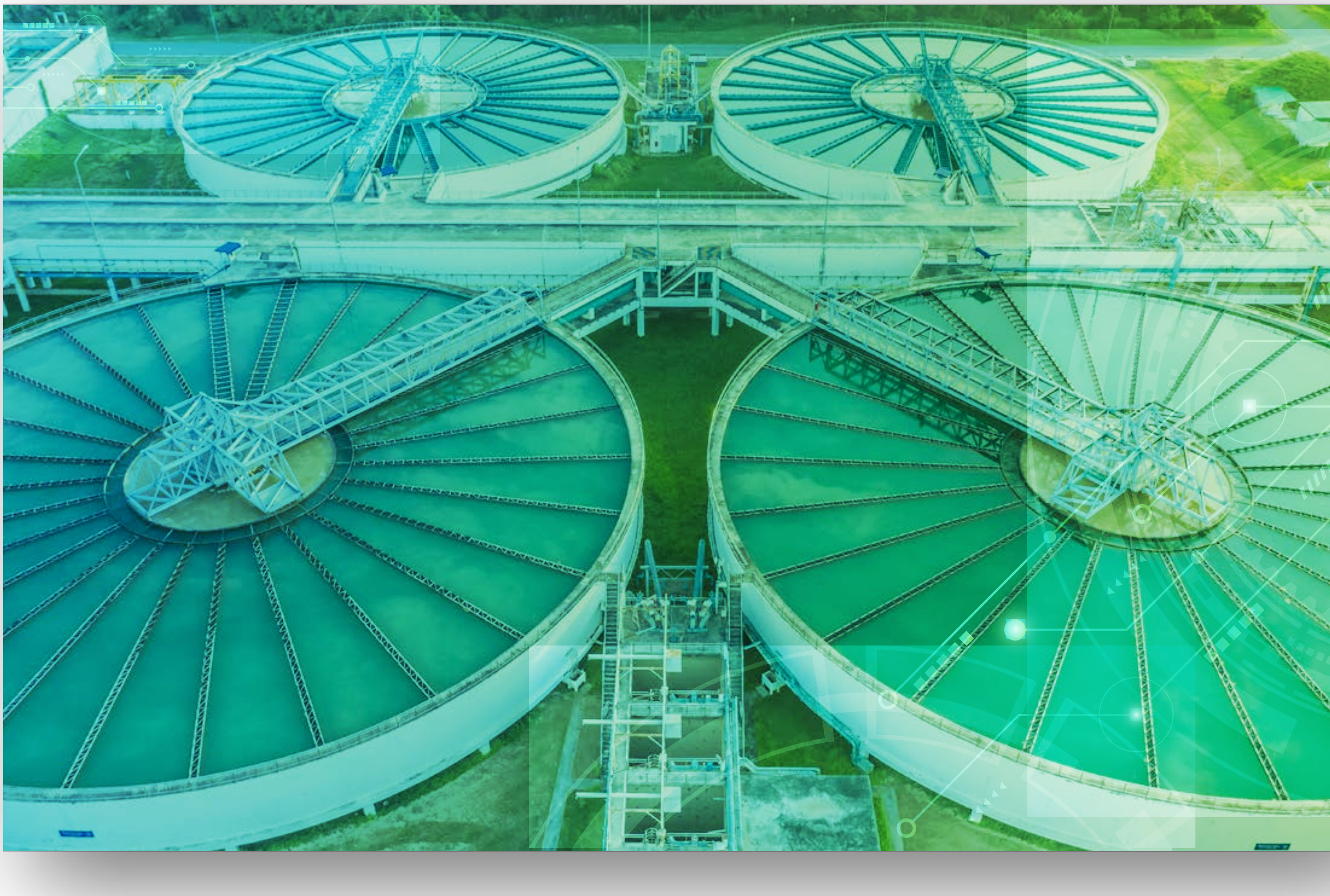
Infrastructure: XENOTIME leverages virtual private server and compromised, legitimate network infrastructure.

Targeted Industrial Assets: Triconex Safety Instrumented Systems (SIS)

Major Incidents: 2017 TRISIS attack on oil and gas entity in Saudi Arabia

Table 2. Example Threat Profile for XENOTIME, a Dragos Activity Group Focused on Industrial Cyber Attacks

[v] Threat profiles can provide easy access and communications around threats, particularly for risk monitoring activities, which will be highlighted throughout the this document. SANS provides an in-depth discussion about threat profiles here: https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492



Each asset and system type will likely map to specific threats, since a threat evaluation is not limited in scope. For example, a threat profile could specifically call out an activity group or a broader concern with insider threats. Regardless of how the threat evaluation is scoped, it is vital that the output be tied back to specific assets, systems, or industrial process. Doing so links the threat to an eventual impact, as covered in the next risk management step.

THREAT TREE	DEFINITION
HUMAN ACTORS USING TECHNICAL MEANS	The threats in this category represent threats to the asset via the organization's technical infrastructure or by direct access to a container that hosts the asset. They require direct action by a person and can be deliberate or accidental in nature.
HUMAN ACTORS USING PHYSICAL ACCESS	The threats in this category represent threats to the asset that results from physical access to the asset or a container that hosts the asset. They require direct action by a person and can be deliberate or accidental in nature.
TECHNICAL PROBLEMS	The threats in this category are problems with an organization's technology and communication systems. Examples include hardware defects, software defects, malicious code, and other system-related problems.
OTHER PROBLEMS	The threats in this category are problems or situations that are outside the controls of an organization. This category of threats includes natural disasters and interdependency risks.

Table 3. Threat Trees used in OCTAVE, which could be used in non-Activity Group threat evaluations.[8]

STEP 03 | CYBER-BASED IMPACT ANALYSIS

Once critical systems have been outlined, along with the potential threats to those systems, asset owners and operators need to consider the impact associated with the loss of those systems.

This initial step is first ignoring any potential security protection in place and examining any previous Crown Jewel Analysis performed. This helps establish an unmitigated severity of consequences, or potential impact, to further inform the criticality of the risk.

IMPACT CRITERIA

Each organization needs to leverage objective impact criteria to aid risk evaluation. Based on business impact, the criteria can then be used to measure how severe specific risks are to the organization. These criteria can help level-set engineers, management, risk leaders, and executives on industrial cyber risks by uniformly mapping impacts. The Dragos process establishes impact criteria from industry standards, like ISA/IEC 62443-2-1[9] and NIST SP 800-82,[10] while providing the flexibility for industrial organizations to categorize impacts based on their unique operations.

For OT systems, these impacts will be far more severe than traditional IT-only cybersecurity incidents. While there are some truly catastrophic impacts from IT systems, potential impacts to the environment, property, and health and human safety are significantly higher for most asset owners and operators.

Along those lines, much of this information already exists or can be attained through discussion with engineers, internal compliance teams, legal counsel, and insurance managers.

Each of these stakeholder groups has most likely calculated the value of these impacts and the associated thresholds, which should also be briefed to executives. The Dragos risk management process requires these diverse stakeholder groups to collaborate on establishing and using the impact criteria on at least an annual basis.

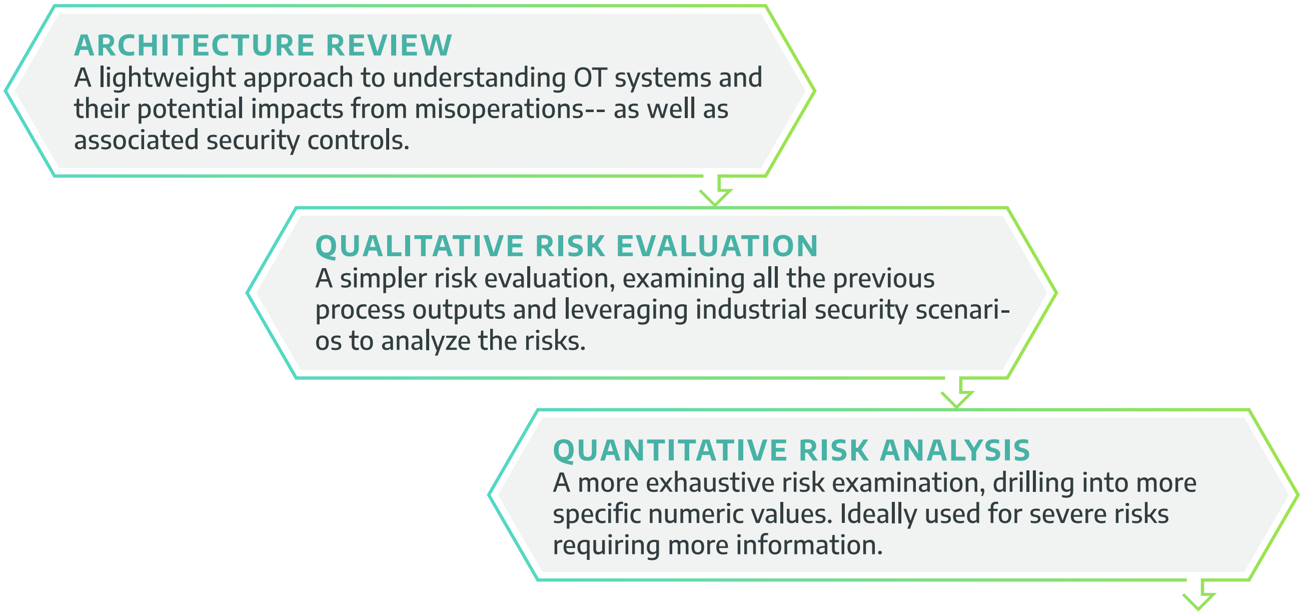
An example of industrial cyber risk impact criteria can be found below in Table 4:

