# The Converged Defense: A Framework for IT/OT Ransomware Readiness in Energy and Manufacturing

## Executive Summary

The escalating threat of ransomware against industrial sectors represents a fundamental shift in the cyber risk landscape. For energy and manufacturing organizations, these attacks are no longer mere data security incidents; they are direct threats to operational continuity, physical safety, and national security. The deliberate targeting of Operational Technology (OT) aims to disrupt physical processes, creating immense pressure for ransom payments by threatening production stoppages that can cost millions per day. This reality demands a new paradigm for resilience—one that transcends traditional security silos and forges a unified defense across Information Technology (IT) and OT domains.

This report introduces *The Converged Defense Framework*, a comprehensive and pragmatic methodology for establishing ransomware readiness in the energy and manufacturing sectors. It is designed for executive leadership and their teams to navigate the complex technical and cultural challenges of securing modern industrial environments. The framework is built upon three core pillars:

1. **A Standards-Based Foundation:** The framework is anchored in the globally recognized ISA/IEC 62443 series of standards, utilizing its risk-based philosophy and structured assessment processes (Initial and Detailed Risk Assessments) to establish a common language and a rigorous methodology for securing Industrial Automation and Control Systems (IACS).
2. **A Practical, Mediated Diagnostic Process:** The framework begins with a hands-on, collaborative diagnostic workshop using the U.S. Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Security Evaluation Tool (CSET) and its Ransomware Readiness Assessment (RRA) module. This process is guided by a neutral, third-party facilitator whose role is to mediate discussions, build consensus, and help the joint IT and OT teams create a shared, honest baseline of their current capabilities.
3. **A Focus on Cultural and Organizational Alignment:** The framework explicitly acknowledges that the greatest vulnerability in industrial cybersecurity is often the cultural divide between IT and OT teams. It provides actionable strategies, including cross-functional workshops, team alignment exercises, and threat modeling sessions, designed to break down silos, forge a common language of risk, and establish a converged governance model for enterprise-wide security.

By following this step-by-step guide, organizations can move beyond theoretical compliance to build a tangible, tested, and sustainable program for ransomware resilience. The immediate benefits are derived from the collaborative workshops, which uncover critical misalignments and generate quick wins. The long-term value lies in the creation of a continuously improving security program, validated by annual tabletop exercises and measured by business-relevant metrics. This framework reframes the ransomware threat not as an unsolvable technical problem, but as a manageable business risk that, when addressed holistically, strengthens operational resilience and secures the enterprise's core mission.

## Part I: Foundations of Industrial Ransomware Resilience

This section establishes the foundational context for the framework, detailing the evolution of the ransomware threat in industrial environments and introducing the core standards and tools that will be leveraged to build a robust and resilient defense.

### 1.1 The Modern Industrial Threat Landscape: From Data Theft to Physical Disruption

The definition of a ransomware attack—malware that encrypts files for a ransom—is dangerously incomplete in the context of industrial operations. The modern threat landscape has evolved far beyond data theft into a new class of cyber-physical attacks where the primary goal is the disruption of physical processes to exert maximum financial and operational leverage. For asset owners in manufacturing and energy, understanding this paradigm shift is the first and most critical step toward building an effective defense.

The strategic calculus of ransomware in industrial environments fundamentally shifts from data confidentiality to operational continuity. An analysis of major incidents reveals that the primary objective of threat actors is not merely to encrypt files, but to induce a *loss of control* or a *loss of view* over physical processes, thereby maximizing operational disruption and financial leverage. If operators cannot trust their Human-Machine Interfaces (HMIs) or if Programmable Logic Controllers (PLCs) are executing malicious commands, the risk escalates from data loss to potential equipment damage, production halts, environmental incidents, and even threats to human safety. This reframes the threat from a traditional cybersecurity issue to a core operational and safety imperative. The critical metric is no longer just the Recovery Time Objective (RTO) for data, but the "Time to Safe Operations."

Several high-profile attacks serve as stark illustrations of this new reality:

* Case Study: Norsk Hydro (2019)  
  The attack on Norsk Hydro, a global aluminum manufacturer with operations in 40 countries, demonstrates the catastrophic financial impact of an OT-focused ransomware attack. The LockerGoga ransomware variant forced the company to shut down numerous plants and revert to manual operations for weeks. The decision not to pay the ransom did not prevent staggering business losses estimated at around $70 million. The incident highlights how a single compromised email attachment can propagate across a global enterprise, crippling both IT and OT systems and leading to a prolonged and costly recovery.
* Case Study: Colonial Pipeline (2021)  
  This seminal event underscored the profound interconnectedness of IT and OT systems in critical infrastructure. The ransomware attack targeted the company's IT billing and administrative systems. However, the fear that the infection could spread to the OT network controlling the pipeline itself prompted the company to proactively shut down the physical pipeline. This decision led to widespread fuel shortages across the U.S. Southeast, demonstrating how a compromise of IT systems can have a direct and cascading physical impact. The attack revealed that the perception of risk at the IT/OT boundary, managed by human decision-makers, is as critical as the technical controls themselves.
* Case Study: JBS Foods (2021)  
  The attack on the world's largest meat processor was a direct assault on production. The ransomware incident forced the shutdown of multiple meatpacking plants in North America and Australia, halting a significant portion of the world's meat supply. To prevent further disruption and the public leakage of stolen data, JBS ultimately paid an $11 million ransom. The case exemplifies how attackers target industries where downtime is exceptionally costly, knowing that the pressure to resume operations quickly makes a ransom payment more likely.

Statistical evidence confirms that these are not isolated incidents. The manufacturing sector is disproportionately targeted by ransomware groups, accounting for nearly 70% of all industrial ransomware attacks. The financial toll is immense; the median ransom payment in the manufacturing sector is now $500,000, while the average cost to recover from an attack—excluding the ransom itself—often exceeds $1 million. Compounding this, threat actors are accelerating their campaigns, with the average time from initial intrusion to ransomware deployment shrinking to less than four days.

The analysis of these events reveals that the IT/OT boundary is the primary battleground. Initial compromises frequently occur within the more exposed IT network, after which attackers pivot to the OT environment where they can inflict the most significant operational damage and create the greatest leverage. A purely OT-focused security strategy is therefore insufficient. Ransomware readiness must be a converged strategy that treats the IT/OT interface not as a simple firewall, but as a complex, socio-technical system that represents the most probable and impactful attack vector.

### 1.2 Anchoring in Standards: The ISA/IEC 62443 Approach

In the face of such complex threats, a common framework is essential for building a coherent defense. The ISA/IEC 62443 series of standards provides this foundation. It is not a rigid compliance checklist but a strategic, risk-based philosophy for securing Industrial Automation and Control Systems (IACS). Crucially, it is designed to be a holistic framework that bridges the gap between IT and OT, as well as between process safety and cybersecurity, making it the ideal "common language" for a converged defense.

For executive leadership, several core concepts of ISA/IEC 62443 are particularly important:

* **Zones and Conduits:** This is the standard's foundational approach to network segmentation. It involves grouping assets with similar security requirements into logical "zones" and defining the controlled communication channels between them as "conduits". In the context of ransomware, which relies on lateral movement to spread, this model creates defensible "islands." A breach in a less-critical zone (e.g., the enterprise IT network) can be contained and prevented from reaching the high-consequence zones (e.g., the process control network). The process of defining zones and conduits is not merely a technical exercise; it is a governance exercise. It forces the organization to formally map its operational environment and, in doing so, implicitly negotiate the boundaries of responsibility between IT and OT. A conduit between an IT-managed zone and an OT-managed zone becomes a formal interface with a defined risk owner and mutually agreed-upon security controls.
* **Security Levels (SLs):** The standard defines four Security Levels, which provide a powerful way to translate technical security requirements into a business-level discussion about risk appetite. Rather than asking an unanswerable question like "Are we secure?", the SL model asks, "How sophisticated of an attacker do we need to defend against?".
  + **SL 1:** Protection against casual or coincidental violation.
  + **SL 2:** Protection against intentional violation using simple means.
  + **SL 3:** Protection against intentional violation using sophisticated means.
  + SL 4: Protection against intentional violation using advanced means with extended resources.  
    By assigning a Target Security Level (SL-T) to each zone, the organization makes an explicit business decision about its risk tolerance. For example, designating a critical control zone as SL-T 3 acknowledges that the business is accepting the risk of compromise from an SL-4 attacker (e.g., a well-funded nation-state) but has deemed it necessary to defend against sophisticated criminal groups. This transforms security from an open-ended technical problem into a defined business objective.
* **Foundational Requirements (FRs):** These are the seven core security capabilities that an IACS must possess. They include functions like Identification and Authentication Control, Use Control, System Integrity, and Data Confidentiality. The rigor with which these requirements are implemented determines the achieved Security Level (SL-A) of a system or zone.

