TEVORA™

Case Study

Tevora Helps Global Medical Device Provider Implement Top-Tier Enterprise Risk Management Program

As organizations continue to pivot and adapt to more sophisticated and technologically complex challenges, obtaining a holistic view of risk across the enterprise becomes increasingly difficult. Are all potential risks being successfully identified? What criteria are used to differentiate risks? Are risks prioritized and remediated in a timely manner? These are some of the challenges our partners come to Tevora with when building their enterprise risk management (ERM) program.

In this case study, we'll describe how Tevora helped a global provider of cloud-connected medical devices to streamline and improve their ERM program, providing them with a state-of-the-art risk management program that is more effective and less expensive to operate. To protect our client's confidentiality, we'll refer to them by the fictitious name of Global Medical Devices (GMD).

Expertise-as-a-Service

GMD engaged Tevora to address several risk management challenges they were experiencing and ultimately construct a top tier ERM program to protect and serve the organization's best interests.

Tevora experts and specialists began conducting interviews of the current GMD ERM team, key stakeholders and leaders, and all subject matter experts performing current security operations. This first step provides our experts with the context necessary to curate solutions that best meet the business needs.

Assessing the Challenge

Working in conjunction with the GMD team, the Tevora team became intimately aware of the GMD environment and the struggles they faced.

Here's a summary of the key ERM challenges identified:

Ineffective Risk Prioritization

No clear and standardized risk methodology was in use, which prevented GMD from effectively organizing risks or prioritizing initiatives.

Misdirected Risk Assessment Questionnaires

Questionnaires used to gather risk assessment information were flawed; many questions did not contribute to actionable risks, which unnecessarily added time and complexity to the risk assessment process. Conversely, the questionnaires did not ask questions that would be required of an effective risk assessment.

Risk Assessment Backlog

All risk assessments were performed by an insufficient number of GMD Information Security (InfoSec) staff, who were stretched thin and working long hours. The shortage of InfoSec staff led to a significant backlog of risk assessments, causing delays in identifying and addressing highly impactful risks.

Lack of Communication Between Information Security (InfoSec) and Business Units

In their rush to complete risk assessments and reduce the backlog, InfoSec staff often failed to fully communicate with business units and vice versa. As ERM programs are built on the intersection of business and security, this unreliable communication could not support an organization as expansive as GMD.

Excessive Time Required to Complete Risk Assessments

Conducting a risk assessment was a time-consuming affair, with some assessments taking multiple days, or even weeks, to complete. This, combined with the very few resources, created the backlog.

Minimal ERM Program Methodology

GMD relied on an undocumented, rudimentary methodology for managing enterprise risk, which did not scale well as the organization quickly expanded with recent successes.

Inaccurate Risk Assessments

As a result of the challenges described above, many risk assessments failed to identify significant risks to the organization. As this was the main tool for risk identification, there was very little confidence that the enterprise was not susceptible to attack.

Risk Management Improvements

With the challenges identified and well understood, we presented a series of improvements and initiatives to address the issues systemically. GMD management approved and Tevora continued the partnership with GMD staff by holding weekly team meetings to plan implementation, review progress, and handle any roadblocks as they arise.

The key improvements included:

Implementation of Tevora's HydraRisk Model

Tevora's proven HydraRisk model, with provided documentation, drastically improved GMD's risk management process. By combining both quantitative and qualitative analysis to risk ratings, GMD was far more equipped to prioritize and manage all identified risks. See below for more information on the HydraRisk Model.

Modified Questionnaires

Tevora experts worked with the GMD team to identify the information needed to conduct accurate risk assessments. The two teams added or modified questions throughout the risk assessment questionnaire to ensure only pertinent information was requested and no questions solicited unnecessary information.

Implemented Risk Prioritization

As part of the HydraRisk Model implementation, Tevora enhanced the risk management process to categorize all risks based on priority levels (Critical, High, Medium, and Low). This standardization allowed the separate business units within GMD to operate more efficiently when developing initiatives for remediation.

