



The Report further elucidates the readiness assessment for each information domain and category of risk, and then recommends best practices and application controls that could be implemented to mitigate each area of risk. These controls range from recommended changes to formal corporate policy, to operational guidelines involving procedures, personnel, education, and training, to more involved modifications to process, workflow, infrastructure, and automation.

	Information Domain									
	Email	Instant Messaging	Desktop/Laptop	Removable Devices	Collaboration Applications (SharePoint)	File Shares	ERP	PLM	Databases	Helpdesk/Support
Electronic Data	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Green	Green
Collaboration	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Green	Green
Mobility	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Green	Green
Supply Chain	Red	Red	Red	Red	Red	Red	Yellow	Yellow	Green	Green
Global Operations	Yellow	Green	Green	Green	Green	Green	Green	Green	Green	Green

Information Risk Heat Map

Finally, the report organizes recommendations into a three-phase action plan, starting with “low hanging fruit,” or controls that can be implemented quickly with low cost and high value. The next phase involves tactical wins—recommended controls that require deeper process, workflow, or infrastructure changes. The final phase involves “strategic opportunities”—controls that are longer range and introduce new processes or significant changes to existing processes.

A Place to Start

Readying a complex organization for export compliance will always be a daunting task. The NextLabs Compliance Readiness program can provide organizations with an objective evaluation of their current information assets, systems, processes, procedures, people, and documentation. The end result is an actionable plan and a clear place to start. After their assessment, the industrial automation company was equipped with the knowledge it needed to optimize its management of controlled technical data, which freed it up to pursue business opportunities in the Aerospace & Defense sector.

About NextLabs

NextLabs leads the industry in specialized knowledge of compliance challenges across the Aerospace & Defense, High-Tech Manufacturing, Information Technology, and Chemical sectors. NextLabs was an SC Magazine Awards Finalist for Best Regulatory Compliance Solution, and a 2009 Red Herring 100 winner for its Information Risk Management platform—the “internationally proven solution in information security and compliance arenas.”

“What makes NextLabs cool is its ability to integrate Data Protection and Entitlement Management to address data protection scenarios, especially for collaborative environments.”

— Gartner 2010, *Cool Vendors in Identity Management*

Export Compliance Readiness



Taking the proactive approach to optimize the management of controlled technical data

Summary

With a customer base spanning over 80 countries and almost as many industries (from Pharmaceuticals, to Textiles, to Electronics, to Food and Entertainment, to Automotives, Oil and Gas, and Mining), one of the world’s largest providers of industrial automation solutions sought to expand its business further into the Aerospace and Defense market. However, due to strict regulations governing how defense-related exports and technical data must be handled, such as the International Traffic and Arms Regulation (ITAR), Security Officers were first tasked with assessing the compliance readiness of the company’s current infrastructure.

They turned to NextLabs for an Export Compliance Readiness Assessment. In a systematic evaluation driven by clearly-defined metrics, the NextLabs Assessment team examined the company’s information domain—that is, its systems, processes, procedures, and policies—to benchmark against industry peers and determine readiness. The analysis was distilled into an easy-to-understand Risk Heat Map that pinpoints potential areas of risk, along with recommended applications controls and an implementation plan consistent with the company’s compliance goals.

- Industry**
 Industrial Automation, Integrated Systems, and Factory Management
- Customer**
 Annual sales \$4.8 billion, 19,000 employees serving customers in more than 80 countries
- The Compliance Challenge**
 Supplying integrated systems and support services to customers and OEMs in defense and government markets
- Assessment Goals**
 To evaluate the effectiveness of current ITAR and UK MOD compliance programs

 To proactively identify strategies to improve management of controlled technical data
- The Deliverable**
 NextLabs Risk Assessment Report including Risk Heat Map, Best Practices and Application Controls, and Tiered Implementation Plan

Understanding the Challenge

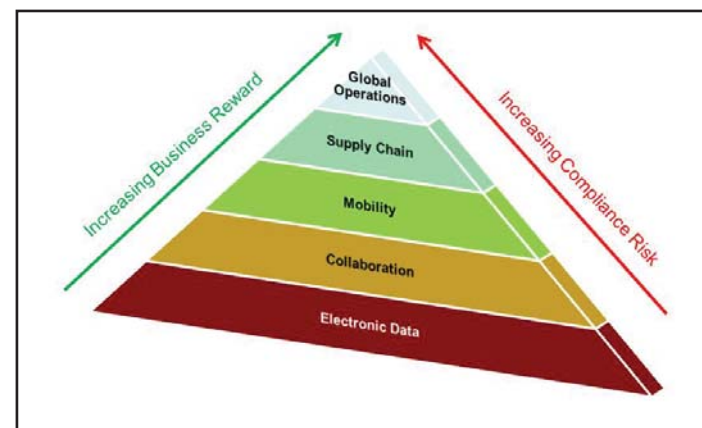
Many businesses are grappling with the complexity of export compliance regulations for controlled technical data. For instance, taking ITAR as just one example, regulations tend to prohibit the export of “Defense Articles,” which typically means both products, and technical data and services associated with those products. “Export” to non-US countries without a proper export license constitutes a violation, as well as the *access of controlled technical data* by foreign persons, including access by foreign workers on US soil. Routing or storing technical data through servers or storing data in file shares located in other countries can also constitute a violation. Clearly, these regulations present hurdles to businesses that seek to collaborate and share technical data across global supply chains, in international trade with overseas customers, while manufacturing for foreign clients, with a workforce that is both highly mobile and increasingly global. The goal of the NextLabs Export Compliance Readiness Program is to help organizations understand what these regulations mean for their current business models and IT infrastructure.