DESCRIPTION	IMPACT RANKING
Financial: Up to $X losses in recovery costs and property damage. **Safety:** Possibility of minor injury; no fatalities. **Business Continuity:** Very short term (up to X days) business interruption/expenses. **Environmental:** No environmental impacts. **Reputational:** No reputational harm or loss of public confidence. **National:** Little or no impact to business sectors beyond the organization. Little to no impact on community services.	**Very Low**
Financial: $X to $Y losses in recovery costs and property damage. **Safety:** On-site injuries that are not widespread; no fatalities or injuries anticipated off-site. **Business Continuity:** Short term (>X days to Y weeks) business interruption/expenses. **Environmental:** Minor environmental impacts to immediate incident site area only, less than X year(s) to recover. **Reputational:** Low loss of reputation or public confidence; possible regulatory query; significant local press coverage. **National:** Potential to impact a business sector or local community services.	**Low**
Financial: Over $X to $Y losses in recovery costs and property damage. **Safety:** Possibility of widespread on-site injuries; no fatalities or injuries anticipated off-site. **Business Continuity:** Medium term (X weeks to Y weeks) business interruption/expenses. **Environmental:** Environmental impacts to on-site and/or off-site impact, Y year(s) to recover. **Reputational:** Medium loss of reputation or public confidence; regulatory action; national press coverage. **National:** Potential to impact a business sector or local community services.	**Moderate**
Financial: Over $X to $Y losses in recovery costs and property damage. **Safety:** Possibility of X to Y on-site fatalities; possibility of off-site injuries. **Business Continuity:** Long term (X months to Y months) business interruption/expenses. **Environmental:** Very large environmental impacts to on-site and/or off-site impact, Y to Z year(s) to recover. **Reputational:** High loss of reputation or public confidence; legal prosecution; extensive national press coverage. **National:** Impacts to business sectors beyond the organization. Disruption to community services.	**High**
Financial: Over $X losses in recovery costs and property damage. **Safety:** Possibility of any off-site fatalities from large-scale disaster; possibilities of multiple on-site fatalities. **Business Continuity:** Very long term (over X months/years) business interruption/expenses. **Environmental:** Major environmental impacts to on-site and/or off-site, more X years/poor chance to recover. **Reputational:** Very high loss of reputation or public confidence; international press coverage. **National:** Impacts to business sectors beyond the organization. Disruption to community services or national economy.	**Very High**

Table 4. Example Impact Criteria

STEP 04 | RISK EVALUATION

Risk evaluation techniques will vary from organization to organization based on resources, maturity, and other drivers. This industrial cyber risk module relies on using consistent threat information and organization-specific impact criteria to create scenarios and evaluate their potential impact. In order to effectively measure risk, organizations will need to be consistent in how risk is evaluated. That said, in resources-constrained environments, there will be a hierarchy or maturity scale for how to evaluate industrial cyber risk:



ARCHITECTURE REVIEW
A lightweight approach to understanding OT systems and their potential impacts from misoperations-- as well as associated security controls.

QUALITATIVE RISK EVALUATION
A simpler risk evaluation, examining all the previous process outputs and leveraging industrial security scenarios to analyze the risks.

QUANTITATIVE RISK ANALYSIS
A more exhaustive risk examination, drilling into more specific numeric values. Ideally used for severe risks requiring more information.

Figure 3. Workflow for Industrial Cyber Risk Evaluations

CYBER RISK SCENARIOS

Risk evaluation techniques should include scenario-driven analysis for OT-specific incidents. Cyber risk scenarios, failure scenarios, or specific outputs from Crown Jewel Analysis add additional consideration of specific events to:

- Tie the risks to relevant threat profiles
- Highlight specific vulnerabilities from architecture reviews
- Validate findings from security team leaders and promote further mitigation
- Add scenarios to a table-top exercise library

This can also provide further buy-in for executives and other stakeholders through workshops focusing on specific failure scenarios.

USING IMPACT CRITERIA FOR RISK EVALUATION

Any of the scenario-based risk evaluations should use consistent risk ranking, as introduced in Table 4 with the example impact criteria.

WHEN EXAMINING THE OUTPUT FROM A RISK EVALUATION, INDUSTRIAL ORGANIZATIONS SHOULD ASK THE FOLLOWING QUESTIONS AND FRAME THE OVERALL RISKS:

FINANCIAL IMPACT

Based on scenarios, what would be the financial consequences associated with the cyber risk? This analysis should be quantitative, based on real-world financial data, but it could also be qualitative where no or little data exists to start (e.g., high/medium/low). Financial impacts can be broken into capital expenditures (CapEx) and operating expenses (OpEx), or other terms risk managers and executives already leverage to discuss financial risks, including analysis of property and casualty insurance coverage.

SAFETY IMPACT

Based on scenarios, what associated health and human safety concerns can be linked to the cyber risk? This analysis would potentially include impacts to on-site engineers, workers, or local communities impacted by an OT-based cyber incident. Again, this analysis could be both quantitative or qualitative based on organizational resources and maturity.

BUSINESS CONTINUITY IMPACT

Leveraging existing business impact analysis (BIA), what operational outages are associated with the cyber risk or failure scenarios? Impact must be quantitative.

ENVIRONMENTAL IMPACT

This data may exist in disaster recovery documentation, property and casualty insurance, or regulatory filings. Based on the existing data, what is the associated environmental impact due to an OT-based cyber incident? This value could be quantitative or qualitative.

REPUTATIONAL IMPACT

Larger enterprises may leverage a formal sentiment analysis using commercial services to complete an evaluation. This evaluation analyzes the consequences a cyber incident may have on stature or credibility for the industrial firm or utility with key stakeholders such as customers, regulators, and shareholders.

(OPTIONAL) NATIONAL IMPACT

Unlike many other IT-focused organizations, asset owners and operators with industrial control systems are often linked to critical infrastructure for their respective countries. There may be many risks that need to be identified, evaluated, and treated based on national impacts or concerns. These may not ever be quantifiable, but instead be based on qualitative analysis with government stakeholder input.

ARCHITECTURE REVIEW (AND SECURITY CONTROLS EVALUATION)

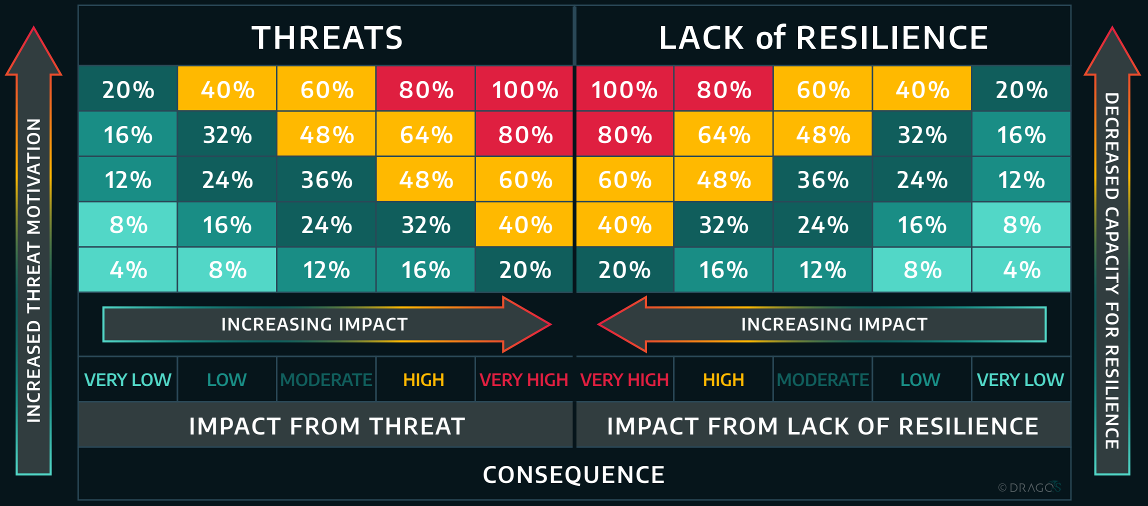
For specific OT risk evaluations, organizations need to reference a recent architecture review. The goal of the review is to ascertain specific vulnerabilities that can be mitigated within the OT system and verify the use the OT security controls. A technical penetration test is not only unnecessary for OT systems, but not recommended for production systems where IT-centric tools may cause reliability issues. However, in environments where it is possible, penetration tests will provide valuable insights into the effectiveness of security controls.

