SPOTLIGHT

Sponsored by: DigitalXForce

A new generation of cybersecurity GRC and IRM solutions based upon "digital trust" is crucial in today's fast-paced threat landscape. It is time to significantly reduce human bias and increase real-time, continuous, and data-driven risk and compliance practices that result in trusted organizations.

It's Time to Take GRC and IRM to a New Level

January 2024

Written by: Philip D. Harris, CISSP, CSSK, Research Director, Governance, Risk and Compliance

Introduction

Traditional governance, risk, and compliance (GRC) and integrated risk management (IRM) have been slowly evolving over the past few years. However, with this evolution, there has been an insignificant improvement to the organization's security posture. Key issues with today's GRC/IRM programs include rampant bias, low productivity, lack of trackability, reliance upon outdated and fabricated artifacts, costly and ineffective methods, and a very compliance-centric approach.

To disrupt the GRC/IRM markets, what is needed is a reduction in human bias (a result of qualitative analysis) by providing real-time data, risk quantification, automation, and continuous security control testing that provides a clear picture of the organization's security posture while enabling overall compliance.

AT A GLANCE

WHAT'S IMPORTANT

Digital trust in the context of governance, risk, and compliance with integrated risk management means that there is confidence in the outcomes of risk and compliance activities. Therefore, risk managers, executives, and board members have a real-time and quantitative view of the current risk and compliance posture on a continuous basis. They can then use this view to make critical business decisions that can potentially affect revenue, brand, and reputation.

Situation Overview

There are many distinct types of GRC/IRM programs today that all circle around regulatory compliance but do not show true risk as a natural outcome. These programs are focused on showing risk assessment results where organizations try to attain some sort of risk level or compliance score. There is no correlation between these levels or scores and how these contribute to the security risk posture. The main reasons for this discrepancy include human bias, qualitative analysis, subjectivity, interpretation, or lack of knowledge or context.

In effect, two different risk assessments for the same platform, technology, or process performed by different analysts can yield different results because of personal bias. Each analyst will interpret existing security policies and controls and then create a subjective opinion of their findings. Analysts also may not possess the appropriate skill set to identify recommendations that are useful for remediation, or worse, the recommendation is so expensive or complex that remediation is prohibitive, requiring sensible compensating controls. In this case, the analyst may not possess the overall architectural context to create these compensating controls.

Inevitably, personal bias can be detrimental and produce wildly different results that executives and the board cannot depend upon to make their decisions. Yet, in many cases, executives make decisions based on disparate results anyway because there is nothing else available on which to make risk decisions. Breaches continue to happen, and bias contributes to this ongoing situation because risks are not properly identified and analyzed and remediated objectively.

GRC and IRM must be transformed in such a way that they express the trusted nature of the outcomes of the GRC and IRM programs themselves. These outcomes can then be trusted by the CISO, CRO, C-suite, and members of the board. Several factors can contribute to creating GRC and IRM outcomes that can be trusted. These factors include:

- Real-time and continuous risk analysis to improve compliance and cybersecurity posture management
- Data-driven and automated integrated risk management and security control testing
- Complete and comprehensive integrations across the IT estate and security tools so no digital risk is missed or forgotten
- Quantifiable metrics to create a consolidated and complete view of compliance and security risk posture
- Prioritized and actionable road map
- A policy framework that is complete and constantly updated as industry and regulatory landscapes change
- Readily available executive dashboards that reflect an up-to-date and trusted view of the current state of risk and compliance across the organization

Accurate results and outcomes will increase exponentially with the use of real-time automation and integrations. This in turn will result in a better understanding of how trustworthy an organization is to its clients, investors, and the overall marketplace. Risks should be clearly understood and include common profiling across the IT estate and lines of business to know exactly what is being assessed. The security control testing and associated risks should correlate against common control frameworks and regulations. These quantifiable risks and recommendations should then guide the security implementation road map and investments.

Risk management can no longer be subjective or biased with a significant percentage of the actual results driven by human beings. Reducing human involvement in assessment processes will increase the overall accuracy of the results and significantly reduce subjectivity. Analysis will become much easier with the rise of digital technologies and artificial intelligence. Customers expect organizations to use their best efforts to safeguard their confidential information and provide reliable data protection. Outcomes generated in a "security blueprint" or road map format become living attributes that continually evolve along with the IT estate and business environment. Hence security risk assessment results are fact based, data driven, actionable, and trustworthy.

What Is Digital Trust?

Digital trust in the context of GRC and IRM means that there is confidence in risk outcomes and compliance activities such that an organization or, more specifically, risk managers, CROs, CCOs, CISOs, the C-suite, and board members can confidently and reliably understand their current risk state and compliance posture at all times, empowering them to make critical business decisions that could prevent negative security events and incidents affecting revenue, brand, and reputation. With digital trust, executives can have full visibility into their digital ecosystem and associated security risks.