By adopting this standard, an organization can shift its security conversation from subjective arguments to a structured, risk-based dialogue. It provides a shared vocabulary and a clear methodology for defining security targets and measuring progress toward achieving them.

### 1.3 From Theory to Practice: The 62443 Risk Assessment Lifecycle

ISA/IEC 62443-3-2 outlines a practical, two-phase risk assessment process that operationalizes the standard's philosophy. This lifecycle provides a resource-efficient workflow for identifying, analyzing, and prioritizing ransomware risks in an industrial environment.1

* Phase 1: Initial Risk Assessment (IRA)  
  The IRA (also known as a High-Level Risk Assessment) is designed to rapidly identify the highest-risk areas within the IACS by focusing on the worst-case consequences of a compromise.1 Its methodology simplifies the classic risk equation (  
  Risk=Consequence×Likelihood) by making a critical assumption: **Likelihood is treated as 1**.1 This forces the assessment team to temporarily set aside debates about the probability of an attack and focus entirely on the potential impact.  
  This "Likelihood = 1" assumption is a powerful tool for bridging the IT/OT divide. IT teams are often focused on threat actor capabilities and attack probabilities, while OT teams find these discussions abstract and prefer to focus on credible process failure modes. By assuming the attack *will* happen, the IRA directs the conversation to a topic where both teams have deep and complementary expertise: consequence. The plant engineer can precisely articulate the operational, financial, and safety impact of a specific controller failing, while the IT security analyst can map that impact back to the broader enterprise risk posture.  
  When adapted for ransomware, the IRA process involves assuming that each critical OT asset (e.g., an HMI, an Engineering Workstation, a process historian) is successfully encrypted or maliciously controlled. The team then evaluates the consequences, quickly surfacing the operational "crown jewels" that must be protected at all costs.
* Phase 2: Detailed Risk Assessment (DRA)  
  Following the IRA, the DRA provides a more granular analysis of the high-risk zones and assets that were identified.1 In this phase, the concepts of  
  **Likelihood** and existing **Countermeasures** are reintroduced. The DRA involves a systematic examination of credible threat vectors (e.g., phishing, insecure remote access, supply chain compromise), system vulnerabilities (e.g., unpatched operating systems, weak configurations), and the effectiveness of any security controls already in place.1  
  For ransomware, the DRA would model specific Tactics, Techniques, and Procedures (TTPs) against the high-risk zones. For example, for a zone containing critical Engineering Workstations, the DRA would analyze the likelihood of a phishing email leading to credential compromise, the vulnerabilities present on the workstations, and the effectiveness of countermeasures such as endpoint detection and response (EDR), application whitelisting, network segmentation, and backup and recovery procedures.3

This two-phase approach creates an efficient feedback loop. The IRA prevents "analysis paralysis" by focusing the expensive and time-consuming DRA only on the areas of greatest concern. The findings from the DRA then inform the refinement of the Zone and Conduit architecture and the specific security requirements needed to achieve the target Security Levels, allowing for a continuous, iterative cycle of risk management.

### 1.4 Establishing a Baseline: The CISA Ransomware Readiness Assessment (RRA)

While the ISA/IEC 62443 risk assessment provides the formal methodology, a practical starting point is needed to ground the process in the organization's current reality. The CISA Cyber Security Evaluation Tool (CSET) and its specific Ransomware Readiness Assessment (RRA) module serve this purpose perfectly.4

CSET is a free, stand-alone desktop application provided by CISA that guides organizations through a systematic evaluation of their IT and OT security practices. The RRA is a purpose-built module within CSET designed as a self-assessment to help organizations gauge their specific readiness to defend against and recover from a ransomware incident.

The RRA's structure is one of its key strengths. It organizes its questions into a tiered progression of practices categorized as **Basic, Intermediate, and Advanced**. This allows organizations of all maturity levels to assess their posture and develop a logical, phased improvement plan, ensuring foundational controls are in place before moving to more advanced capabilities. Upon completion, the tool generates an analysis dashboard with graphs and tables that provide both a high-level summary and a detailed breakdown of strengths and weaknesses.

Within this framework, the RRA's primary value is not as a solitary audit tool but as a *mediated diagnostic tool*. The questionnaire becomes the structured agenda for an initial, facilitated workshop involving both IT and OT stakeholders. A facilitator guides the joint team through each question, forcing a discussion and a consensus on a single, honest answer for the organization as a whole. This process is invaluable for uncovering misalignments and knowledge gaps. For example, when asked about offline backups, the IT team may confidently answer "Yes," only for an OT engineer to point out that the critical PLC configurations are not included in the IT-managed backup scope.

By starting with this facilitated RRA, the organization achieves two critical objectives. First, it creates a unified, consensus-based snapshot of the current state that is owned by all stakeholders. Second, it democratizes the risk assessment process. The subsequent, more technical ISA/IEC 62443 analysis is grounded in a reality that has been co-created and validated by the very people who operate and maintain the industrial environment. This ensures buy-in from the outset and makes the final recommendations far more likely to be accepted and implemented.

## Part II: Bridging the Great Divide - Unifying IT and OT Cultures

The most sophisticated technical controls will fail if the people and processes meant to manage them are misaligned. The cultural and operational divide between Information Technology (IT) and Operational Technology (OT) teams is one of the most significant and persistent challenges in industrial cybersecurity. This section deconstructs the root causes of this conflict and provides actionable strategies for building the unified culture necessary for a converged defense.

### 2.1 Different Worlds, Shared Mission: Deconstructing the IT/OT Conflict

The friction between IT and OT teams is not a result of incompetence or intransigence, but rather a logical outcome of two distinct professional cultures that have evolved to optimize for fundamentally different environments and objectives.7 Understanding and respecting these differences is the prerequisite for bridging the divide.

* **Conflicting Priorities:** The core of the conflict lies in their foundational priorities. The IT world is governed by the "CIA Triad": Confidentiality, Integrity, and Availability. The primary mission is to protect data. In the OT world, the paramount priorities are Safety and continuous Uptime. The mission is to protect physical processes and people. This leads to dramatically different perspectives. For IT, a server becoming temporarily unavailable is an inconvenience; for OT, a controller becoming unavailable can mean a production shutdown costing millions of dollars per hour or, in the worst case, a hazardous event.
* **Divergent Risk Perceptions:** These differing priorities shape how each team perceives and manages risk. IT security professionals manage risk by embracing change; they perform frequent vulnerability scans, apply patches as soon as they are available, and regularly update systems to defend against the latest threats. OT engineers, conversely, manage risk by *resisting* change. For them, an unscheduled modification to a running system is a primary source of operational risk. The engineering mantra is "if it isn't broken, don't fix it," leading to a preference for maintaining stable, proven systems, even if they are technologically obsolete. An unpatched but stable controller is often seen as less risky than a newly patched one that has not undergone extensive regression testing.
* **Vastly Different Technology Lifecycles:** IT environments are characterized by rapid evolution, with hardware and software lifecycles typically lasting 3-5 years. OT systems, such as PLCs and Distributed Control Systems (DCS), are engineered for longevity and reliability, often remaining in service for 20 to 30 years. This results in a widespread prevalence of legacy systems running on unsupported operating systems like Windows XP or NT, which cannot be easily patched or secured with modern tools like EDR.
* **Communication Gaps and Jargon:** The two disciplines speak different languages. An IT professional's "vulnerability scan" is a prudent security measure. To an OT engineer, it is a potentially dangerous action that could generate unexpected network traffic and crash a delicate PLC. This linguistic and conceptual gap breeds misunderstanding and mistrust, hindering effective collaboration.
* **Ambiguous Organizational Ownership:** Historically, OT systems were the exclusive domain of engineering and plant operations. As these systems have become networked, the responsibility for their security has become ambiguous. Often, corporate CISOs are given accountability for OT security without the requisite engineering knowledge or credibility on the plant floor. Conversely, plant managers who own the operational risk often lack the cybersecurity expertise to manage it effectively. This leads to a dangerous vacuum of clear ownership and governance.

