

WHITE PAPER

Accelerating Value Creation and Enabling Dynamic Risk Management Through EMC's GRC Solutions

Sponsored by: EMC Corporation

Vivian Tero
January 2010

IDC OPINION

The governance, risk, and compliance (GRC) infrastructure competitive market is expected to total \$48.7 billion in 2009 and grow to \$76 billion in 2013, a CAGR of 10.2%. Corporations are already employing EMC solutions to execute their GRC objectives. Today, EMC continues to improve the capabilities of its portfolio and support enterprise GRC objectives. The company's opportunities stem from its relatively large install base. EMC's broad portfolio of GRC-aware hardware and software assets strengthens the vendor's competitive position to provide an end-to-end GRC infrastructure solution. EMC intends to be a key enabler of dynamic GRC management as corporations adopt private cloud and public cloud environments. To do this, EMC should consider the following:

- ☒ The Archer Technologies and Kazeon acquisitions fill critical capability gaps in EMC's GRC strategy. EMC should consider enabling deeper integration of these acquisitions with the rest of its product portfolio to automate key compliance execution, testing, and remediation processes. EMC should provide customers with an integration and transaction layer, which would harvest, collect, process, translate, and store compliance data from various systems. In addition, EMC should offer up a decision and inference engine, which would normalize compliance data and provide rich contextual analysis. The integration and transaction layer, in combination with the decision and inference engine are core to automating the appropriate responses and remediation actions.
- ☒ The Archer GRC solution suite facilitates the mega processes of enterprise governance, risk and compliance across IT, Operations, Finance and Legal domains. The solutions are built on the Archer Smart Suite Framework and provides a flexible platform, supporting heterogeneous third party applications, that provides componentized GRC solutions for policy management and administration, risk management, compliance management, audit management, incident management, business continuity management, vendor management, threat management, and enterprise GRC management. For this report the analysis will be focusing on the IT GRC domain.
- ☒ EMC Consulting provides strategy and design services to help customers evaluate and plan a road map with consideration for the architecture, operations, and processes. EMC should consider offering solutions and accelerator programs that would bundle EMC's consulting services with its hardware and software across various aspects of GRC such as eDiscovery, data privacy and data loss prevention, IT risk management, and GRC for the cloud.

- ☒ As virtualization moves from testing and deployment environments into production, it opens up new ways of rationalizing IT infrastructures, especially servers and storage. EMC should use this as an opportunity to demonstrate to its customers how they could employ their investments in EMC's hardware, consulting services, and software solutions to manage risks and compliance in virtualized environments. EMC Consulting should also be able to help its customers manage the trade-offs between the operational benefits and the green benefits of virtualization and the potential risks of these environments.

IN THIS WHITE PAPER

This IDC white paper discusses EMC Corporation's product portfolio and its ability to support policy management, technical execution, monitoring, audit, reporting, and remediation of IT operations GRC and information management GRC activities as they evolve from a static to a more dynamic, real-time posture. IT GRC and information management GRC are the major categories of the broader GRC infrastructure competitive market. EMC's solutions portfolio in software, hardware, and services positions the vendor as a key player in the GRC infrastructure market.

METHODOLOGY

IDC has been publishing the governance, risk, and compliance (GRC) infrastructure (formerly known as compliance infrastructure) taxonomy and market size since 2005. This IDC white paper maps the EMC products, consulting services, and technologies portfolio to the GRC infrastructure competitive market. The document discusses EMC's market position and highlights the company's capabilities to address current and emerging GRC infrastructure requirements. It concludes with a discussion on EMC's challenges and opportunities and recommendations on how EMC can best compete against its peers. IDC also identifies opportunities for customers to harness their EMC technology investments to address their GRC objectives and prepare their IT infrastructure to take advantage of emerging technologies while reducing operating costs.

SITUATION OVERVIEW

The confluence of the following developments underscores the criticality of enabling better alignment across information management, storage, information security, and IT operations disciplines within an organization and the need for transparent, sustainable, and dynamic risk management:

- ☒ Aggressive growth in digital data increases enterprises' compliance, management, and security obligations.
- ☒ The adoption of emerging technologies such as "cloud computing" and virtualization is creating the hyper extended virtual enterprise and resulting in more complex risk mitigation, compliance, and governance activities.
- ☒ Expected increases in the volume of litigation events and more regulatory oversight will raise the volume of compliance- and security-intensive data.