Increased Involvement of Business Units

Tevora modified GMD's risk assessment processes to have the business units perform all Medium and Low priority risk assessments - allowing InfoSec staff to focus efforts on Critical and High priority risk assessments.

For the Critical and High assessments, we modified processes to require InfoSec to consult the Business Units and ensure alignment on the potential business impacts of each risk.

Benefits

As a result of the partnership with Tevora, GMD now maintains a top tier ERM program and is delighted with the achieved results. Below are some of the benefits GMD has enjoyed after implementing an effective risk management program:

Faster Risk Assessments

GMD has significantly reduced the time it takes to perform each risk assessment. Most assessments are now completed in one day rather than multiple days or weeks.

Backlog Eliminated

The backlog of risk assessments has been eliminated, allowing InfoSec resources to focus on new initiatives.

Improved Accuracy

The accuracy of risk assessments has improved substantially, and GMD is no longer seeing significant risks go undetected due to inaccurate, incomplete, or delayed risk assessments.

Improved Prioritization

GMD is now focusing its most valuable resources on the highest priority risks.

Eased Burden on InfoSec Staff

With a portion of their work now moved to business units, InfoSec staff |is now able to focus their efforts on Critical and High risks and take the time needed to do thorough and accurate risk assessments.

Improved Communication and Engagement with Business Units

With the new processes, there is more dialog between InfoSec and the business units - improving the quality of risk assessments and increasing the business units' understanding of the organization's risks.

Improved Documentation

GMD's risk management processes are now thoroughly documented, which provides clarity to existing process users and facilitates the training of new users.

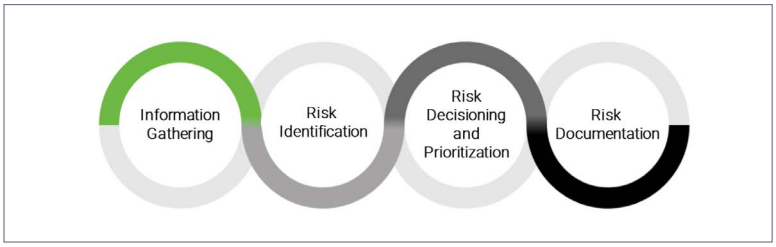
With a portion of their work now moved to business units, InfoSec staff is now able to focus their efforts on Critical and High risks and take the time needed to do thorough and accurate risk assessments.

HydraRisk Model

The HydraRisk Model is a proprietary quantitative and qualitative hybrid risk model developed by Tevora. While it draws from NIST 800-30 and NIST CSF, many aspects of the model are based on lessons learned from Tevora's extensive work with clients to help them implement risk models.

Tevora's model merges the best components of all other models to help organizations effectively assess strategic and security risks. HydraRisk accomplishes this without requiring deep statistical resources and requirements. However, it does provide more quantitative metrics than a purely qualitative model. These quantitative metrics provide organizations with strong justification for expenses required to mitigate identified risks.

The four steps of the HydraRisk risk management process are summarized below.



For more details on the HydraRisk Model, check out our recent blog post.

A Trusted Partner

Tevora has developed a strong partnership with GMD, and we are frequently asked to provide security services outside of the risk management domain. We also serve as advisors for many of their important business and technology initiatives.

Additional Resources

Check out these additional resources to learn more about Tevora's risk management services.

Tevora's Enterprise Risk Management Services

Blog Post: Tevora's HydraRisk Model—A Fresh and Unique Approach to Risk Assessments

ERM Program Development Datasheet

Managing Third-Party Risk Webinar

Blog Post: 4 Tips for a Successful HIPAA Risk Assessment

We Can Help

If you have questions about Tevora's enterprise risk management services or would like help implementing solutions in your environment, Tevora's team of security and risk management specialists can help. Just give us a call at 833.292.1609 or email us at sales@tevora.com.