This cultural conflict creates a perfect vulnerability for ransomware adversaries. Attackers exploit the characteristics of both domains: they leverage the openness and connectivity of the IT environment to gain initial access, then pivot into the OT environment, where the static, legacy, and often unmonitored systems provide a fertile ground for persistence and causing maximum operational impact. The very factors that create the cultural divide also create the ideal conditions for a successful cross-domain attack.

### 2.2 Forging a Common Language: A Lexicon for Converged Risk

To overcome these deep-seated divisions, IT and OT teams must develop a shared vocabulary for discussing risk. This new lexicon must move away from domain-specific jargon and focus on terms that are meaningful to both engineers and IT professionals, ultimately translating technical issues into their tangible business impact.

The most effective common language is the language of business. Both the plant manager and the CIO are accountable for contributing to the organization's core mission. By framing security discussions around shared business objectives—such as production uptime, product quality, worker safety, and regulatory compliance—both sides can align on the priority of a risk, even if they approach the technical solution from different perspectives. A conversation about a specific vulnerability should not be about the CVE score, but about the potential cost of a production line shutdown that the vulnerability could enable.

Several strategies can help forge this common language:

* **Frame Security in Engineering Terms:** Engineers are trained in systems thinking, risk analysis, and understanding interconnected processes. Security initiatives should be presented in this context. For example, instead of discussing malware TTPs, the conversation can be about how a cyber event could cause a process deviation, trip a safety system, or result in an out-of-spec product.
* **Translate Controls into Operational Benefits:** The "why" behind a security control must be articulated in terms of operational resilience. "Network segmentation" is IT jargon. "Creating isolated zones to ensure a ransomware attack on the corporate email server cannot shut down the main boiler" is an operational benefit that an engineer can understand and support.
* **Use Standards as a Neutral Framework:** As established, standards like ISA/IEC 62443 and diagnostic tools like the CSET RRA provide a structured, neutral vocabulary (e.g., Zones, Conduits, Security Levels, Basic/Intermediate/Advanced practices) that can be formally adopted as the common lexicon for the security program.
* **Mandate Cross-Functional Training:** Organizations must invest in joint training programs. IT security staff should receive basic training on industrial processes, control systems, and the paramount importance of safety. OT engineers and operators should receive training on fundamental cybersecurity threats, such as phishing and social engineering, and their specific responsibilities in the security program. This shared education builds mutual empathy and respect.

To facilitate this translation, a practical tool can be employed during workshops and team meetings. The following matrix provides examples of how to reframe common IT security concepts into a converged language focused on business impact.

| IT Term | IT Interpretation | OT Interpretation | Converged Language (Business Impact) |
| --- | --- | --- | --- |
| **Vulnerability Scanning** | Proactive security hygiene to find flaws. | A dangerous process that can crash sensitive PLCs. | **System Health Check:** A carefully scheduled, non-intrusive process to identify weaknesses that could lead to downtime. |
| **Patch Management** | A routine, critical process to reduce risk. | A high-risk, planned outage that can introduce instability. | **System Modernization:** A managed lifecycle program to ensure critical systems are resilient against known failure modes. |
| **Incident Response** | Isolate, eradicate, recover data. | Maintain safe operations at all costs, even if it means losing forensic data. | **Operational Resilience Plan:** A unified plan that prioritizes worker safety, then process stability, then forensic investigation. |
| **Zero Trust** | Assume breach; verify everything. | How can I do that on a 30-year-old PLC? | **Controlled Access:** Ensuring only authorized people and devices can communicate with critical systems, using compensating controls for legacy assets. |

### 2.3 The Principles of Converged Governance

A shared language is a necessary but insufficient condition for success. It must be supported by a formal, converged governance structure that establishes clear ownership, roles, and responsibilities for OT security, elevating it from a niche technical issue to a C-level strategic priority.

The historical ambiguity of OT security ownership, caught in the void between engineering and IT, is a critical vulnerability that must be resolved. A mature OT security program requires unambiguous executive support and a well-defined governance model. The Board of Directors and C-suite must be actively engaged in discussions about the business risks posed by OT cyber threats, as these now represent a direct threat to revenue, brand reputation, and shareholder value.

This requires an evolution of the CISO's role. The Chief *Information* Security Officer must become a Chief *Enterprise Risk* Security Officer, with a mandate that covers the security of both the digital and physical realms of the organization. To be effective, the CISO must build credibility with engineering leadership and be capable of translating OT cyber risk into metrics that are meaningful to the board.

Given the distributed nature of manufacturing and energy operations, a purely centralized, top-down security model imposed by corporate IT is unlikely to succeed. Each plant or facility often has unique systems, processes, and risk tolerances. A more effective approach is a **federated governance model** that balances central oversight with local execution. In this model:

* **The Central CISO Organization:** Sets the enterprise-wide OT security policy and standards (based on ISA/IEC 62443), manages the overall risk register, provides shared services (such as a Security Operations Center with OT expertise and an enterprise-wide incident response team), and secures funding for major initiatives.
* **The Plant/Facility Leadership (e.g., Plant Manager):** Retains ultimate accountability for the operational risk within their facility, including cyber risk. They are responsible for ensuring local implementation of corporate policies and for funding site-specific security controls.
* **The OT Security Liaison:** A designated role at each major facility (or for a region) who acts as the bridge between the central CISO team and local OT engineering. This individual, often an engineer with a passion for security, is trained by the central team and is responsible for overseeing the implementation of security controls, conducting local risk assessments, and acting as the point person during an incident.

This federated structure respects local operational autonomy while ensuring a consistent standard of security and governance across the enterprise, creating a scalable and sustainable model for managing converged IT/OT risk.

## Part III: The Mediated Readiness Framework - A Step-by-Step Implementation Guide

This section provides the practical, step-by-step methodology for implementing the Converged Defense Framework. It is a phased approach centered on a series of facilitated workshops designed to build consensus, identify risks, and develop an actionable roadmap for improving ransomware readiness.

### 3.1 Phase 1: Preparation and Alignment

Thorough preparation is the foundation upon which the entire framework is built. This initial phase is dedicated to securing the necessary buy-in, assembling the right team, and establishing the rules of engagement to ensure the subsequent workshops are productive and successful.

1. **Secure Executive Sponsorship:** The initiative must begin with clear and visible sponsorship from the highest levels of both the IT and OT organizations (e.g., the Chief Information Officer and the Chief Operating Officer or equivalent). The project must be framed not as a technical security audit, but as a critical business resilience initiative designed to protect operational continuity and revenue. This top-level support is essential for securing resources and ensuring cross-departmental cooperation.
2. **Select the Third-Party Facilitator:** The choice of facilitator is one of the most critical decisions in the process. The ideal candidate is not necessarily a deep technical expert in IT or OT security. Instead, the primary qualifications are expertise in facilitation, mediation, and conflict resolution. The facilitator's role is to be a neutral guide for the process—to create an environment of psychological safety, ensure all voices are heard, manage disagreements constructively, and steer the group toward consensus. Their neutrality is paramount for bridging the inherent trust gap between the IT and OT teams. An external facilitator is often more effective as they are free from internal biases and organizational politics.
3. **Form the Cross-Functional Working Group:** The success of the workshops depends on having the right people in the room. The working group must be a true cross-section of stakeholders with deep knowledge of their respective domains. The core team should include:
   * **From IT:** IT Security Analysts, Network Architects, Server/Infrastructure Administrators.
   * **From OT:** Control Systems Engineers (ICS/SCADA), Plant Managers or Operations Supervisors, Maintenance Technicians, Process Safety Engineers.
   * Leadership: Representatives from both IT and OT management to provide context and authority.  
     This diverse group ensures that discussions are grounded in both security best practices and operational reality.
4. **Conduct the Kick-off Meeting:** The facilitator leads an initial kick-off meeting with the assembled working group. The agenda for this meeting is to:
   * Clearly define the project's goals, scope, and timeline.
   * Have the executive sponsors reiterate their commitment to the process.
   * Most importantly, facilitate the co-creation of a **"Team Agreement"** or charter. This is a simple but powerful exercise where the group itself defines the ground rules for how they will interact, make decisions, and handle disagreements throughout the process. This act of co-creation builds ownership and sets a collaborative tone from the outset.

