

NORTH AMERICAN TRANSPORT GIANT STRENGTHENS CYBERSECURITY WITH IMPROVED RISK TRANSPARENCY AND RESPONSE

For one of North America's largest transport companies, the opportunity to continue serving millions of customers depends, to a large extent, on the organization's ability to manage and mitigate cyber threats. Earlier, cybersecurity was just one part of the company's larger technology and IT security program. But as the focus on cyber steadily increased, stakeholders set out to establish a dedicated cybersecurity governance, risk management, and compliance initiative.

☰ Focused Approach to GRC

After several years of working with internal experts to manage cybersecurity requirements, the organization approached MetricStream for an integrated GRC solution. They wanted a single, unified platform that would enable them to simultaneously manage all their IT risks and IT compliance requirements.

☰ Increased Focus on IT and Cyber Risks

Today, the MetricStream solution for IT risk management has given the organization a centralized and flexible system to manage and track various IT risks, including cybersecurity risks. It also supports a consistent risk and control vocabulary which simplifies risk communication and reporting.

Built on a common GRC platform, the solution enables a standardized, streamlined process for IT risk documentation, risk assessments, control management, issue detection, and resolution. The solution has also helped the company build clear risk governance structures with well-defined roles and risk owners across the three lines of defense.

Advanced business intelligence reports and dashboards provide an in-depth, near real-time view of IT and cybersecurity risks aligned to business risks, thus enabling senior stakeholders and board members to make faster and better-informed decisions.

In addition to the IT risk management solution, a separate exceptions management solution has been built by MetricStream to help the company raise exceptions as part of their risk assessments. Users can add a monetary value to each risk exception to understand its business impact on the company.

Challenge

- Absence of a baseline security guide to track and monitor cybersecurity risks
- Insufficient focus on IT risks

Solution

- IT risk management
- IT compliance management

Value Delivered

- Optimized overall cybersecurity investment
- Standardized classification of systems as per GRC cybersecurity definitions
- Simplified the risk taxonomy across the enterprise
- Improved visibility into top risks across the three lines of defense
- Helped link cybersecurity risks to business risks for faster decision making

☰ Federated IT Compliance

Using the MetricStream solution for IT compliance management has made it easier for the company to handle and track compliance with various IT and cybersecurity regulations and standards. The solution supports the process of scheduling assessments, automating them, and performing control tests based on specific company procedures.

It also enables a federated approach to IT compliance management through which the company can link IT compliance controls and assessment activities according to specific regulatory requirements. Alerts, notifications, and updates on IT regulatory content, as well as actionable insights from various online sources, are delivered on an automated basis.

The solution provides comprehensive visibility into the IT compliance process through a built-in reporting and dashboard engine.

In addition to a range of standard reports, MetricStream has built a detailed “security book” report for the company which offers a complete snapshot of the cyber-risk posture of each business asset.

☰ Extending the Maturity of GRC

The company now plans to continue their GRC journey with MetricStream by extending their GRC platform to include new solutions for third-party management, as well as policy and document management. The former will enable the company to efficiently identify, assess, mitigate, and monitor IT vendor risks, while also managing vendor compliance. The latter will help the company map their policies to regulations, risks, and controls, thus making it easier for users to identify and close compliance gaps or deficiencies proactively.