QUALITATIVE RISK EVALUATION

Due to the sheer size and complexity involved in industrial processes, the Dragos process requires a basic qualitative risk evaluation for every identified risk. These are considered a gut-check and not something that would be the basis for the comprehensive risk management program. The qualitative risk evaluation helps to ensure risks are quickly identified and managed if they exceed a certain threshold. Qualitative risk evaluations use a scale of qualifying attributes to describe the impact associated with the risk (identified in the previous step) with the remainder of the established risk equation. Recall that this guideline defines the industrial cyber risk equation previously defined as:

$$\textit{Industrial Cyber Risk} = \textit{Consequence} \times \frac{(\textit{Threat} \times \textit{Vulnerability})}{\textit{Resilience}}$$

Where consequence is defined by the impact criteria, threat is defined by the threat profiles, and vulnerabilities and resilience are established through the architecture review process.



THREATS					LACK of RESILIENCE				
20%	40%	60%	80%	100%	100%	80%	60%	40%	20%
16%	32%	48%	64%	80%	80%	64%	48%	32%	16%
12%	24%	36%	48%	60%	60%	48%	36%	24%	12%
8%	16%	24%	32%	40%	40%	32%	24%	16%	8%
4%	8%	12%	16%	20%	20%	16%	12%	8%	4%
VERY LOW	LOW	MODERATE	HIGH	VERY HIGH	VERY HIGH	HIGH	MODERATE	LOW	VERY LOW
IMPACT FROM THREAT					IMPACT FROM LACK OF RESILIENCE				
CONSEQUENCE									

🔴 VERY HIGH RISK 🟡 HIGH RISK ⚪ MODERATE RISK ● LOW RISK ● VERY LOW RISK

Figure 4. Example Heat Map for Qualitative Industrial Cyber Risk Evaluations

The heat map above evaluates consequence for both threats and a "lack of resilience," which would note where a system lacks capacity to respond, similar to the disaster risk discussed in the first chapter. Since resilience is in the denominator of the industrial cyber risk equation, increasing resilience will decrease the potential impact from a vulnerability (and therefore its corresponding risk). In this example, an industrial organization can then qualify "very high, high, moderate, low, and very low" risk based on a balanced discussion of the consequences and relative resilience of the system, based on security controls informed from an architecture review.

SIMULTANEOUSLY, RISK SCENARIOS CAN BE EVALUATED BASED ON THE ORGANIZATION'S THREAT PROFILES.

QUANTITATIVE RISK ANALYSIS

Unlike qualitative analysis, quantitative analysis uses a scale of numeric values to establish a risk score. This scoring rubric must be defined by observable data points, such as historic losses and similar events. Unfortunately, much of the data is lacking in ICS cybersecurity due to the rarity of Stage 2 attacks. However, organizations that need to produce quantitative risk analysis for executives can leverage trending data from threat sources and public incidents to help establish expectations on any quantitative risk values. There are several popular quantitative risk analysis tools on the market, but most will not be useful for industrial control systems.[vi] Instead, it would be more valuable to asset owners and operators to use quantification for impacts and threat trends, which can be tailored to individual organizations.

The more popular method within industrial cyber risk quantification analysis involves event tree analysis. Event tree analysis is a modeling technique based on a waterfall technique representing a series of conditions that could arise following a cybersecurity event. This would be an in-depth examination building on the risk scenarios described previously in this chapter and help further refine impact estimates and threat profiles.

Quantitative risk analysis will require additional resources to perform when compared to the lighter weight qualitative evaluations and should therefore be reserved for risk scenarios with more severe impacts. Some commercially available modeling techniques will require using unknown quantities and building scientific estimations for probability, including:

- **Monte Carlo Experiments** which help establish probabilistic interpretation for cyber risk through random sample values across a set of inputs, determining impacts, and building a distribution.
- **Bayesian Analysis** relies on building from prior distributions and utilizing observed data to create a statistical understanding of probability.

[vi] Many industrial organizations may already use quantifiable methods to estimate cyber risk for information-centric risks. In those cases, it may be necessary to use similar methods to ensure cyber risk discussions are uniform within the risk management program

There are some difficult problems to contend with when utilizing these methods across industrial environments. For example, many of these models will output an annualized loss expectancy (ALE) from a cyber risk scenario. ALE is a useful tool in risk management and can be leveraged for information-centric cyber risk where there is an expected "annualized loss" from data breaches. In industrial environments, however, such a metric would provide a poor interpretation of severe, yet binary, impacts like the loss of critical equipment due to a cybersecurity incident.

As highlighted in Figure 3, quantitative techniques are extremely valuable, but should be reserved for "very high" or "high" risks identified from previous qualified risk scenarios.

STEP 05 | RISK TREATMENT

Risk treatment consists of any pre-incident strategies to manage the identified risk. The initial output of the risk evaluation helps decide what the initial response, or risk prioritization, should be. For example, the heat map in Figure 4 outlines five potential risk prioritizations based on the associated color of the map. An example set of risk prioritization, and their responses, could be described as the language in the table below.

VERY HIGH RISK	**REQUIRES IMMEDIATE ATTENTION.** Very high risks imply a motivated and capable threat actor, or a non-resilient system, is at risk to have high or very high consequences. These risks require immediate treatment and constant monitoring.
HIGH RISK	High risks, while not requiring urgent attention, do need to be tracked on a regular basis (measure in days or weeks, not months). This would include regular briefings across the organization and should be used to prepare if this elevates to a "very high" risk.
MODERATE RISK	Moderate risks should be considered manageable across the treatment options—these risks may have specific treatment plans, including mitigation strategies with budgets and resource discussions.
LOW RISK	Low risks may benefit from regular review, but otherwise may be managed in combination with other risks.
VERY LOW RISK	Very low risks may not require any action and be considered acceptable risks for the organization.

Table 5. Example Industrial Cyber Risk Prioritization

Prioritizing cyber risks based on the industrial cyber risk equation ensures that organizations are focusing on risks that are both impactful to the organization, but also rooted in threat activity and resilience capabilities. Understandably, each risk will need to be treated differently based on the specific risk and prioritizations.

RISK RESPONSE AND DISPOSITIONS

Once prioritized, each risk needs to be treated with a risk response. A risk response is a strategy and set of actions that must be implemented to manage the risk. Strategy development begins with a statement of intent, or risk disposition, for addressing the risk.[vii]

THIS DIAGRAM SHOWS EXAMPLES OF POTENTIAL RISK DISPOSITIONS, EXPANDING ON THE PROCESS IN FIGURE 1.

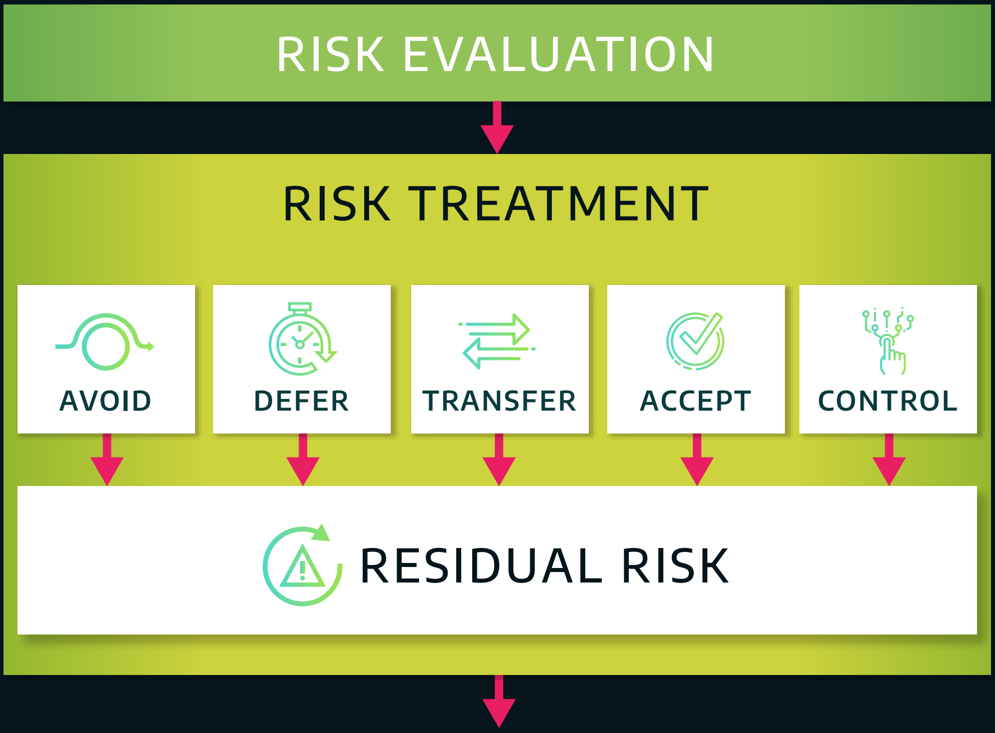


Figure 5. Industrial Cyber Risk Treatment and Response

Risk response options and dispositions may vary across organizations and need to be tailored based on governance, resources, and stakeholder involvement. The generic categories highlighted in Figure 5 can be used flexibly within the Dragos risk management process.

