THE CHALLENGE
A robust IT security and risk management program must be able to identify and implement the most current data protection standards, using a complete policy framework as a foundation. For many organizations, it is a constant struggle to define, publish and establish clear guidance for IT operations. Scattered repositories of policies, standards and controls, along with ambiguities in the different ways departments classify, implement and track policies, make it difficult to establish controls across the IT infrastructure and business.

Insufficient governance around operational procedures limits the ability of IT and security managers and administrators to connect controls to corporate policies. A common yet undesirable approach many organizations undertake by default is use of basic desktop office tools that were never designed to perform this function. The lack of centralized change control within these tools results in ineffective manual tracking and policies falling out of alignment with changing business objectives. This misalignment is further complicated by ineffective and missing processes and frameworks to handle policy deviations and exceptions.

IT and security frameworks like the ISO 27000 series, COBIT, and the NIST 800 series help establish common controls across IT and security programs. However, maintaining policies and standards that align with these frameworks can be a significant challenge, especially when additional regulatory data protection requirements are factored in. Policies can also quickly become outdated or duplicated as different operational groups react to changes in the business. The resulting gaps can lead to increased costs or reduce the IT organization’s ability to understand and meet regulatory obligations, resulting in severe fines and penalties as well as damage to brand and reputation.

OVERVIEW
RSA® Archer® IT & Security Policy Program Management provides the framework for establishing a scalable and flexible environment to manage corporate and regulatory policies and ensure alignment with compliance obligations. This includes documenting policies and standards, assigning ownership, and mapping policies to key business areas and objectives. Out-of-the-box content includes the most current security frameworks and control catalogs, such as the ISO 27000 series, COBIT 5, NIST 800 series, and PCI-DSS.

With RSA Archer IT & Security Policy Program Management, you can effectively manage the entire policy development lifecycle process. You gain the agility and flexibility to handle policy exceptions amidst an increasing volume of changes in a complex regulatory compliance landscape.
KEY FEATURES

• Comprehensive governance framework and taxonomy
• Automated workflow and change management
• Exception management and governance through appropriate risk acceptance and

KEY BENEFITS

With RSA Archer IT & Security Policy Program Management, you will see:

• Reduced time and effort required to create, modify and manage policies
• Less time required to research and identify key control requirements
• Improved ability to link regulatory requirements to internal controls

FOR MORE INFORMATION

To learn more about how EMC products, services, and solutions can help solve your business and IT challenges, contact your local representative or authorized reseller—or visit us at rsa.com. If you are an existing RSA Archer customer and have questions or require additional information about licensing, please contact RSA Archer at archersupport@rsa.com or call 1-888-539-EGRC.

RSA and the RSA logo, are registered trademarks or trademarks of Dell Technologies in the United States and other countries. © Copyright 2018 Dell Technologies. All rights reserved. Published in the USA. 01/18 Data Sheet H14991.

RSA believes the information in this document is accurate as of its publication date. The information is subject to change without notice.