



Product Data Sheet

## Simplified IT Compliance:

The RSA enVision® Platform – Helping Establish Cost-effective, Efficient, Secure Framework-based Compliance Programs

### At a Glance

- Giving you comprehensive, real-time visibility and control across your entire enterprise
- Helping you to comply with multiple compliance regulations, all from a single system
- Supporting the creation of a proactive, tailored IT compliance framework
- Delivering a broad range of reports to support global compliance requirements

### More Efficient and Effective Compliance Across Multiple Regulations

Companies worldwide face a barrage of compliance requirements stemming from governments, industry groups, partners and internal policies. The response is usually reactive, with companies managing compliance on a project-by-project basis. The result is often redundant technology implementations and exorbitant compliance-related IT costs.

There is a solution: global standards that provide IT security frameworks for establishing the most cost-effective, proactive approach to managing compliance requirements – and information risk more generally. By basing your

enterprise-wide compliance activities on these industry standards, such as ISO 27002, ITIL, CoBIT and COSO, you can make significant progress towards complying simultaneously with multiple regulations – including the Payment Card Industry Data Security Standard (PCI DSS), HIPAA, Sarbanes-Oxley and EU Data Protection requirements – without duplicating effort and investment, and without introducing conflicts in policies and controls. These frameworks also have the potential to optimize overall security and operational effectiveness by closing gaps in your organization's IT security program.

### The Technology Requirements Behind a Compliance Framework

One of the fundamental reasons for an over-arching framework for compliance is that, if implemented properly, it delivers visibility of the risks your organization and its sensitive information face, and what your state of compliance is.

This visibility depends on controls that give you complete, accurate and up-to-date information about the users, assets, data, processes and policies at work across your entire IT infrastructure. And, since you're adopting a compliance framework to simplify the burden of compliance, you'll want the collection and management of this information to be seamless and automated.

That's exactly what the RSA enVision® platform delivers. It has been designed specifically to support the principles that underlie compliance frameworks like ISO 27002, among others, delivering simplified compliance through enterprise-wide information risk management.



The Security Division of EMC



---

## What is the RSA enVision Platform?

---

The RSA enVision platform is an all-in-one log-management solution designed for simplifying compliance, enhancing security operations and optimizing IT and network operations through the automated collection, analysis, alerting, auditing, reporting and secure storage of all logs. By collecting log data about network, file, application and user activity, it can help you demonstrate or prove your degree of compliance and identify areas of non-compliance too.

The RSA enVision platform provides extensive capabilities that are vital to instituting a framework-based program. It:

- Automatically identifies IT assets, data and baseline activities right across the organization, which is essential for effective assessments of risk and formulating accurate plans of action.
- Automatically collates, manages and securely archives event logs drawn from all IT components, even those managed by third parties, to foster improved security right across the enterprise.
- Continually monitors network components and business information systems for activity, security incidents and events, giving you the means to meet all the compliance demands of access and configuration control, malware detection, policy enforcement, user monitoring and management, and environment and transmission security.
- Alerts administrators to relevant security incidents in real time, to allow prompt corrective action. Incident management is a critical part of effective compliance.

### Simplify Reporting Across the Compliance Ecosystem

The RSA enVision platform also provides extremely sophisticated reporting functionality to simplify the process of demonstrating ongoing compliance with regulatory requirements. To meet the compliance regulations affecting your business, and to suit your specific compliance framework and policies, your administrators can create their own reports using an intuitive wizard interface. You can also draw on a suite of over 1,100 report templates targeted to cover the major global compliance regulations, including SOX, HIPAA, PCI DSS, FISMA and SAS 70.

Crucially for a standards-based framework approach to compliance, the RSA enVision platform includes a comprehensive suite of out-of-the box reports aligned directly with sections of the popular ISO 27002 standard. This means that if you've adopted a framework like ISO 27002 to manage all your compliance requirements more effectively, you'll already have a lot of the reporting functionality you need, right out of the box. More than 20 reports for ISO 27002 are built in, including:

- Control of human resources data (section 8.3)
- External contractors report (sections 8.1.3, 10.7.3)
- Malicious software activity (section 10.4.1)
- Password changes and expirations (section 11.3.1)
- User activity from external domains (section 11.4.2)
- Computer account logon activity (section 11.5.b)
- Computer account status by account (section 11.5.1)
- Operation change control report (section 11.6)
- Control of operational software (section 12.4.1)
- Control of system test data (section 12.4.2)
- Source code access (section 12.4.3)
- Control of collected evidence (section 13.2)
- Control of system audit data (section 15.3.2)

Using the intelligence that the RSA enVision platform provides through these reports, you can accelerate your progress towards establishing a simplified compliance program. RSA enVision reporting gives you the visibility you need to assess initial inventory and risk assessment more easily, implement controls effectively, and track progress to produce ongoing improvements in compliance.

