

Managing Risk on the Journey to Virtualization and the Cloud

An ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) White Paper
Prepared for RSA, The Security Division of EMC

August 2010



*IT & DATA MANAGEMENT RESEARCH,
INDUSTRY ANALYSIS & CONSULTING*

Table of Contents

Executive Summary	1
IT is On a Journey.....	2
What Does This Journey Mean for IT Risk Management?	2
Managing Risk Along the Way.....	4
The RSA Solution for Cloud Security and Compliance	4
From Physical to Virtual	5
Define Requirements.....	5
Deployment in Test and Pre-production.....	6
Into Operations.....	6
From Virtualization to IT-as-a-Service and the “Internal Cloud”	7
From Internal to External Cloud: Risk and Control in Third Party IT-as-a-Service	8
EMA Perspective.....	9
About RSA, The Security Division of EMC.....	10

Executive Summary

Virtualization has set IT free from many of its legacy constraints on resource optimization. But as virtualization enables IT to evolve into highly flexible service architectures such as cloud computing, these new approaches to technology also introduce new risks. How can enterprises best manage the wide range of risk and compliance challenges that accompany the many opportunities introduced by these innovations?

When it comes to risk management, the journey of IT from the physical to the virtual, and from there to internal as well as external approaches to cloud computing and IT-as-a-service is, in many ways, no different from other new advances in technology. Many organizations find success in building maturity at each stage of the journey, leveraging the tools and applying the lessons learned at each phase in order to build further maturity going forward.

This highlights the many advantages that can be gained from an approach to risk and compliance management that can be extended across physical as well as virtual and cloud environments, both inside and outside the enterprise. A unified platform for managing risk and compliance efforts can improve efficiencies by extending proven principles to these new environments, and centralizing visibility into risk management and control that assures greater consistency in a comprehensive, systematic approach.

In this paper, ENTERPRISE MANAGEMENT ASSOCIATES® (EMA™) highlights how the RSA Solution for Cloud Security and Compliance offers such an approach. Centered on the well-accepted RSA Archer eGRC platform and enVision® platform technologies for security and compliance information and event management, the RSA Solution provides:

- A strategic platform for managing risk and compliance and achieving the insight necessary to keep virtual infrastructure current with the risk landscape.
- A comprehensive set of best practice controls to establish a hardened deployment baseline for virtual infrastructure security.
- Depth of content in standards, guidance and regulatory requirements essential to risk management and compliance, including content specific to physical, virtual and cloud environments.
- Workflow and process management tools that help assure consistency in risk management and compliance efforts.
- Distribution of management information and tracking data where needed, replacing more primitive approaches such as spreadsheets and office documents.
- Automation of alerting, key metrics and other ongoing status information delivered through role-based views and dashboards.

With a unique relationship with the virtualization resources of VMware, the storage, information and infrastructure management resources of EMC, and the comprehensive portfolio of RSA, The Security Division of EMC, the RSA Solution for Cloud Security and Compliance offers a distinctive and well-accepted approach to these challenges that extends across physical virtual and cloud computing environments. With tangible examples offered at each stage, this paper illustrates how such an approach enables enterprises and service providers alike to embrace the journey to virtualization and the cloud with greater confidence.

A unified platform for managing risk and compliance efforts can improve efficiencies by extending proven principles to virtual and cloud environments.

IT is On a Journey

Businesses today are in the midst of a technology revolution that is re-shaping the nature of IT. This revolution is playing out in stages, with organizations at various points along the journey:

- **From the Physical to the Virtual:** Virtualization is unlocking the ability to optimize IT resources as never before. Early on, many organizations grasped virtualization's promise for resource consolidation and improved system utilization. Today, many more are recognizing its potential to abstract business applications from underlying physical resource constraints to deliver a much more dynamic and fluid environment. This environment can be much more responsive to the needs of the business, allowing organizations to bring valuable business services up—and down—much more easily, moving them across physical servers as needed in order to best meet business demands.
- **From Virtualization to the “Internal Cloud”:** The fluidity unlocked by virtualization enables organizations to deliver IT as a service, on multiple levels. For the internal group seeking to build their own information resources, IT can offer virtual infrastructure. This enables these groups to build their own IT resources, but on infrastructure virtualized and maintained centrally by IT. For the group that requires higher-level components from which to build applications, IT can offer application platforms as a service, offloading the maintenance of these platforms from the business organization, and assuring a higher level of control from the data center. And for internal groups requiring IT to deploy and manage applications entirely, IT can expose these applications effectively as a hosted service inside the enterprise.
- **From Internal IT to External Cloud Computing:** Third party service providers also recognize the opportunity to deliver IT as a service. In exchange for the ongoing price of a subscription, businesses can offload multiple—and often unpredictable—burdens and expenses of capital investment, ongoing maintenance, and personnel expertise the ownership of IT requires. These values hold promise regardless whether third party IT services are offered as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or with the increasingly popular alternative of hosted applications delivered as Software as a Service (SaaS). These service provider environments are purpose-built for high elasticity. For the large enterprise, they offer widely accessible, enterprise-scale IT on demand. For the small- to medium-sized business, they bring access to a level of technology that might otherwise be beyond reach.

What Does This Journey Mean for IT Risk Management?

Clearly, the evolution of IT from physical to virtual and to cloud computing—both internal and beyond—is disruptive. It gives IT considerably more leverage in serving the business in multiple ways—but with new opportunity also come new risks for which businesses must prepare.

For example, in making the journey from the physical to the virtual realm:

- **Consolidation can compromise visibility and control:** Many principles of IT security are based on concepts of physical and logical isolation of resources into policy “zones.” The DMZ is one of the best-known examples of this concept. This is a zone where resources serve as a buffer between sensitive internal IT systems and exposure to external networks. In a virtualized environment, the ability to consolidate multiple servers or applications on a single host can disrupt these separations and limit visibility into interactions between virtual machines and a shared host, potentially wreaking havoc on a security policy predicated on physical or logical isolation of resources.

- **Administrative roles may be consolidated as well:** In the physical realm, the clear distinctions between physical networks and systems often led to equally clear distinctions between network managers, systems administrators, and IT security professionals. Today, expertise in virtualization technology has led to the emergence of the virtualization administrator (also sometimes known as the virtual data center administrator). Because the virtual environment may span multiple layers of IT—from networking and storage through multiple hosts and applications, all on a single consolidated physical host—this role may have access to a set of privileges much wider than any individual network, system or security role may have afforded in the past.

When virtualization enables the delivery of IT as a service inside the enterprise, the organization may maintain complete internal control over such issues as configuration management. However, risks remain:

- **Consolidated resources can increase risk exposure:** In a cloud computing environment where virtualized resources are shared across a common physical infrastructure, consolidation may expose one organization’s sensitive functionality—or data—to another. This may have a direct and negative impact on compliance requirements such as controlled access to business performance data required under the Sarbanes-Oxley Act, for example, or assuring the confidentiality of employee health or compensation information. Separation of duties may be directly threatened by virtualization administrator roles that have too-wide a scope of privilege across multiple virtual environments.

When cloud computing is outsourced to a third party service provider, these risks may be amplified:

- **Outsourcing may further reduce visibility and control:**

A cloud computing service provider may enable customers to maintain visibility into virtualized resources delivered on demand—but it may be less forthcoming with the underlying physical environment. To be clear: it’s not that the cloud service provider has something to hide. Paradoxically, this may in part be a side effect of one of virtualization’s values. Virtualization can provide a level of isolation from other resources that can also help isolate security and compliance threats. But when it obscures visibility into the underlying environment, organizations may be at risk when, for example, service providers decide to move virtualized customer resources to a different data center, which may result in compliance violations when sensitive data crosses national or regional borders. Reduced visibility into the service provider’s environment may also heighten the risk that the wide latitude afforded to virtualization administrators at the service provider could be abused, which may place sensitive customer data and information resources at risk.