The Expanding Digital Universe Will Increase Enterprises' GRC Obligations

The IDC Digital Universe study sized the digital universe at 487 billion gigabytes in 2008. (For more on this topic, see IDC's study *As the Economy Contracts, the Digital Universe Expands*, May 2009, sponsored by EMC). The study concludes that the size of the digital universe will double every 18 months. By 2012, five times as much digital information will be created versus 2008 and the Digital Universe will reach 2,500 billion gigabytes. This growth is underpinned by the explosion of digital cameras, televisions, surveillance, sensor-based applications (such as GPS), datacenters supporting cloud computing, and social networks. Aggressive data volume growth and the introduction of new applications and media types in the corporate environment increase an individual's digital shadow, resulting in a corresponding rise in the volume of data that corporations must secure and manage.

All of this digital data needs to be evaluated for its GRC profile so that the proper disposition, availability, and security protocols are applied in compliance with business, regulatory, and legal obligations. Given the volumes involved, manual processes would be too unwieldy and prone to noncompliance and inconsistent policy enforcement. Automating the policy compliance enforcement, auditing, monitoring, and remediation activities provides operational and risk mitigation benefits.

Virtualization, Cloud Computing, and the Extended Virtual Enterprise Raise Management Complexity and Create New GRC Challenges

The IDC Digital Universe study concludes that although 70% of digital data is created by individuals, corporations are responsible for the retention and security of 85% of said data. The introduction of new technologies, including social networking technologies, into the IT environment poses additional compliance and risk management challenges.

- ☒ IDC research on the digital universe notes that virtualization technologies will double the number of physical and logical servers in the next four years. This increase in information capacity creates management and security challenges. For example, security issues in a virtualized environment are more complex because organizations now have to keep track of both physical host security and virtual machine security. A security breach in one layer wreaks havoc on the other. Monitoring for noncompliance events in both physical host and virtual machine is another complex issue. Organizations will need to plan for additional resources and trade-offs so as not to adversely impact operational service levels as they deploy agents and monitoring software.
- ☒ Cloud computing presents companies with opportunities to realize operational efficiencies and enable a more agile IT infrastructure. Also, virtualization provides substantial security benefits. For example, the enforcement of antimalware and other security technologies at the hypervisor layer reduces the need to deploy security agents and desktop virtualization, thereby making desktops more secure and manageable. Despite these benefits, cloud computing also presents new security and legal challenges. True cloud services are defined by shared infrastructure and application services. A cloud infrastructure deepens the technical reach of partners, suppliers, and customers into each other's

ecosystems. Multiple integrations across on-premise (internal cloud), off-premise (external cloud), and hybrid (private cloud) infrastructure are expected to become the norm as more corporations realize the operational benefits of this architecture. The security challenges relevant to this environment — such as being able to provide more granular authentication and auditing, ensuring persistence in data retention policies, and addressing the legal ambiguity regarding the government's rights to seize and search data in the cloud — remain primary issues that drive information governance. These practices should include policies on what data can and should be moved to the "cloud," protocols on how to control "acceptable use" and how to ensure secure information-sharing practices, and protocols to ensure cloud service providers are able to support the organization's risk and compliance management obligations.

- ☒ The emergence of smart grids and smart appliances results in utility companies and governments collecting billions more pieces of information about individual activities, giving these organizations the ability to reconstruct our daily lives. Privacy advocates worry that today, the regulations do not prevent these corporations from selling this data to third parties.

Data Volume Growth + More Regulatory Oversight = Increases in GRC-Intensive Data

As a result of the global financial crisis, regulatory pressures, and more emphasis on risk management, corporations are expecting a rise in the volume of legal disputes and regulatory audits. For example, the Health Information Technology for Economic and Clinical Health (HITECH) Act provision of the American Reinvestment and Recovery Act of 2009 (ARRA 2009) includes critical changes in HIPAA data privacy requirements. In the EU, Data Privacy Restrictions and enforcement of national blocking statutes in instances where U.S. eDiscovery requirements conflict with EU country-specific data privacy regimes can be complex and pose potentially costly data collections in the absence of careful planning. The inherent conflict between U.S. eDiscovery rules and EU data privacy is unlikely to be resolved soon.

As a result of these developments, IDC forecasts that compliance-intensive data, as a proportion of the digital universe, will increase from 25% in 2008 to 35% in 2012. During this period, security-intensive data will increase from 35% of the digital universe in 2008 to 45% of the digital universe in 2012.

