DATA SHEET

ARCHER

Archer® IT & Security Policy Program Management

Use Case for IT & Security Risk Management

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 guidelines 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 challenging to establish controls across the organization's IT infrastructure.

Insufficient governance around operational procedures limits the ability of IT and security managers and administrators to connect controls to corporate policies. The default approach for many organizations is the use of standard desktop office tools never designed to perform this function. The lack of centralized change control within these tools results in ineffective manual tracking and policies that are 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 Policies can quickly become outdated or duplicated as different operational groups react to changes in the business. Resulting gaps can increase costs or reduce the ability of the IT organization to understand and meet regulatory obligations, leading to severe fines and penalties as well as damage to brand and reputation.

Overview

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 Archer IT & Security Policy Program Management, you can effectively manage the entire policy development lifecycle process. You can handle policy exceptions amidst an increasing volume of changes in a complex regulator compliance landscape.

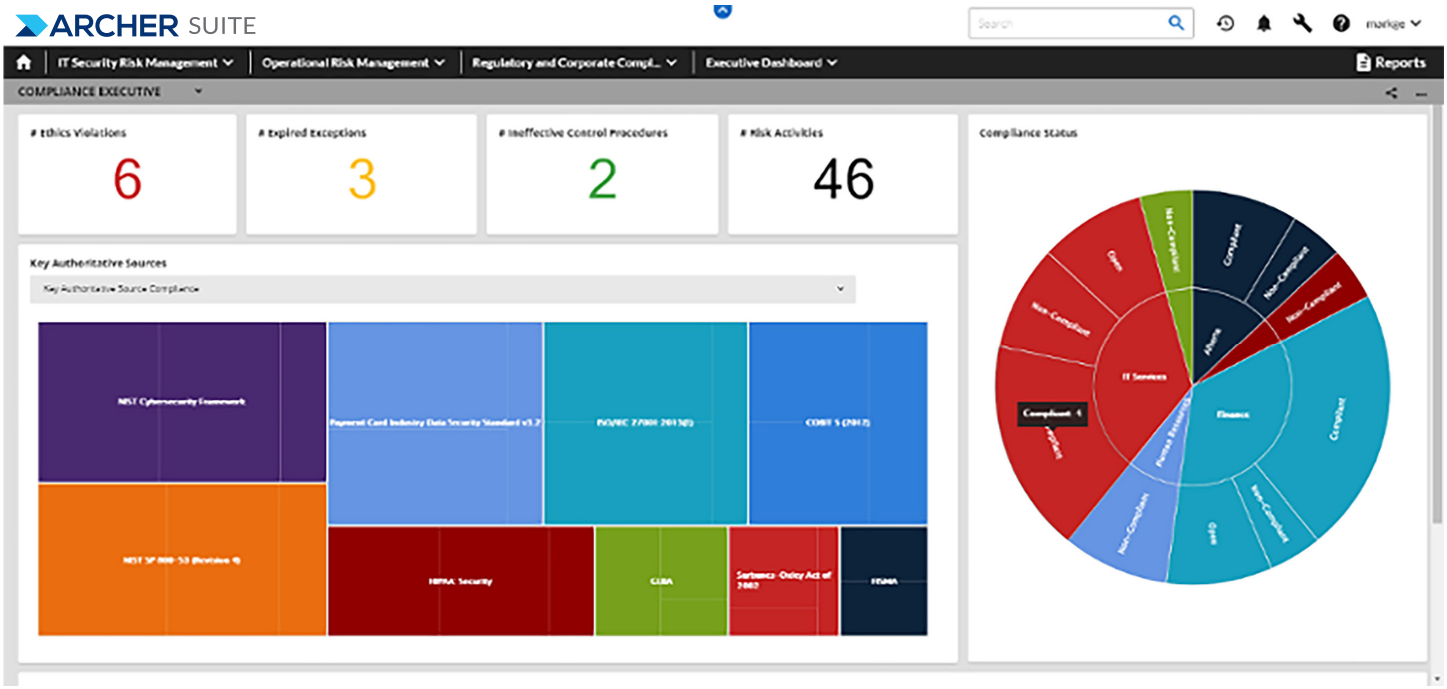
Key Features

- Comprehensive governance framework and taxonomy.
- Automated workflow and change management.
- Exception management and governance through appropriate risk acceptance and signoff.

Key Benefits

With Archer IT & Security Policy Program Management, you can:

- Reduce time and effort required to create, modify and manage policies.
- Reduce time required to research and identify critical control requirements.
- Improve ability to link regulatory requirements to internal controls.



Discover More

Archer, an RSA company, is a leader in providing integrated risk management solutions that enable customers to improve strategic decision making and operational resiliency. As true pioneers in GRC software, Archer remains solely dedicated to helping customers understand risk holistically by engaging stakeholders, leveraging a modern platform that spans key domains of risk and supports analysis driven by both business and IT impacts. The Archer customer base represents one of the largest pure risk management communities globally, with over 1,500 deployments including more than 90 of the Fortune 100.

ARCHER
An RSA Business