### Directly Addressing ISO 27002 Clauses

Alongside its advanced reporting capabilities, the RSA enVision platform's inventory, baselining, trend analysis, monitoring and alerting functionality helps address many of the specific best practices set out in the ISO 27002 standard, delivering actionable information that you can use to prove the effectiveness of your policies and controls. Highlights are shown in the following table.

Section	ISO 27002 Best Practice	How the RSA enVision platform helps
<b>Section 10: Communications and Operations Management.</b>		
10.1.1	Document operating procedures	Monitors, collects and correlates audit logs from over 150 types of event sources to establish a baseline and provide important data for documenting operating procedures. Maintains information such as user IDs, dates and times of key events, and successful and unsuccessful attempts to access key resources, among others. Delivers automated lifecycle management to ensure that logs are retained for an appropriate period of time.
10.1.3	Segregate duties and responsibilities	Enforces segregation of duties by allowing personnel to access event logs to do their jobs, without granting them privileged direct access to the critical IT systems that generate the logs.
10.2.2	Monitor third-party activity	Monitors IT systems being managed by third parties, ensuring that all elements are being managed in a compliant manner.
10.3.1	Monitor systems to prepare for future capacity and performance needs	Correlates events across a wide range of infrastructure components to alert operators of possible issues before they can affect users, enabling organizations to manage system capacity more effectively.
10.6.1	Establish network security controls	Monitors network components such as switches, firewalls, IDSs and VPN systems, in order to immediately alert security personnel if any security-relevant events occur.
10.8.5	Protect business IT systems	Monitors business information systems, providing visibility into whether compliance and security policies are being adhered to, and alerting administrators of policy violations.
10.10.2	Monitor system usage	Continuously monitors and correlates events from systems across the infrastructure. In addition, alerts can be generated to notify administrators of any unauthorized activities.
10.10.3	Protect audit logs	Protects log evidence by storing it on a range of secure back-end storage options.
10.10.4	Log power-user activity	Collects and monitors any type of log, including system administrator logs.
10.10.5	Review fault logs	Collects any fault-log entries generated; automatically alerts operators when faults occur.
<b>Section 12: I.S. Acquisition, Development and Maintenance. How to use techniques like encryption to prevent the leakage of sensitive data.</b>		
12.5.1	Establish formal change control procedures	Monitors the environment and reports on any changes that occur, for correlation with an approved change process.
<b>Section 13: Information Security Incident Management.</b>		
13.1.1	Report security events ASAP	Detects potential security events and notifies administrators in real time.
13.2.2	Monitor and measure the impact of security incidents	Effectively monitors, and reports on, the types of security incidents which take place, to help the business quantify the impact of security threats.
13.2.3	Retain evidence related to security events	Provides a searchable database of all event logs collected to allow quick and easy discovery of all events related to a particular security incident.
<b>Section 15: Compliance. How to meet internal and external compliance requirements.</b>		
15.2.2	Review technical security compliance	Continually monitors events in the IT environment to automatically detect and report any non-compliant activities.
15.3.2	Protect information system audit tools	Builds in extensive access controls, giving users necessary access to event log information without giving them direct access to the event logs themselves.



## About RSA

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, data loss prevention & encryption, 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).

## Further Information

To learn more about RSA's framework-based compliance approach, go to [www.rsa.com/compliance](http://www.rsa.com/compliance), where you will find:

- An overview on the standards-based framework approach
- A solutions brief outlining how RSA can help you implement a framework that's right for your organization
- A services data sheet exploring the support RSA offers and our five-step process for implementing a framework
- A product data sheet exploring the full range of solutions that complement the RSA enVision platform in the implementation of a compliance framework



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

The Security Division of EMC

RSA, the RSA logo and enVision are registered trademarks or trademarks of RSA Security Inc. in the U.S. and/or other countries. EMC is a trademark of EMC Corporation. All other trademarks mentioned herein are the properties of their respective owners.

ISOENV DS 0408