The data volume growth in compliance- and security-intensive data will also be spurred by the expected increase in the number of disputes companies will face in the next two years. Keep in mind that Rule 26 (a) of the 2006 amendments to the Federal Rules of Civil Procedure added electronically stored information (ESI) as its own category and applies to all types of digital content (including emerging data and media types). The widespread use of these Web 2.0 applications and new mobile devices among organizations therefore imposes future potential eDiscovery burdens. Smart corporations are advised to adopt sound information governance practices as their first line of defense against future eDiscovery and compliance burdens.

Complex IT Environments and GRC-Intensive Data Volume Growth Underscore the Value of Automation, Transparency, and Dynamic Risk Management

Risk management and compliance is just one facet of a corporation's overall governance activities, which also include value delivery, resource management, performance measurement, and strategic alignment. Strategic alignment focuses on aligning IT with business operations. Value delivery focuses on ensuring that IT is optimized and is able to deliver the promised benefits against the business strategy. Resource management is all about the optimal allocation and management of corporate resources. Performance measurement tracks and monitors strategy implementation, resource use, and measures of success, typically using key performance indicators (KPIs) and key risk indicators (KRIs).

Corporations today realize the urgency to accelerate value creation and manage risks more dynamically. Developments in the past five years have clearly demonstrated that siloed security, IT operations compliance, and information retention projects are not sustainable strategies. Organizations with global operations recognize that chasing compliance can become unwieldy as data volumes continue to grow and as multijurisdiction regulations change. The increase in the number of reported data privacy breaches illustrates the misalignment of a firm's information management with its information security practices. Adding more hardware to increase capacity can potentially create future discovery liabilities. Moving data "into the cloud" without carefully planning for secure data sharing and "information governance" across internal and external partners and employing server and storage virtualization without proper IT governance protocols could potentially create new risk vectors. The use of virtualization and cloud computing architecture potentially increases the complexity in a corporation's compliance and risk management activities. These developments underscore the criticality of automation, transparency, and dynamic risk management.

Corporations are deploying applications that centralize policy management and orchestrate and automate the testing and reporting of information management GRC and IT operations GRC activities. Compliance and risk management define the processes, controls, and actual computing assets impacted. Examples of these processes and controls include the physical host and virtual machine security, asset management, change and configuration management, network management, and disaster recovery and backup operations, to name a few. Despite these developments, transparency and dynamic risk management remain problems for most corporations.

Why is this so? First, most corporations today still conduct periodic assessments that are process and/or application specific. Second, despite the fact that the majority of existing systems management, security, networking and network management, and datacenter operations applications are GRC aware (i.e., information on the state of compliance or noncompliance with the desired state is embedded in these systems), the notion of continuous controls (which is largely a business audit term) remains a foreign concept for IT operations. Corporations have not managed to comprehensively harvest from IT management systems the information required to analyze compliance. Third, noncompliance events and weaknesses in the controls are typically manifested across several technical controls, so there is the challenge of

recognizing a symptom versus the actual weakness or breach. Fourth, given the complexity and increasing porosity of most IT environments today, understanding the dependencies across multiple IT systems and processes becomes even more important. For example, if a virtual machine is compromised, what does this mean for the other virtual applications running on the same physical host server?

Analyzing noncompliance-related events and control weaknesses in a fluid and dynamic enterprise demands strict adherence to timing requirements and presents contextual relevance complexities, data volume overload, and data normalization challenges. Corporations should consider approaches that would allow them to take advantage of the near-real-time data analysis reporting provided by existing system infrastructure applications and employ KPI and KRI concepts to normalize the data from multiple functional applications and enable more GRC-related contextual analysis. Doing so would enable them to realize near-real-time transparency into the compliance and risk posture of the organization. It would also facilitate organizations' ability to manage risks more dynamically.

GOVERNANCE, RISK, AND COMPLIANCE INFRASTRUCTURE

GRC is a term used to describe the way organizations are starting to manage strategic, tactical, and operational initiatives with common processes that, when implemented well, promise to improve governance, optimize risk, and demonstrate compliance. Today, in most organizations, these processes can be found embedded within silos with little opportunity to share, correlate, or leverage that information to gain actionable knowledge about options to best take in decision making.