### 3.2 Phase 2: The Diagnostic Workshop - The Facilitated RRA Session

This is the first major hands-on exercise of the framework. It typically takes the form of a one- or two-day, in-person workshop where the facilitator guides the cross-functional working group through the CISA CSET Ransomware Readiness Assessment (RRA). The objective is not merely to complete the questionnaire, but to use it as a tool to spark dialogue and build a shared, consensus-based understanding of the organization's current state.

The workshop process is as follows:

* **Setup:** The workshop requires a dedicated room with a large screen to display the CSET application, along with ample whiteboard space and facilitation supplies (e.g., sticky notes, markers).
* **The Facilitated Assessment:** The facilitator projects the CSET RRA interface and proceeds through the questionnaire, question by question. For each question (e.g., "Are backups for critical OT systems stored offline and tested regularly?"), the facilitator opens the floor for discussion.
* **Building Consensus:** Members from IT and OT provide their perspectives. The IT team might describe the corporate backup policy, while the OT team provides the on-the-ground reality of which systems are or are not covered. The facilitator's role is to guide this discussion, asking clarifying questions and ensuring the team arrives at a single, honest answer ("Yes," "No," "Partially Implemented," etc.) that reflects the true state of the organization. The goal is accuracy, not achieving a "good score." All disagreements are surfaced and talked through until a consensus is reached.
* **Rich Documentation:** A designated scribe captures not only the final consensus answer for each question but also the key points of the discussion, including areas of disagreement and specific examples provided by the team. This qualitative data is often more valuable than the quantitative score itself, as it provides the context behind the gaps.

This process delivers immediate benefits by forcing conversations that would otherwise never happen. It systematically uncovers disconnects between policy and practice, and between IT's perception and OT's reality. For instance, IT may believe a corporate incident response plan covers the entire enterprise, while OT may reveal that it is unworkable on the plant floor due to safety protocols or a lack of appropriate communication channels.

The following sample agenda provides a template for structuring this critical workshop.

| Day 1 | Topic | Objective | Facilitation Techniques |
| --- | --- | --- | --- |
| **Morning** | **Session 1: Kick-off & Alignment** | Establish goals, roles, and rules of engagement. Build psychological safety. | Icebreakers (e.g., 3 Question Mingle), Team Agreement Creation. |
|  | **Session 2: RRA Introduction & Domain 1 (Asset Management)** | Introduce the CSET RRA tool. Begin the assessment process on a foundational topic. | Facilitated Q&A, Consensus building (e.g., Roman Voting for quick checks). |
| **Afternoon** | **Session 3: RRA Domain 2 & 3 (Controls & Access, Vulnerability Mgmt)** | Continue assessment, focusing on areas of likely IT/OT disagreement. | Active Listening exercises, Paraphrasing to ensure understanding. |
|  | **Session 4: Day 1 Debrief** | Summarize findings, identify emerging themes, and check in on team dynamics. | Plus/Delta, Dot Voting on key challenges. |
| **Day 2** | **Topic** | **Objective** | **Facilitation Techniques** |
| **Morning** | **Session 5: RRA Domain 4 & 5 (Protective Tech, Incident Response)** | Assess technical controls and response planning. | Scenario-based questions ("What would we do if..."), Whiteboarding response flows. |
| **Afternoon** | **Session 6: RRA Domain 6-10 (Recovery, Testing, etc.)** | Complete the RRA questionnaire. | Energizers, small group breakouts to discuss complex topics before plenary discussion. |
|  | **Session 7: Initial Results Review & Workshop Close-out** | Review the CSET dashboard results. Agree on next steps for Phase 3. | Affinity Mapping of key weaknesses, Action planning. |

### 3.3 Phase 3: The Risk Correlation Workshop - Mapping RRA Gaps to 62443 Risk

Following the diagnostic workshop, this phase translates the practical, consensus-based findings from the RRA into the formal risk management language of ISA/IEC 62443. This crucial step connects the "what" (the identified readiness gaps) with the "so what" (the specific operational risks and the required level of protection).

The primary input for this workshop is the completed CSET RRA report, including the detailed notes from the Phase 2 discussion. The facilitator leads the team through the following process:

1. **Identify Critical Gaps:** The team reviews the RRA results to identify the areas with the lowest scores, the most significant "No" answers, or the most contentious discussions. These represent the organization's most pressing weaknesses in ransomware readiness.
2. **Conduct a Simplified IRA:** For each critical gap, the team performs a targeted Initial Risk Assessment (IRA) as defined in ISA/IEC 62443-3-2.1
   * **Example:** Suppose a critical gap identified in the RRA was the lack of tested, offline backups for OT systems.
   * **Asset Identification:** The team identifies the specific critical assets affected by this gap (e.g., the PLCs and HMIs for the primary production line).
   * **Consequence Analysis:** Applying the IRA's "Likelihood = 1" principle, the team assumes these assets are irretrievably lost in a ransomware attack. The OT engineers then describe the worst-case consequence: "The entire plant would be down for an estimated three weeks while we wait for the vendor to fly in and reprogram the controllers from scratch. This would result in $15 million in lost revenue and potential contractual penalties from our key customers."
3. **Define Target Security Levels (SL-T):** Based on the severity of the identified consequence, the team assigns a Target Security Level (SL-T) to the zone containing those assets. A catastrophic financial or safety impact warrants a high SL-T (e.g., SL-3 or SL-4), indicating the need for protection against sophisticated and highly motivated attackers.

The output of this workshop is a prioritized list of high-risk zones and conduits. Each item on the list is now enriched with a clear, business-focused consequence statement and a formally defined SL-T. This document provides the direct input and justification for the subsequent Detailed Risk Assessment and roadmap development. This mapping process makes the abstract concepts of ISA/IEC 62443 tangible. An OT engineer may not intuitively grasp the meaning of "SL-3," but through this exercise, it becomes directly linked to preventing a specific, catastrophic $15 million outage that they themselves described.

### 3.4 Phase 4: The Threat Modeling Workshop - From Gaps to Scenarios

With the high-risk "crown jewel" zones identified and their required protection levels defined, this workshop shifts the focus from "what are we protecting?" to "*how* would an attacker compromise it?". This is a proactive and creative exercise designed to brainstorm credible attack scenarios, which will inform the development of specific and effective security controls.

This workshop uses a collaborative threat modeling methodology that is accessible to a mixed IT/OT audience. While several methodologies exist, **STRIDE** is an excellent choice for this context. It is a mnemonic for six categories of threats (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege) that provides a simple yet comprehensive framework for structured brainstorming. For more OT-specific tactics, the facilitator can also reference the **MITRE ATT&CK for ICS** framework.

The process is as follows:

1. **Select a Target:** The facilitator chooses a high-risk zone identified in Phase 3, for example, the "Process Control Engineering Zone" which contains the Engineering Workstations.
2. **Model the System:** The team collaboratively draws a simple data flow diagram (DFD) of the target system on a whiteboard, showing the key components, data flows, and trust boundaries.
3. **Brainstorm Threats using STRIDE:** Using the STRIDE mnemonic as a prompt, the facilitator guides the team in brainstorming potential attacks. The power of this exercise comes from the convergence of IT and OT perspectives.
   * **Spoofing:** IT security can describe how a phishing email could be crafted to look like it's from a PLC vendor. OT engineering can confirm which vendors they work with and what kind of information would make such an email look legitimate.
   * **Tampering:** IT can explain how malware could modify files on the workstation. OT can identify the specific PLC logic file that, if subtly altered, could cause the most dangerous physical malfunction (e.g., disabling a safety interlock or over-pressurizing a vessel).
   * **Denial of Service:** IT can describe how ransomware encrypts a hard drive. OT can describe the cascading operational impact when the Engineering Workstation is unavailable during a plant upset, preventing engineers from troubleshooting the problem.

