tracesecurity
Compliance, simplified.

White Paper

Transforming IT GRC into a Mainstream Business Application

An integrated, cloud-based approach to data security and compliance.

tracesecurity
Compliance, simplified.

877-275-3009 tracesecurity.com sales@tracesecurity

Executive Summary

In an economy riding on an Internet backbone and driven by shared data, organizations face unprecedented challenges in protecting company and customer data, and complying with an ever-changing body of related government, industry and corporate mandates.

For all but the largest organizations, fully meeting all the complex requirements for data protection and compliance is nearly impossible – not just because of the cost of all the required applications and system infrastructure, but also due to the lack of **A)** dedicated IT security specialists, and **B)** detailed knowledge regarding current regulatory and industry mandates.

To correct this, a new IT governance, risk and compliance (GRC) prescription is overdue – one that provides true enterprise-class capabilities that can be found in large organizations, but without the enterprise burdens of infrastructure investment, specialized personnel and administration of multiple vendors. With the development of TraceCSO, TraceSecurity has fulfilled that prescription and, in doing so, has created an exciting new standard for IT GRC.

A Growing Market Dilemma: How Can Organizations of Any Size Cope with the Complexities of IT GRC?

Data is the lifeblood of business – coursing through the Internet and across global trading communities, connecting hundreds of thousands of companies and hundreds of millions of consumers. In this vast digital marketplace, companies are under increasing pressure to protect both proprietary data and sensitive customer information and to comply with a growing body of security-related government regulations, industry mandates and supply chain rules. Falling short in these measures can lead to costly consequences.

The most recent Data Breach Investigation Report from Verizon cites the increasing volume of serious data breaches, identifying the loss of 174 million data records in 855 separate incidents in 2011 alone. Various studies have estimated average costs to corporations to be as high as $7 million per data breach, and over $200 per affected record. There is also the cost of regulatory non-compliance, which can range from stiff fines to criminal prosecution; and the penalties that result from the failure to meet supply chain mandates, which can include steep charge backs and lost business.

No Longer Just a Big Company Imperative

Very large organizations can afford to invest in customized solutions to meet data security and compliance requirements. Most also have the scale and resources to weather the repercussions if those measures fail.

But very few small and medium enterprises have the means to absorb the impact of regulatory penalties, class-action lawsuits, lost business and diminished market value. Today, there are approximately seven million companies in the U.S. that are large enough to have employees on a payroll. Hundreds of thousands of these companies are in financial services, retail, healthcare and other industries where IT GRC is becoming an increasingly urgent issue. Yet, the vast majority of these companies have no dedicated IT security specialists, let alone a Chief Security Officer.

For most organizations, adopting an IT GRC strategy is a journey into the unknown, and the hurdles are imposing:

The Cost of Acquiring and Administering All the Essential IT GRC Capabilities

Developing and managing a comprehensive IT GRC strategy using conventional point solutions is both expensive and inefficient. Expensive, because such an approach requires the deployment and support of disparate applications from multiple vendors; inefficient, because these point solutions aren't designed to work together, and will likely become less compatible over time as they follow different evolutionary tracks.

The Challenge of Staying Current with Fast-Evolving Security Threats and Security-Related Regulations

There's a long-accepted principle in law that "ignorance of the law does not constitute a defense." In the world of data security and compliance this principle is compounded by the growing volume of data, the multiple sources and purposes of data, and the manner in which data is often shared by multiple parties within a broad trading community. And, it is especially compounded by the multitude of rules and jurisdictions that dictate policies and practices. Consider the bewildering alphabet soup of security-related regulations, including SOX, HIPAA, GLBA, EUDPD, PCI-DSS and thousands of other discrete rules and citations around the world. In this environment, many organizations are at risk in ways they don't fully grasp.

The Burden of Capturing and Leveraging Data Generated Across the Functional Areas

Ultimately, the value of an IT GRC strategy is determined by its effectiveness in helping an organization achieve governance, risk and compliance objectives. It must capture and process data to reveal the organization's risk posture, enforce security policies, support audits, and provide insights that contribute to critical business decisions. None of these tasks can be optimized with a tactical, patchwork approach.

Rethinking IT GRC Management For All Organizations

Like many other strategic applications, IT GRC management has developed and matured in large enterprise environments, often with highly customized features and capabilities that serve unique corporate requirements. Yet, even within many large and sophisticated companies, GRC capabilities are yet to be fully integrated and centrally managed, with functions such as vulnerability management, policy and training still managed as separate point solutions.

Given the urgency of the need, smaller organizations can ill-afford a similar maturity path. To be fully secure and compliant, small and medium-sized enterprises (SMEs) need proven enterprise-class capabilities – but their IT GRC solution must come already streamlined, standardized and integrated. As with ERP, CRM and other strategic applications that have migrated "down-market," IT GRC is now refined enough to be "mainstreamed." This transformation – from a complex assortment of disparate technologies to a straight-forward business application with built-in intelligence – will enable application effectiveness, and competent use by non-technical personnel.

The movement to accelerate such refinement of IT GRC management is gaining broader currency as industry experts increasingly recognize that GRC can be an evolutionary business management approach that helps any organization reap the benefits of approaching governance, risk and compliance in a cohesive, planned manner. Further, a study of "best-in-class" enterprises reveals that those leading organizations view GRC beyond a defensive solution and potentially as a contributor to company growth strategies.