Defining GRC Infrastructure

The GRC infrastructure components include the integration of the following disciplines:

- ☒ **IT compliance.** IT compliance includes the corporation's information management and storage infrastructure, acceptable use, data privacy, application availability and performance, and information security policies and technical protocols. IT compliance primarily centers on addressing legal and regulatory risks, although it may also include elements of policy compliance, strategic, and IT operational risks.
- ☒ **IT risk management.** IT risk management enforces a structure that enables IT organizations to manage uncertainty in the IT environment such as application outages, the creation of new vulnerabilities resulting from unplanned changes, or violations of the firm's information management and retention policies. IT risk management goes beyond the IT security discipline and includes IT operations, applications development, and information and storage management practices.
- ☒ **IT governance.** Effective IT governance formalizes IT oversight and accountability. It facilitates resource allocation and decision making, as well as compliance and audits, by documenting processes, controls, and decision authority.

The GRC infrastructure Landscape: IT Operations GRC and Information Management GRC

Figure 1 illustrates IDC's view of the GRC infrastructure market and its solution components. Governance, risk management, and compliance disciplines are inexorably intertwined. These solutions are employed to enforce operational and

financial management accountability and facilitate the allocation of people, processes, and IT assets; at the same time, they enable the organization to meet its information management, resiliency, availability, and security objectives. GRC infrastructure solutions can be grouped into two major categories:

- ☒ **IT operations GRC.** The objective of IT operations GRC is to demonstrate that applications, databases, and computing resources supporting critical IT processes meet their defined service-level and control objectives. Critical IT processes are typically impacted by various regulations or service-level obligations. IT processes that have IT operations GRC control objectives include application development; change management; user role provisioning; asset management; identification, access, and authentication management; physical security; and network, application, and data availability.
- ☒ **Information management GRC.** Legal discovery, regulation-mandated information retention, master data management, and data privacy are the primary motivators for investments in information management GRC. Corporate activities are primarily focused on the retention and disposition of data, eDiscovery, and acceptable use policies.

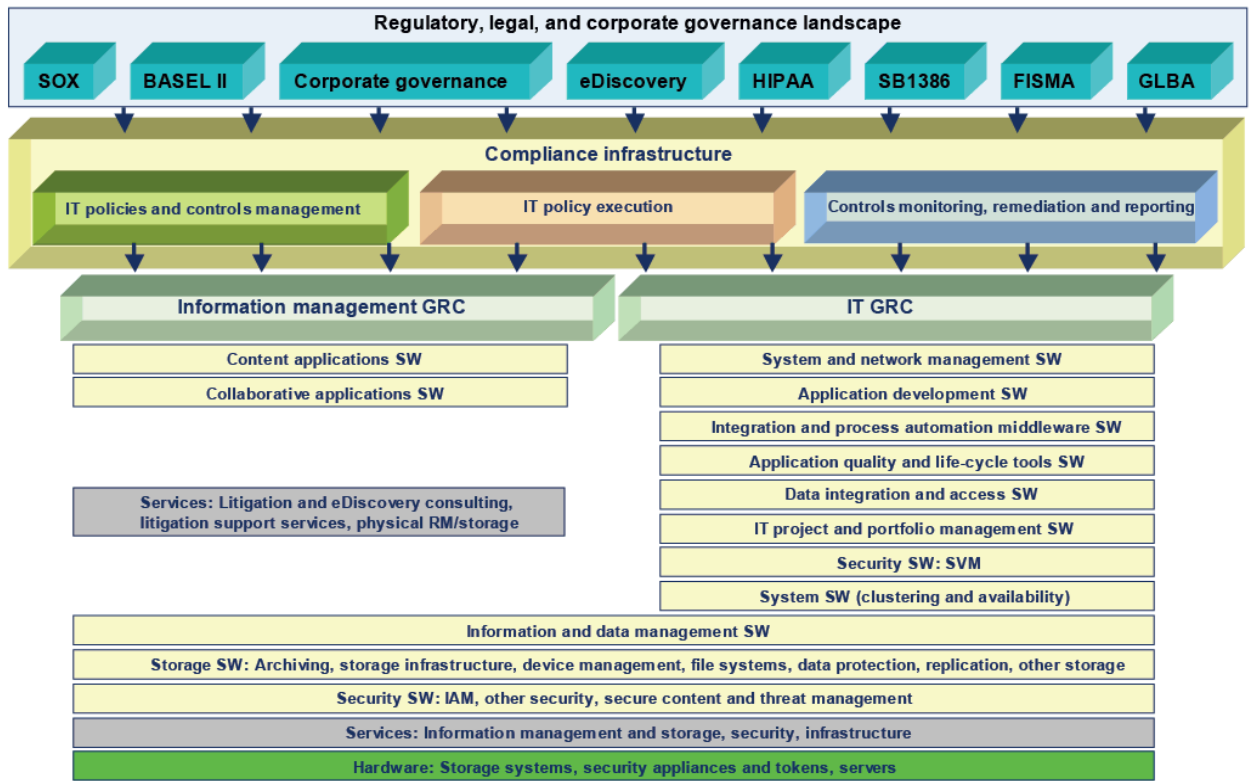
The technical processes and policies for demonstrating controlled access, data privacy, and information integrity are the primary areas of overlap across information management GRC and IT operations GRC.