[vii] The CERT Resilience Management Model highlights use of risk dispositions in practice RISK:SG4:SP3, and also recommends further categorizing risks for general risk management programs. Since this guideline is focused on industrial cyber risk, it is recommended that organizations leverage their overarching risk management program in examining risk dispositions and strategies.

AVOIDING CYBER RISK

While “avoiding” industrial cyber risk may be the most ideal response, it is commonly the most difficult. Avoidance, in consideration of both cyber threats and system resilience, may require altering operations to avoid risks while still providing essential industrial services. These altered operations may require new process design or switching to manual operations.

ACCEPTING CYBER RISK

It is necessary to leverage a consistent scoring system or criteria for evaluating cyber risk. The acceptance of cyber risk indicates the impact is minor enough for the organization to manage the financial, reputational, and physical damages that may result from the potential cyber event. These risks can be budgeted for or otherwise absorbed.

DEFERRING CYBER RISK

Sometimes we do not have enough information about a specific risk to warrant an immediate action. Rather than potentially impact operations, deferring industrial cyber risk acknowledges that further research is required until the need to address the risk is apparent. Deferred risks are tracked and monitored, with research resources allocated to ensure the risk is treated appropriately.

CONTROLLING CYBER RISK

This is the primary state for many security teams. Controlling, or mitigating, cyber risk involves adding new processes, technologies, or workforce controls to reduce the cyber risk. Traditional IT and OT security mitigation plans need to be leveraged and include the use of:

- Preventative controls: focused on reducing a specific instance of a vulnerability
- Deterrent controls: focused on discouraging a threat actor
- Detective controls: providing warning of an attempt or successful cyber event
- Corrective controls: focused on offsetting or minimizing the impact after a cyber event
- Compensating controls: providing additional protection or adjusting for a weakness in another control

In industrial environments, these controls may also map to safety exposure, depending on the impacts of a specific risk. The Hierarchy of Controls for safety hazards could provide additional information on desired controls for operations, such as engineering controls or elimination of the hazard (and risk) entirely.[11]

TRANSFERRING CYBER RISK

Transferring cyber risk needs to leverage some sort of insurance mechanism, similar to those used for safety and property insurance, but applied to specific identified cyber risks. Just like any security control, cyber insurance options need to be tailored to the operating environment and impacts. Not all insurance products are equal, and risk managers in industrial protection need to be informed about the insurance market and the specific risks that cannot be tolerated, accepted, or mitigated (and therefore need a transfer mechanism). There is no additional security benefit to installing a firewall appliance with “any:any” as a firewall rule. For transferring risk, using an untailored insurance product provides a sense of false security.

RESPONDING TO RESIDUAL RISK

No matter how many security controls are in place, no risk will ever be zero. Residual risk refers to any risk that remains after the risk response decisions have been implemented. Residual risks should be outlined in the risk disposition, considered for additional monitoring activities, and tracked accordingly.

USING COST/BENEFIT ANALYSIS

When determining any risk response, security leaders need to determine, with help from the asset owner and risk owner, what the associated costs will be for the risk treatment. This will help the risk owner decide what approach will be best for mitigating or transferring the risk. For example, if a specific risk includes mechanical breakdown and replacement of a $250 million turbine, but the set of preventative and detective controls is only $300 thousand, then the risk owner may decide to invest in the new security capabilities rather than face the potential impact of losing the turbine due to a cybersecurity attack. Similarly, if the insurance policy is $50 thousand annually for the same security risk, the risk owner may decide to immediately address the risk through transfer prior to installing the correct security controls. Neither decision can be appropriately made without a cost/benefit analysis (CBA). The CBA needs to express the cyber impact in monetary terms that allows for a more consistent approach to applying risk treatment strategies.

RISK MONITORING

Most industrial firms and utilities already have a risk monitoring capability. This may be in the form of monthly meetings with leadership, memos, or other existing tools. The primary vehicle for monitoring cyber risk is a robust risk register.

RISK REGISTER

A risk register is a structured repository of identified risks, as defined in the Cybersecurity Capability Maturity Model (C2M2).[12] This repository is where business leaders and management may refer to their entire set of risks, inclusive of cyber risk. It should be viewed as a record or ledger of risks that have gone through the Dragos industrial cyber risk management process.

Risk registers, if used correctly, can ensure industrial firms and utilities have a consistent view of associated cyber risks. This also helps facilitate risk management decisions by continually asking if the right risks are tracked and measured according to a repeatable process.

THE RISK REGISTER REFLECTS EACH OF THE PREVIOUS MODULES DESCRIBED ABOVE AND SHOULD INCLUDE:

RISK IDENTIFIER: This could be a simple sequential number, code name, or other unique identifier in the risk register

PRIORITY: A relative indicator of the unique risk's ranking or criticality based on impact and risk treatment criteria

RISK DESCRIPTION: A brief description of the cyber risk that could impact the organization and related OT or IT systems

RISK CATEGORY: Based on the organization's lexicon or risk taxonomy, a grouping of the similar risks that can be used for additional analysis

RISK EVALUATIONS: Based on the previous risk evaluations, the risk register should include the following evaluation indicators from the Risk Evaluation criteria:

- ✓ Environmental Impact
- ✓ Reputational Impact
- ✓ (Optional) National Impact
- ✓ Financial Impact
- ✓ Safety Impact
- ✓ Business Continuity Impact

RISK RESPONSE: A brief description of the risk response category and strategies used to treat the risk

COST/BENEFIT ANALYSIS: A bulleted list of costs associated with the proposed (or current) risk response

RISK OWNER: The name, title, role, facility, or department that is responsible for managing and monitoring the risk response

STATUS: A one-word or phrase flag for tracking the current condition of the risk (e.g., open/closed/retired/updated)

An example industrial cyber risk register can be seen below:[13]

ID	PRIORITY	RISK DESCRIPTION	RISK CATEGORY	INDUSTRIAL CYBER RISK EVALUATION						RISK RESPONSE	COST/ BENEFIT ANALYSIS	RISK OWNER	STATUS
				FINANCIAL IMPACT	SAFETY IMPACT	BUSINESS CONTINUITY	ENVIRONMENTAL IMPACT	REPUTATIONAL IMPACT	NATIONAL IMPACT				
1	**Very High**	An advanced threat activity group targets our safety systems, leading to complete plant shut down and associated property damage.	**Cyber Incident:** Loss of Safety	**$70.5M**	M	M	L	M	L	Install additional OT monitoring at the plant. Increase operator training for incident response and recovery.	**$350k** for monitoring & training.	Plant Management	Open
2	**Moderate**	ICS vendor is compromised, resulting in malware sent to all field devices in the form of a "legitimate" software update.	**Cyber Incident:** Supply Chain Compromise	**$1.2M**	M	M	L	M	M	Include procurement language for supply chain risk. Add technical evaluation to all patch management cycles.	**$50k** for insurance & an additional $150k for new patch management and supply chain recommendations	OT Security Team	Open
3	Low	Operator uses infected USB to transfer project files across plant operations. Untargeted malware causes network latency issues.	**Cyber Incident:** Engineering Workstation Compromise	**$750k**	L	L	L	L	L	Limit ports and services across Level 3 and Level 2 assets, including physical ports. Include additional security awareness for plant personnel.	**$25k** in hourly work to create OT-based strategy for plant operations and USB protections.	Plant Management	Open

Table 6. Example Industrial Cyber Risk Register

Risk monitoring activities require updating the risk register regularly and leveraging the results in routine risk communication activities. It is necessary to have different risk granularity requirements for risk management, executives, and operations/engineers based on their preferred terms of regular meeting schedules.