This collaborative process produces a rich list of credible, context-specific threat scenarios. These scenarios are invaluable inputs for the Detailed Risk Assessment and for designing "fit-for-purpose" security controls that address the most likely and most impactful attack paths.

| STRIDE Threat | IT Team's Primary Contribution | OT Team's Primary Contribution |
| --- | --- | --- |
| **Spoofing** | How attackers impersonate users/devices (phishing, ARP spoofing). | Which user roles (e.g., maintenance engineer) have the most critical access. |
| **Tampering** | How data can be altered in transit or at rest (malware, man-in-the-middle). | Which specific data points or logic files, if altered, would cause the most severe physical consequence. |
| **Repudiation** | The importance of non-repudiable logs for forensic investigation. | The operational reality of shared logins on HMIs and the difficulty of implementing individual accounts. |
| **Information Disclosure** | What constitutes sensitive data (PII, credentials) and how it's exfiltrated. | What constitutes sensitive process information (e.g., recipes, setpoints, network diagrams). |
| **Denial of Service** | How network or host-based DoS attacks are executed. | The cascading operational impact of a single critical device becoming unavailable. |
| **Elevation of Privilege** | How attackers move from user to admin privileges on a Windows host. | How an attacker with engineer-level access could impact safety-instrumented systems. |

### 3.5 Phase 5: The Roadmap Development Workshop - Building the Action Plan

This final workshop in the series is where all the preceding work is synthesized into a prioritized, actionable, and resourced strategic plan. The goal is to move from analysis to action, creating a formal Ransomware Readiness Roadmap that will be presented to executive leadership for approval and funding.

The inputs for this workshop are the consolidated outputs from all previous phases: the CSET RRA report highlighting capability gaps, the prioritized list of high-risk zones with their associated business consequences and SL-Ts, and the list of credible threat scenarios from the threat modeling session.

The workshop follows these steps:

1. **Brainstorm Countermeasures:** The team reviews the top-priority risks (e.g., "Ransomware on Engineering Workstations leading to production halt"). For each risk, the group brainstorms a list of potential countermeasures or mitigation activities. These should span people, process, and technology, and could include:
   * **Technical Controls:** Implement EDR and application whitelisting on workstations; create a secure, segmented network zone for engineering assets; implement a secure remote access solution with MFA.
   * **Procedural Controls:** Develop a formal OT patch management policy that balances security needs with operational stability requirements; create and test an OT-specific incident response playbook.
   * **People Controls:** Conduct targeted phishing awareness training for all control system engineers and operators.
2. **Prioritize Initiatives:** The list of potential countermeasures can be long. The team must prioritize them to create a realistic, phased roadmap. A simple but effective method is to plot each initiative on a 2x2 matrix of **Impact** (how much it reduces risk) vs. **Effort** (cost and complexity to implement). Initiatives in the "High Impact, Low Effort" quadrant become the immediate priorities. Facilitation techniques like **Dot Voting** can be used to quickly achieve group consensus on the relative priority of each item. The prioritization should also align with the RRA's tiered structure, ensuring that foundational "Basic" gaps are addressed before moving to more advanced controls.
3. **Develop the Roadmap:** The prioritized initiatives are then organized into a formal roadmap, typically structured with short-term (e.g., 0-6 months), mid-term (e.g., 6-18 months), and long-term (e.g., 18+ months) timelines. For each initiative, the roadmap should clearly define:
   * A clear description of the work.
   * The business risk it mitigates.
   * A designated owner (a specific individual, not a department).
   * An estimate of the required resources (budget, personnel).
   * Key success metrics.

This final document is the culmination of the entire mediated process. Because it was built with consensus from all key stakeholders, it carries significant weight and is far more likely to be approved, funded, and successfully implemented.

## Part IV: Industry-Specific Roadmaps and Challenges

While the Converged Defense Framework provides a universal methodology, its application must be tailored to the unique operational realities, technologies, and risk profiles of different industrial sectors. This section adapts the framework for the specific challenges of distributed manufacturing and the complex energy sector.

### 4.1 Framework for Distributed Manufacturing

The manufacturing sector faces a unique "perfect storm" of cybersecurity challenges. Rapid digital transformation and the push toward "smart factories" are merging modern IT and IoT infrastructures with legacy OT environments that were never designed for connectivity. This is occurring across a landscape of geographically dispersed plants, each with its own unique equipment, processes, and leadership, making centralized security governance exceptionally difficult.

* **Primary Challenge: Legacy Systems and Technical Debt:** Many factories rely on critical control systems that are decades old, running on unsupported operating systems like Windows XP. These systems are often "black boxes" from vendors who may no longer be in business. They cannot be easily patched, updated, or have modern security software like EDR installed without significant risk of causing an operational failure.
* **Primary Challenge: Distributed and Heterogeneous Operations:** A large manufacturer may operate dozens of plants globally. Each plant can have different production lines, different generations of equipment from various vendors, and a different plant manager with their own budget and priorities. This heterogeneity makes it impossible to apply a one-size-fits-all security solution.

**Applying the Framework to Manufacturing:**

The roadmap for a distributed manufacturing organization must prioritize solutions that can scale across this complex environment and address the legacy system problem without disrupting production.

1. **Prioritize Centralized Visibility and Decentralized Control:** The first step is to answer the fundamental question: "What do we have?" The roadmap must prioritize the deployment of technologies and processes to build and maintain a comprehensive asset inventory across all plants. Given the sensitivity of OT networks, this should be achieved primarily through **passive network monitoring tools** that can identify and profile assets without intrusive scanning. This creates a centralized view of assets and vulnerabilities for the corporate security team, while allowing local plant teams to manage their own environments.
2. **Focus on Compensating Controls for Legacy Systems:** Since directly hardening legacy systems is often not feasible, the strategy must be to "wrap" them in layers of protective controls. This makes the ISA/IEC 62443 model of **Zones and Conduits** the single most important architectural principle. The roadmap must focus on:
   * **Aggressive Network Segmentation:** Isolating critical legacy systems into their own highly restricted network zones to prevent ransomware from spreading to them.
   * **Hardening the Conduits:** Implementing strict firewall rules, intrusion detection systems, and continuous monitoring on the communication paths that connect these legacy zones to the rest of the network.
3. **Develop a "Plant Security Playbook" and a Scalable Rollout Model:** The 5-phase workshop process should be conducted at a representative "model" plant. The detailed roadmap developed for this plant becomes the basis for a standardized but customizable **Plant Security Playbook**. A central corporate team can then act as internal consultants, helping to roll out this playbook to other sites. Each site will have a designated **OT Security Liaison** who leads the local implementation, adapting the playbook to their specific environment. This federated approach allows for consistent security standards while respecting local operational autonomy.

A critical "quick win" for distributed manufacturing often lies not in a complex technology deployment, but in a new, rigorously enforced policy for **secure remote access**. External remote services used by equipment vendors and system integrators for support are a primary initial access vector for attackers. These connections are often poorly managed, using shared credentials, persistent connections, or insecure protocols. Implementing a centralized, secure remote access solution that enforces multi-factor authentication, uses jump servers as intermediaries, and provides time-limited, audited, and supervised sessions can dramatically reduce the attack surface across all plants with a relatively low investment.

### 4.2 Framework for the Energy Sector

The defining characteristic of the energy sector is its nature as critical national infrastructure, underpinned by a vast, deeply interconnected, and global supply chain. For energy companies, ransomware readiness is inextricably linked to cyber supply chain risk management (C-SCRM). An attack on a single, critical supplier can have cascading effects across the entire grid or fuel distribution network.

* **Primary Challenge: Extreme Supply Chain Complexity and Interdependence:** The energy sector is an intricate web of dependencies. A single piece of critical equipment, like a transformer or a turbine controller, may contain hardware and software subcomponents from hundreds of different global manufacturers. The transition to clean energy and smart grid technologies is further increasing this complexity, introducing new digital components and vendors into the ecosystem.
* **Primary Challenge: Supplier Vulnerabilities as a Primary Attack Vector:** Threat actors are increasingly targeting the supply chain as the path of least resistance. Suppliers are often smaller and have less mature cybersecurity programs than the large asset owners they serve, making them attractive targets. A staggering **45% of cybersecurity breaches in the energy sector originate with third-party vendors**, a figure significantly higher than the 29% average across all other industries. A compromised software update, a malicious firmware implant, or a stolen credential from a vendor can provide a "backdoor" into the most sensitive parts of the nation's energy infrastructure.
* **Primary Challenge: Lack of Visibility and Transparency:** Energy companies have very limited visibility into the security practices of their suppliers' suppliers (the "fourth-party" risk). Furthermore, a culture of non-disclosure can exist, where suppliers may hide a breach for fear of damaging their business relationships or facing contractual penalties, leaving their customers unknowingly exposed.