Three main technology components facilitate governance, risk, and compliance management activities in the infrastructure layer:

- ☒ **GRC policy and controls management.** These solutions support the creation, documentation, business process workflow automation, and mapping of policies to the relevant applications, databases, systems, physical assets, and business and systems custodians.
- ☒ **GRC policy execution and operationalization.** These solutions enforce and automate the technical processes that would allow the organization to meet its defined control objectives.
- ☒ **GRC controls monitoring, audit, reporting, and remediation.** These solutions enable continuous controls monitoring of activities in the system infrastructure and information management layers. Solutions in information management, storage, security, and system and network management are GRC aware and have native capabilities to monitor, audit, remediate, manage incidents, and report compliance or noncompliance with policies. Monitoring and testing of controls are typically done on a periodic basis (through manual or automated evidence collections). Over time, IDC anticipates that corporations will take advantage of the system infrastructure and information management applications' embedded GRC-aware capabilities to enable dynamic GRC management. When this happens, the notion of IT continuous controls becomes a reality.

FIGURE 1

IDC's GRC Infrastructure Market Model, 2009



Source: IDC, 2009

EMC'S GRC SOLUTION STRATEGY AND PORTFOLIO

The GRC infrastructure competitive market totaled \$46.9 billion in 2008, a 12% rise over the 2007 total of \$41.9 billion. Revenue is expected to total \$48.7 billion in 2009 and grow to \$76 billion in 2013, a CAGR of 10.2%. Table 1 maps the overall GRC infrastructure revenue to the EMC GRC products by secondary markets. The table illustrates that corporations are already employing EMC solutions to operationalize, execute, and ensure continuous controls of GRC policies in the infrastructure layer.

TABLE 1

Mapping IDC's GRC Infrastructure Market Revenue to EMC's Portfolio, 2009

GRC Segment	IDC's Secondary Market	2008 Total GRC Revenue (\$)	EMC Product and Services Portfolio
Information management (IM) GRC	Content and collaborative applications software	3,252	CMA product line: Documentum, eRoom, CenterStage, Captiva, SourceOne Email

TABLE 1**Mapping IDC's GRC Infrastructure Market Revenue to EMC's Portfolio, 2009**

GRC Segment	IDC's Secondary Market	2008 Total GRC Revenue (\$)	EMC Product and Services Portfolio
			Management, SourceOne eDiscovery (Kazeon)
IT operations GRC	System and network management	894	Ionix product line: Voyence, nLayers, Smarts, Infra, ControlCenter, Configuresoft
IT operations GRC	Integration and process automation, application server, and application development middleware and quality life-cycle tools	260	NA
Supporting both IT operations GRC and IM GRC	Information and data management, data access analysis and delivery, and ERM software	2,611	NA
Supporting both IT operations GRC and IM GRC	Storage, security, and system software	10,129	BRS product line: Avamar, Data Domain, DiskXtender, Rainfinity, RecoverPoint, VMware, RSA, enVision, PowerPath, NetWorker, Archer Technologies Storage product line: Centera, Celerra, Symmetrix, CLARiiON VMware product lines
Supporting both IT operations GRC and IM GRC	Services	21,220	EMC Consulting Division
Supporting both IT operations GRC and IM GRC	Hardware	8,565	Storage product line: Centera, Celerra, Symmetrix, CLARiiON
Total		46,929	

Source: IDC, 2009

EMC's GRC Strategy and Capabilities

GRC programs have evolved from predominantly manual activities since their initial introduction in the early 2000s. Back then, the primary focus was on risk and compliance analysis and on documenting policies and processes. From 2005 to the present, GRC program management has matured to a point where many corporations

are employing automation to rationalize controls and map dependencies between policies, control objectives, IT controls, and the corresponding assets. In addition, corporations are employing tools to automate the periodic testing of both manual and automated controls through the use of surveys and automated evidence collection protocols. Enabling continuous controls monitoring in the IT infrastructure layer is a relatively new concept for the IT operations disciplines despite the fact that the majority of existing infrastructure assets today have the ability to provide near-real-time evidence collection and reporting. Evidence data rationalization and normalization to support contextual analysis of events remains an issue.

