AuditOne LLC

Risk-Managed Internal Audit and Credit Review Expertise

NEWS

AuditOne Advisory – Assessing Cloud and Technology Service Providers for Cybersecurity Preparedness and Resilience

AuditOne, LLC September 18, 2017

AuditOne Advisory

From Bud Genovese, Chairman

As part of vendor management, we have seen a recent examiner focus into how you monitor cloud and technology service providers for cybersecurity preparedness and resilience. Kevin Tsuei and Jon West, part of AuditOne's Technology Audit group, have prepared concise guidance on how to conduct the review and suggestions on what to look for. Please share this with colleagues with responsibilities related to vendor management and technology oversight. Thank you, –Bud

---

Assessing Cloud and Technology Service Providers for Cybersecurity Preparedness and Resilience

By: Jon West, Senior Audit Associate, and Kevin Tsuei, Technology Practice Co-Director, AuditOne, LLC

In our review of recent examination reports for various of our firm's clients, we noted some attention to a new topic: a requirement that vendor reviews include the vendor's cybersecurity preparedness and resilience, incident response procedures, and awareness of emerging technologies. However, the question confronted by Financial Institutions (FIs) is how to conduct such a review.

As a firm responsible for the auditing of FIs, we have worked with regulators, clients, and our own IT team to create a solution to this business problem. Like most of our clients, we rely on technology service providers to help us run our business. We primarily utilize cloud services, specifically Software as a Service (SaaS) and Platform as a Service (PaaS). These service providers have brought with them many business benefits to AuditOne, primarily providing us with scalability and ease of deployment. We, like our

clients, follow strict ongoing service provider monitoring practices using the necessary due diligence materials (i.e., financial statements, independent audits (e.g., SOC reports), proof of insurance, business continuity planning, and disaster recovery test results).

However, how can we evaluate a service provider's cybersecurity readiness? The FFIEC released guidance on Outsourced Cloud Computing in July 2012. The guidance provides us with a checklist as part of cloud service provider due diligence, and we have included that list below as well as some suggestions on what to look for:

Risks	To what extent does this service provider present Strategic, Financial, Reputational, or Compliance risks?
Data Classification	Does the data contain NPPI information? Confidential information about the FI? Or does it contain only non-confidential information?
Costs	Expense of cloud providers can be significantly higher than hosting on-site if a certain amount of growth is experienced by your FI. Ensure that management is aware of when a relationship with this vendor may cease to make sense, including the costs of transitioning to hosting your own solution.
Encryption for Data-at-Rest and Data-in-Motion	Is data being securely encrypted as it is transferred from one location to another? If applicable, is data that is in storage being securely encrypted?
Multi-tenancy Risks	Is your data on the same server as another FI? What is the risk that malware introduced by other FIs could compromise your confidential data?
Business Continuity/ Disaster Recovery Program	Uptime for these service providers is generally of great significance to an FI's daily functioning. Ensure that a commensurate amount of scrutiny is applied to their ability to continue providing service without interruption during a disaster.

Certainly, these factors are highly important. However, they might not be enough to fully assess a service provider's cybersecurity preparedness and resilience. To give an idea of the kind of factors to take into consideration, here are the internal controls we audit when we do an evaluation of an FI's cybersecurity readiness: IT/GLBA/Cybersecurity risk assessment, policies, management oversight, staffing, threat and vulnerability detection, IT asset management, change management, threat intelligence, incident response planning and testing, infrastructure management, patch management, access and data management, training, and the service provider's own third-party management. Not all of these will be directly relevant to your own assessment of individual vendors, but this will give you an idea of the range of relevant considerations.

As part of our ongoing monitoring process for our own third-party providers, we found that many of these cybersecurity controls can be found in their SOC reports. However, there are typically some gaps between the cybersecurity control list above when compared to our service providers' audit reporting. As a result, we will reach out to our service providers directly for additional information, and we've found them generally willing and able to provide additional security information (e.g., white-paper) to close this gap. Should this not be the case during your due diligence process, do be sure to retain documented evidence of your efforts, should your auditor or examiner request to verify your process.

It is noted that smaller technology service providers may well not have the means to conduct periodic SOC audits. While we strongly encourage these firms to obtain a SOC review (note: our affiliate company AuditOne Inc. offers very competitively priced SOC reviews), it is understandable that the cost might be too much. In these cases, it is management's responsibility to conduct its own audit/review of its service providers' key controls as they relate to cybersecurity. We plan in the upcoming months to publish further Advisories on this topic and to elaborate on the relevant cybersecurity controls to look for and to audit.

We hope that our checklists and guidance can help you enhance your initial and ongoing monitoring of your technology (including cloud service) providers. If you would like to learn more about vendor management best practices, we recommend the on-demand WiBinar that we recently hosted with Western Independent Bankers, which you can find at: https://www.wib.org/web/Online/Events/Event_Display.aspx?EventKey=W317070020.

AuditOne LLC – Company Overview

AuditOne LLC is a leading provider of risk management services to financial institutions in the Western US and nationally. Our sole focus enables us to deliver effective and efficient internal audit and credit review services. This exclusive focus translates into exceptional benefits to our financial institution clients. We have experience with all regulatory authorities and offer a full selection of audit services comprising BSA/Anti-Money Laundering Program, Automated AML System Validation, Asset/Liability Management (ALM) and IRR Audits, ADA Website Compliance Reviews, IT/Information Security/Cybersecurity, Network Penetration Tests, Credit Review/ALLL, ACH Rules Compliance, Operations, Trust Audits, SOX/FDICIA Testing, and many specialty areas within each of these.

For information on how our services can help reduce risk at your institution, contact Jeremy Taylor, CEO, at: Contact Us. Also, for more information about AuditOne LLC and all our audit services see www.AuditOneLLC.com.

AuditOne has been audited for compliance with the QAR requirements of the Institute for Internal Auditors (IIA).

AuditOne, LLC | LinkedIn

Address:
6131 Orangethorpe Avenue, Suite 470
Buena Park, CA 90620

Phone: 562.802.3581