SDS
SECURE DIGITAL SOLUTIONS

Governance, Risk, and Compliance (GRC) White Paper

Table of Contents:

Conducted by Secure Digital Solutions April 2014

1550 Utica Ave Suite 420 Minneapolis, MN 55416
main: 952-544-0234 www.securedigitalsolutions.com

PROACTIVE > SECURE > CONFIDENT

Secure Digital Solutions (SDS) is a vendor-independent professional services firm specializing in information security, IT compliance, and privacy related solutions. Governance, risk, and compliance (GRC) services include: vendor risk management, compliance readiness, incident management, DR / BCP management, ISO27002 control management and security program maturity with an executive dashboard.

SDS has clients that range from for Fortune 1000 companies in the healthcare, finance and retail as well as client relationships with higher education, retail, legal services and government entities.

In the State of Information Security Second Annual Assessment Study 2013, conducted by SDS, respondents identified GRC as one of their top priorities. This white paper explores key considerations on the topic of GRC.

Purpose

The intent of this whitepaper is to reveal to senior management and executives the benefits of implementing an integrated GRC framework within their business. The reader will obtain critical information regarding the current trends with GRC, business case, and how organizations can obtain a return on their GRC investment.

Introduction

Governance, Risk and Compliance (GRC) management is an effective means for organizations to gather important risk data, validate compliance, and report results to management. Definitions of GRC vary as do the potential applications, uses, and organizational approaches to implementation. Often, GRC capabilities are implemented in silos across organizations (e.g., vendor management, compliance management etc…) failing to integrate and synthesize the collective results, therefore duplicating effort and not taking full advantage of GRC as a cohesive program and the benefits this delivers.

This white paper explores the GRC landscape and includes the following topics:

- What is GRC?
- GRC Concepts
- Integrative Approach and Methodology
- Current Trends
- Business Case for GRC
- GRC market - Solutions and Vendors
- Return on Investment (ROI) Discussion
- Summary

What Is GRC?

Wide-ranging definitions of GRC exist among industry experts and vendors, yet GRC encompasses activities such as corporate governance, enterprise risk management (ERM) and corporate compliance with applicable laws and regulations.[1] SDS extends this definition to incorporate additional areas including Vendor Management, DR / BCP Management and Incident Management.

An effective GRC framework enables organizations to integrate and coordinate risk and compliance initiatives with business processes, providing a holistic view of the organization's risk and compliance postures and enabling management to make informed decisions on how to allocate resources and mitigate risks effectively.

1 Wikipedia, Governance, risk management, and compliance, last modified on September 30, 2013

GRC Concepts:

- Governance describes the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.
- Risk Management is the set of processes through management identifies, analyzes, and where necessary, responds appropriately to risks that might adversely affect realization of the organization's business objectives.
- Compliance means conforming to stated requirements, as defined by laws, regulations, standards, contracts, strategies, and policies. Examples include: Gramm Leach Bliley Act, Payment Card Industry Data Security Standards, Sarbanes Oxley Act, National Institute of Standards and Technology (NIST), International Organization of Standardization, Generally Accepted Privacy Principles, etc.

Integrated Approach and Methodology

Rather than acquiring separate solutions for compliance, IT and other business units, organizations are increasingly choosing to use a single enterprise GRC platform and when necessary, integrating solutions to satisfy specific GRC needs. "Reporting and managing through a single platform potentially gives executives, auditors and managers a holistic view of the enterprise's risk and compliance postures, as well as views sorted by requirement, entity and geography."[2] The platforms typically provide functionality that integrates over a wide range of GRC business requirements (see Table 1.0).

An integrated GRC platform takes information from multiple sources and provides a source of intelligence and reporting (see Diagram 1.0). Dashboards and data analytics tools allow administrators to identify and organize risk exposure, map policy compliance to external regulations or quickly administer vendor or client audits.