EMC strongly believes in the progression or maturity of GRC from a static, conjecture-based system of analysis to one based on near-real-time analysis of empirical information. EMC posits that it has a broad set of technologies not only to enforce and implement controls but also to collect and harvest the information required to manage risk and demonstrate compliance.

EMC aims to enable its customers' ability to leverage and extend their existing investments in EMC software, hardware, and consulting services to integrate siloed and discrete GRC capabilities to manage GRC infrastructure processes holistically. This approach is intended to support a fluid IT architecture enabling the organization to take advantage of emerging technologies and both private and public cloud services. This approach, EMC argues, would enable corporations to better align the business with policy, compliance, and risk appetite. In this vision, all IT management processes are supported: business assurance, policy, information life-cycle management, backup recovery and archiving, storage, and change and configuration and security management. GRC analysis will be based on near-real-time empirical information (leveraging the GRC-aware embedded capabilities of the information and system infrastructure), as opposed to conjectural, survey-based data. This improved transparency means that risks are more visible and in near real time, thus enabling organizations to make more informed decisions on their risk management activities and capitalize on new opportunities with agility.

EMC's solutions in system and network management, storage, content management, and security are currently being employed to enforce compliance and risk management objectives in addition to supporting IT operations and service levels. These applications and systems provide the evidence and data points needed for auditing, reporting, and invoking the appropriate remediation actions. Several of these applications currently provide near-real-time reporting and alerting capabilities and can feed information to visualization and analytics tools.

EMC Information Management GRC Solutions Portfolio

EMC has a broad product portfolio in information management GRC, from content management and collaborative applications to eDiscovery — all supported by consulting and deployment services. This portfolio includes the following divisions:

- ☒ The Content Management and Archiving (CMA) division of EMC offers Documentum suite for content management. Documentum modules for compliance management, records retention and policy services, information rights management, trusted content, and content storage services are core to enabling information management GRC.

- ☒ CMA also delivers collaborative applications and enterprise portals through its CenterStage and eRoom product lines.
- ☒ EMC recently acquired Kazeon, an eDiscovery vendor, and is integrating the Kazeon product's search, content analytics, and eDiscovery workflow capabilities into an eDiscovery solution under the SourceOne brand.
- ☒ The Storage and Backup Recovery Systems (BRS) division of EMC, the birthright of the company, has industry-leading solutions supporting storage management and tiering, replication, secure backup, recovery, and archiving. A recent acquisition, Data Domain, adds strong data deduplication capabilities to the EMC product portfolio. These solutions are employed by EMC customers to jointly address their data retention, resiliency and availability, and storage efficiency requirements. Readers should note that the Storage and Backup Recovery Systems (BRS) product line supports both information management GRC and IT operations GRC objectives.

Management of the entire life cycle of information — including creation and capture, acceptable access and use, discovery, classification, retention, backup, recovery, archiving, and, finally, disposition — is becoming increasingly important as the volume of information expands and the number of regulations and compliance obligations increases. Providing sound information governance policies and processes is a challenge as the volume, type, and location of information grow exponentially.

These solutions are critical to dynamic GRC because they support business resilience, lower costs by allowing customers to protect information based on its classification, reduce risk by reducing the footprint and instances of sensitive information, and encourage content reuse.

EMC IT Operations GRC Solutions Portfolio

EMC has a broad portfolio supporting IT operations GRC, specifically its Ionix and RSA product lines as well as its Global Consulting service offerings.

The Ionix division of EMC focuses on solutions that span datacenter operations and compliance, IT operation intelligence, service discovery and mapping, network and systems resource management, service and configuration management, storage resource management, and virtualized datacenter management. Over the past five years, EMC has assembled, through acquisition and organic growth, an extensive portfolio of technologies that provide IT management across the datacenter — including Smarts, nLayers, Voyence, Infra, ControlCenter, FastScale, and Configuresoft. Ionix represents the culmination of this strategy. It brings together these products under one unified family and offers customers management capabilities across their physical and virtual IT infrastructures, supporting and enabling configuration management database (CMDB)/configuration management system (CMS) population, change management, and application troubleshooting. This portfolio is employed by EMC customers to enable IT service delivery, business continuity, and site recovery across physical and virtual infrastructures.

