

## RSA® Data Loss Prevention RiskAdvisor Service, Department Offering

Automated discovery and remediation planning for unprotected sensitive information throughout the enterprise

### At a Glance

- Mapping of business functions to scanned systems
- Automated discovery and catalog of sensitive and regulated data using the RSA Data Loss Prevention (DLP) Suite
- Scanning a fixed number of desktops, laptops and file shares
- Compilation of a Data Discovery Findings Report and recommended next steps

### Manage Your Business and Help Prevent Data Loss

By defining sensitive data, determining where that data resides and how it got there, the RSA DLP RiskAdvisor service provides a basis for optimizing business processes that administer sensitive information and for formulating a data loss prevention strategy in order to manage and secure potential exposure. The RSA DLP RiskAdvisor provides an excellent baseline for a broader DLP strategy.

More than 150 million information records containing customer personally identifiable information have been breached since January 2005 according to the Privacy Rights Clearing House, a non-profit consumer information and advocacy organization. The loss of sensitive data, both regulated and unregulated, which is often strewn throughout an organization, can materially impact your bottom line, alienate your customers and damage your corporate reputation. As a result, data loss prevention is both a regulatory requirement and a business priority.

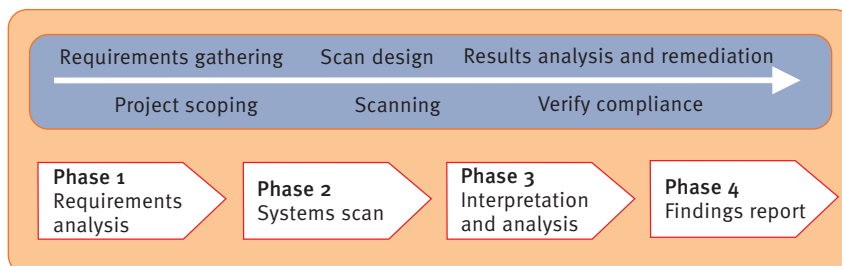
The RSA DLP RiskAdvisor Department service has been specifically designed as a first step to address these challenges. It can help organizations transform their data security posture from threat oriented to risk oriented. This service is designed to help organizations of all sizes stop playing defense, and start taking charge of their sensitive information. The RSA DLP RiskAdvisor Department service leverages the RSA DLP suite for automated discovery of unprotected sensitive information and provides a snap-shot of potential exposure. The result is the rapid identification of sensitive data on target file-shares and desktop infrastructure components. The RiskAdvisor service encompasses a high-level mapping of business functions to sensitive data, to help determine how that information was put at risk.

### Overview

The RSA DLP RiskAdvisor utilizing proven RSA DLP Suite technology, is structured in four phases with varying durations depending on final project scope.

#### Phase I. Requirements Analysis, Project Kick-off, Scoping and Logistics

This phase confirms the business drivers, finalizes the project scope, develops a deployment technical design and represents engagement logistics, project activities and resources in a project plan.





### Phase II. Onsite Software Installation and Preliminary Scan

This phase includes installation of the RSA DLP Suite scanning software, as well as execution of a preliminary scan against the specified in-scope systems, in order to verify that these target systems meet the technical requirements for successful scanning.

### Phase III. Interpretation and Analysis

In this phase the data-discovery rule-sets can be recalibrated, as necessary. The scan is executed and findings from the scan are prioritized. A high-level business process review is also employed to help eliminate false positives (accidental detection of sensitive data) and false negatives (non-detection of sensitive data).

### Phase IV. Findings Report & Knowledge Transfer

This phase includes the development of the Findings Report, which includes:

- Executive summary,
- Methodology, scan results and interpretation and analysis and
- Recommendations/preliminary remediation road map.

The Executive Summary provides a high-level view of the The Executive Summary provides a high-level view of the data discovery results, as well as an overview of RSA recommendations. The scan results/vulnerability analysis summarizes the list of machines scanned, a list of files found containing targeted data, and a profile of the incidence of targeted data within those files. Also included, for broader scope engagements, is a high level mapping of business processes which have put sensitive data at risk. Finally, the deliverable proposes remediation that may include both business process and security recommendations.

---

## Real Solutions Drive Real Value for DLP RiskAdvisor Customers

---

A financial services customer recently needed to understand risks to the business with regard to credit card information residing on laptops across the company. Upon determining the business drivers, RSA conducted an initial scan and found over 240,000 files containing credit card numbers. Upon filtering those files to exclude test data sets used by

the engineering group, there were still 70,000 sensitive files identified and tagged. RSA delivered a detailed findings report and sent emails to each end user requesting that they either delete or encrypt the sensitive files identified. End users had sensitive information sprawled throughout My Documents folders, temp folders and recycle bins. A follow up scan later located only 18,000 files, thus lowering the overall risk to the business. This engagement was also the catalyst for a new security education program. Next steps will be to implement new IT processes to automatically delete the recycle bin and temp folders when users shut down their machines.

### Why RSA?

RSA, The Security Division of EMC, is the expert in information-centric security, enabling the protection of information throughout its lifecycle. RSA enables customers to cost effectively secure critical information assets and online identities wherever they live and at every step of the way, and manage security information and events to ease the burden of compliance. RSA offers industry-leading solutions in identity assurance & access control, encryption & key management, data loss prevention, 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.

### Take the next step

RSA DLP RiskAdvisor Department Service includes the following:

- One geographic location,
- Multiple data types assessed,
- One NT or AD Domain,
- Up to 2500 devices scanned,
- Up to 5 TB of file share data scanned, and
- High-level business process review.

Contact your RSA sales representative today for more information, or visit [www.RSA.com](http://www.RSA.com)