2 Gartner.com, Magic Quadrant for Enterprise Governance, Risk and Compliance Platforms, October 4, 2012

Diagram 1.0 - GRC Key Functions and Integrated Solution

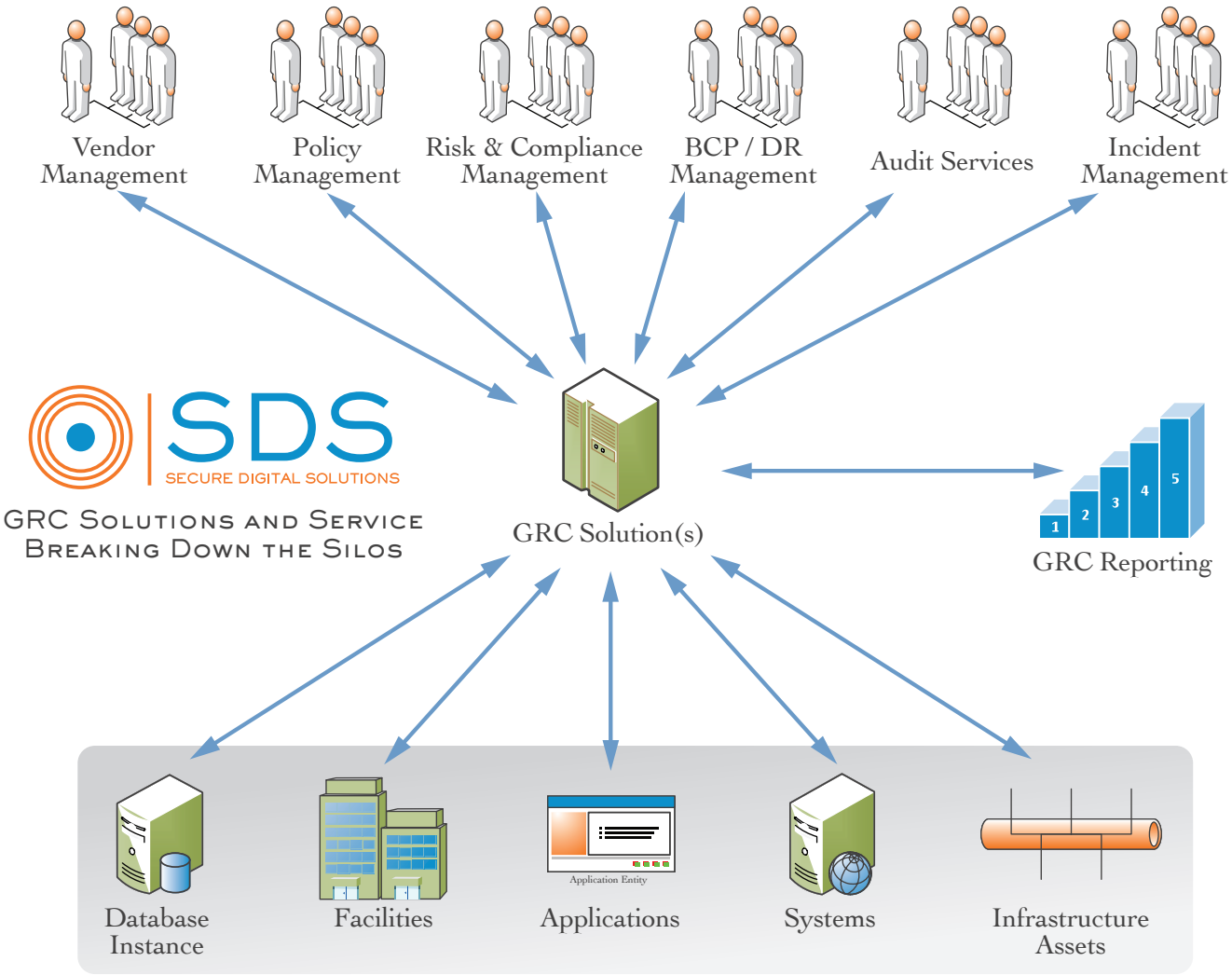

Table 1.0 – Functions Supported by GRC

Functions Supported By GRC Platforms	Description
Vendor Management	Facilitates risk-based vendor selection, relationship management and compliance monitoring.
Policy Management	Supports documentation, workflow, policy lifecycle from creation to review, change and archiving of policies and mapping of policies to authoritative sources.
Risk & Compliance Management	Supports risk management professionals with the documentation, workflow, assessment and analysis, reporting and remediation of risks. Allows organization to truly understand their risk posture and manage it in a cost effective manner. Additionally, this area enables organizations to better manage their compliance position through performing surveys and self-assessments, attestation, testing and remediation. Supports the ability to respond to changes in regulations.
BCP / DR Management	Combines business continuity, disaster recovery and crisis management. Assess the criticality of your business processes and technologies and develop business continuity and disaster recovery plans using automated workflow for testing and approval. Furthermore enables the organization to perform a Business Impact Analysis to better understand the value of the business processes and the people, applications and systems that support those processes.
Audit Services	Supports internal auditors in managing work papers and scheduling audit-related tasks, time management and reporting.
Incident, Threat and Vulnerability Management	Records events, tracks investigations and causes and reports on incidents. Additionally, this function documents regional or country threats, consolidates vulnerability, malicious code and patch information from security intelligence providers, and captures vulnerability results from scan technologies.
Asset Management / CMDB	Manages critical relationships and dependencies within the enterprise by identifying and mapping applications, systems, databases, infrastructure assets and facilities, to key business processes for effective compliance, business continuity and disaster recovery tasks.

