



The Security Division of EMC

RSA Solution Brief

# Information Risk Management: Moving from Compliance to Governance in Financial Services



By implementing sound Information Risk Management practices and selecting proven technology solutions to manage information security, FSIs can efficiently focus resources on IT governance. Rather than wastefully create internal silos to document compliance with each relevant regulatory requirement, a governance strategy – combined with an information-centric approach to security – enables FSIs to comply with multiple regulations while protecting information across the organization throughout its lifecycle to ensure compliance with multiple regulations.

---

## Information Risk Management Enables Effective Governance

---

An effective Information Risk Management strategy can help financial services institutions (FSIs) accelerate their business by allowing them to take on the greatest amount of risk they are willing to accept while capitalizing on new market opportunities. Effective strategies hinge on an information-centric approach to risk management that recognizes, assesses and mitigates the risk that information is exposed to throughout its lifecycle. Information Risk Management also enables effective IT governance, helping FSIs to comply with a wide range of regulatory requirements while freeing up corporate resources to pursue strategic business initiatives beyond compliance.



*“Today’s FSIs face an alphabet soup of regulatory requirements that are constantly proliferating and changing. Too often, FSIs meet these mandates case-by-case with a task-oriented and tedious assemblage of the processes and data needed to fulfill each discrete requirement.”*

Rodney Nelsestuen  
Senior Research Analyst  
Financial Services Strategies and IT Investments  
TowerGroup

## Moving from Compliance to Governance

Security is a root concern of all regulatory requirements but the complexity and reporting requirements of compliance can be overwhelming. Legislation generally does not specify the steps or solutions by which security objectives are to be met. This offers FSIs flexibility, but also uncertainty regarding the best path for achieving compliance.

Ad-hoc approaches to compliance are no longer practical. FSIs are forced to take a fresh look at their security practices and the technology infrastructure that supports them. As a result, regulatory compliance begins with identifying sensitive/privileged/regulated data and then applying best practices to secure it. Compliance should be viewed as a means to an end, and compliance efforts need to be constantly evaluated and modified. Compliance therefore becomes a process, not an objective. This process is the essence of governance.

Governance strategies should guide the efficient use of IT resources while supporting business objectives such as driving revenue growth and improving customer and partner relationships. FSIs who implement effective Information Risk Management can more readily integrate compliance efforts with business objectives. For example, if an FSI implements information access controls to comply with a specific regulation, those same controls can be leveraged across regulations, across information silos or across business units to mitigate information risks broadly.

How can we efficiently ensure compliance with multiple regulations without creating multiple bureaucracies that drain our resources?

---

## Breaking Down Silos of Information

---

Manual processes for generating compliance reports are labor-intensive and error-prone – and they do not scale. By focusing on complying with regulations individually, FSIs risk developing regulation silos that engage in redundant activities. If multiple business units rely on overlapping information to prove compliance, their efforts result in uncoordinated bureaucracies that focus on similar regulatory requirements in an inconsistent manner.

Successful IT security governance takes a holistic, flexible and proactive approach to minimize risk across all areas of the enterprise and create business value beyond compliance. Effective governance strategies enable the reuse of data and IT resources across compliance efforts.

### Selecting an Information-centric View of Security

Proactive FSIs are consolidating disparate and disconnected views of risk. By taking an information-centric view of security and relying on Information Risk Management solutions to establish controls, policies and procedures, FSIs can implement effective governance strategies that enable streamlined enterprise-wide compliance reporting.

RSA, the Security Division of EMC, is the premier provider of security solutions for business acceleration and Information Risk Management. As the chosen security partner of the world's leading financial institutions, RSA helps organizations succeed by solving their most complex and sensitive security challenges with an information-centric view of security.

No other vendor combines the product strength, services expertise, solution depth and financial services industry expertise that RSA offers.

Additionally, all of the securities firms in the Fortune 500 and 24 of the top 25 global banks deploy EMC infrastructure. As trusted advisors, RSA and EMC offer proven products and services that allow FSIs to build IT governance structures that leverage compliance activities for productive organizational growth.

---

## Implementing a Systematic Approach to IT Security Governance

---

Regulations aren't prescriptive. Instead they require FSIs to implement "reasonable and appropriate measures" for IT security, or in other words, best practices. Standards bodies develop best practices and control frameworks that guide FSIs in developing their internal policies and procedures for protecting information.

The International Standards Organization (ISO), a standards-setting body with strong links to governments, establishes best practices and international standards, and the Control Objectives for Information and Related Technology (COBIT) is a set of best practices for IT management created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITG). COBIT and ISO provide managers, auditors and IT with a set of generally accepted measures, indicators, processes and best practices to assist them in maximizing the benefits of appropriate IT governance policies and controls in a company.



*“EMC, along with RSA, is taking the right approach by encouraging customers to focus on securing the information itself no matter where it resides or how it is transmitted, while providing a robust access control and audit infrastructure for safeguarding the information.”*

Steve Norall  
Senior Analyst  
Taneja Group

RSA works closely with standards organizations and FSIs to understand common requirements for protecting information. RSA solutions enable a systematic approach to IT security governance, helping FSIs to implement best practices, manage information risk and address multiple regulations with fewer resources.