The Requirements:

An ideal integrated IT GRC platform solution would be characterized by a number of key attributes, including:

- **Completeness:** Whereby all core IT GRC functions are tightly integrated and centrally managed.
- **Visibility and Accountability:** With the capability to provide a clear, coherent projection of risk posture, along with easy to understand, actionable recommendations and/or automated responses.
- **Compliance Awareness:** Enabling functions to be automatically mapped to the broadest possible database of current standards and regulations.
- **Cloud-Based Delivery:** Eliminates the need for on-premise hardware and infrastructure, and allows easy scalability.

TraceCSO: Purpose-Built To Meet The IT GRC Challenge

TraceSecurity has introduced TraceCSO as the first and only complete, cloud-based IT GRC solution, specifically designed to encompass the primary capabilities detailed above. It answers the IT GRC challenge by allowing organizations to automate data protection and compliance functions, including the oversight role of the Chief Security Officer. It does this by combining six key elements:

1. A Complete, Integrated Suite of IT GRC Management Functions

TraceCSO incorporates risk, compliance, policy, training, audit, incident response, BIA/BCP, vulnerability, vendor and process management. They are fully integrated to allow all functional areas to communicate and automatically update the organization's risk and compliance posture. This dramatically streamlines the entire risk management and compliance process.

2. Guaranteed Currency with All Global Standards and Regulatory Mandates

TraceCSO is integrated with the Unified Compliance Framework (UCF) to ensure that policies and practices are up-to-date with the most recent versions of every IT-security-related mandate in the world – over 25,000 citations and regulations from hundreds of authorities. The UCF is the only industry-vetted compliance database that reduces this vast regulatory maze to a much smaller set of "harmonized" controls – providing a single point of management over hundreds of complex compliance requirements. TraceCSO leverages the UCF to automatically map the overlap between multiple authority documents, create control lists for specific IT areas, and clarify conflicts created by overlapping authority documents.

3. User Interface for Easy Management and Comprehensive Reporting

The TraceCSO user interface uses an easy-to-read dashboard that offers an intuitive setup process, as well as tools such as wizards and step-by-step guides. The UI also communicates a wealth of risk status information at a glance. It provides all the controls needed to access and leverage data in forms ranging from executive summaries to over 30 discrete reports covering 10 functional areas. It enables users to:

- Create and view reports
- Create module-specific reporting based on the same data as presented in dashboards
- Package multiple reports into an aggregate report
- Provide text responses to graphical and table data to appear in reports
- Generate and archive reports, freezing them in PDF format

4. Built-In Integration and Support Services

TraceSecurity's world-class security expertise is part of the complete TraceCSO solution and is applied at multiple levels:

- Configuration and deployment – Assures the solution is properly integrated and functions as needed to meet an organization's specific requirements.
- Product support – Keeps the solution up-to-date and performing at an optimal level for the life of the subscription.
- Baseline consulting – Applies security and compliance expertise to resolve routine IT GRC issues up to a specified number of hours, based on the subscription level.

5. The Availability of Professional Services and Strategic Consulting

In addition to IT GRC software, many organizations also need assistance that goes beyond the built-in integration and support services detailed above. They may require greater assistance in evaluating their solution needs, deploying applications in their IT environment, and optimizing their IT GRC solution in an evolving business environment. That is why the TraceCSO solution not only delivers a full suite of IT GRC software applications, but also serves as the management and reporting environment for TraceSecurity's complete portfolio of professional services and consulting practices. These include:

- Security Assessment
- Risk Assessment
- IT Security Audit
- Penetration Testing
- Social Engineering
- Application Testing
- Wireless Assessment
- Security Training

6. Affordable, Scalable Cloud-Based Delivery

A simple yearly subscription delivers the full-force of a complete, always current, enterprise-class solution – without the need for capital investment or additional personnel.

Conclusion: The TraceCSO Approach Delivers Strategic Impact

TraceCSO is a ground-breaking innovation that finally puts enterprise-class IT GRC management within the reach of any organization most of which don't have the benefit of a Chief Security Officer or a dedicated IT security team. By transforming IT GRC into a unified and easy-to-manage business application, it changes the game in big ways:

It introduces automatic security and compliance, with built-in expertise and best practices that eliminate guesswork, as well as the need for internal security specialists. The interface, controls, documentation and reporting functions are simple and can be easily mastered by non-technical users.

It delivers dramatic savings, with a simple year-to-year browser-based subscription model. It is affordable, scalable, and eliminates the need for capital investment. This results in a savings of more than 80% over the installed cost of comparable point solutions, and a total cost of ownership (TCO) estimated to be up to 50% lower.

It enables rapid deployment, because it is a unified, browser-based platform and includes expert implementation services from TraceSecurity. Typically, TraceCSO can be up and running in a matter of weeks, without any business disruption – versus conventional solutions that have been known to require deployment schedules exceeding 12 months.

It accommodates on-going change, thanks to its platform architecture, integration with the UCF database, and combination with TraceSecurity professional services and consulting. TraceCSO is the market's only long-term IT GRC solution. It is complete in its functionality, designed to accommodate new functions and features, easily scales to thousands of users, and is always current with every regulatory and industry mandate in the world.

About TraceSecurity

TraceSecurity is a leading provider of cybersecurity and compliance solutions that helps organizations of all sizes reduce the risk of cyber breaches and demonstrate compliance. With a combination of software and services, TraceSecurity can help organizations manage their information security program and supplement it with third-party validation.