Current Trends

Many organizations have an established security or risk management department or program. These security and risk programs were driven by compliance initiatives originating from Sarbanes Oxley, PCI, HIPAA, or GLBA, etc… Consequently, these regulations or standards engage organizations to instill security controls to help safeguard regulated or managed data e.g. SOX or PCI or HIPAA.

Many organizations have procured a GRC solution, but have failed to fully realize the positive impacts it can have. The reasons these organizations have not been able to garner the effectiveness of their GRC solution is they typically fragment or silo each solution. By segmenting GRC the organization cannot fully realize the benefits of sharing data and technology across multiple departments throughout the enterprise. For example, Risk Management does not typically leverage information from the Business Impact Analysis to determine a true valuation on their information assets.

Managing GRC in silos can result in initiatives being uncoordinated, even though risk and compliance issues are intertwined and controls are shared, leading to confusion, inefficiency, duplication of efforts, and remedial actions within one organization. This in turn, wastes resources – employee time and budget allocations can be spent in duplicate.

Business Case for GRC

Organizations face increasing complexity and change in regulatory environments, calling for a more structured approach for managing governance, risk, and compliance. In the past, resources were consumed in manually collecting, manipulating, and reporting data just to get to a baseline understanding of an organization's risk profile. Little time was left for analysis and problem-solving.

An effective integrated GRC platform enables the centralization of data gathering and reporting that creates a human capital resource shift to strategic thinking and increasing business responsiveness to rapidly changing landscapes. Internal resources can be effectively utilized and focused on valued assets within high risk areas. An integrated GRC Program provides management with information they need to make well informed decisions on managing risk and auditing compliance in a cost effective manner.

An enterprise GRC platform helps optimize risk mitigation at the lowest possible cost, as well as help companies devise risk management measures to identify, manage, monitor and report on risks across the business before they materialize into loss.[3]

Effective GRC programs create alignment with a standard set of principles defined through policy statements that support security initiatives with business objectives. These business objectives come in the form of workflows, assessments, compliance mapping to policy and controls, as well as overall Risk Metric Intelligence (RMI).

GRC platforms satisfy the needs of multiple stakeholders, including:

- Business executives that need to identify and manage risk
- Managers with responsibility for meeting regulatory compliance requirements
- Legal counsels grappling with e-discovery and records retention

3 Unleashing GRC intelligence: Driving performance with insight – IBM, September 2011

GRC Market - Solutions and Vendors

A range of GRC solutions exist in the market, however, considerable time and effort should be spent researching for the solution best suited to fulfill your business goals and requirements. The following categorize the three main types of GRC solutions and GRC as a Service (GRCaaS):

- **Extremely Customizable and High Cost:** These GRC solutions are built to be 100% aligned with your current business processes, however they typically require a full-time system administrator or developer. Companies hire consultants to custom configure and develop the initial deployment of the GRC solutions. This allows the company to get their GRC solution up and running, while identifying internal resources to administer and manage the program after the solutions are implemented. These solutions are typically purchased by mid- to large-market companies.

- **Customizable and Moderate Cost:** Mid-tier GRC solutions allow for certain customization, however limitations exist on what capabilities and customizations are available. These solutions also normally call for consultants to assist, however the amount of time is typically less than the extremely customizable GRC solutions. Internal resources are required to be able to manage the solution(s) once outside resources are transitioned from the project. These GRC solutions are purchased by all types of organizations, large or small.

- **Limited Customization and Lower cost:** The limited customization solutions are a cost effective method for integrating GRC if an organization can align their processes to fit the tool functionality. These solutions do not require much external consultant time, however they do need an internal resource to administer and manage the solution. Smaller organizations tend to leverage this type of GRC solution. Additionally, the smaller organizations do not have dedicated Risk or Security staff, therefore, they hire vendors to help manage the GRC solution for them on a part time basis, e.g. develop security policy, manage vendor relations, and track compliance.

