NAVEX GLOBAL®

Major Health Information Network Connects To Better Information Security

SOLUTION

LP LOCKPATH®
INTEGRATED RISK MANAGEMENT

| EP | NE | PT | RR | LP |

HIGHLIGHTS

COMPANY

Major health information network

CHALLENGE

Complex compliance and poor visibility into risks

SOLUTION

NAVEX Global GRC Platform, Lockpath

RESULTS

Better visibility into risks, and ease of regulatory compliance

Managing Compliance and Risk with Lockpath

Map requirements to controls, risk, policies and procedures for a holistic view of compliance

Manage internal controls with the ability to identify duplicate and ineffective controls

Prove compliance with a defensible record showing who, when, how and why

Monitor, analyze and treat risk using virtually any risk management methodology

Provide management with the right information to make risk-based, data-driven decisions

Challenge: Manual Processes Fall Short For Complex Compliance & Risk Management

Companies of all sizes have information security challenges, whether it's dealing with access, managing risks associated with information security or remaining compliant with ever-changing privacy laws.

For the nation's largest health information network, its information security challenges were larger in scope and complexity, especially since the data it processed often involved personally identifiable information (PII). The company had to comply with the Health Information Portability and Accountability Act (HIPAA),, as well as other regulations and industry standards like Electronic Healthcare Network Accreditation Commission (EHNAC), Sarbanes-Oxley (SOX), Payment Card Industry Data Security Standards (PCI DSS) and the International Organization for Standards (ISO).

In addition to complex compliance challenges, the health information network faced headwinds with managing risk. Without an accurate picture of current and pressing risks, there was no data or metrics to report to management and inform their decisions.

It was also a struggle for the company's Information Security department to secure funding. Viewed as a cost center, it was hard to convey priorities and justify budget requests without insight and understanding of IT and information security risks.

Solution: NAVEX Global's GRC platform, Lockpath

The health information network selected NAVEX Global's governance, risk management, compliance (GRC) platform, Lockpath, for its capabilities in integrated risk management (IRM). Lockpath enables organizations to gain a comprehensive view of their business and operations from a risk perspective—connecting individual risk disciplines and managing them in one centralized program.

The company took advantage of Lockpath's centralized compliance library, which houses all compliance activities, regulations, industry standards, best practice frameworks, even extensive international privacy laws. The company's controls were also linked in the central location, enabling one control to satisfy compliance with multiple requirements. For a company complying with several different regulations, standards and frameworks, compliance got a lot easier.

Risk management went from a headwind to a tailwind. Lockpath provided access to risk data and metrics that were easy to share with management in reports and dashboards. Risk data and metrics also informed Information Security's

LP **LOCKPATH**®
Integrated Risk Management

Integrated Risk Management

Integrated Risk Management (IRM) is the collection of practices and processes that offer a comprehensive way to identify, assess and prioritize risk throughout an organization. Lockpath, a GRC and Integrated Risk Management solution from NAVEX Global, equips users and business leaders to manage risk from the endpoint to the enterprise.

Lockpath's integrated risk management capabilities address eight business use cases:

- » Compliance and policy management
- » Vendor risk management
- » IT risk management
- » Continuous monitoring
- » Business continuity management
- » Operational risk management
- » Audit management
- » Health and safety management

operations. They could instantly review a list of risks for a proposed project and then prioritize funding for remediation efforts. Likewise, Information Security was able to prove the validity of expenditures by linking risks to business objectives and compliance initiatives.

Collaboration and communications that were once weaknesses became strengths. Information Security used Lockpath to collaborate and communicate with other areas of the company, including the executive level. Every department was suddenly on the same page. Everyone with access could view projects and tasks with current status and priority. As a result, the company was able to significantly reduce issue resolution time.

They relied on Lockpath's role-based dashboards to present a high-level visual report to the company's executive leadership. Data points in the report linked to multiple sources for added validity. With trust and verification, Information Security had more control over spending and better justification for budget requests.

Results: Better Risk Visibility & Ease of Compliance

For the health information network's Information Security department, the adoption of Lockpath made all the department's activities more efficient and effective.

Compliance that was complex and time-consuming became easier and more productive. Visibility into risk management that was non-existent before came into view and is now measurable and reportable.

Lockpath increased collaboration efforts and streamlined communications, which were significant pain points when information was shared using e-mails and spreadsheets. This is best illustrated with an ISO 27001 requirement from an internal audit corrective plan: Upgrade all locks in the company's physical environments. Using Lockpath, the ISO requirement and internal audit task were linked, eliminating redundancy and confusion about whether the user completed the task. This one example typifies hundreds of others that reflect Information Security's efficiency gains.

Time saved using Lockpath has opened doors for Information Security to take on additional responsibilities—internal auditing, business continuity, and operational risk management—without adding staff. Management took notice, and leadership elevated the role of Information Security within the company.