RISK COMMUNICATION

The most common area of weakness for cyber risk management is communication. As highlighted in the Dragos Industrial Cyber Risk Management process in Figure 1, risk communication is required throughout the entire methodology, including the steps mentioned above. Practitioners often invest time and resources in their specific risk assessment methodology but fail in expressing the importance of treating risks across an organization. The Dragos process includes several tools to help practitioners engage management and executive leadership in risk management discussions, leveraging existing standards and processes tailored for OT-specific concerns.

RISK TAXONOMY AND LEXICON

Risk communication requires a common language to discuss risk across engineering, IT, OT security, managers, and executives. Ideally, the lexicon would also be used by other risk leaders, including owners of legal, compliance, safety, and financial risk. This would ensure, regardless of the specific risk equation for a unique discipline, that "risk = risk = risk." The Dragos process initially tackles the idea of common language with impact criteria, like the example in Table 4. The impact criteria are flexible enough to be used across all other types of risk facing industrial organizations. If leveraged properly, this would help map risks so executives can discuss investing in different risk treatment options. It also aids in discussions where different risks (legal, safety, compliance, or cybersecurity, for example) can be evaluated uniformly.

Like impact criteria, risk taxonomies are another useful tool for communication. Taxonomies are used in other disciplines and are leveraged in communicating how categories are related. For example, biologic classification uses taxonomic rank to discuss groups of organisms—species, genus, family—all better describe how lifeforms are linked.

> "THE TAXONOMY FRAMEWORK PROVIDES A CHECKLIST OF THREATS THAT COULD CAUSE DISRUPTION TO BUSINESS OPERATIONS. THE SYSTEMATIC FRAMEWORK PROVIDED BY A TAXONOMY PROVIDES A STRUCTURE TO MONITORING THE EMERGING RISKS OF INTEREST.
>
> – CAMBRIDGE CENTRE FOR RISK STUDIES

The industrial cyber risk taxonomy is defined as a blueprint for classifying various exposures of danger, harm, or loss. As with other aspects of this guideline, if a risk taxonomy already exists for an industrial organization, it should be leveraged for cyber risk, too.

Even in the case where a taxonomy does not address specific cybersecurity concerns, it may be adapted to include technical terms, like the example below:

1. ACTIONS OF PEOPLE	2. SYSTEMS AND TECHNOLOGY FAILURES	3. FAILED INTERNAL PROCESSES	4. EXTERNAL EVENTS
1.1 Inadvertent 1.1.1 Mistakes 1.1.2 Errors 1.1.3 Omissions **1.2 Deliberate** 1.2.1 Fraud 1.2.2 Sabotage 1.2.3 Theft 1.2.4 Vandalism **1.3 Inaction** 1.3.1 Skills 1.3.2 Knowledge 1.3.3 Guidance 1.3.4 Availability	**2.1 Hardware** 2.1.1 Capacity 2.1.2 Performance 2.1.3 Maintenance 2.1.4 Obsolescence **2.2 Software** 2.2.1 Compatibility 2.2.2 Configuration Management 2.2.3 Change Control 2.2.4 Security Settings 2.2.5 Coding Practices 2.2.6 Testing **2.3 Systems** 2.3.1 Design 2.3.2 Specifications 2.3.3 Integration 2.3.4 Complexity	**3.1 Process Design or Execution** 3.1.1 Process Flow 3.1.2 Process Documentation 3.1.3 Roles and Responsibilities 3.1.4 Notifications and Alerts 3.1.5 Information Flow 3.1.6 Escalation of Issues 3.1.7 Service Level Agreements 3.1.8 Task Hand-Off **3.2 Process Controls** 3.2.1 Status Monitoring 3.2.2 Metrics 3.2.3 Periodic Review 3.2.4 Process Ownership **3.3 Supporting Processes** 3.3.1 Staffing 3.3.2 Funding 3.3.3 Training and Development 3.3.4 Procurement	**4.1 Disasters** 4.1.1 Weather Event 4.1.2 Fire 4.1.3 Flood 4.1.4 Earthquake 4.1.5 Unrest 4.1.6 Pandemic **4.2 Legal Issues** 4.2.1 Regulatory Compliance 4.2.2 Legislation 4.2.3 Litigation **4.3 Business Issues** 4.3.1 Supplier Failure 4.3.2 Market Conditions 4.3.3 Economic Conditions **4.4 Service Dependencies** 4.4.1 Utilities 4.4.2 Emergency Services 4.4.3 Fuel 4.4.4 Transportation

Table 7. Example Risk Taxonomy from the Software Engineering Institute[14]

MITRE ATT&CK AND ATT&CK FOR ICS

One useful tool for cyber risk and OT-specific classifications can be found in the MITRE ATT&CK Framework and accompanying ATT&CK for ICS. Both frameworks apply a consistent language and set of terms to describe impacts derived from a cybersecurity attack, inclusive of OT environments.

COMBINING ATT&CK WITH AN OPERATIONAL RISK TAXONOMY, LIKE THAT IN TABLE 7, WILL ALLOW BOTH SECURITY LEADERS AND RISK LEADERS TO QUICKLY SPEAK IN A COMMON LANGUAGE, BREAKING DOWN TRADITIONAL BARRIERS BETWEEN BOTH ORGANIZATIONS.

RISK COMMUNICATION PROCESS

For example, the Dragos process can be used to support the National Institute of Standards and Technology (NIST) Cybersecurity Framework information and decision flow seen below.

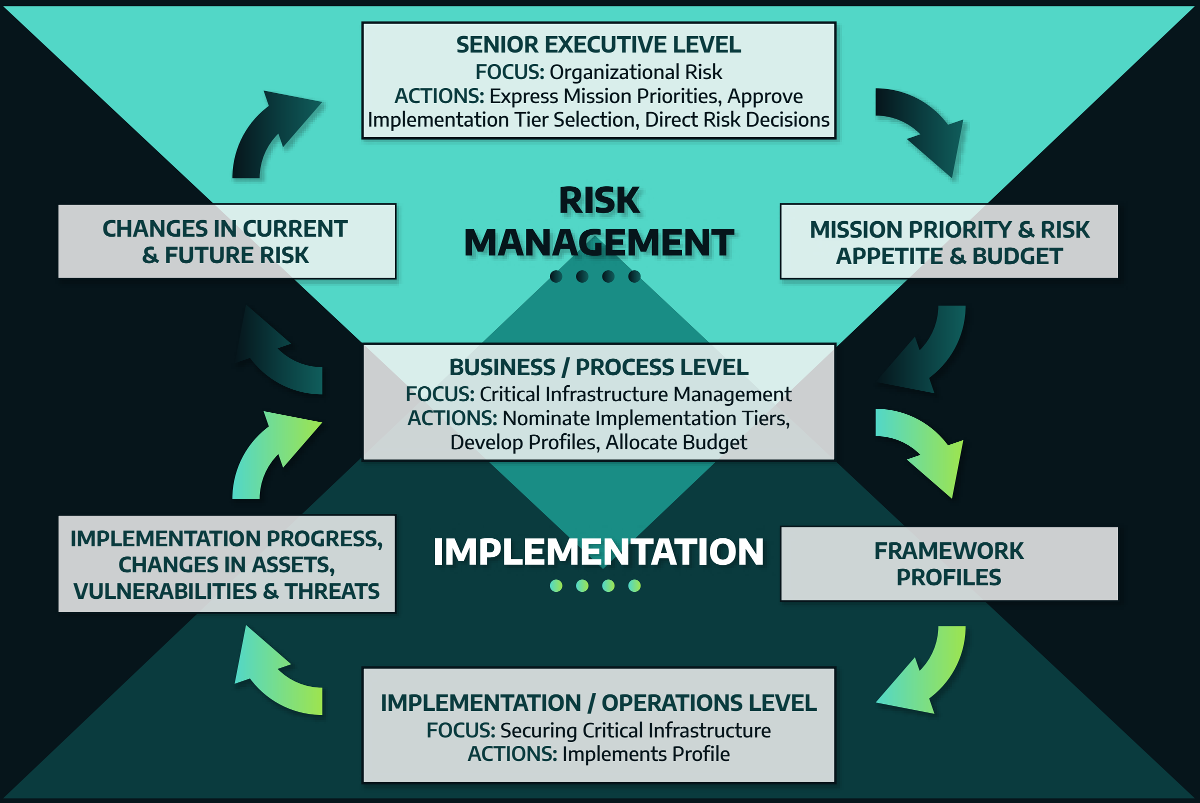

SENIOR EXECUTIVE LEVEL
FOCUS: Organizational Risk
ACTIONS: Express Mission Priorities, Approve Implementation Tier Selection, Direct Risk Decisions
CHANGES IN CURRENT & FUTURE RISK
RISK MANAGEMENT
MISSION PRIORITY & RISK APPETITE & BUDGET
BUSINESS / PROCESS LEVEL
FOCUS: Critical Infrastructure Management
ACTIONS: Nominate Implementation Tiers, Develop Profiles, Allocate Budget
IMPLEMENTATION PROGRESS, CHANGES IN ASSETS, VULNERABILITIES & THREATS
IMPLEMENTATION
FRAMEWORK PROFILES
IMPLEMENTATION / OPERATIONS LEVEL
FOCUS: Securing Critical Infrastructure
ACTIONS: Implements Profile

Figure 6. Notional Information and Decision Flows from the NIST Cybersecurity Framework[viii]

This can be approached in a series of steps, highlighting the communication process for risk management:

RISK GOVERNANCE IS ESTABLISHED AND EXECUTIVE LEADERSHIP SETS GUIDANCE.