Continued.

- **GRC as a Service (GRCaaS):** A newer service being offered by consulting firms today is GRC as a Service (GRCaaS). GRC as a Service is a unique offering that allows organizations to leverage the benefits of a GRC tool while working with experienced and trained consultants that implement, advise and manage GRC environments. Security firms are providing specialized GRC expertise for organizations that either do not have the resources or would prefer to outsource their GRC solution management. GRCaaS provides a partnership between the security firm and the organization. They work together to determine what GRC solution and services are necessary to accomplish the business goals. Thus allowing the security firm to provide the business with the information they need to make informed security and risk decisions without the need of a full-time security and risk staff.

Return on Investment (ROI) Discussion

Return on Investment (ROI) discussions are challenging regarding GRC solution implementations for two reasons. First, GRC focuses on improving an organization's risk and compliance status, increasing security controls and finding the balance between accepting or rejecting risks. Second, GRC solution implementation and maturing an organization's risk and security posture occurs over a course of years. Therefore, ROI calculations may not show immediate (within the first year) financial performance results.

However, knowing and understanding corporate budgets and decision-making, ROI metrics become necessary to calculate and present to executives. Categories for ROI metrics are as follows:

- **Decreasing time = Increasing Efficiency:** Managers record the current time it takes employees to complete GRC tasks. For example, the time to manage the policy approval workflow, conduct business impact assessments or map policies to compliance regulations. Then managers project the future estimate of time to perform these same tasks after a GRC solution is implemented. Now, managers produce a time

Continued.

comparative analysis to provide evidence of increased efficiencies and in turn, discuss how employees will use their "extra time" to devote to supporting other company initiatives. SDS has seen such increased efficiency in organizations that have adopted some GRC solutions.

- **Effective Vendor Management = Reduced Duplication of Vendors:** Centralizing vendor relationships into a single managed GRC solution will enable the business to identify duplication of vendor relationships including contracts and manage vendor risk with a consistent methodology.

- **Decreasing Risks = Cost Reductions:** A GRC tool provides a database of risk information from all areas of the business and produces a comprehensive view of risk areas and impact. Organization strategies target the highest risks for remediation or address incidents effectively. This strategy results in less audit findings, reduced costs for security breaches and quicker remediation for risks because of the reduced number of risks.

- **Decreasing Silos = Strategic Performance:** As an organization shifts operating from the GRC "silo" perspective to the GRC "integrated" perspective, that organization is equipped to use the comprehensive GRC information for making informed choices across typically siloed areas of business. Examples of informed choices – faster availability of information to hire or assess vendors, administer information security awareness training and support marketing campaigns advertising the security program for your organization.[4]

4 See Computer World UK. Forrester Analysts. January 27, 2011.

Summary

Taking an integrated GRC process approach provides a centralized method for gathering important risk data, conducting assessments and most importantly, reporting to management the findings and overall risk and compliance posture the organization is currently facing, thereby empowering effective decision-making.

- A good GRC program is at a minimum:

Defensible	Flexible	Consistent	Risk-reducing

- A superior GRC program will also:

Identify inefficiencies and opportunities for cost savings	Minimize financial loss as a result of unidentified risk or non-compliance

Secure Digital Solutions can help with your GRC needs

- SDS is a vendor-independent firm that provides GRC services for organizations in healthcare, finance, higher education, retail, legal services and government
- SDS offers GRC as a Service (GRCaaS) that is a fit for organizations of all sizes
- The SDS team of professionals brings a minimum of ten years of experience to each client engagement, with a proven track record aligning data security to business objectives
- SDS consultants hold industry recognized certifications in their selected disciplines

Your Situation	Take Action, Contact SDS
If you are considering buying a GRC tool...	SDS can help with due diligence and guide you in selecting a GRC tool that's right for you.
If you already have a GRC tool...	SDS can help you configure and optimize your current GRC solution and provide greater ROI for your investment.
If you are looking for a firm to manage your security needs...	SDS has GRCaaS to offer our clients, allowing the business to focus on their critical needs.

For More Information

Email: Sales@SecureDigitalSolutions.com

Phone: 952-544-0234

Web: www.securedigitalsolutions.com

Address:

Secure Digital Solutions

1550 Utica Ave. Suite 420

Saint Louis Park MN 55416