Overview

A major multinational organisation in the Oil and Gas sector needed to achieve compliance with the national laws in which the European Union’s NIS Directive is transposed. The project included multiple sites across three different countries.

Applied Risk was approached as their trusted partner to advise on mandatory OT security practices and define a “toolkit” describing a minimum set of requirements and building an implementation roadmap in preparation for external audits.

A framework was developed, which not only enabled the client to address compliance requirements, but was further utilised to drive effective OT security improvements across the entire organisation.

Client Challenges

During the initial discussions, it became clear that three major challenges needed to be overcome:

- Multiple geographically dispersed sites needed to be assessed, each site with unique local requirements. Integration with existing cyber security management processes was required.

- Various internal business units would have to be involved. In addition, the scope would also include third parties (e.g. integrators, vendors and suppliers).

- A multitude of country specific laws, regulators, standards and definitions, as well as varying national NIS thresholds for incident reporting.

“The team remarkably addressed our business needs. Due to their experience within operational environments, allied to their knowledge of cyber security frameworks across IT and OT, as well as risk assessments and implementation, they were quickly up to speed.

The program and roadmap supported us in closing the project within time and exceeded quality.”

– OT Security Manager at Oil & Gas company

Looking for guidance in meeting globally recognised standards and mandatory cyber security regulations? Contact sales@applied-risk.com for more information.
A bespoke approach which translated complex requirements into actions.

Once business units were identified as Operators of Essential Services (OES), scoping was conducted in order to define critical business processes, systems and third parties, followed by multiple Health Check Assessments to measure effectiveness of the implemented barriers/controls at every OES location against the requirements. This gap analysis resulted in the design of a remediation roadmap, with activities being implemented for different sites.

Special emphasis has been placed on implementing the NIS Incident Notification process to assigned regulators. This process involved stakeholders and business units across the globe (e.g. legal, crisis management, CSIRT, IT Operations, etc.). Improvements have been implemented into the existing incident management plan and simulations conducted, to ensure key stakeholders were equipped to play their role within the process.

The Applied Risk team of experienced consultants provided end-to-end guidance following Applied Risk’s ARM methodology: Assess, Remediate, Manage. As a result, the client was well prepared to demonstrate compliance in the external audits, all of which have been successfully passed.

Looking for guidance in meeting globally recognised standards and mandatory cyber security regulations? Contact sales@applied-risk.com for more information.
Successful Impact

By following its comprehensive methodologies, Applied Risk’s team was able to provide guidance throughout the entire journey for one of the largest energy companies. Complex regulatory compliance requirements were successfully translated into concrete actions which were laid out on a clear roadmap. Pragmatic improvements were created to help the client’s teams be well prepared for the external audits.

Successfully achieving EU NIS Directive compliance was only one of the success factors:

- A plan was devised to help remediate shortfalls with a practical toolkit-based approach. The tailored set of recommendations allowed the business to make informed decisions to address their unique requirements.

- The NIS EU Directive requirements were integrated within the organisation’s day-to-day processes and governance model. Focal Points were assigned and the stakeholders have been trained to fulfil their role in the process.

- Insights gained into the organisation’s OT security maturity will also contribute towards improving the ability to sustainably manage cyber risk at the different locations.

- The compliance journey served as a tool to create more effective OT security within the organisation, reducing the risk for unexpected downtime and loss of production.

Applied Risk’s approach ensured that achieving compliance was not just a box-checking exercise, but will be further utilised to drive effective security improvements across the entire business.

Looking for guidance to meet cyber security standards and regulations?

Is your organisation seeking end-to-end compliance support which goes beyond box-checking?

Get in touch with Applied Risk today to begin your EU NIS Directive compliance journey. We can provide you with a concrete and clear-cut roadmap to achieve compliance, and ultimately strengthen your OT cyber security posture. Contact us today!