The failure of GRC and IRM programs to provide security protection to the organization could potentially lead to financial, brand, and reputational impacts that could be disastrous for an organization. These impacts can be especially damaging as reliance on these tools creates a false sense of security, thus making the organization susceptible to threats such as cyberattacks, fraud, and litigation.

Digital trust refers to the level of confidence that individuals and businesses have in the security, privacy, and reliability of digital transactions and interactions. Digital trust is important for businesses because it helps build customer loyalty, drives revenue growth, and empowers executives and board members to place confidence in their security design and operations beyond point-in-time audit results. By having real-time, data-driven, and continuous assessments of their environment, organizations can finally enable digital trust and have the outcomes supporting it.

A trustworthy GRC and IRM program allows companies to use real-time data to make informed decisions in response to their present state, the marketplace, and current or anticipated concerns. Digital trust, in the context of this paper, is intended to disrupt GRC and IRM as we know it. The disruption comes in the form of removing human subjectivity and bias out of risk and compliance management, increasing the amount of real-time risk analysis and compliance data collected from the organization's environment, to obtain actionable and reliable results.

With digital trust, there will be confidence backed up by tangible results, and organizations will be more transparent in revealing their true security posture, adherence to regulatory compliance, and data protection maturity. Customers will benefit through higher standards of data protection and be assured that their data is being managed responsibly. Risk and compliance programs will prove beneficial and dependable, playing key roles in ensuring that the overall control environment is maintained, updated in real time, and consistently reliable.

How Is Digital Trust Different from Traditional GRC and IRM?

In many cases, current GRC and IRM programs offer qualitative assessments that only serve as a "check the box" activity mostly driven by individual analysts. These GRC and IRM programs are heavily audit and compliance centric and miss the mark on what is needed in security posture management. This shortcoming increases the ineffectiveness of the risk or compliance assessment because a high degree of bias and subjectivity is injected, whether consciously or unconsciously.

Risk and compliance assessments are mostly qualitative, and even when documentary evidence is required, it is easily manipulated, is made to fit, and rarely provides a real-time representation of the effectiveness of the control in question. Ultimately, evidence, usually in the form of a screenshot or sample data, serves to document that the control requirements are met without providing any real acknowledgment of the effectiveness of the control from an implementation perspective.

Check-the-box exercises only help meet the compliance requirement but do not demonstrate the true security posture of the organization. Digital trust enables a secure environment with sufficient visibility to see into and confirm regularly

that the security tools and processes in place are functioning to provide the intended results versus a fabricated illusion. The distinction comes down to whether an organization merely wants to appear compliant or chooses to design a secure environment.

Organizations need a new unified view of the digital (cybersecurity and privacy) risk that enables digital trust to help prioritize and remediate cyberthreats in any landscape regardless of complexity. This unified view must be powered by automation. Through a unified digital trust platform, organizations can benefit from data-driven, real-time, and continuous integrated risk management with end-to-end visibility, governance, analytics, and reporting to optimize and automate cyber-risk and compliance postures.

What results from a digital trust–enabled GRC and IRM program are several key capabilities, including:

- Compliance and cybersecurity posture management are comprehensive. This approach is distinct from programs and platforms that depend on qualitative workshops and security control questionnaires, which can be time-consuming and less effective.
- Real-time and continuous risk management is made possible through automated integration with digital assets and security tools. This strategy ensures efficient and effective risk management through continuous monitoring and utilization of advanced security tools.
- Quantifiable security metrics are more necessary now than ever before. With the increased accuracy and timeliness of risk and compliance information, organizations can quantify risk management and can determine the financial impacts between managing and not managing risks appropriately. This approach allows organizations to prioritize their efforts and resources more effectively than they can do with platforms that cannot quantify security risks, KPIs, and KRIs. Organizations can make data-driven, dollar-based decisions and focus on the areas that require the most attention to reduce overall security risk.
- Actionable remediation plans and living road map blueprints are now possible and can assist in the ongoing monitoring of risk and compliance management from an execution and cost management perspective. Organizations can address risk and compliance issues more efficiently and effectively by prioritizing remediation efforts based on those specific vulnerabilities and risks that have the most security and monetary impact to the organization.
- Automated security policies and operational procedures are so critical in today's fast-paced threat landscape. Organizations need to automatically monitor, update, and manage security policies and operational procedures that keep current with the industry and regulatory requirements that are in a constant state of evolution. This unique capability will save time and effort, enabling organizations to maintain up-to-date and relevant security practices.
- Executives and board members are requesting automated and real-time dashboards. As the regulatory landscape evolves, executives and board members are charged with having more direct involvement and knowledge of their organizations' risk and compliance postures at any given time. These key decision makers can become an integral part of the risk management process by making informed decisions quickly and effectively.

