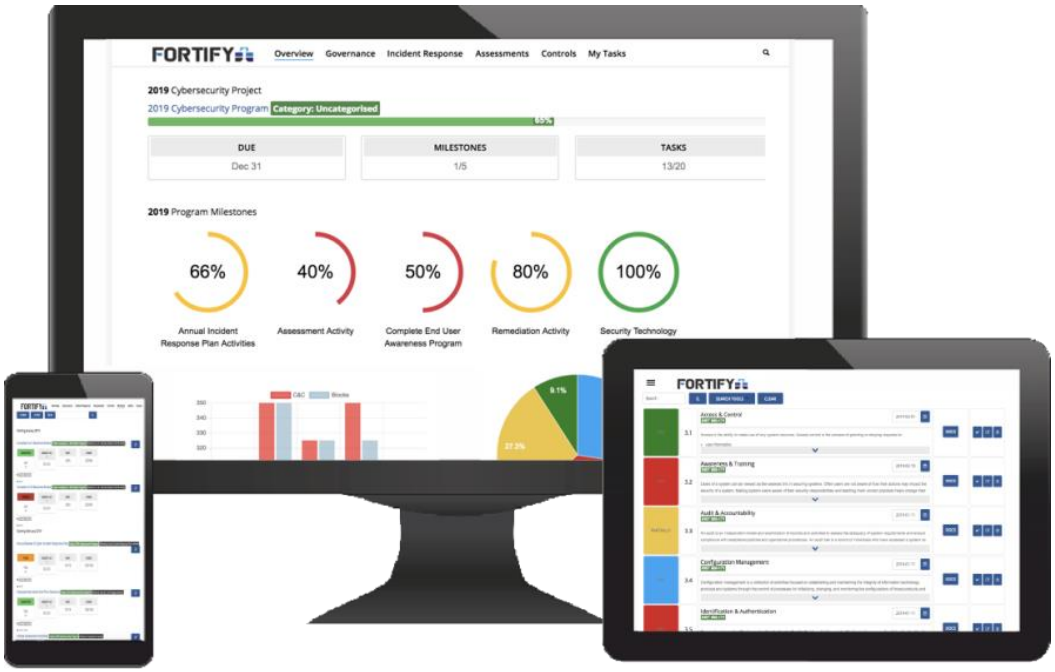
FORTIFY

Solution and Services Overview

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. Fortify1 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.

Fortify1'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 four 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. CSRM has project management functionality that provides administrators the tools required to organize projects and track progress of associated tasks. CSRM is flexible, configurable and can provide extensive functionality to fit large enterprises or be appropriately scaled to meet the needs of smaller businesses.



CSRM's four components include:

Governance

Incident Response

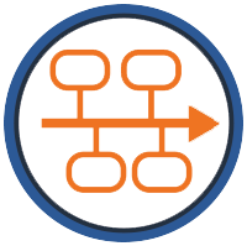
Risk Assessments

Internal Controls

Governance	As the cyber threat landscape continues to increase in frequency and complexity it is expected that managers, executives and directors of organizations demonstrate their involvement in the decisions that steer an organizations approach to managing cybersecurity risk. CSRM provides a governance specific timeline, designated document repositories, and reporting dashboards to inform stakeholders of the progress and status of their cybersecurity governance actions.
Cybersecurity Incident Response (CSIRP)	Cybersecurity frameworks such as National Institute of Standards and Technology (NIST) and Internal Organization for Standardization (ISO) consider cybersecurity incident response planning a suggested best practice. CSRM automates the approach to response planning and development. Whether a business is just beginning the planning process or already has a defined plan, the CSIRP component adds value by leveraging an online, expandable and collapsible format that is searchable, flexible and scalable.
Risk Assessments	A cybersecurity program should be periodically evaluated to determine its effectiveness. These evaluations can include a formalized risk assessment, network penetration testing, or maturity assessments. The Risk Assessment component has a customizable structure that automates the risk assessment process and includes integrated reporting functionality of results and associated remediation activities.
Internal Controls	Identifying, evaluating, and cataloguing internal controls that align with the risk management activities of a cybersecurity program is key to providing stakeholders insight to the security protocols administered by an organization. The Internal Control component has a customizable structure that automates how businesses manage the internal control evaluation process. It includes integrated reporting functionality of test results and associated remediation activities, and is designed to simplify the approach for supporting an audit or demonstrating compliance with regulatory requirements.

