

NAVEX Customer Success Story

Major Health Insurer Manages Vendor Risk with NAVEX IRM



Highlights



INDUSTRY

**Major
Health Insurer**



CHALLENGE

Comply with HIPAA data security requirements and other regulations and frameworks



SOLUTION

Third-Party Risk Management

Solution

SINGLE-PRODUCT

NAVEX IRM

INTEGRATED RISK MANAGEMENT

Comprehensive Vendor Risk Management

- Create and manage vendor profiles
- Conduct vendor assessments efficiently
- Link vendors to policies, risks, controls and more
- Communicate and collaborate with third parties
- Conduct performance reviews
- Perform ongoing monitoring

Challenge: Manual Processes Prove Inefficient for Managing Vendor Risk in Today's Regulatory Environment

Like most in the healthcare industry, a major health insurer complies with the Health Insurance Portability and Accountability Act (HIPAA), as well as many other regulations and requirements. A primary HIPAA compliance requirement is assessing vendors regularly, as well as assessing vendors' third parties. Compliance failures can lead to stiff fines.

Previously, the health insurer relied on manual processes for vendor risk management activities like issuing assessments. A manual approach can be suitable for a small business with a handful of vendors, but for a health insurer with HIPAA requirements, it can be risky and error prone. The need for efficiency and accuracy turned the major health insurer into an early adopter of governance, risk management and compliance (GRC) platforms. However, the GRC platform the company chose was overly rigid and required technical expertise to configure. The process of managing vendor risk assessments was so complicated that the risk management team reverted to using manual processes.

With the challenge still present, the health insurer conducted a search for a more advanced GRC platform that offered the functionality to comply with healthcare regulations, required little or no IT assistance and a high degree of user adoption.

Solution: NAVEX's Advanced Governance, Risk Management and Compliance (GRC) Platform

The health insurer's search for a GRC platform led the company to NAVEX's IRM, which offers a flexible and scalable solution for integrated risk management and includes the ability to streamline vendor risk assessments.

NAVEX IRM was easy to configure to the health insurer's processes. Since implementation, NAVEX IRM has enhanced the health insurer's ability to identify, analyse, track and report on vendor risks with quick user adoption. Features like drag-and-drop reporting and an intuitive interface made it possible for users to create reports quickly and easily.

To learn more about NAVEX IRM® solutions or to schedule a demo, please visit www.navex.com or call us at **+44 (0) 20 8939 1650**.



A Defined Process for Managing Vendor Risk

With NAVEX IRM, the health insurer's IT Risk team can enforce its defined vendor risk assessment process. Doing so ensures vendors have the proper security controls in place to meet HIPAA requirements for protecting patient data.

The team assesses vendors by issuing 10-20 questionnaires internally with staff who each represent a segment of the vendor base. Each questionnaire is designed to measure the inherent risk of the vendor based on the classification and volume of data that the vendor accesses, stores, processes or outsources. Of these initial questionnaires that canvas the entire vendor base, any vendors that score and qualify as high inherent risk are required to complete a comprehensive vendor security assessment questionnaire.

Comprehensive questionnaires help the health insurer identify security control gaps that are tracked as findings within NAVEX IRM's risk register. The number of findings, along with the inherent risk score, drive the overall third party risk score as low, medium or high for each vendor. As third parties remediate their findings, their risk score is reduced, which lowers the insurer's overall third party risk.

In addition, NAVEX IRM enables the IT Risk team to map assessment questions to controls within the Health Information Trust Alliance Common Security Framework (HITRUST CSF). This allows the IT Risk team to measure all vendors against a healthcare industry framework that also maps to HIPAA.

Data from completed questionnaires can be formulated as an ongoing report that lists vendors compliant with HIPAA and which ones are not. The information easily produced in NAVEX IRM communicates the overall vendor risk to executive management.

Reporting Keeps Management Informed

With NAVEX IRM, the health insurer has a central repository for all risk data. This data is correlated, analysed and delivered in management and executive-ready reports with the ability to drill-down to supporting data.

For example, the IT risk manager uses the platform to produce automated monthly metric reports for his CISO. The reports are easily generated every month, and if the CISO requests additional detail, NAVEX IRM simplifies creating a new report with additional data.

Using NAVEX IRM, the health insurer can report on everything from internal IT risks and cybersecurity incidents to IT audit findings and vendor risks.

NAVEX IRM

INTEGRATED RISK MANAGEMENT

Integrated Risk Management

Integrated Risk Management (IRM) is the collection of practices and processes that offer businesses a comprehensive view of how they identify, assess and prioritise risk throughout their organisation. NAVEX IRM, a GRC and Integrated Risk Management solution from NAVEX, equips users and business leaders to manage risk from the endpoint to the enterprise.

NAVEX IRM'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

Results: Turning Risk Into Opportunity

While HIPAA fines for vendor data breaches capture the headlines, this major health insurer is capturing data on its vendors and managing vendor risk. Efficiencies using NAVEX IRM also afford the IT Risk team more time to perform due diligence, which helps protect the company. Each year, the IT risk manager expands his department's reliance on NAVEX IRM, which now encompasses managing cybersecurity incidents, IT audit and assessment findings. Moving forward, the plan is to continue leveraging NAVEX IRM to engage in more efficient ways of managing risk and compliance.

WWW.NAVEX.COM | info@navex.com | +44 (0) 20 8939 1650

NAVEX is the worldwide leader in integrated risk and compliance management software and services. Our solutions are trusted by thousands of customers around the globe to help them manage risk, address complex regulatory requirements, build corporate ESG programmes and foster ethical workplace cultures.

© 2022 NAVEX GLOBAL, INC. ALL RIGHTS RESERVED. | 06.06.22