- **Shared tenancy amplifies consolidation risks:** Shared virtualized infrastructure may pose risks such as separation-of-duties violations inside the business. With an external third party provider, however, these risks may include entirely foreign organizations and individuals—and some of these may not have the best intentions in mind with respect to their “neighbors” in the cloud.

Many organizations see high risk in these new and disruptive changes. In some cases, the security or compliance risks may still be unknown, or not yet fully known. Already, cloud service providers and their customers have disputed with each other over responsibilities for risks such as data breach or loss.

Another concern arises in the continued usefulness of legacy risk controls. Most organizations have made a significant investment in these controls. Aligning existing tools and processes to new approaches

Virtualization is unlocking
the ability to optimize IT
resources as never before.

can be painful, let alone expensive. Many wonder whether their entire legacy investment in IT risk management may itself be at risk. Cloud service providers, meanwhile, may wonder how best to meet their customers' risk management expectations—while protecting themselves as well.

Managing Risk Along the Way

These risks cannot be addressed in an isolated or reactive fashion. In order to have the best chance at success throughout this journey, organizations must take a structured, systematic and coordinated approach to risk management at each stage, building maturity at each phase that supports the next stage in turn.

This includes cloud service providers as well, who must additionally recognize that they must support not only the visibility and control customers need, but also that which they need to protect themselves against a wide range of risks both old and new.

How can all these organizations achieve this ideal without sacrificing the many opportunities the journey affords? Many have taken a stepwise approach in their progress toward IT-as-a-service, from virtualization in test and development environments, then into production, then extending virtualized infrastructure into an IT service architecture. Risk management can follow a similar path, provided the organization has the platform that enables a planned, systematic approach to risk management, from the physical to the virtual and to the cloud.

Organizations must take a structured, systematic and coordinated approach to risk management at each stage, building maturity at each phase that supports the next stage in turn.

The RSA Solution for Cloud Security and Compliance

With its long experience as a global technology provider to organizations as well as service providers of all sizes—and with a unique relationship to VMware, one of the best-known names in virtualization and cloud computing technologies—RSA, The Security Division of EMC, stands in a distinctive position to help organizations shape their IT risk and compliance management strategy throughout the journey to virtualization, IT-as-a-service, and the cloud.

The RSA Solution for Cloud Security and Compliance is centered on the Archer eGRC framework, which offers a single, unified platform from which to manage both strategy and tactics for addressing security and compliance risks on this journey at every stage. This platform provides:

- A highly granular set of controls to establish a security and compliance posture based on recommended practices.
- Mapping of these controls to a wide range of Control Standards and Authoritative Sources which, in many cases, can provide direct correlation and continuity between existing physical controls and corresponding controls in the virtual or cloud environment, and easing the burden of compliance with multiple requirements.
- A mechanism for distributing security and compliance information and tracking among appropriate parties, replacing cumbersome, highly limited and potentially unreliable approaches such as spreadsheets and office documents.
- Automated status measurement on an ongoing basis, with appropriate views and dashboards based

on the user's role in the organization, and with alerting capabilities to notify responsible parties whenever urgent issues arise.

The RSA Archer eGRC platform gives organizations the strategic focus they need from which to design, implement, monitor and control a systematic, stepwise approach to risk management as organizations progress on their journey toward a service-oriented approach to IT. As the heart of the RSA Solution for Cloud Security and Compliance, it complements RSA technologies for strong authentication, information protection, and security information and event management (SIEM), aligning with EMC and VMware technologies for virtualization, systems, network and storage management.

From Physical to Virtual

The RSA Solution for Cloud Security and Compliance enables organizations to define, deploy and manage risk and compliance controls in their progression from physical to virtualized IT:

Define Requirements

Risk management must be designed into initial concepts for virtualization deployment. The RSA Solution for Cloud Security and Compliance provides definition and support at this stage, in areas such as:

- Hardening of the VMware virtualization platform—including vCenter management resources—based on VMware guidelines and accepted industry practice.
- Appropriate segmentation of virtual resources in multi-tenant environments. Application of physical controls and control concepts to virtual infrastructure, extending the value of the existing investment in IT risk management to the virtual realm.
- Identifying the need for controls specific to the virtualization environment, such as security for inter-VM networking within the virtualized physical host, “virtualization aware” event management that can identify inappropriate deployment or consolidation of VMs, configuration management that recognizes the need to update offline VM images in order to keep online VMs in compliance, or data loss prevention tools designed for virtualized environments.
- Appropriate hosting of virtualized resources within compliance requirements, and appropriate deployment of virtual machines (VMs)—as well as VM changes—in production. This aspect is vital to assuring that, when changes such as patches or reconfigurations are required for security or compliance reasons, they are fully propagated to VMs and their reference images in a timely fashion. In particular, this helps to assure that unpatched or insecure configurations are not brought online because reference images were offline when a patch or configuration event occurred.
- Change control procedures to help mitigate risks associated with VM sprawl and mobility.
- Least privilege access control with separation of duties to help mitigate risks from privilege abuse and VM theft.

One of the best-known names in virtualization and cloud computing technologies—RSA, The Security Division of EMC, stands in a distinctive position to help organizations shape their IT risk and compliance management strategy throughout the journey to virtualization, IT-as-a-service, and the cloud.

Deployment in Test and Pre-production

The RSA Solution for Cloud Security and Compliance provides workflows and process controls to assure that risks are managed throughout the initial deployment of virtualization in test or pre-production environments. These tactics help to assure that risks are managed systematically, building practical experience that assures more reliable consistency for risk management in production through:

- Process definitions to assure that important objectives are met and critical requirements not omitted in initial deployment.
- Validation that required controls and compliance requirements are implemented as expected, through checkoffs of milestones as well as monitoring of management tools and technologies.
- Reporting that supports compliance or other policy or management objectives.
- Alerting that notifies responsible personnel of emerging issues in real-time, enabling operations teams resolve issues before they have larger consequences.

This approach helps to identify, address and resolve issues that could have a serious impact in the production environment, supporting key objectives of a test or pre-production deployment.

Into Operations

As organizations move virtualization into production deployment, the RSA Solution for Cloud Security and Compliance leverages the experience gained in design and pre-deployment, and assures that risk management specific to the production environment is equally consistent:

- Structured workflows and processes defined in pre-production are transitioned to the production environment, while the risks of transition are mitigated by workflows that define a sequence for successful production deployment.
- Because operational roles in virtualization management such as the virtualization administrator collapse multiple responsibilities into fewer roles, greater visibility is needed into the production environment to assure separation of duties through granular access controls, and segregation of resources based on their sensitivity.
- The RSA Solution unifies visibility across multiple controls to deliver the needed level of awareness, with ongoing tracking into current status, real-time alerting on the most important events as they arise, and support for prioritizing the most important risk issues critical to a successful management program.
- When leveraging enVision in this solution, this includes real-time visibility and alerting that spans both physical and virtual environments. This extends the value of existing physical controls to the virtual environment where appropriate, while at the same time defining and implementing controls unique to virtualization.

The RSA Solution for Cloud Security and Compliance enables organizations to define, deploy and manage risk and compliance controls in their progression from physical to virtualized IT.

From Virtualization to IT-as-a-Service and the “Internal Cloud”

Some seem to believe that to deploy virtualization is to deploy IT-as-a-service. While virtualization is a key enabler of such an approach, it is far from a true IT service architecture. The RSA Solution for Cloud Security and Compliance helps organizations build their maturity in moving from a technology-centric deployment of virtualization, to leveraging its advantages in a service-centric approach to IT delivery:

- A service-oriented approach typically requires the definition of Service Level Objectives (SLOs) that must be met as part of a Service Level Agreement (SLA). These may include service uptime or availability objectives and guarantees, as well as downtime provisions for scheduled maintenance when required.
- The RSA Solution supports these objectives by assuring that security management processes do not interfere with service delivery requirements. Visibility into management processes helps coordinate security, risk management and compliance activities, making them more transparent to customers and end users and helping to assure a more seamless service experience.
- When security or compliance events arise, real-time alerting can help to contain incidents before they impact service delivery, reducing risks arising from unplanned work or incident response.
- Even scheduled downtime can have an impact when the IT service strategy is the continuous availability of services on demand. Virtualization helps minimize these risks by enabling VMs to be moved to alternate physical hosts when downtime is planned for physical maintenance. The RSA Solution not only helps coordinate these new IT activities, but also helps to assure that security or compliance risks are not exposed in the process.
- These capabilities have real business value. They help assure more consistent achievement of service objectives, which in turn improves the reliability and efficiency of service delivery. This, in turn, supports more profitable IT operations through improved IT service quality, consistency and reliability, and reduces risks—and the cost impact—of SLA violations. As an added benefit, the more consistent management of IT that supports these values also tends to reduce security exposures, which improves the overall risk posture.

The RSA Solution for Cloud Security and Compliance helps organizations build their maturity in moving from a technology-centric deployment of virtualization, to leveraging its advantages in a service-centric approach to IT delivery.

Among the values of the RSA Solution that support these objectives are:

- Monitoring that provides a comprehensive view into multiple aspects of control implementation. This is vital to knowing when to “flip the switch” and activate service commitments.
- Trending that provides insight into the status of movement toward an IT service architecture, as well as trends that reveal risk or compliance issues that could have an impact on service delivery.
- The development of useful metrics for monitoring control activities that affect service performance.
- High-level dashboarding of key metrics and reports that provide an appropriate level of insight to executives or other key stakeholders.

From Internal to External Cloud: Risk and Control in Third Party IT-as-a-Service

The RSA Solution for Cloud Security and Compliance helps enterprises build the maturity they need to deliver IT as a service within the enterprise and for private cloud computing strategies. This maturity will be essential as organizations weigh the opportunities of turning to public cloud service providers. Cloud computing as a third party service offers a number of advantages—but it is not without its risks. A wide range of assessment and audit tools and risk controls will be imperative for visibility and risk management in a third party environment not entirely under the direct control of the customer.

- Where possible, public cloud customers should be able to use the same tools they are using to manage risk and compliance in internal infrastructure, where those tools have been updated to include support for assessments and audits of providers. These tools must be able to correlate controls to Authoritative Sources that define compliance requirements or recommended management practices.
- Consistent processes will need to be defined for managing vendor risk. Audit data documenting performance to defined standards, questionnaires submitted to vendors about their risk controls and those available to customers, information regarding Service Level Agreements, or other forms of inquiry must be collected and managed according to a defined plan of action for assessing vendor risk. Follow-up items will have to be called out following any such evaluation, as well as processes for determining which vendor risks are resolved or mitigated, which risks will be accepted, and which will not. Customers will have to track the progress and outcomes of these matters and the resulting nature of the business relationship with the provider. These items document the customer's own diligence in compliance and risk management. For example, the Cloud Security Alliance, a group that has shown early leadership in defining security for cloud computing, is developing a set of questions and points to explore with cloud service providers that customers can use in their assessment of cloud vendor risk.

One of the many benefits of using a risk management framework such as the RSA Archer eGRC platform is that, when such content becomes available to public cloud users, the platform can be readily updated with new and emerging guidance, which can then be folded directly into processes defined and managed within the framework for evaluating vendor risk according to accepted industry practice. As an added benefit, organizations will be able to use this approach not only to assess risks among third party providers, but to assess internal risk management and compliance efforts as well.

These capabilities may be equally valuable to cloud service providers, who must extend maturity in IT service delivery into a realm where the service becomes a profit center in its own right. This means the highest degree of reliability and cost containment in order to assure a successful business—and that means risk control.

With the alignment of the RSA family with the virtualization assets of VMware and the storage, information and infrastructure management resources of EMC, the RSA Solution for Cloud Security and Compliance offers a well-proven set of systematic tools for assuring consistency in enterprise governance, risk management and compliance initiatives in IT.

EMA Perspective

As with all new technology initiatives, the management of risk is often best achieved in a phased approach to adoption. The journey from physical IT to virtualization, and from there to IT service architectures and both internal and external approaches cloud computing, is no exception.