**Applying the Framework to the Energy Sector:**

The ransomware readiness roadmap for an energy organization must be fundamentally a supply chain security roadmap.

1. **Embed Cybersecurity into Procurement and Legal Contracts:** Security can no longer be an afterthought. The roadmap must drive the integration of specific cybersecurity requirements into the entire procurement lifecycle, from Request for Proposal (RFP) to contract execution and renewal. Key contractual requirements should include:
   * The mandatory provision of a **Software Bill of Materials (SBOM)** for all procured software and firmware, providing a detailed inventory of all components and libraries.
   * The right to conduct security assessments and audits of the supplier's development and operational environments.
   * Strict requirements for timely vulnerability disclosure and incident reporting.
2. **Implement a Tiered Vendor Risk Management Program:** Not all suppliers pose the same level of risk. The roadmap must establish a process for categorizing vendors based on factors like their level of access to sensitive networks and data, and the criticality of the product or service they provide. High-risk vendors (e.g., the provider of the SCADA or Energy Management System) must undergo in-depth assessments, including on-site reviews and penetration tests. Lower-risk vendors might only require a completed self-assessment questionnaire.
3. **Leverage the Framework for Collaborative Supplier Assurance:** The 5-phase workshop methodology can be extended beyond the organization's internal teams to include critical suppliers. Joint threat modeling workshops can be conducted with key partners to identify shared risks in the interfaces between systems. The CSET RRA can be adapted into a standardized supplier assessment questionnaire to create a consistent baseline for evaluating vendor readiness.

Ultimately, in a sector as interconnected as energy, no single organization can achieve resilience in isolation. The security of the grid is only as strong as its weakest link. Therefore, the long-term goal of the framework must be to foster a "defend-as-one" ecosystem. This means large asset owners should view it as a strategic imperative to help uplift the security posture of their smaller, less mature suppliers. The roadmap should include initiatives for active participation in industry Information Sharing and Analysis Centers (ISACs), sharing threat intelligence, and developing and distributing security best practice guides to the broader supply chain community. This transforms C-SCRM from a compliance exercise into a program of collective defense.

## Part V: Sustaining Momentum - From Project to Program

Completing the initial workshops and developing a roadmap are significant achievements, but they are only the beginning. Ransomware readiness is not a one-time project that can be checked off a list; it is a continuous program that must be managed, measured, and improved over time. This final section outlines the key elements required to sustain momentum and embed the Converged Defense Framework into the organization's operational DNA.

### 5.1 Metrics and Executive Reporting

To maintain long-term executive support and secure ongoing funding, the progress and value of the OT security program must be communicated in the language of the business. Technical metrics, while important for practitioners, are often meaningless in the boardroom. The program must translate its activities into clear, business-relevant metrics that demonstrate risk reduction and improved resilience.

* **Shift from Technical to Business-Oriented Metrics:** Instead of reporting on the "number of vulnerabilities patched," the program should report on the "percentage reduction in risk to critical production lines." Instead of "firewall rules implemented," the metric should be "number of critical control zones successfully isolated from the corporate network."
* **Leverage the RRA as a Strategic Scorecard:** The CISA CSET RRA provides a powerful and intuitive tool for tracking progress over time. The initial assessment conducted in Phase 2 establishes a quantitative baseline score across the Basic, Intermediate, and Advanced categories. Subsequent annual or biennial assessments can be used to measure and report on the percentage of improvement in each category. This provides a simple, visual, and compelling way to demonstrate the program's impact to executive leadership and the board.
* **Structure of Executive Reports:** Regular reports to management should be concise and impact-focused. A recommended structure includes:
  1. An **Executive Summary** highlighting key achievements and the current risk posture.
  2. A **Dashboard of Key Metrics**, including the RRA scorecard and trends in risk reduction for the top 5 critical systems.
  3. A **Summary of Major Risks Mitigated** during the reporting period.
  4. A **Forward-Looking View** of emerging threats and the resources required for the next phase of the roadmap.

### 5.2 The Annual Cadence: Ransomware Tabletop Exercises (TTX)

A plan that has not been tested is merely a theory. The most effective way to validate incident response plans, uncover hidden gaps in process, and build "muscle memory" for a crisis is through a regular, facilitated tabletop exercise (TTX). This should be an annual capstone event for the OT security program.

A TTX is a simulated, discussion-based exercise where key stakeholders are gathered to walk through a realistic ransomware attack scenario in a safe, controlled environment. The goal is not to test technical controls, but to test the organization's decision-making, communication, and coordination processes under pressure.

* **Participants:** The TTX must involve the same cross-functional group from the initial workshops (IT, OT, leadership), expanded to include representatives from Legal, Corporate Communications, Human Resources, and potentially key third-party incident response partners.
* **Facilitator's Role:** A skilled facilitator is crucial. They present the initial scenario and then introduce a series of pre-scripted "injects" throughout the exercise. These injects are designed to escalate the crisis, introduce new complexities (e.g., a data leak, media inquiries, a compromised backup), and force the team to make difficult decisions with incomplete information.8
* **Output:** The primary output of the TTX is a formal **After-Action Report**. This document, prepared by the facilitator and observers, captures what went well, what challenges were encountered, and provides a list of concrete, actionable recommendations for improving the incident response plan, communication protocols, and decision-making authorities.

The following table provides sample, industry-specific injects that could be used in a ransomware TTX to test the unique challenges of each sector.

| Time | Manufacturing Scenario Inject | Energy Scenario Inject |
| --- | --- | --- |
| **08:00** | **Initial Incident:** Operators at Plant A report the HMI for Production Line 1 is frozen, displaying a ransom note. | **Initial Incident:** The corporate SOC detects anomalous outbound traffic from a third-party vendor's remote access server in the network DMZ. |
| **09:30** | **Escalation:** The IT team confirms ransomware on the Engineering Workstation. The plant manager wants to disconnect the entire plant from the corporate network. The CISO is concerned about losing the ability to investigate. **Decision Point:** Do you disconnect? | **Escalation:** The vendor confirms they have been hit by ransomware. Your SCADA system vendor reports that the compromised third party provides a software component used in their HMI product. **Decision Point:** Do you revoke the SCADA vendor's access? |
| **11:00** | **Business Impact:** Corporate logistics reports that just-in-time deliveries to a major auto manufacturer will be missed within 24 hours, triggering massive contractual penalties. **Decision Point:** Who communicates with the customer? | **Public Impact:** A local news station calls, asking for comment on a rumor that your grid control systems have been compromised by a foreign actor. The rumor started on social media. **Decision Point:** What is the public statement? |
| **13:00** | **Recovery Challenge:** The IT team reports the local backups at Plant A were also encrypted. The only good backups are at the corporate data center, but restoration will take 72 hours. The vendor for the PLC on Line 1 has gone out of business. **Decision Point:** Do you consider paying the ransom? | **Supply Chain Cascade:** Two other utilities report similar anomalous activity. CISA issues an alert linking this to a widespread campaign targeting the specific SCADA software component. **Decision Point:** How do you coordinate with industry peers and government agencies? |

### 5.3 Continuous Improvement

Ransomware readiness is not a static state to be achieved, but a dynamic capability that must be continuously maintained and adapted. The Converged Defense Framework is designed to be integrated into a perpetual lifecycle, aligning with the core principles of the ISA/IEC 62443 security lifecycle: Assess -> Implement -> Maintain -> Assess.

* **Integrate Lessons Learned:** The findings from the annual RRA assessment and the TTX's After-Action Report must be fed directly back into the program. They should be used to update the organization's risk assessments, refine the strategic roadmap, and improve specific security policies, procedures, and playbooks.
* **Monitor and Adapt to the Threat Landscape:** The tactics and techniques of ransomware actors are constantly evolving. The organization must establish a process for consuming threat intelligence from sources like CISA, industry ISACs, and security vendors. This intelligence must be used to regularly update threat models and risk assessments, ensuring that the security posture is adapted to counter the most current threats.
* **Invest in Continuous Monitoring:** A foundational element of the "Maintain" phase is the continuous monitoring of the OT network. Technologies that provide deep visibility into OT assets and communications are essential for detecting anomalous activity that could indicate the early stages of a ransomware attack, allowing for a much faster and more effective response.

