FORTIFY

Benefits of Cybersecurity Risk Manager by Role

Cybersecurity Risk Management Simplified…

Cybersecurity risk management has traditionally focused on front-line technologies in the areas of threat prevention, threat detection, and event monitoring, commonly referred to as the technical side of cybersecurity. Most businesses direct all of their efforts towards these technical defenses. However, as the cyber threat landscape has continued to increase in frequency and complexity it is now expected that managers, executives and directors demonstrate their involvement in decisions that steer a business's approach to managing cybersecurity risk. Fortify 1 refers to this as the non-technical side of cybersecurity risk management. Many businesses are not aware of the risks associated with the failure to demonstrate diligence in the non-technical side of cybersecurity risk management which includes increased exposure to litigation and the possibility of non-compliance with regulatory requirements. An effective cybersecurity program requires the demonstration of holistic risk management achieved through organizational alignment, insight, and awareness that includes both the technical and non-technical sides.

Fortify 1's Cybersecurity Risk Manager (CSRM) offers businesses a way to simplify their approach in demonstrating how they manage both sides of cybersecurity risk. CSRM is an easy to implement, single point solution that is comprised of five core components that are designed to contain the evidence necessary to demonstrate how governance and oversight is applied, how risks have been identified, evaluated, mitigated, and remediated, as well as the plan and playbook that will be followed for responding to a breach.

Depending on an individual's role in the organization CSRM can provide the following benefits that can assist in their ability to effectively manage all aspects of cybersecurity risk.

Role

Governance	Benefits of CSRM
Board of Director Executive Management	• Understand how risks have been identified, evaluated, mitigated, and remediated by the organization. • Understand the approach for creating cybersecurity risk awareness throughout the organization. • Gain visibility into policies and procedures adopted by the organization for managing cybersecurity risks. • Understand the organization's plan and playbook that will be followed when responding to a breach. • Understand where the organizations stands in its ability to comply with state data privacy laws or other regulatory requirements. • Use reporting dashboards and interactive timelines that highlight how cybersecurity risks are being managed by the organization in easy to understand, streamlined formats. • Interactive timelines highlight governance and oversight actions that have been applied in steering the organization's approach in holistically managing cybersecurity risk.

Security Management	Benefits of CSRM
Chief Information Officer (CIO) Chief Information Security Officer (CISO)	• Simplifies the process of communicating with directors and executive management through use of reporting dashboards and interactive timelines that highlight how cybersecurity risks are being managed by the organization in easy to understand, streamlined formats. • Develop and apply policy and procedures designed to mitigate cybersecurity risk exposure. • Automated process for risk identification, evaluation, and remediation. • Automated process for documenting, retaining, and reporting on internal control evaluation results. • Drive continuous improvement through program management which allows assigning and tracking of tasks.
IT Management IT Security Technical Team	• Use interactive timelines that highlight the technical security work being performed to protect corporate assets such as threat prevention, threat detection, and event monitoring. • Use interactive timelines that highlight road map activities designed to evolve and mature the organizations cybersecurity risk management practices. • Provides visibility into cybersecurity policy and procedures that have been established to minimize exposure to cybersecurity risks. • Streamline your approach for preparing and evolving a Cybersecurity incident response plan. • Automate the process for conducting periodic risk assessments and internal control evaluations to determine the effectiveness of IT processes that support cybersecurity risk management. • Integrated risk assessment and internal control reporting functionality provides a real-time view into control gaps or deficiencies that require remediation. • Gain visibility into how cybersecurity risk is being managed throughout the entire organization.
Program Administrator	• Log and track IT security actions that demonstrate the organizational focus that has been taken to protect sensitive data and information. • Automate the approach to incident response planning and development through a hosted solution, • Demonstrate the organizations understanding and evaluation off risk exposure. • Automate the internal control evaluation process including integrated reporting functionality of test results and associated remediation activities. • Simplifies the approach for demonstrating compliance with state data privacy laws or other regulatory requirements. • Project management functionality can organizes projects, assigns tasks, and track and report progress.
Compliance	**Benefits of CSRM**
Legal	• Single point solution that highlights all the activity that has been taken by the organization to manage cybersecurity risks including structured repositories that contain supporting evidence. • Facilitates breach investigation by having instant access to all the evidence that aligns with cybersecurity risk management actions taken by the organization. • Demonstrate how the organization applies cybersecurity related policies and procedures to ensure responsible governance and oversight.
Internal Audit	• Customizable components simplify the periodic risk assessment and control evaluation processes. Integrated reporting functionality provides organization wide visibility into evaluation results and any corresponding remediation activities and status. • Facilitates a third party audit or review by regulators by having instant access to structured repositories that contain all the evidence that supports compliance with stated requirements.