Benefits

Among the several benefits of enabling GRC and IRM with digital trust are the following:

- There is the potential for removing upward of 75% of human involvement in the assessment process, significantly reducing bias and subjectivity and opening the way to accurate and count-on-able results and outcomes.
- Risk and compliance analysts can play a much more significant role in dealing with complex risk or compliance issues that cannot be automated and pursue other higher cybersecurity priorities.
- Outcomes generated in a "security blueprint" or road map form can become "living" outcomes that will change and adjust to the evolution of the IT estate as well as changes in the business.
- Results are fact based, highly accurate, objective, and tangible, enabling executives to make highly effective decisions that are easily understood.
- The continuous risk assessments allow organizations to stay up to date on the latest and greatest security threats and risks.

Considering DigitalXForce

DigitalXForce aims to be at the forefront of revolutionizing the cybersecurity landscape and instilling digital trust in the modern era. It offers a unified SaaS digital trust platform that provides real-time, data-driven, continuous integrated risk management. By leveraging data-driven insights, security blueprints, and regulatory control mapping, DigitalXForce optimizes and automates the digital risk posture of organizations.

The company was born out of a realization that existing IRM and GRC platforms were falling short of securing digital businesses. In response, DigitalXForce provides a mission-driven digital trust platform designed to simplify cybersecurity and privacy through automation, ensuring digital trust inside out. The platform offers a comprehensive range of capabilities, including attack surface management, risk quantification, automated audit, and compliance. Its innovative approach empowers organizations to enhance their security posture while maximizing their investments in digital transformation.

Leveraging DigitalXForce, organizations will be able to derive the "digital trust" score (much like a credit score) that can serve as an industry standard to demonstrate an organization's security posture maturing rating for secure digital business. In addition, organizations will be able to derive a quantitative and objective plan for improving their cybersecurity posture while demonstrating compliance with applicable regulations. Cyberinsurance underwriting and third-party risk management (TPRM) will be based on objective risk ratings derived through security control implementation versus qualitative application forms. DigitalXForce will allow organizations to derive a security blueprint and compliance reports out of the box.

Challenges

DigitalXForce is striving to disrupt the market by becoming the industry's first digital trust platform for the new era. As with any vendor intending to disrupt markets in a major way, the task for DigitalXForce will be to continuously provide a consistent message to the marketplace that truly differentiates its solution from current players. DigitalXForce must redefine the market from one that emphasizes GRC and IRM to one that offers digital trust powered by enhanced GRC

and IRM capabilities. This shift — in addition to marketing momentum — will be necessary for DigitalXForce to disrupt the market.

Conclusion

A digital trust–enabled GRC and IRM program allows companies to make informed decisions about their present state by using real-time data on a continuous basis. Organizations can accomplish this approach primarily by reducing human bias, automating security control testing, performing real-time security risk analysis, and generating bottom-up risk quantification.

IDC believes this new approach in the GRC and IRM markets is critical, and to the extent that DigitalXForce can address the challenges described in this paper, the company has a significant opportunity for success.

About the Analyst

Philip D. Harris, CISSP, CCSK, *Research Director, Governance, Risk and Compliance*

Phil Harris is the research director for CRMS. He is responsible for developing and socializing IDC's point of view on governance, risk, and compliance across people and process focused on creating a foundation of privacy and trust with enterprises, IT suppliers, and service providers.

MESSAGE FROM THE SPONSOR

Digital Trust Platform provides data driven, real time, and continuous Cybersecurity Risk Management that is simplified, measurable, integrated and actionable. DigitalXForce is a NIST 800-53/NIST CSF driven SaaS platform to protect enterprise digital assets by integrating security services into a central hub model while maximizing visibility, effectiveness, and efficiency with unified view through measurable KPIs/KRIs.

The core capabilities of DigitalXForce include, but are not limited to:

- Identify all Digital Assets and establish Attack Surface
- Integrates with deployed cybersecurity tools and services
- Real-time and continuous security control testing
- Develop Security Blueprint, Security Policies, Plans, Standards and Procedures
- Develop Security Scorecard, Dashboard and Security Plan of Action
- Third-Party Risk Management
- Cyber Insurance Policy Underwriting
- Integrated Risk Management

Organizations need a unified view of the Digital Cybersecurity & Privacy (Digital X) Risk that can help them prioritize and remediate the cyberthreats in the complex hybrid landscape powered by automation. DigitalXForce is valuable for any organization looking to enhance its cybersecurity and privacy posture and protect its critical assets from cyber threats.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com