FOLLETT CORPORATION

Follett Corporation gains visibility into Internal Controls and PCI DSS compliance data

AT-A-GLANCE

Key Requirements

- A common platform for all governance, risk, and compliance (GRC) programs
- Workflows that streamline and automate the compliance process
- User-friendly, flexible deployment with quick time-to-value
- Executive-level visibility to gather and summarize results, and access dashboards and real-time reports
- Automation of communication processes for completed testing

Solution

- A single enterprise platform for compliance and policy development and management
- Workflow management that streamlines policy reviews, auditing, and remediation
- Reporting and dashboards providing visibility and supporting decision-making at various levels of management
- Campaigns utilized to send automated messages via Outlook including due dates

"Working with RSA, we have been able to accelerate our internal control compliance processes. At Follett the internal control program utilizes the COSO Framework as a model. We used to have our data in lots of spreadsheets distributed around the business. With a centralized repository we have been able to utilize data in various reports, spreadsheets, and presentations throughout the organization. Now we have a single platform that gives us real-time visibility and insight."

JOE AGNEW, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, FOLLETT CORPORATION

Across its six business units, Follett Corporation's services include management of over 900 college book stores, supplying educational materials to PreK-12 schools and libraries, supplying public libraries, and software for use in PreK-12 schools. Follett International spans the business units, providing their services to customers worldwide. The company generates more than $2.7 billion in annual sales revenue.

KEY REQUIREMENTS

As a company handling credit card payments, Follett must meet a high level of compliance (i.e. level one) of the Payment Card Industry Data Security Standard (PCI DSS), and it also structures an internal control program utilizing the COSO Framework as a baseline without requiring annual certification by an external auditor. "PCI DSS compliance is critical for us. If we failed to meet our obligations, we could face monthly fines from card associations," said Joe Agnew, Vice President and Chief Information Security Officer at Follett Corporation. "We comply with internal controls because of our values, and the need to demonstrate to board members, owners, and relevant outside parties that the company is confident in the numbers it is reporting."

The internal control program was based upon spreadsheets distributed around the businesses while the compliance process was manual, time-consuming and inefficient, providing limited enterprise-level visibility into Follett's overall compliance. "Our internal control program compliance processes used a significant number of spreadsheets and Word documents, spread around the business, which were difficult to keep up to date and to track. There was little or no visibility into the data in the spreadsheets from an

enterprise level," said Agnew. "Our PCI DSS compliance process is not as far-reaching but uses similar manual processes and spreadsheets to support annual certification. This is why we are currently in the process of automating that process with RSA® Archer™."

Results

- Enterprise-level visibility supporting efficient governance of compliance processes
- Ability to collaborate across the businesses on creating and maintaining policies and compliance documentation
- Extensible platform that can be used for corporate policies and other regulatory requirements in the future
- Testing completed in a more efficient and effective manner with less manual follow-up required

Follett needed a common platform for all its governance, risk, and compliance (GRC) programs, with dashboards and reports that provide visibility into the current compliance status. The solution needed to standardize compliance documentation, provide central visibility, offer workflows that streamline and automate the compliance process, and be easy to deploy with quick time-to-value.

Follett also wanted to take the opportunity to standardize and centrally locate the 200 policies used in its internal processes, from HR, through legal, IT, auditing, and finance.

SOLUTION

Follett used RSA Archer Policy Management and RSA Archer Compliance Management to build a single enterprise platform for compliance and policy development and management. "RSA Archer gives us flexible control of our compliance processes and systems," said Agnew. "Once you've set it up, you only need a few people trained on the framework to maintain it, modify it, and grow it."

He adds: "RSA Professional Services accelerated our learning curve. You can't learn everything you need to know in a week's training course, so they provided a lot of resources and expertise that we could draw upon."

The platform provides a single store for all compliance data and policies, together with workflow management that streamlines audits and remediation. "It's a really good example of how you can bring solid governance to a compliance process," said Agnew. "We manage it from a central core which supports that enterprise-level visibility, and we can automate the workflow too. We've been able to drive a lot of efficiencies in our compliance process and find and effectively resolve any issues that would have been more difficult to find before.

"Our internal control solution automates communication of testing each quarter and year," Agnew continued. "It automates the linking of risks to processes and controls, assertions to accounts and controls, and controls to processes, creating an avenue to ensure risks are mitigated by relevant controls within the process. It also helps us to track and capture results. We document the sign off and certifications annually, which are utilized by C-level executives to ensure controls are in place and work effectively. About 50 of our associates have access to reports so we always know where we are."

Members of the finance team are able to create their own reports for internal control compliance, and to share them with others in the company. "The platform brings the right information to the right person at the right time," said Agnew.

The same system will soon support Follett's PCI DSS compliance, with numerous people having access to flexible dashboards and reports for a real-time view of compliance. "It will enable us to keep our hands on the process all year around, rather than finding out once a year that we're out of compliance with something that we need to quickly react to. RSA Archer will maintain ongoing visibility of any issues pending certification that we can proactively address. This is especially important with PCI which can tend to be a moving target."

RESULTS

Follett's internal control compliance processes are now well understood and consistently maintained, and all information and systems are continuously accounted for. The workflow enables Follett to keep its compliance documentation updated, and the dashboards provide visibility of the company's compliance posture at all times. The same process and methodology will soon produce the same benefits for PCI DSS.

Follett was able to reduce cost as a result of using the RSA Archer solution to streamline the internal controls compliance processes. The availability of real-time information allowed the process to be managed and governed more efficiently.

Follett has also created a platform it can easily extend for other compliance purposes, and which it already uses to standardize, centralize, distribute, and maintain corporate policies as diverse as its social media policy, dress code, contract requirements, and book store operating agreements. "RSA Archer is a facilitator of discussion," said Agnew. "People can now work together easily on developing and updating policies. It's something we've wanted to do for years, but we never had a mechanism that would make it easy for the different businesses and functions to collaborate on a policy or a contract review, with clear workflows to hand over responsibility when it's someone else's turn to contribute. Now we do."

"You can get RSA Archer to do anything you want. Once you've set it up, you only need a few people trained on the framework to maintain it, modify it, and grow it."

JOE AGNEW, VICE PRESIDENT AND CHIEF INFORMATION SECURITY OFFICER, FOLLETT CORPORATION

CONTACT US

To learn more about how RSA products, services, and solutions help solve your business and IT challenges contact your local representative or authorized reseller – or visit us at www.RSA.com