A Systematic Approach

A typical Readiness Program lasts 3-5 weeks, and begins with an initial project kick-off meeting to clarify requirements and goals. In these early stages, the Assessment Team maps out area in the company’s information domain where controlled technical data is stored, accessed, used, or routed. While these domains vary from organization to organization, they typically include email and communication applications, desktops and laptops, collaboration applications such as Microsoft SharePoint, file shares, ERP applications, databases, support or help desk applications, and bug-tracking tools. In the early stages, the Assessment team also helps the organization understand which assets constitute technical data that is subject to export control regulations. This determination can be based on subtle distinctions that are neither clear nor well-documented.

Next, the Assessment Team carefully examines each domain, drilling down into the obvious and not-so-obvious places where technical data tend to reside.

In structured interviews, informal conversations, and a review of documentation, the Assessment team investigates five specific areas of information risk.



Areas of Information Risk

The five categories reflect the strategic information objectives companies typically engage as they move toward more collaborative, global business models. As an organization’s information objectives move up the levels of the pyramid, the organization reaps greater business rewards—in efficiency, productivity, and the ability to address more and more markets. However, the organization simultaneously increases the risk of compliance with respect to controlling technical data. Each layer in the pyramid thus corresponds to increased opportunity and increased challenges in information risk.

Electronic Data

When controlled technical data is electronic, it is easily accessed, moved, and copied. This raises questions for:

- Data Storage: Where is controlled data stored? What policies govern storage?
- Access Control: What controls exist to ensure access to data is consistent with regulatory requirements?

Collaboration

Collaboration risks manifest themselves when users share data with one another directly, or make data available for sharing. This raises questions for:

- Internal Communications: Is controlled technical data being shared using email, Instant Messaging, or web meetings?
- File Sharing and Collaboration: Is controlled technical data being shared in loosely governed collaboration applications, like file shares, SharePoint, Lotus Notes, and the like?

Mobility

Users increasingly employ mobile electronic devices and remote access capabilities to access and move data. This raises questions regarding:

- Mobile Workforce: Is access being granted to Telecommuters, Remote Employees in other countries, Field Service Technicians, or support and help desks in other countries?
- Mobile Devices and Media: Is controlled data being copied to laptops and USB devices?

Supply Chain Risks

Users commonly need to interact and exchange data with suppliers, partners, and customers. This raises questions regarding:

- External Communications: Are export licenses being properly tracked? Is data labeled appropriately? Are channels for controlled technical data exchange secure? Are there controls for authorized versus unauthorized recipients?
- Handling Third Party Data: What is the procedure for managing marked or unmarked controlled technical data originating from third parties?

Global Operations

Operations Risks occur when global teams and infrastructure are used to create, store, and manage controlled data. This can raise issues with:

- Isolating Global IT Operations: Where does IT infra-

structure reside?

- Managing Global IT Infrastructure: Who is providing application and infrastructure support? How is this support being provided?

Down to the Details

Structured interviews delve into operations and IT details around all five categories of risk. For example, in the information domain of File Shares, and the risk area Electronic Data Storage and Access, interviewers might ask:

- Is ITAR data stored in specific locations on file servers and shares?
- Do you contract with third parties for the hosting, management, administration, helpdesk services, or maintenance of your server infrastructure?
- What are the roles of non-US persons in the administration of the server infrastructure?
- How do you control, monitor, and audit access to servers from devices not known to your system?
- What are the processes for backing up and restoring data on the servers?
- Are data backups stored on US soil?

The Take-Away

After the information gathering phase is complete, the Risk Assessment team analyzes findings across information domains and categories of risk. Their goal is to identify “hot spots”—areas where both the *magnitude* and *likelihood* of risk is high. That is, the probability that an event will be subject to export control regulation is strong, and the event is likely to occur frequently. Security teams can review their readiness “at-a-glance” in the Assessment Report’s Risk Heat Map.