Through an initial series of meetings, risk leaders can vet the Dragos process for use in existing risk management practices. This will provide insight into how the organization discusses non-cyber risks and can relay impact criteria and use of the risk register. Executives should provide insights on resource constraints and what financial, reputational, safety, and environmental impacts reach thresholds for different risk treatment options, including purchasing insurance or limits on cost/benefit analysis. This should create risk guidance for management and operational leaders. The initial communication may be a mix of quantitative and qualitative measurements.

[viii] The NIST Cybersecurity Framework was designed to create a flexible approach for critical infrastructure protection across multiple sectors, and is based on asset owner/operator feedback, including multiple referenced cybersecurity standards and guidelines: https://www.nist.gov/cyberframework

BUSINESS-LEVEL MANAGEMENT PERFORM INDUSTRIAL CYBER RISK EVALUATIONS BASED ON THE ESTABLISHED CRITERIA.

This includes methods to implement risk evaluations across business units or facilities. Risk treatment types can be linked to specific guidance or security controls, as highlighted in Figure 5. Risk transfer mechanisms require additional governance with financial risk managers that purchase insurance products.

RISK IS MANAGED AT THE IMPLEMENTATION/OPERATIONS LEVEL WITH CONSISTENT FEEDBACK TO MANAGERS USING THE RISK REGISTER.

As the ledger of identified risks, it is important to maintain the risk register as a living document and force communications from implementation to management via a singular tool. There may be need for more complicated project management processes to highlight milestones and deliverables, but the ultimate reporting needs to be maintained in the risk register for consistency.

EXECUTIVES ADAPT GOVERNANCE BASED ON REPORTS FROM BUSINESS-LEVEL MANAGEMENT LEVERAGING THE RISK REGISTER.

These reports should contain aggregate results based on risk prioritization. This will require trial and error as managers learn what risk metrics are used by (and useful for) executive leadership. As one of the more critical feedback loops, progress from the risk register further informs and refines risk tolerances and budget conversations, which continues the risk management and governance lifecycle.

Similar to Control Objectives for Information Technologies (COBIT), this process can be defined in terms of roles, responsibilities, and actions, as outlined below:[15]

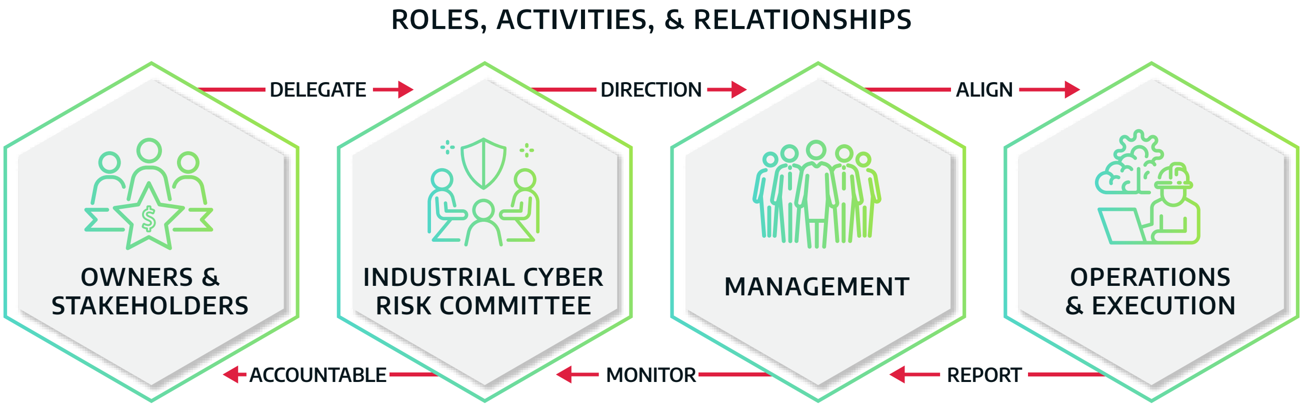


Figure 7. Dragos Industrial Cyber Risk Management: Roles, Activities, and Relationships

Leveraging the NIST Cybersecurity Framework is just one example. The Dragos process in this guidance document is designed to integrate with ISO 27000, NIST 800-39, ISA/IEC 62443, NERC CIP, EU NIS Directives, DHS CFATS, and other industrial security and risk management guidelines, regulations, and processes.

RISK GOVERNANCE

Cyber risk as a field is relatively new compared to other areas of risk management. This is especially true for OT security, where cybersecurity has only recently become a budgeted line item for industrial organizations. Changes to the culture of risk management will be difficult for any organization, but especially those that are just now managing a cybersecurity program. Maturity in any cyber risk program helps ensure sustainability. Any cyber risk management process, including what is outlined in this guideline, needs to have an appropriate governance structure to be successful.

Governance can be established at any industrial organization, regardless of size, sector, or function. The key is to scope the governance structure to not overwhelm resources (including executives) and establish a battle rhythm to solve risk management issues as they occur.

The suggested governance for this approach includes a cyber risk management committee, with a core team of IT and OT security professionals tied to other business units and stakeholders. Figure 8 below outlines an example organizational structure for a committee or team with the appropriate roles.

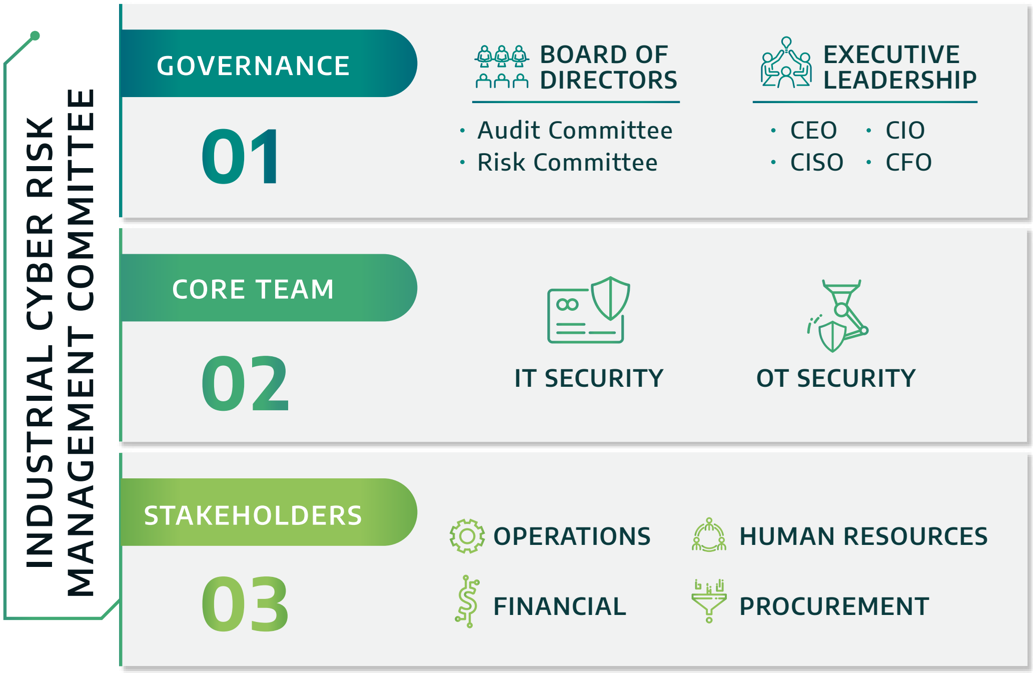


Figure 8. Example Industrial Cyber Risk Governance Structure

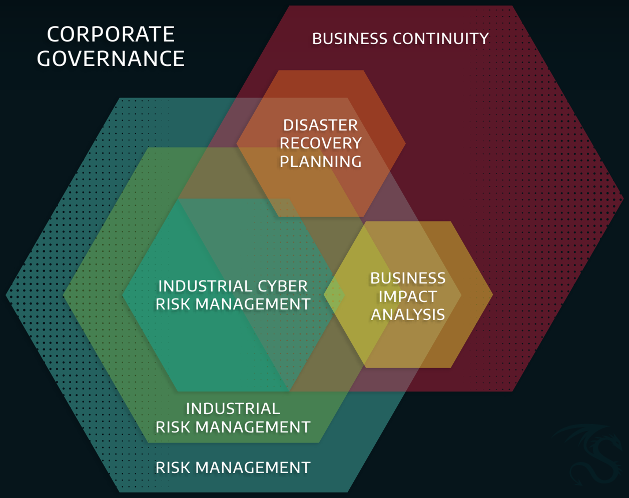

CORPORATE GOVERNANCE
BUSINESS CONTINUITY
DISASTER RECOVERY PLANNING
INDUSTRIAL CYBER RISK MANAGEMENT
BUSINESS IMPACT ANALYSIS
INDUSTRIAL RISK MANAGEMENT
RISK MANAGEMENT

