SOLUTION BRIEF

CYBERSECURITY SOLUTION

Protect Your Digital Enterprise by Reinforcing Cyber Governance

Overview

Today's cyberattacks are bigger, more sophisticated, and more destructive than ever. All it takes is one breach to devastate an organization and tarnish its brand. Therefore, CISOs and CIOs[1] must be able to stay one step ahead, proactively anticipating and minimizing IT and cyber risks. This kind of foresight is particularly critical as organizations adopt new digital platforms, cloud-based systems, and mobility solutions, all of which increase the attack surface.

At times, the weakest cybersecurity link may lie in a vendor's IT system—which means that organizations have to not only monitor their own IT risks, but also those of their third parties. They also need to comply with a range of IT regulations like GDPR, the SOX Act, FFIEC mandates, PCI-DSS, GLBA requirements, HIPAA, and NERC-CIP[2], as well as IT governance standards such as those set by NIST and ISO 27001/2[3].

Managing all these requirements and risks the traditional way—i.e. using siloed systems and manual processes—is neither effective nor efficient. IT and cyber risks, regulations, controls, and related data are only growing more numerous and complex. To gain better control over them, many organizations are looking to integrate and streamline their cybersecurity management efforts.

MetricStream CyberSecurity Solution

The MetricStream CyberSecurity Solution provides a single point of reference to manage multiple cybersecurity related activities, including IT and cyber risk management, IT and cyber compliance management, policy and document management, and IT and cyber vendor risk management.

Built on a scalable MetricStream Platform, the solution cuts across enterprise siloes, aggregating and integrating data on IT and cyber risks, threats, compliance, policies, and controls. Centralized IT and cyber risk, and control libraries simplify risk analysis by establishing consistent risk taxonomies across the enterprise.

The solution maps IT policies to IT regulations, risks, and controls, helping users identify and minimize compliance gaps. It also provides valuable intelligence on the risks implicit in IT vendor relationships. Powerful reports and dashboards deliver a 360-degree, real-time view of IT and cyber risk, compliance, policy management, and IT vendor posture, enabling organizations to anticipate and mitigate IT and cyber risks in a timely manner.

Business Outcomes

66%	Reduction in the time taken to complete risk assessments
39%	Reduction in expected regulatory losses and other expenses
38%	Reduction in the cost of managing vulnerabilities and their impact
30%	Reduction in the number of man-days required to manage a scaled-up level of vulnerability management
50%	Time savings in tracking and linking policies to regulations
50%	Reduction in the time and costs required to complete third-party risk assessments, and to identify risks

Capabilities

IT and Cyber Risk Management

Adopt a streamlined and business-driven approach to IT and cyber risk management and mitigation. Define and maintain data on IT and cyber risks, assets, processes, and controls. Assess, quantify, monitor, and manage IT and cyber risks using industry standard IT risk assessment frameworks.