By embracing this cycle of continuous improvement, an organization can move from a reactive security posture to a proactive state of resilience, transforming its ransomware readiness program from a short-term project into an enduring strategic advantage.

## Part VI: Convergence and Divergence: Tailoring the Framework for Manufacturing and Energy

While the core principles of the Converged Defense Framework—bridging the IT/OT divide, anchoring in standards, and using a mediated, collaborative process—are universally applicable, the specific risks and operational realities of the manufacturing and energy sectors demand tailored approaches. Both sectors face threats to their OT environments, but the nature of their operations, their risk tolerance, and their organizational structures create significant distinctions that must be addressed for any readiness framework to be effective.9

### 6.1 The Common Ground: A Unified Foundation

At their core, both manufacturing and energy are cyber-physical industries where digital commands have kinetic consequences.10 This shared reality means the foundational elements of the Converged Defense Framework remain constant:

* **The IT/OT Cultural Divide:** The fundamental conflict between IT's focus on data (Confidentiality, Integrity, Availability) and OT's focus on physical processes (Safety, Uptime) is a universal challenge in both sectors.10 Therefore, the need for a common language of risk and mediated workshops to build consensus is paramount for both.
* **A Standards-Based Approach:** ISA/IEC 62443 provides a risk-based, defense-in-depth philosophy that is equally relevant for a production line or a power grid. Its concepts of Zones, Conduits, and Security Levels offer a common, environment-agnostic language for defining and achieving security objectives.10
* **A People-Centric Process:** The framework's emphasis on facilitated workshops (using CSET RRA, IRA/DRA, Threat Modeling) is designed to empower the people who own the operational risk. This principle holds true whether the stakeholder is a plant manager in a factory or a grid operator at a utility.

However, beyond this common foundation, the paths to resilience diverge significantly, shaped by the distinct business models, risk profiles, and organizational structures of each sector.

### 6.2 The Great Divergence: Two Sectors, Two Risk Profiles

The primary distinction between the two sectors lies in their core operational structure and the resulting nature of their greatest cyber risks. Manufacturing is often characterized by a collection of discrete, geographically dispersed operational "kingdoms," while the energy sector functions as a deeply interconnected, interdependent ecosystem.11

#### 6.2.1 Manufacturing: The Challenge of Distributed Sovereignty

The central challenge for a large manufacturing enterprise is managing security across dozens or even hundreds of globally distributed plants, each with its own leadership, budget, culture, and unique mix of (often legacy) technology.12 This creates a problem of "distributed sovereignty," where a centralized, one-size-fits-all security policy from corporate IT is often impractical and ineffective.15

* **Divergent Risk Management:** The risk calculus is dominated by **internal operational variables**. The primary concern is an event that halts a production line, leading to direct and immediate revenue loss. While supply chain issues exist, the most acute risk is often the failure to secure the assets within the plant's own four walls. The biggest challenge is often the disparity in security posture between different sites, with some plants being far less protected than others.15
* **Divergent Framework Application:** The Converged Defense Framework must be adapted into a **federated model**.
  + **"Model Plant" Rollout:** The 5-phase workshop process should be conducted first at a representative "model" plant. The outputs—the risk assessment, threat models, and roadmap—are then used to create a standardized but customizable **"Plant Security Playbook."**
  + **Empowering the Plant Manager:** The plant manager is the ultimate owner of operational risk and must be a central figure in the process.17 The framework must provide them with the tools and authority to implement the playbook in a way that makes sense for their specific environment.
  + **Local Execution:** A central corporate team, armed with the playbook, acts as an internal consultancy, traveling to different regions to facilitate the workshop process with local teams. This ensures global consistency in methodology while allowing for local adaptation in execution. This approach respects the autonomy of each plant while elevating the security baseline across the entire enterprise.

#### 6.2.2 Energy: The Challenge of Interconnected Ecosystems

The energy sector's primary challenge is not internal fragmentation, but the immense complexity and interdependence of its external ecosystem.23 An energy company is a node in a vast, interconnected grid of suppliers, partners, and customers, all of which are critical to its operation. A single vulnerability in a small, third-party software vendor can create a systemic risk to the entire national grid, as demonstrated by attacks like the one on Colonial Pipeline.25

* **Divergent Risk Management:** The risk calculus is dominated by **external, supply-chain variables**. While internal security is crucial, the most significant and difficult-to-manage threats often originate from third-party vendors.28 Research shows that 45% of cybersecurity breaches in the energy sector originate with third parties, a rate significantly higher than in other industries.28 Geopolitical tensions further amplify this risk, as state-sponsored actors frequently target critical infrastructure.24
* **Divergent Framework Application:** The Converged Defense Framework must be adapted to become an **outward-facing, ecosystem-wide assurance program**.
  + **Supply Chain as the Focus:** The risk assessment and threat modeling workshops must extend beyond internal assets to explicitly model the digital supply chain. This involves mapping critical third-party dependencies and analyzing the security posture of key vendors.
  + **Procurement as a Control Point:** The framework's outputs must directly inform procurement and legal processes. Security requirements, such as the mandatory provision of a Software Bill of Materials (SBOM) and the right to audit, must be embedded in all supplier contracts.
  + **Collective Defense:** The strategy must embrace industry-wide collaboration. This includes active participation in Information Sharing and Analysis Centers (ISACs) and extending support to help smaller, critical suppliers improve their own security posture. For the energy sector, resilience is a collective responsibility, not an individual achievement.23

### 6.3 The Global-Local Nexus: Empowering the Front Lines

For any multinational manufacturing or energy company, a successful cybersecurity program cannot be dictated solely from a central headquarters. While a global strategy is essential for consistency and efficiency, its implementation must be owned and executed by local teams who understand the specific operational context, regulatory environment, and cultural nuances of their region.31

Effective security requires a holistic approach that integrates people, processes, and technology, with a strong emphasis on empowering local personnel.33 The Converged Defense Framework is designed to facilitate this by making local teams essential participants in the process. The mediated workshops are most powerful when they bring together corporate IT security experts with the local plant engineers and operators who possess the invaluable ground-truth knowledge of how systems actually work.

This global-local partnership is critical for several reasons:

* **Regional Expertise:** Local teams are best positioned to understand and navigate region-specific regulations, such as the EU's NIS2 Directive, and to build relationships with national cybersecurity agencies and industry groups.28
* **Contextual Risk Assessment:** A vulnerability that is a high priority in one country may be a lower priority in another due to different threat landscapes or operational dependencies. Local teams can provide this crucial context, ensuring that resources are applied where they are most needed.
* **Building a Global Culture:** By involving local teams in the development of their own security roadmaps (within the global framework), the organization fosters a sense of ownership and accountability. Security is no longer something "done to them" by corporate, but something "done by them" for the resilience of their own operations. This approach, which combines global reach with local expertise, is the key to building a truly resilient and sustainable cybersecurity program in a complex, international environment.31

## Conclusion

The convergence of IT and OT has created unprecedented efficiencies for the energy and manufacturing sectors, but it has also erased the traditional air gaps that once protected critical industrial processes from cyber threats. Ransomware actors have ruthlessly exploited this new reality, turning production lines and power grids into levers for financial extortion. The evidence is unequivocal: industrial ransomware is a direct threat to business continuity, economic stability, and national security.

Addressing this threat requires a profound shift in mindset and strategy. The siloed approaches of the past, where IT managed data and OT managed machines, are no longer viable. The Converged Defense Framework presented in this report provides a structured, actionable, and sustainable path forward. Its methodology is built on the recognition that true resilience is a socio-technical achievement. The most advanced firewalls and endpoint detection tools are of little use if the people and processes governing the IT/OT boundary are misaligned.

Therefore, the core of this framework is not a technology, but a process: a series of mediated, cross-functional workshops designed to break down cultural barriers, forge a common language of risk, and build a shared sense of ownership for the security of the entire enterprise. By anchoring this collaborative process in the rigorous, risk-based philosophy of ISA/IEC 62443 and using the practical CISA CSET RRA as a diagnostic tool, organizations can move beyond compliance checklists to build a security program that is both technically sound and culturally embedded.

While the foundational principles of this framework are universal, its application must be nuanced. For the distributed world of manufacturing, it becomes a federated model empowering local plant leadership. For the interconnected ecosystem of the energy sector, it transforms into an outward-facing supply chain assurance program. In both cases, success hinges on empowering local teams with the knowledge and authority to execute a global strategy within their unique context.