CSRM's features include:

Executive Dashboard



Interactive Timelines

Project Management

Reporting

Executive Dashboards	Present a dashboard of cybersecurity activity most meaningful to your organization. Display summary information, project and milestone status, operational metrics, key assessment activity and roadmap actions.
Interactive Timelines	Risk management activities such as operational security, security technology implementations (software & hardware), governance (meetings, discussions and decisions), end user awareness training, risk assessments, and third party security evaluations are considered program initiatives. CSRM uses interactive timelines to highlight these initiatives and provides stakeholder's information in an easy to consume format of how cybersecurity risks are being managed by the organization.
Project Management	Track cybersecurity and data privacy program activity with our project management feature. Create and track milestones, assign tasks and reference project dashboards. Display project activity progress on the dashboard to provide insight for stakeholders.
Integrated Reporting	Reference reports tied to project activities, timelines, assessment surveys and compliance status. Download reports to CSV, Excel and PDF formats.

Product Subscription and Licensing

CSRM is a subscription-based solution and is priced based on company size and specific configuration requirements. Fortify1 offers flexible subscription payment options to suit the needs of businesses of all sizes and budgets.

Product Delivery and Support

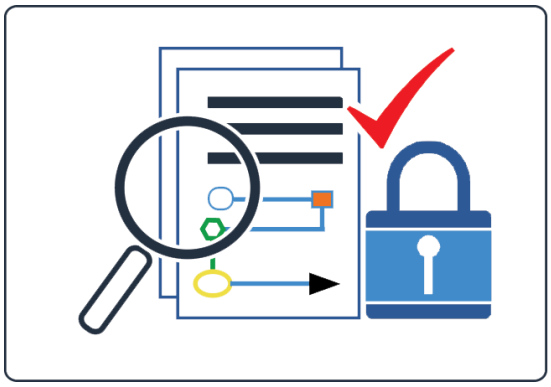
CSRM is delivered as a secured hosted solution and is not offered as an on premise option. Fortify1 provides technical and implementation support as well as training for all subscribers. Implementation support and training may vary based on company size, number of users, etc.

Services

Fortify1 offers a range of services to meet various client needs as they evolve their cybersecurity program to navigate the changing regulatory environment or meet demands from stakeholders who are responsible for cybersecurity risk management oversight.

Compliance Advisory

Risk Assessment



Risk Assessment

A documented risk assessment has been identified as a suggested, or required practice, in many state regulatory compliance standards. Fortify1 can assist clients in fulfilling this requirement as part of pre or post implementation activities. Specifically, Fortify1 will prepare a risk register that identifies the population of risks associated with information systems and system availability, collection and storage of non-public information, cyber threats facing the organization, and other applicable business operations. For each risk Fortify1 will align a suggested best practice internal control, or controls, that should be functioning in order to mitigate the associated risk. Fortify1 will evaluate the clients internal control environment to identify existing controls that address the suggested best practice control. In the event a control gap is identified Fortify1 will assist clients in their remediation efforts to enhance their internal control environment so that any uncontrolled risks are properly mitigated.

Compliance Advisory

Fortify1's compliance advisory service is focussed on assisting clients evaluate their ability to comply with state or federal regulatory requirements that they may be subject to. Specifically, Fortify1 will perform procedures to obtain evidence about the suitability of the design and operating effectiveness for internal controls that are in place to satisfy specific compliance requirements or stated best practices. In the event a control deficiency is identified during the evaluation phase of the engagement Fortify1 will assist clients in their remediation efforts to enhance their internal control environment in order to fulfil stated requirements. At the conclusion of the engagement Fortify1 will deliver a set of work papers for each internal control that outlines the test procedures performed and references to information that supports the basis for how the conclusion was reach for the suitability of design and operating effectiveness.

Post Implementation Assistance

Fortify1 can assist clients with post implementation activities in order to expedite getting their CSRM instance established. This may include creating interactive timelines, creating customized document repositories, populating repositories with supporting information, assistance with program management functionality, incident response plan migration or development, and installation of a response planning playbook.