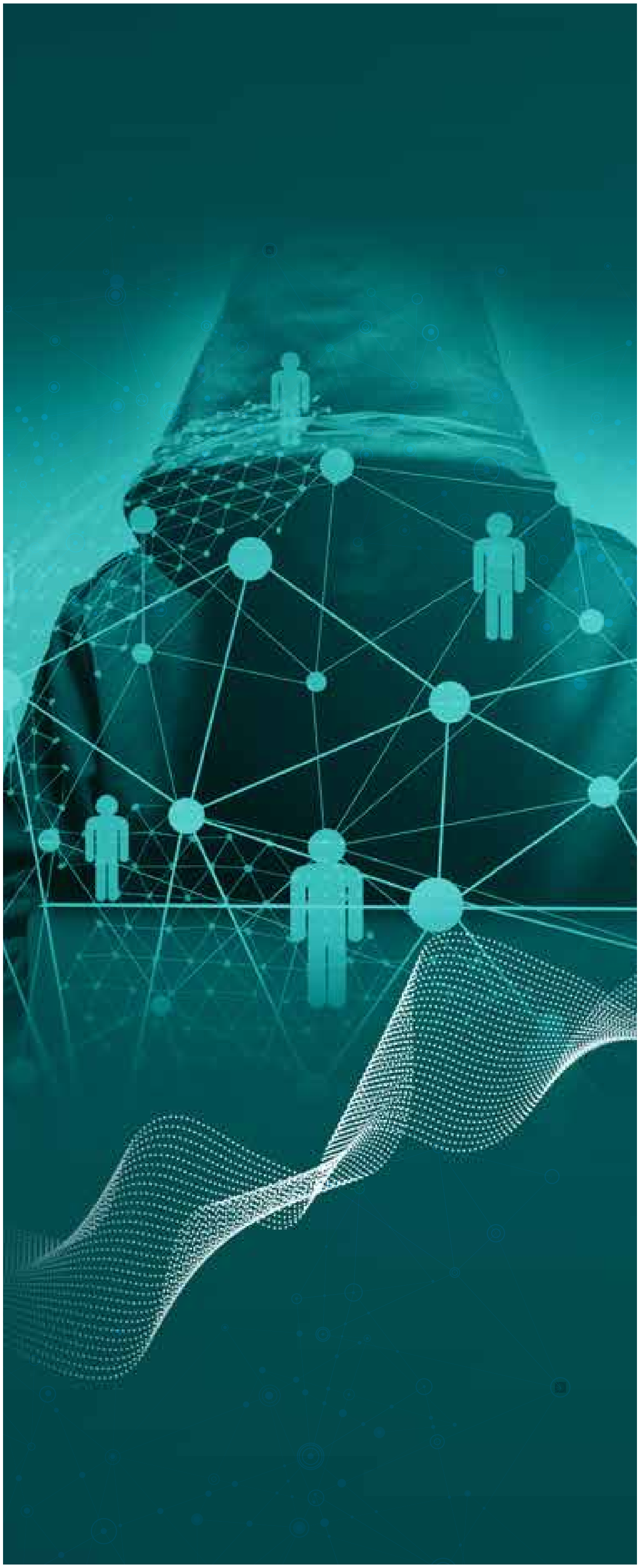
Identify and document issues from IT and cyber risk assessments through a closed-loop process of issue investigation, root cause analysis, and remediation. Generate user-configurable risk reports, risk heat maps, and role-based executive dashboards to transform raw IT and cyber risk data into actionable business intelligence.

Strengthen IT security by proactively aggregating and correlating threats and vulnerabilities across business-critical information assets. Consolidate IT assets in a common library by integrating with Configuration Management Databases (CMDB). Map these assets to business entities, as well as threats and vulnerabilities.

Integrate with multiple end-point IT security and infrastructure management tools and security intelligence feeds to identify and prioritize IT risks. Monitor the threat landscape, zero-day advisories, and threat bulletins by subscribing to RSS or email-based threat alerts.

Identify and document the issues arising from threat and vulnerability management in a structured manner. Generate real-time intelligence on threats and vulnerabilities through graphical dashboards and reports with drill-down capabilities.

Communicate your IT and cyber risk exposure in dollar values, using the Cyber Risk Quantification capabilities. With support from the FAIR model, provide the accurate and defensible monetary impact of cyber risks like data breaches, identity theft, infrastructure down time, etc. Fulfill regulatory requirements needing organizations to disclose cyber risk factors in financial terms. Enable executives to prioritize cyber investments better, driving alignment between cyber programs and business goals.



IT and Cyber Compliance Management

Manage and monitor compliance with a range of IT regulations and standards in an integrated manner. Create and maintain a central structure of the overall IT and cyber compliance hierarchy, including processes, assets, risks, controls, and audits. Integrate with the Unified Compliance Framework (UCF), mapping 9,300+ IT control statements to 1,200+ regulations.

Configure and execute IT and cyber compliance surveys, certifications, and control self-assessments using pre-defined templates and schedules. Link IT and cyber compliance controls and assessment activities based on the organization's specific regulatory requirements. Trigger a systematic process to document, investigate, and resolve IT and cyber compliance and control issues.

Receive alerts on IT and cyber regulatory updates and other actionable insights by subscribing to structured content channels. Gain top-level visibility into IT and cyber compliance processes across geographies, business units, and functional departments through real-time reports, user-specific dashboards, and graphical snapshots.

Policy and Document Management

Enable a systematic approach to IT policy management across business units, divisions, and global locations. Gain a centralized portal to store, manage, and access IT policies. Create policies by entering generally mandated information into the system, or by uploading an existing attachment.

Strengthen IT compliance by linking IT policies or sections of policies to regulations, risks, controls, legal requirements, processes, and organizations. Trigger policy review and revision cycles through automated notifications and task assignments.

Publish and schedule policies for distribution. Send automatic notifications to the target audience, alerting them to the new policy and the required attestation tasks. Track each stage of the IT policy management lifecycle in real time through powerful reports and dashboards.