Figure 9. Nested Relationship between Risk Management and Business Continuity[16]

While risk management and incident response are typically distinct functional areas within an organization, there may be overlap in the overall committee structure depending on available resources and expertise. Any shared resources should be well-versed in both disciplines (which may require additional training), as the skill sets are different.

This governance structure may include other stakeholders from business continuity that may have additional resources dedicated for modeling recovery activities needed for cyber risk analysis. Since the Cyber Risk Characterization process requires business impact analysis and other products of business continuity, organizations should make appropriate changes to include business continuity (or disaster recovery) as needed.

Other governance activities within Dragos Industrial Cyber Risk Management process include:

- Executive sponsorship of the cyber risk management program, including funding and establishing processes for oversight and execution.
- Creating metrics for success and implementation across the IT and OT cyber risk program.
- Formal and informal review processes for cyber risk management activities (including the use of internal audit teams) to ensure continued success and support for the program.

Establishing appropriate governance for cyber risk management is the most challenging aspect of implementing the Dragos process at any organization due to the natural conflict with cultural norms, fear and uncertainty, and lack of initial documentation. Each of those issues may be addressed with constant communication and feedback. The best indicator for success in implementing any new program is the support of executive leadership and sponsorship. Without buy-in from leaders, organic change is extremely difficult.

A QUICK DETOUR ON EXECUTIVE RISK REPORTS

The Dragos process is designed to engage executives in their working language while also allowing OT and IT security leaders to manage risk effectively. One of the goals of communication with executives is to establish what the acceptable level of loss exposure would be, including OT-based cybersecurity incidents. The answer cannot be, “we do not accept any level of loss,” because that is not true nor accurate to business or critical infrastructure. There are acceptable levels of loss in property, safety, and environmental risk, and OT security is no exception. Once executives and management align on the levels of acceptable risk, business and security decisions can be finalized based on the Dragos process.

To maintain communication on what risks are still acceptable compared to those that need immediate risk treatment, managers and risk leaders need to prepare executive-level risk reports. These reports need to be based on the risk register and will need data analysis to provide dashboards and additional value. The reports are only as valuable as the data being entered into the risk register itself. Reports will likely have the following characteristics:

- Normalization of industrial cyber risks across the enterprise. If different business units or facilities rank similar risks with different impacts (for example, one lists an attack on safety systems as a low while another facility ranks it as high), that needs to be normalized. Using a risk taxonomy and enterprise-defined terms will help ensure similar risks are evaluated consistently.
- Reports should highlight outstanding risk treatment activities and a common understanding of actual and potential risks for the entire industrial organization.
- Dashboards and metrics should include information on the potential risks based on the industrial cyber risk impact criteria (financial, safety, business continuity, environment, reputational, and national impacts).
- Highlight any recent findings or changes in the overall cyber risk, including internal data (like new risk evaluations) and external data (such as newly monitored threats).

The data from these reports should drive new conversations on changes to the overall risk appetite for the organization, including budgets and resourcing to address gaps, and provide governance for cyber risk activities.

Many executives ask for benchmarks, trends, and to know more about other peer groups addressing cyber risk. For obvious reasons, much of this data does not exist. Organizations should strive to manage this problem as best as possible, especially in critical infrastructure.

INDUSTRIAL CYBER RISK & DRAGOS

Cybersecurity for industrial firms, utilities, vendors, and other stakeholders consists of several risks that are difficult to manage.

The impacts due to a cybersecurity incident are much worse than traditional IT cyber risk (financially, reputationally, and potentially for national interests, including potential impacts to health and human safety). OT security is often underfunded with minimal data to support adding security controls to industrial control systems.

The Dragos Industrial Cyber Risk Management process changes that. By creating a repeatable and consistent methodology to assess, manage, and communicate cyber risk across an entire enterprise, the Dragos process augments any existing risk management process to succeed in addressing OT security challenges. This guideline can be implemented with existing security and compliance programs to provide alignment with executives, managers, and engineers.

APPENDIX: RISK MANAGEMENT APPROACHES

Over thousands of years, multiple concepts have survived across civilization to create the idea of a risk management process.

At its core, risk management is driven by avoiding danger and harm, and the related concepts are universal regardless of discipline/sector/concept. If a pilot talks about aviation risk, there is a general understanding it may involve airplanes. If a plumber discusses risk with a septic tank, there is a base understanding that things could get messy for the customer.

Those universal elements have survived and are leveraged in various standards. Standard Development Organizations (SDOs), like the International Organization of Standardization (ISO), create drafting teams and build international consensus on methods for managing risk across a multitude of industries including financial risk, engineering risk, manufacturing risk, and legal risk. While there are several risk management standards that exist, the core concept is similar across all of them. There are only so many ways to describe framing, communicating, and addressing a risk.

A starting point for understanding general risk management can be found in ISO 31000.[17]

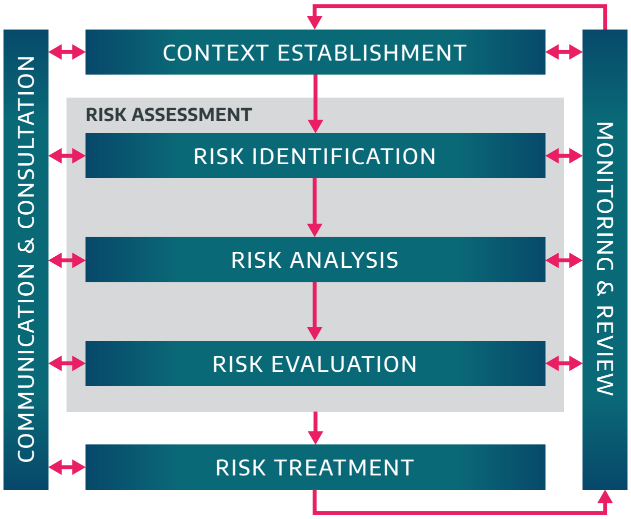


Figure 10. ISO 31000 Risk Management Process

Each step in ISO 31000 is established to help create a sustainable risk management program. The major elements include the following:

- **Context Establishment** includes scoping of the risk program, boundaries, and organization. This also includes objective criteria for use by the entire organization, like what consequences or impacts may be faced, and the thresholds of an "acceptable risk."
- **Risk Assessment** is the main element of a risk management program. It requires inputs, provides outputs, and needs constant maintenance for consistency in performance over time. Risk assessments include the following key terms:
    - **Risk Identification** includes the systems, facilities, or assets being assessed, where to look for risks, how to identify impacts, and what controls may already be in place to mitigate the risk.
    - **Risk Analysis** is usually broken into two categories; qualitative and quantitative. The analysis may be a combination of both and is intended to measure the risk. In most cases, this is based on evaluating potential scenarios, though more advanced techniques leverage actuarial tables and larger data repositories. In most disciplines, a quick qualitative analysis is performed first, followed by something more quantitative for substantial risks. Quantitative analysis usually requires more resources to perform.
    - **Risk Evaluation** is the application of the risk analysis to the criteria established previously by the context of the risk management program.
- **Risk Treatment** occurs after the risk has been ranked and prioritized throughout the evaluation process. It is then considered for a mitigation strategy, transfer of the risk (usually to insurance), or acceptance/avoidance of the risk.
- Throughout the entire program, there need to be processes for **Monitoring and Review** of the risks, and **Communications and Consultation** across the organization.

