CUSTOMER Q&A

FEDERAL HOME LOAN BANK OF ATLANTA

Federal Home Loan Bank of Atlanta Creates a Unified GRC Strategy with RSA Archer

AT-A-GLANCE

Challenges

- FHLBank Atlanta has a responsibility to meet strict compliance regulations that cover a variety of types of risk.
- It needed to ensure its approach to technology risk management was centralized, consistent, and easy to report back to the board in terms that the business units could understand.

Results

- The organization implemented the Policy, Risk, Enterprise and Business Continuity modules of Archer, as well as building a number of tailored on-demand applications.
- By linking all areas of technology risk management together, the business operates more efficiently, and risk reporting is made much clearer and simpler.
- Automating processes has driven significant time savings for risk managers across the organization.

"RSA Archer has brought many siloes together and we're finding that linking business continuity to security and vendor risk provides a more comprehensive risk picture. These teams can connect what they're doing and we're all on the same page now."

JOE WATKINS, DIRECTOR OF TECHNOLOGY RISK MANAGEMENT, FEDERAL HOME LOAN BANK OF ATLANTA

FHLBank ATLANTA
A FEDERAL HOME LOAN BANK

RSA

FHLBank Atlanta is a cooperative bank that offers financing, community development grants, and other banking services to help member financial institutions make affordable home mortgages and provide economic development credit to neighborhoods and communities. It is one of 11 regional banks in the Federal Home Loan Bank System, which raises funds in the global financial markets and distributes the proceeds to members and local communities.

Why is GRC important to you?

GRC plays two different roles at the executive and the management level. Firstly, it makes sure that we are meeting our compliance requirements by establishing controls and clarifying what we need to do to meet them. It also ensures that we're managing risk to the appropriate level. The board and the executive team sets the organization's risk appetite, and GRC allows us to measure the program and make sure that we're following what they ask for.

We have an enterprise risk management function that looks at a macro-level view of things like operational risk, credit risk, and reputation risk. My team is tasked with drilling down further and focusing on technology risk. The two areas very quickly align and make sure we're in lockstep.

How did you choose RSA Archer?

We went through a very detailed selection process before choosing RSA Archer as our GRC solution. A key factor in that decision was usability. We had used previous GRC products with difficult interfaces, from both an end-user as well as an administrator perspective, and so when we were looking at Archer and actually doing sandbox testing, we could see just how much easier it would be.

How are you using the solution?

We have four modules in place now: Policy, Risk, Enterprise and Business Continuity. We've also built a number of on-demand applications (ODAs), where we needed a specific point solution for things like managing end-user computing spreadsheets and inventories. We're also looking at expanding into using the Security and then Vendor Management modules as well.

What impact has the solution had on your business?

The biggest benefit to the Bank has probably been our ability to link areas together. The approach to technology risk management within the Bank has matured over time. Security does what it does very well; it manages the security risk. Business continuity manages their risk. Compliance and control evaluations manage their risk. Archer has enhanced our ability to bring these areas together and we're finding that linking business continuity to security and to vendor risk, provides a more comprehensive risk picture. These teams can connect what they're doing and we're all on the same page now.

It makes a difference to reporting too. For example, if a service provider is suffering from credit viability or another increasing risk area, we need to be able to report that up the chain to make executive management aware. Being able to do that through linking with business continuity and the business processes we can do that in terms that, they'll appreciate and be able to act on.

The biggest cost that we have in our GRC program is time. RSA Archer is enabling us to automate a lot of governance processes, like updating inventories, performing risk assessments, mapping controls to many different industry frameworks and gathering assessment/audit. By automating it, we're getting time back to devote to other tasks. Experts in the field can be re-directed to more proactive risk management rather than always being reactive.

How is RSA Archer helping with application lifecycle management?

In the past we would look at an application that may be unsupported or soon-to-be unsupported, and the business unit would make a decision on whether they wanted to accept the operational risk of going onto an unsupported platform. With the use of Archer we're now able to identify and take into account other types of risk, and apply the right frameworks and assessments to make sure we're taking the bigger picture into account.

How does RSA Archer support your business continuity strategy?

We're using Archer to take over 100 controls around change management and backup and map them to various industry standards like NIST, ISO and COBIT. For example, we've just completed an endeavor to map our control framework to the NIST critical infrastructure guidelines that came out recently, identify gaps and then work to remediate those gaps. Once this is done, we can monitor and evaluate our controls and policies, which we anticipate will have a cost-saving impact for us when it comes to doing audits and assessments. The auditors will no longer have to go around each team to gather the information they need – they can get it all centrally from Archer.

What tips can you offer others?

Think about risk in business terms, not just as a technology issue. If I'm looking at it from a security perspective I can't say that, 'we have a vulnerability that's high risk', because ultimately the business units and the executive management may not truly understand the linkage to a real-world impact. By starting with business continuity and linking that to security risk, now we can actually say 'this vulnerability affects this server which affects this application which affects this business process which has this business risk'. Now we understand the impact of that vulnerability all the way to a tangible cost and a tangible real-world operational impact.

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