IT Vendor Risk Management

Gain a single point of reference to identify, assess, mitigate, and monitor IT vendor risks while also managing vendor compliance. Accelerate vendor registration and onboarding by automating multiple workflows. Define the frequency of vendor assessments based on the associated risk profiles.

Simplify due diligence by leveraging pre-defined questionnaires to assess vendor risks. Easily assign tasks and document interactions with vendors. Leverage powerful reports, analytics, and business intelligence capabilities to help management teams make informed decisions based on a sound understanding of vendor risks, compliance, and performance.

Business Continuity Management

Delivers pre-embedded business continuity plan templates, and helps edit them based on industry standards and frameworks (all changes or edits are reflected across multiple linked continuity plans).

Provides a configurable scoring logic, metrics, and algorithms to calculate recovery objectives (Recovery Time Objective (RTO), Recovery Point Objective (RPO), and Maximum Tolerable Period of Disruption (MTPD)); helps track multiple recovery strategies through Gantt charts.

Integrates with Emergency Mass Notification Systems (EMNS) for users to send notifications to individuals or groups through multiple contact paths.

Provides configurable reports and dashboards with information on gaps between recovery requirements; allows users to drill down to view the finer levels of details.

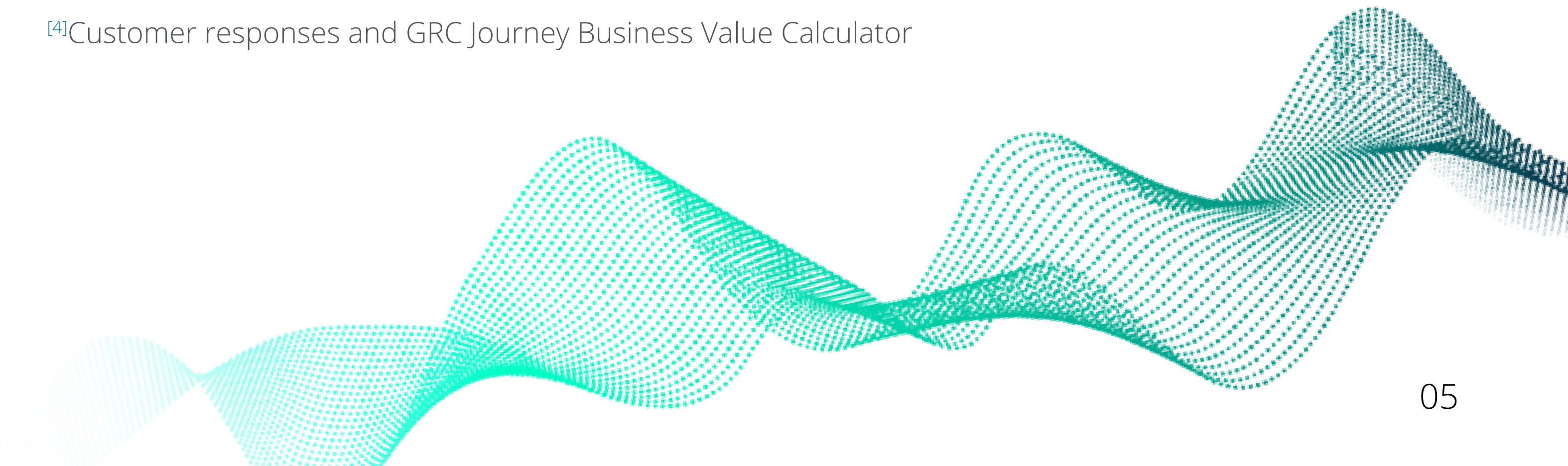
Provides native mobile apps on Windows and iOS platforms, enabling authorized users to easily access and download BCM plans on their tablets, smart phones, or laptops.

[1] CISOs – Chief Information Security Officers; CIOs – Chief Information Officers

[2] GDPR – General Data Protection Regulation; SOX – Sarbanes Oxley Act; FFIEC - Federal Financial Institutions Examination Council; PCI-DSS - Payment Card Industry Data Security Standard; GLBA - Gramm–Leach–Bliley Act; HIPAA - Health Insurance Portability and Accountability Act; NERC-CIP - North American Electric Reliability Corporation – Critical Infrastructure Protection

[3] NIST - National Institute of Standards and Technology

[4] Customer responses and GRC Journey Business Value Calculator



metricstream

CONTACT US | REQUEST A DEMO