While this is an oversimplification, there is nothing unique about risk management when cybersecurity is added. The workflow for ISO 27005 highlights just that.[18]

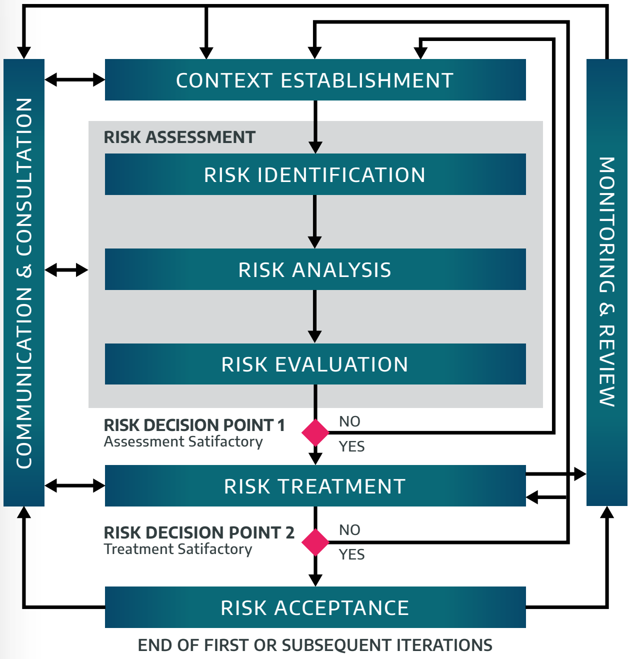


Figure 11. ISO 27005 Information Security Risk Management Process

The change in Figure 10 from Figure 11 is that risk acceptance is specifically shown in the cybersecurity standard and an additional question is added about if the assessor adequately treated the risk. The risk management process remains largely unchanged, and this is true for many industries that handle risk. The concentration should be on how differences are communicated to executives and other stakeholders.

These concepts are reflected throughout this guidance document, which expands on the IT-centric scope of standards like ISO 27005 with ICS-specific concepts.

REFERENCES

American Petroleum Institute. 2013. Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries (ANSI/API STD 780). Washington: https://standards.globalspec.com/std/1603209/ansi-api-std-780

Caralli, Richard., Allen, J., Curtis, P., White, D., & Young, L. 2016. CERT Resilience Management Model, Version 1.2 (CERT-RMM CMU/SEI-2010-TR-012). Pittsburgh: Software Engineering Institute, Carnegie Mellon University. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=508084

Caralli, Richard., Stevens, J., Young, L., & Wilson, W. 2007. Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process (Technical Report CMU/SEI-2007-TR-012). Pittsburgh: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=8419

Cebula, James., Popeck, Mary., & Young, Lisa. 2014. A Taxonomy of Operational Cybersecurity Risks Version 2 (CMU/SEI-2014-TN-006). Pittsburgh: Software Engineering Institute, Carnegie Mellon University. http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=91013

European Union Agency for Cybersecurity (ENISA). 2006. Risk Management - Principles and Inventories for Risk Management / Risk Assessment methods and tools. https://www.enisa.europa.eu/publications/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

European Union Agency for Cybersecurity (ENISA). 2008. Threat and Risk Management: Business Continuity & Resilience. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience

Information Systems Audit and Controls Association (ISACA). 2012. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. https://www.isaca.org/resources/cobit

International Organization for Standardization. 2018. Risk management – Guidelines (ISO Standard No. 31000:2018). https://www.iso.org/standard/65694.html

International Organization for Standardization. 2018. Information technology — Security techniques — Information security risk management (ISO Standard No. 27005:2018). https://www.iso.org/standard/75281.html

International Society of Automation. 2019. Security for industrial automation and control systems, Part 3-2: Security risk assessment for system design (ISA 62443-3-2 Draft). https://www.isa.org/standards-and-publications/isa-standards/find-isa-standards-in-numerical-order/

Irwin, S. 2014. Creating a Threat Profile for Your Organization. Bethesda: SANS Institute. https://www.sans.org/reading-room/whitepapers/threats/creating-threat-profile-organization-35492

Jones, A. and Kovacich, J. 2015. Global Information Warfare: The New Digital Battlefield, Second Edition. 10.1201/b19282.

Mathis, C. and Pollman, G. 2019. Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping. Hanover: Dragos, Inc. https://www.dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/

Mohr, R. 2016. Evaluating Cyber Risk in Engineering Environments: A Proposed Framework and Methodology. Bethesda: SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/paper/37017

National Institute of Standards and Technology (NIST). Framework for Improving Critical Infrastructure Cybersecurity. Gaithersburg: National Institute of Standards and Technology, doi: 10.6028 https://doi.org/10.6028/NIST.CSWP.04162018

Paulsen, C. and Byers, R. Glossary of Key Information Security Terms. NIST Interagency Report 7298 Revision 3. Gaithersburg: National Institute of Standards and Technology, doi: 10.6028 https://doi.org/10.6028/NIST.IR.7298r3

Poljanšek, K., Marin Ferrer, M., De Groeve, T., Clark, I., (Eds.). 2017. Science for Disaster Risk Management 2017: Knowing Better and Losing Less. EUR 28034 EN, Publications Office of the European Union, Luxembourg, 2017, ISBN 978-92-79-60679-3, doi:10.2788/842809, JRC102482 https://drmkc.jrc.ec.europa.eu/portals/0/Knowledge/ScienceforDRM/Science_for_DRM_2017.pdf

Stine, K., Quinn, S., Witte, G., Scarfone, K., Gardner, R. 2020. Integrating Cybersecurity and Enterprise Risk Management. NIST Interagency Report 8286. Gaithersburg: National Institute of Standards and Technology, doi: 10.6028 https://csrc.nist.gov/publications/detail/nistir/8286/final

United States Department of Energy. 2014. Cybersecurity Capability Maturity Model. Washington: https://www.energy.gov/oe/downloads/cybersecurity-capability-maturity-model-february-2014

United States Department of Energy. 2012. Electricity Subsector Cybersecurity Risk Management Process. Washington: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-1

ENDNOTES

[1] NISTIR 7298, “Glossary of Key Information Security Terms.” https://doi.org/10.6028/NIST.IR.7298r3

[2] Federal Information Processing Standard Publication 200, “Minimum Security Requirements for Federal Information and Information Systems.” https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

[3] United Nations Offices of Disaster Recovery Risk Reduction, “Sendai Framework for Disaster Risk Reduction 2015-2030” adopted at the Third UN World Conference on Disaster Risk Reduction in Sendai, Japan, March 2015. Terminology updated in 2017: https://www.preventionweb.net/sendai-framework/sendai-framework-for-drr

[4] Dragos. “Improving OT Defense and Response with Consequence-Driven ICS Cybersecurity Scoping.” https://www.dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/

[5] Science for Disaster Risk Management 2017 examines the disaster risk elements from the Sendai Framework in Chapter 2.

[6] Lee, R & Assante, M. 2015. The Industrial Control System Cyber Kill Chain. Bethesda: SANS Institute. https://www.sans.org/reading-room/whitepapers/ICS/paper/36297

[7] ATT&CK for ICS Framework. https://collaborate.mitre.org/attackics

[8] Further examples on how OCTAVE uses threat trees can be found from the Software Engineering Institute: https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=8419

[9] SA–62443-2-1–2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program: https://ww2.isa.org/templates/one-column.aspx?pageid=111294&productId=116731

[10] NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security: https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final

[11] The National Institute for Occupational Safety and Health (NIOSH) has more information about the Hierarchy of Controls here: https://www.cdc.gov/niosh/topics/hierarchy/default.html

[12] The US Department of Energy created a generic version of the Cybersecurity Capability Maturity Model (C2M2), which can be used by any industrial sector leveraging control systems: https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0

[13] Additional information on risk registers in both enterprise risk management (ERM) and cybersecurity can be found in NISTIR 8286: https://csrc.nist.gov/publications/detail/nistir/8286/final

[14] More information about taxonomies can be found from SEI’s Taxonomy of Operational Cyber Security Risks: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=91013

[15] The COBIT Framework, created by the Information Systems Audit and Control Association, can be leveraged for industrial cyber risk, similar to other risk programs. More information about COBIT can be found here: https://www.isaca.org/resources/cobit

[16] ENISA further outlines a generic relationship between risk management and business continuity here: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/bcm-resilience/bc-rm-interfaces

[17] International Organization for Standardization. (2018). Risk management – Guidelines (ISO Standard No. 31000:2018)

[18] International Organization for Standardization. (2018). Information technology — Security techniques — Information security risk management (ISO Standard No. 27005:2018)

DRAGOS

SAFEGUARDING CIVILIZATION

TO LEARN MORE ABOUT HOW DRAGOS CAN HELP YOUR ORGANIZATION DEVELOP YOUR ICS SECURITY CAPABILITIES, VISIT US HERE