---

## Addressing Multiple Regulatory Requirements

---

Risk assessments determine which assets to protect by revealing the relationship between the value of the information and its vulnerability to threats. High-value data is naturally the most important information to protect, and highly vulnerable applications are naturally the most commonly targeted.

Based on this analysis, FSIs can prioritize security requirements and document governance decisions to prove they are taking reasonable steps to protect information. The sidebars highlight a few of the many major regulations with which FSIs need to comply. However, this list is not exhaustive. FSIs need to protect information to ensure compliance with a much broader spectrum of local, national and global regulations.

Common IT security requirements among financial services industry regulations include log management; data retention; data loss prevention; authentication and authorization; data protection and compliance monitoring. RSA solutions address all of these requirements, helping your organization move from compliance to governance and align security with business objectives.

How can we prove the identity of online customers and secure the financial assets they entrust us to protect?

Can we make our governance and compliance reporting more effective?

### Sample Regulations Impacting Global FSIs.

**PCI DSS** Payment Card Industry (PCI) Data Security Standard (DSS) is a set of best practice requirements for protecting credit card data throughout its lifecycle.

*The PCI standard centers on six high-level control objectives. Broad security requirements support each control objective, and are further dissected through over 200 sub-requirements that specify the technologies, policies and procedures necessary for protecting cardholder data.*

**Reg NMS** U.S. Regulation National Market System (Reg NMS) was established to strengthen the regulatory structure of U.S. equity markets. It is intended to protect investors by raising expectations for institutions to deliver the best available price and opportunity in the market at the time of trade.

*It requires trading centers to establish, maintain and enforce written policies and procedures for increasing the quality and timeliness of trading.*

**Basel II** Basel II intends to better align bank capital requirements with underlying risk.

*Banks are required to monitor, mitigate and disclose risk. The lower the operational risk, the lower the capital requirements. Basel II applies to global financial services organizations.*

**FACTA** The Fair and Accurate Credit Transactions Act of 2003 has been updated with "Identity Theft Red Flag" rules.

*FACTA now requires FSIs that hold consumer accounts, or other accounts for which there is foreseeable risk of identity theft, "to develop and implement an identity theft prevention program for combating identity theft in connection with new and existing accounts."*

### Sample Regulations Impacting Global FSIs

**MiFID** Markets in Financial Instruments Directive (MiFID) is a European Union Law that provides a regulatory regime for investment services across its member states.

*Its main objective is to increase competition and consumer protection in investment services. FSIs performing investment services within the EU must comply with MiFID requirements for authorization, regulation and passporting.*

**SEPA** Single Euro Payments Area (SEPA) aims to improve the efficiency of cross-border Euro payments.

*SEPA includes pan-European payment instruments for credit transfers, direct debits and debit cards, and it impacts banks operating in EU member states and other countries throughout Europe. It includes the development of common financial instruments, standards, procedures and infrastructure for enabling secure and timely cross-border payments.*

### RSA Professional Services

RSA Professional Services can help you realize the benefits of Information Risk Management. You can leverage our proven methodology, our experience in the financial industry and our ecosystem of partners to ensure that risks are properly identified and classified, policies and procedures are adequate to support your compliance objectives, strategies are aligned with industry best practices and technology choices and implementations are effective in helping you move beyond compliance to governance.

### How can we centralize governance while ensuring compliance with a wide range of regulations?

RSA can help you develop and implement an IT security governance program which can:

- Discover and classify data according to well defined standards
- Identify gaps between current policies, procedures and controls versus industry best practices and standards (such as ISO 27002, COBIT, ITIL, etc.)
- Define a process for remediation and re-evaluation

### Log Management and Data Retention

RSA's market-leading solution for security information and event management (SIEM) enables FSIs to capture, monitor and report on all activity related to IP devices. The RSA enVision™ platform captures and stores up to hundreds of thousands of data events per second, providing an enterprise view of activity from any number of sources, including perimeter and network devices, operating systems and proprietary applications. RSA enVision technology offers robust and flexible log management and reporting capabilities that allow FSIs to streamline data collection and analysis and reduce the costs of documenting compliance.



*“Compliance has become a core skill that every FSI must have in today’s highly regulated industry. New threats and risks are emerging that leading institutions will address through proactive governance with those issues with a holistic approach.”*

Rodney Nelsestuen  
Senior Research Analyst  
Financial Services Strategies and IT Investments  
TowerGroup

## Will our compliance infrastructure scale to meet emerging compliance requirements?

EMC's Documentum® platform automates the entire content lifecycle of your sensitive data so that your content remains complete, accurate and safely stored – all while enforcing your compliance and retention policies. You'll mitigate the risk of non-compliance by leveraging full auditability at all stages of content creation, approval and use. Additionally, the EMC Documentum Operational Risk Management solution evaluates the risk of non-compliance with Sarbanes-Oxley, Basel II and other key regulations as auditors benefit from automated risk assessment, work papers, review and document management.