The journey begins with a single, facilitated conversation. It progresses through the systematic identification of risks, the collaborative modeling of threats, and the joint development of a prioritized roadmap. It is sustained through continuous measurement, regular testing via tabletop exercises, and an unwavering commitment to improvement. For executive leaders in energy and manufacturing, the mandate is clear: champion the cultural convergence of IT and OT. It is the essential prerequisite for building a technical defense capable of withstanding the modern ransomware threat and securing the future of industrial operations.

#### Works cited

1. Cybersecurity Risk Assessment According to ISA/IEC 62443-3-2, accessed August 15, 2025, <https://gca.isa.org/blog/cybersecurity-risk-assessment-according-to-isa-iec-62443-3-2>
2. Practical Guide to Performing Risk Assessment as per IEC 62443-3 ..., accessed August 15, 2025, <https://hardhatsecurity.com/2024/05/15/practical-guide-to-performing-high-and-detailed-level-risk-assessment-as-per-iec-62443-3-2-and-nist-800-30/>
3. Cybersecurity in Manufacturing: Threats, Trends, and Preparation, accessed August 15, 2025, <https://www.forescout.com/blog/cybersecurity-in-manufacturing-threats-trends-and-preparation/>
4. Cyber Security Evaluation Tool (CSET) - CISA, accessed August 15, 2025, <https://www.cisa.gov/resources-tools/services/cyber-security-evaluation-tool-cset>
5. cisagov/cset: Cybersecurity Evaluation Tool - GitHub, accessed August 15, 2025, <https://github.com/cisagov/cset>
6. Ransomware Readiness Assessment - Centraleyes, accessed August 15, 2025, <https://www.centraleyes.com/ransomware-readiness-assessment/>
7. Top 5 Key Cultural Differences Between IT and OT | OTIFYD ..., accessed August 15, 2025, <https://otifyd.com/blog/top-5-key-cultural-differences-between-it-and-ot/>
8. TABLETOP EXERCISE FACILITATOR GUIDE - Amazon S3, accessed August 15, 2025, <https://s3.amazonaws.com/ultimatesdlc/UConnLib/Tabletop-Exercise-Facilitator-Guide.pdf>
9. How energy and manufacturing can protect against cyber threats | World Economic Forum, accessed August 15, 2025, <https://www.weforum.org/stories/2025/06/cyber-threats-energy-and-manufacturing-ot-technology/>
10. Harmonizing risk and consequence strategies across IT and OT environments for greater cyber resilience, accessed August 15, 2025, <https://industrialcyber.co/features/harmonizing-risk-and-consequence-strategies-across-it-and-ot-environments-for-greater-cyber-resilience/>
11. New Google Cloud–Mandiant report warns of escalating cyber threats to manufacturing, energy OT systems, accessed August 15, 2025, <https://industrialcyber.co/reports/new-google-cloud-mandiant-report-warns-of-escalating-cyber-threats-to-manufacturing-energy-ot-systems/>
12. 8 Challenges to Managing Geographically Distributed Teams - HelpWire, accessed August 15, 2025, <https://www.helpwire.app/blog/distributed-teams-challenges/>
13. "The Challenges of a Geographically Dispersed Project Team", accessed August 15, 2025, <https://www.wcu.edu/pmi/1999/CM04.PDF>
14. Supply Chain Challenges in 2025 & How to Overcome Them - Extensiv, accessed August 15, 2025, <https://www.extensiv.com/blog/supply-chain-management/challenges>
15. Managing geo-distributed businesses | Kaspersky official blog, accessed August 15, 2025, <https://www.kaspersky.com/blog/geo-distributed-businesses-research-2024/>
16. Challenges and Solutions in Working with Green Suppliers: Perspective from a Manufacturing Industry - MDPI, accessed August 15, 2025, <https://www.mdpi.com/2071-1050/16/20/8744>
17. Need to develop OT cybersecurity programs to bridge IT and engineering cultures, defend from cyber threats, accessed August 15, 2025, <https://industrialcyber.co/features/developing-ot-cybersecurity-programs-to-bridge-it-and-engineering-cultures-defend-industrial-systems-from-cyber-threatsneed-to-develop-ot-cybersecurity-programs-to-bridge-it-and-engineering-cultures/>
18. Why organizations must adopt cybersecurity for OT - The World Economic Forum, accessed August 15, 2025, <https://www.weforum.org/stories/2025/01/cybersecurity-protect-ot-industrial-organizations-risk-it/>
19. Operational Technology on Construction Sites: A Review from the Cybersecurity Perspective - ASCE Library, accessed August 15, 2025, <https://ascelibrary.org/doi/10.1061/%28ASCE%29CO.1943-7862.0002193>
20. Industry 4.0 and OT security: A methodology for assessing and securing the operational technology (OT) environment - CGI.com, accessed August 15, 2025, <https://www.cgi.com/sites/default/files/2020-08/industry-4.0-cybersecurity-methodology-en.pdf>
21. OT cybersecurity in manufacturing - PwC, accessed August 15, 2025, <https://www.pwc.com/us/en/industries/industrial-products/library/manufacturing-ot-cybersecurity.html>
22. Navigating Operational Technology (OT) Transformation with Integrated Security - Kyndryl, accessed August 15, 2025, <https://www.kyndryl.com/content/dam/kyndrylprogram/cs_ar_as/operational-technology-systems-management.pdf>
23. Why we need to power cyber resilience in the energy sector - The World Economic Forum, accessed August 15, 2025, <https://www.weforum.org/stories/2025/05/powering-cyber-resilience-energy-sector/>
24. Cybersecurity considerations 2024: Energy and natural resources sector - KPMG International, accessed August 15, 2025, <https://kpmg.com/us/en/articles/2024/cybersecurity-considerations-2024-energy-and-natural-resources-sector.html>
25. Growing Ransomware Threats to the Energy Sector - CyberSaint, accessed August 15, 2025, <https://www.cybersaint.io/blog/growing-cyber-threats-to-the-energy-sector>
26. ARTICLE - Houston Law Review, accessed August 15, 2025, <https://houstonlawreview.org/article/73666.pdf>
27. Biggest Cybersecurity Attacks in Oil And Gas Extraction Industry (2023-2024) - SOCRadar, accessed August 15, 2025, <https://socradar.io/cyber-attacks-in-oil-and-gas-industry-2023-2024/>
28. Cyber Threats in Energy Sector Supply Chains | Risk Ledger, accessed August 15, 2025, <https://riskledger.com/resources/supply-chain-cyber-threats-energy>
29. The Importance of Supply Chain Cyber Security in the Energy Sector ..., accessed August 15, 2025, <https://www.achilles.com/industry-insights/supply-chain-cyber-security-in-energy/>
30. www.achilles.com, accessed August 15, 2025, <https://www.achilles.com/industry-insights/supply-chain-cyber-security-in-energy/#:~:text=The%20energy%20sector's%20supply%20chains,entry%20points%20for%20cyber%20attackers.>
31. Cybersecurity is everyone's responsibility - PwC, accessed August 15, 2025, <https://www.pwc.com/gx/en/issues/cybersecurity.html>
32. Industrial cybersecurity coalitions rise to meet growing OT/ICS cyber threats, build awareness, take action, accessed August 15, 2025, <https://industrialcyber.co/features/industrial-cybersecurity-coalitions-rise-to-meet-growing-ot-ics-cyber-threats-build-awareness-take-action/>
33. OT Cybersecurity – Back to Basics - techUK, accessed August 15, 2025, <https://www.techuk.org/resource/ot-cybersecurity-back-to-basics.html>
34. The Role of Regional Organizations in Strengthening Cybersecurity and Stability - Experiences and Opportunities - UNIDIR, accessed August 15, 2025, <https://unidir.org/files/publication/pdfs/the-role-of-regional-organizations-in-strengthening-cybersecurity-and-stability-experiences-and-opportunities-en-789.pdf>
35. Companies turn to in-house teams for cybersecurity | International Bar Association, accessed August 15, 2025, <https://www.ibanet.org/companies-turn-to-in-house-teams-for-cybersecurity>
36. Industrial Cybersecurity: Applying Zero Trust and CARTA to Operational Technology (OT), accessed August 15, 2025, <https://gca.isa.org/blog/industrial-cybersecurity-applying-zero-trust-and-carta-to-operational-technology-ot>