One of the key points to remember in this journey is that not only a phased but a *systematic* approach often yields the best results. In EMA research into the realities of enterprise governance, risk management and compliance, the highest performers are those who are thorough in achieving *all* milestones of:

- **Defining** objectives
- Actually **implementing** them
- **Monitoring** the environment for expected performance as well as for deviations and events warranting follow-up, and
- **Responding** to events and changes in the risk landscape.

Compare this to the number of organizations who have policies, standards and guidelines, but fail to implement them in operations; or to those who monitor their environment, but fail to respond to changing risks or emerging events. A thorough approach to *all four* milestones is required for consistent success.

These principles can be applied when embarking on each successive stage of the journey to virtualization and the cloud:

- Define requirements for the new, recognizing both the advantages and risks of new approaches. Virtualization, for example, can actually make the environment more resilient to risk than before, thanks to its ability to contain technology threats. The collapsing of multiple roles into the one role of the virtualization administrator, however, offers an example of how virtualization can adversely impact the risk posture, unless the organization is aware of such changes and how best to manage them.
- Identify where existing techniques can be extended to approaches, such as controls on physical IT resources that can be applied in the virtualized environment, or maturity in service delivery that can be leveraged to deliver a higher quality of IT as a service—either for internal or third party customers.
- Understand how management can be unified across physical, virtual and service provider environments to improve the efficiency of risk management and compliance efforts, and to help assure their greater consistency and reliability in practice.

The right platform for consolidating the management of IT risk and compliance priorities can extend one investment across both physical and virtual resources, internally as well as those provided by third parties.

The adaptability of the RSA Solution for Cloud Security and Compliance is well suited to meet these needs. The flexibility and extensibility of the RSA Archer eGRC Platform at the heart of the solution and the real-time information and event management capabilities of RSA enVision lend themselves to harmonizing a wide range of compliance requirements and industry practices, defining processes for making risk management and compliance a reality, providing granular visibility into a wide range of controls, and managing the body of information essential to maintaining control and containing the cost of risk management and compliance efforts.

With the alignment of the RSA family with the virtualization assets of VMware and the storage, information and infrastructure management resources of EMC, the RSA Solution for Cloud Security and Compliance offers a well-proven set of systematic tools for assuring consistency in enterprise governance, risk management and compliance initiatives in IT. It can be extended just as readily to new approaches such as cloud computing, unifying management of both physical and virtual resources under a common umbrella, and helping enterprises as well as service providers manage risk as they capitalize on opportunity on the journey toward what IT is fast becoming.

About RSA, The Security Division of EMC

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance solutions, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments.

Combining business-critical controls in identity assurance, data loss prevention, encryption and tokenization, fraud protection and SIEM with industry leading eGRC capabilities and consulting services, RSA brings trust and visibility to millions of user identities, the transactions that they perform and the data that is generated.

About Enterprise Management Associates, Inc.

Founded in 1996, Enterprise Management Associates (EMA) is a leading industry analyst firm that specializes in going “beyond the surface” to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services for enterprise IT professionals and IT vendors at www.enterprisemanagement.com or follow [EMA on Twitter](#).

This report in whole or in part may not be duplicated, reproduced, stored in a retrieval system or retransmitted without prior written permission of Enterprise Management Associates, Inc. All opinions and estimates herein constitute our judgement as of this date and are subject to change without notice. Product names mentioned herein may be trademarks and/or registered trademarks of their respective companies. “EMA” and “Enterprise Management Associates” are trademarks of Enterprise Management Associates, Inc. in the United States and other countries.

©2010 Enterprise Management Associates, Inc. All Rights Reserved. EMA™, ENTERPRISE MANAGEMENT ASSOCIATES®, and the mobius symbol are registered trademarks or common-law trademarks of Enterprise Management Associates, Inc.

Corporate Headquarters:
5777 Central Avenue, Suite 105
Boulder, CO 80301
Phone: +1 303.543.9500
Fax: +1 303.543.7687
www.enterprisemanagement.com



RSA011a.082310