EMC Centera® content addressed storage systems for active archiving – enable you to safely and cost effectively meet current and future compliance demands, including custom e-mail archiving, records management and e-discovery. Solutions from RSA and EMC allow FSIs to better align records management and information retention policies with storage archiving infrastructure so you can efficiently retain the information needed for compliance reporting over time.

### Information Discovery and Classification

You can't secure what you don't manage, and you can't manage what you don't know exists. Information sprawl across an FSI's complex infrastructure creates islands of information that are difficult to manage. RSA's Information Classification and Discovery solution first discovers and classifies data, then automates policy and enforcement based on your business requirements. Data discovery and classification is a critical first step toward securing data and proving compliance. Achieving this is complicated by the fact that sensitive data exists in different forms – database records, e-mails, images, loose files and contexts – at rest on data center storage, in motion through the network or in use on laptops, mobile devices and portable storage.

### Data Loss Prevention

The RSA Data Loss Prevention (DLP) Suite ensures that sensitive data is not lost or misused or distributed to unintended locations inside or outside your network. These products work alongside desktop software applications, providing transparent protection of sensitive data without changing the way you work. RSA DLP offerings help prevent data from leaving the organization.


### Authentication and Authorization

RSA's authentication and authorization solutions ensure that the right people have the right access to sensitive information, whether they are external partners, customers or internal users. RSA offers a range of solutions that provide strong authentication and a robust access control policy manager that centralizes authentication and authorization administration and enforcement. This solution, which can be implemented across the organization, addresses regulatory mandates that require the protection of sensitive data.



*“RSA DLP Endpoint ... allowed us to find exactly the type of information we were looking for, and send a report on where the information was located to the audit and compliance department. The option of remediating on the spot is also invaluable to us. Just being able to move sensitive information to a secure location, or to change permissions is of major value to Columbia River Bank as we work to protect our sensitive information.”*

Scott Hamilton  
Columbia River Bank



RSA anti-fraud solutions protect organizations and their customers against the latest external threats and help manage the overall risk of remote channel activity. By monitoring behavior and transactions, these solutions protect sensitive customer data and prevent unauthorized access and misuse – regardless of the channel they choose to conduct their business. As part of a comprehensive Information Risk Management strategy, these RSA solutions can help to secure your customers' identities and assets to inspire customer confidence and trust and build your brand value.

### Protecting Sensitive Data and Identities

RSA's Data Encryption and Key Management solutions address data privacy directives by securing the data itself – beyond just securing perimeters and devices. RSA encryption solutions help FSIs inventory and classify their data to deploy security rules while RSA's key management solution simplifies and centralizes key management.

Because information is in constant motion across your enterprise, locking down physical assets is not the entire solution. RSA encryption management solutions provide multi-layered access control and enforcement for files covered by regulatory mandates. These solutions also provide comprehensive auditing and monitoring capabilities to help FSIs provide reporting evidence for regulatory requirements.

Encryption management solutions also interoperate across multiple database management systems and versions, helping FSIs enforce consistent data protection policies across the enterprise – even on legacy databases. They also enforce separation of duties between security and database administrators and support existing policies and solutions for disaster recovery through built-in back-up, replication and clustering capabilities.

Do we have the ability to protect information across its lifecycle?

### Compliance Monitoring, Audit and Remediation

RSA Security and Compliance Information Management Solutions integrate compliance monitoring and audit across diverse systems and enable governance and risk management professionals to map security events to risk metrics and control objectives. To truly assure security policy and corporate compliance, FSIs must create a platform that transforms enterprise-wide data into automated compliance and security information. RSA enVision technology provides a complete view of activity surrounding *All the Data*® on the network.

---

### You've got compliance questions – and we've got the answers

---

Compliance is a critical requirement that increases IT complexity and raises questions.

IT Governance is an ongoing process, not a one-time project. It takes knowledge and experience to build an information security strategy that will help you comply with current and pending regulations. We can help you to implement the best practices in information security based on our expertise and our solutions.

RSA offers the technical, market and industry expertise to answer your compliance questions. Contact us today so we can help you deploy an Information Risk Management solution ideal for your company.

Can we capture log information enterprise-wide and automate the reports needed to ensure compliance?



## RSA is your trusted partner

RSA, The Security Division of EMC, is the premier provider of security solutions for business acceleration, helping the world's leading organizations succeed by solving their most complex and sensitive security challenges. RSA's information-centric approach to security guards the integrity and confidentiality of information throughout its lifecycle – no matter where it moves, who accesses it or how it is used.

RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit [www.RSA.com](http://www.RSA.com) and [www.EMC.com](http://www.EMC.com).

©2008 RSA Security Inc. All Rights Reserved.  
RSA, RSA Security, enVision, *All the Data* and the RSA logo are either registered trademarks or trademarks of RSA Security Inc. in the United States and/or other countries. EMC, Documentum and Centera are either registered trademarks or trademarks of EMC Corporation. Active Directory is a registered trademark of Microsoft Inc. All other products and services mentioned are trademarks of their respective companies.

FSICGF SB 0108



The Security Division of EMC

RSA Security Inc.  
RSA Security Ireland Limited  
[www.rsa.com](http://www.rsa.com)