


A photograph of an industrial facility, likely a power plant or refinery, with several tall smokestacks and complex piping structures. The scene is illuminated by warm, golden light, suggesting dusk or dawn, with a blue and orange sky.

Case Study:

Utility OT Cybersecurity Program Development & Deployment

A photograph of an industrial facility at night, showing various structures, pipes, and lights illuminated against a dark background.

A large utility in North America sought to build and deploy an OT cybersecurity program from the ground up by addressing all phases of the OT lifecycle. This initiative encompassed procurement, mergers and acquisitions, design, engineering, deployment, and run/maintain activities. The client, operating in a highly regulated industry with a diversified portfolio, faced significant challenges in scaling their security program across various business units.

To meet these challenges, Armexa implemented a Buy/Build/Run OT Cybersecurity Governance Program. This included developing risk assessment methodologies, assurance frameworks for M&A, and deploying technology aligned with industry standards such as NIST and IEC 62443. The program's successful rollout began with a pilot in the gas business unit and continued with ongoing collaboration to extend technology deployment across all sites.

The initiative led to the creation of Achievable NIST Standards for their organization, a secure technology deployment methodology, standardized policy/standards templates, and an operationalized cybersecurity lifecycle management process for OT assets.

Industry:

Utilities, Oil & Gas,
Manufacturing

Location:

North America

Armexa Services Provided::

■ Strategy

- OT Cybersecurity Program
- Development OT Roadmap
- Gap Assessment

■ Engineering

- OT Architecture & Design
- Secure Remote Access Implementation
- OT Identity Engineering & Design

Challenge: Scalable cybersecurity program ensuring compliance, efficiency, and integration across diverse business units.

The client's organization included multiple business units spanning regulated industries such as utilities. The primary challenge was to develop a program that could scale and be applicable to these disparate business units while addressing several other critical issues. Resource constraints were a significant hurdle, requiring efficient allocation and management of both human and technological resources. Integrating the cybersecurity program with existing systems was another challenge, necessitating compatibility and seamless operation within established infrastructures. Ensuring continuous compliance with ever-evolving regulatory standards was also incredibly important, demanding a proactive approach to cybersecurity.

Moreover, the program had to be compatible and flexible to meet the needs of both large industrial facilities and smaller operations, ensuring that all units could benefit from robust cybersecurity measures without compromising on efficiency or practicality.

Solution: Integrating risk assessments, compliance frameworks, M&A security, and technology deployment across the client's operations

Armexa collaborated with the client to develop the Buy/Build/Run OT Cybersecurity Governance Program, which included comprehensive documentation such as policies, standards, and job aids, as well as defined lifecycle objectives and program implementation procedures.

Workstream 1: Risk Assessment Methodology, Controls Framework, and Standards Management

- Developed an OT Security Framework based on industry best practices, aligning with NIST, IEC 62443, and CIP standards.
- Identified applicable controls for non-CIP regulated facilities, leveraging past OT Risk Assessments to select the most effective controls.
- Designed the client's OT Security Policy based on the agreed upon OT Security Framework, then develop standards which support the policy.

Workstream 2: Assurance Framework for M&A, Operations, and Capital Project

- Defined roles and responsibilities required for long-term implementation and adherence to security policies and standards.
- Established role-specific expertise levels and training requirements for personnel across verticals such as M&A, operations, and capital projects.



Solution: Multiple Workstreams

Workstream 3: M&A Deep Dive and Gap Assessment

- Conducted an M&A Deep Dive at a selected facility to assess OT cyber risks, mitigation strategies, and actions across the deal lifecycle.
- Performed a Gap Assessment at a selected facility using the OT Security Framework to evaluate alignment and identify security gaps through site interviews and technical evaluations.

Workstream 4: Technology Selection and Pilot/Proof of Concept (POC) Deployment

- Selected a facility to implement new secure remote access technology aimed at risk reduction and compliance with the OT Security Framework.
- Collaborated with the client's procurement team to acquire necessary hardware/software.
- Developed High-Level and Low-Level Designs prior to deployment, staged and configured the technology, and provided post-implementation support until project completion.

Impact: Secure industrial infrastructure and streamlined technological processes

The successful implementation of the OT Cybersecurity Governance Program resulted in enhanced security measures across all business units, starting with a pilot facility. The collaboration with the client's procurement team ensured the acquisition of necessary hardware and software, leading to improved operational efficiency and robust compliance with industry standards. The project's completion brought significant benefits such as an improved and measurably secure industrial infrastructure, streamlined technological processes, and paved the way for sustained protection against cyber threats.

We continue to work with the client to deploy technology at additional sites, ensuring comprehensive cybersecurity coverage from acquisition to divestiture.

This initiative led to the development of an enterprise-wide OT Cybersecurity Framework, Buy/Build/Run Secure Methodologies, and tailored Policy/Standards , which continue to be utilized across the client's business units.