Ionix manages and supports servers, networks, storage, and virtualization within datacenters. EMC Ionix for Service Discovery and Mapping provides the visibility into complex applications and their physical and virtual dependencies. The solution also enables customers to accurately map servers and applications prior to datacenter moves, consolidations, and virtualization migrations. Visibility into the relationships

and dependencies between IT controls and IT assets is core to defining and understanding an organization's risk posture.

EMC Ionix for IT Operations Intelligence provides automated root cause and impact analysis and monitors services across both physical and virtual environments. These capabilities support GRC by integrating automated root cause analytics into service desks for enhanced incident and problem management.

EMC Ionix for Data Center Automation and Compliance provides compliance management capabilities across the IT infrastructure — including servers, storage, application dependencies, and networks. The ability to assess configuration compliance against regulatory, best practices, and internal governance policies and virtualization deployment guidelines is a critical foundational capability for dynamic GRC operations.

Maintaining up-to-date mapping of dependencies between IT assets and processes to technical controls is another foundational capability of dynamic GRC. EMC Ionix for Service Management provides IT Infrastructure Library (ITIL) service management with integration to CMDBs and workflow automation. It has the ability to build a federated CMDB that is auto populated with physical and virtual configuration items (CIs) and dependencies. This is important to dynamic GRC because organizations must have an automated way to maintain profiles of assets in their infrastructures as a first step in assessment.

Security-centric GRC is estimated to account for at least 70% of an enterprise's GRC policies and control objectives. RSA, The Security Division of EMC, supports GRC with solutions for identity and access management, access control, data loss prevention, and security information and event management. While information security is typically considered a subset of risk management, security systems have traditionally led in the implementation of automated solution to manage information-related risk, based on internationally recognized frameworks such as ISO 27001.

Demonstrating secure information sharing and controlled access to key IT operations and information management systems is a core requirement of GRC programs. The EMC solutions that enable these technical processes include RSA Access Manager, RSA Protection and Verification Suite, RSA Digital Certificate, RSA Encryption and Key Management Suite, RSA Federated Identity Manager, RSA SecurID, and RSA Hybrid Authenticators.

Virtualization, cloud computing, and a more mobile workforce are behind the increasing porosity of an enterprise's security perimeter, in the process creating privacy, compliance, and intellectual property protection issues. The RSA Data Loss Prevention (DLP) Suite is intended to mitigate both intentional and inadvertent loss of information from insider threats. RSA DLP includes solutions for discovering unprotected sensitive data in the datacenter (DLP Datacenter), monitoring for unauthorized data sharing on the network (DLP Network), and misuse of data at the endpoints (DLP Endpoint). EMC enables identity-aware DLP for data at rest through the integration of DLP Datacenter and DLP Endpoint Discovery with Microsoft Active Directory Rights Management Services. The integration of RSA DLP Suite with enVision (EMC's security and incident management solution) automates the monitoring, alerting, and remediation workflows.

As organizations grow in complexity, automated systems that proactively monitor for breaches are becoming increasingly required to manage risk. The integration of RSA DLP Suite with enVision facilitates this process.

As of the publication of this document, EMC announced its intention to acquire Archer Technologies, GRC software solutions provider. EMC stated that Archer's GRC solutions would complement EMC's DLP and security portfolio. The Archer Smart Suite Framework is a flexible platform, supporting heterogeneous third party applications, that provides componentized GRC solutions for policy management and administration, risk management, compliance management, audit management, incident management, business continuity management, vendor management, threat management, and enterprise GRC management. Archer provides a rich content library of (1) policies and regulations, (2) best practices recommendations for technical procedures, (3) dependencies mapping tools, (5) componentized workflows for critical risk, compliance and IT operations activities, and (6) a risk management database. The enterprise GRC module also offers EMC the opportunity to enhance transparency between corporate level GRC and the IT infrastructure GRC activities.

Since security accounts for approximately 70% to 80% of a typical enterprise's GRC issues, it makes sense to initially assign Archer to be part of RSA, EMC's security division. Integrating Archer with enVision (security and incident management + log management), the identity management, and DLP portfolio is a critical first step to enabling drill-down transparency on the state of compliance. But the real value for EMC would be to build on Archer Technologies' existing capabilities and enable the application to harvest and normalize the compliance and operational data throughout the corporate network and its cloud partners/providers.

In theory, the integration of Archer with the rest of the EMC software portfolio would allow for a richer contextual view of the compliant or non-compliant state of the enterprise. It would also automate the analysis and prioritization of the appropriate response, as well as the remediation action itself. For example, a customer using normalized compliance data harvested from their enVision and Ionix systems (data center operations and storage resource management) would be able to glean that a series of seemingly innocuous operational and security events are symptoms of a potentially catastrophic IT failure. Better and more dynamic transparency would drive the appropriate response to non-compliant incidents. In short, corporations would be able to recognize the symptom from a serious breach, measure the severity of the non-compliant or risky events, and prioritize remediation actions accordingly. These capabilities fulfill the notion of dynamic risk management in the IT infrastructure layer. These capabilities would be well suited to enabling the execution and management of compliance and risk management activities for both physical and virtualized IT infrastructures from a single management layer.

EMC Consulting Provides Strategy, Design, and Road Maps That Deliver End-to-End Solutions for GRC

An underlying value proposition of the integration of siloed programs is the ability to leverage control testing and analysis across multiple requirements. EMC Consulting assists customers in evaluating and prioritizing their multiple GRC obligations and architecting the appropriate solution with consideration for the architecture, operations, and processes. EMC Global Services employs over 12,000 professionals,

with more than 2,000 advisors focused on helping customers meet their most pressing information challenges. EMC Consulting offers GRC services such as GRC program strategy and implementation, process and risk assessments for the business, application and information governance strategy and program implementation, business continuity services, compliance and records management, eDiscovery consulting services, and cloud consulting services. The consultancy is critical to the growth of EMC's GRC capability as so many corporations not only seek relief from acute pain due to discrete regulatory pressures and risk exposures but also increasingly look to advisory firms to provide the road map to building integrated programs that holistically manage governance, risk, and compliance.

FUTURE OUTLOOK

EMC Market Challenges and Opportunities

While EMC continues improving its capabilities to deliver GRC infrastructure solutions, the company continues to face a number of challenges, including:

- ☒ **Integration and automation of core compliance testing, incident management, and remediation capabilities across EMC's disparate software portfolio.** EMC should consider enabling deeper integration across its product portfolio to automate key compliance execution, testing, and remediation processes. For example, the integration of RSA DLP Datacenter with Microsoft Active Directory Rights Management and enVision enables identity-aware DLP. EMC should consider enabling the solution to be content and device aware through integration with the Configuresoft and Kazeon capabilities. Also, the integration of the Ionix portfolio with enVision can be leveraged to normalize compliance data from multiple applications, provide contextual analysis, and scale out to support both physical and virtualized IT environments. Providing an easy integration layer that facilitates data collection and harvest is a critical first step. EMC should play on the strengths of Archer to support heterogeneous technologies. This integration and transaction layer should be able to collect and process compliance data from third party system and network management, security, networking and storage applications. Data collection and processing of critical compliance data from cloud providers should also be supported by this integration and transaction layer.
- ☒ Enable data normalization and analytic to drive the decision and inference engine. These capabilities, combined with the integration and transaction layer, are critical to automating the appropriate remediation activities. As a first step, EMC should consider building out a library of risk, compliance, and performance indicators that would translate compliance data from various systems into the appropriate role-specific metrics. (CIO, CFO, IT Risk Officer, Compliance Officer, Privacy Officer, Legal). Once the data has been normalized, the analytics, correlation, and scenario planning capabilities would be useful in driving an intelligent response to events.
- ☒ Customer maturity. GRC programs today are still predominantly process or application centric. EMC would need to articulate a maturity path to guide its customers to achieve dynamic GRC.

EMC's strengths and opportunities stem from its relatively large install base, its broad portfolio of GRC-aware hardware and software assets, and its considerable services capability. Also, EMC has placed its stake in the ground, recognizing what is currently executable today, and has articulated how it plans to operationalize its aspirations and vision for enabling integrated GRC solutions that address the complexity arising from new technologies. EMC Consulting, combined with EMC's broad product portfolio, provides customers with end-to-end solutions supporting GRC requirements.

As virtualization moves from testing and deployment environments into production, it opens up new ways of rationalizing IT infrastructures, especially servers and storage. One of the big benefits of virtualization is as an enabler of green IT, as IT infrastructure efficiency and utilization increases dramatically. EMC should demonstrate how corporations should manage risks and compliance in virtualized environments. EMC Consulting should also be able to help its customers manage the trade-offs between the operational and green benefits of virtualization with the potential risks of these environments. Given EMC's broad set of technology, its strong presence in virtualization, and its entrance into the cloud infrastructure market, the company is well positioned to become a leading GRC-enabled virtualized information infrastructure vendor.

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2010 IDC. Reproduction without written permission is completely forbidden.