VIRTUALIZATION
CLOUD
APPLICATION DEVELOPMENT
NETWORKING
STORAGE ARCHITECTURE
DATA CENTER MANAGEMENT
BUSINESS INTELLIGENCE/APPLICATIONS
DISASTER RECOVERY/COMPLIANCE
SECURITY

Risk Management for Cloud Computing

Security concerns remain a hurdle to expansive cloud adoption. Learn how to apply security protocols to your organization's cloud computing endeavors.

TechTarget

Solving the Risk Management Conundrum

As more companies move operations to the cloud, the unique risk management issues that accompany data are a growing concern. A recent SearchCompliance.com survey found that almost 40% of respondents expected their spending on cloud security products to increase in the first half of 2013.

To alleviate these problems, organizations need to ask the right questions of cloud providers and prepare their own governance, risk and compliance processes for the cloud. This handbook offers detailed risk management advice for organizations pursuing cloud computing arrangements.

In "Risk Management Frameworks for Cloud Security," Eric Holmquist lists several readily available risk management frameworks that can be applied to cloud computing, and spells out the 20 questions that should be asked of every cloud provider. In our second article, consultant Ed Moyle looks at how to create harmony between the compliance and information security functions, two sometimes-contentious groups that must be able to work together to ensure a successful cloud deployment.

And finally, SearchCIO.com features writer Karen Goulart examines cloud provider service-level agreements and provides real-world examples of how IT leaders across the country use SLAs to protect their security and compliance processes when using the cloud.

We hope this information helps ease the transition as your organization moves data storage and other business processes to the cloud. ■

Ben Cole
Editor, SearchCompliance.com
bjcole@techtarget.com

Risk Management Frameworks for Cloud Security

Companies looking to expand their infrastructure capabilities are increasingly turning to cloud-based solutions for remote hosting, colocation data centers or full infrastructure outsourcing. Cloud service providers (CSPs) have proven to be a very cost-effective, highly efficient resource for businesses of all sizes, and confidence is growing that the cloud can be an effective way to host data and applications, as well as reduce key infrastructure costs.

But as CSPs continue to evolve, so, too, does the related security infrastructure required to ensure that client data remains safely segregated and accessible only to authorized users.

The key to managing cloud computing information security is to understand that it cannot be managed using an 80/20 rule—that is, mitigating the obvious risks and then dealing with the rest as it occurs. Unlike other forms of operational risks, this is an area that has to be managed to a "zero event"—a data loss just cannot happen. Simply put, businesses can outsource the technology but can't outsource the risk. Therefore, cloud service providers must be managed proactively, aggressively and with a carefully structured approach.

APPLYING RISK FRAMEWORKS

While there are a number of standards and frameworks available, very few specifically address any outsourced IT services, let alone CSPs. Nevertheless, many of these standards and frameworks can be helpful to risk management in the cloud. The frameworks described in the following list address some key cloud risk management processes:

- **COBIT.** The Control Objectives for Information and Related Technology remains the gold standard for IT governance. It is the most widely used control framework and integrates easily with both COSO and ISO 27000x. It is fairly inexpensive and is available to all ISACA members. COBIT is not strong on information security, so it does need to be amended with an organization's specific security standards. However, COBIT's fundamental processes for identifying potential risks and implementing suitable mitigating controls applies and extends to CSP management as much as it does other internal business processes.

COBIT is not strong on information security, so it does need to be amended with an organization's specific security standards.

- **ITIL.** The IT Infrastructure Library provides some strong guidance for the IT environment's service aspect. It is not a governance framework and does not address enterprise architecture, but the ITIL processes depicting the "availability" aspect of IT services certainly relate to the cloud environment. ITIL aligns very well with the COBIT framework and includes a certification process.

- **ISO 27000x.** The international standard for information security practices remains one of the best resources for information security guidance. The standard follows a risk-based approach to prioritizing security emphases and contains practical data control strategies. In addition, the standard goes beyond confidentiality and also covers availability and integrity—all of which are applicable to managing third-party service providers. All CSPs should attest to being ISO 27000x compliant.

- **PCI-DSS.** Although the Payment Card Industry Data Security Standard is only applicable to companies that store or process credit card data, it is

Continued on page 6

TWENTY QUESTIONS FOR YOUR CLOUD SERVICE PROVIDER

- What is the basic systems architecture?
- Where will the data be held, physically and logically?
- Who will have access to the data?
- How, when and where is data encrypted, both at rest and in motion?
- Are clear text protocols allowed on the network and in use?
- How is incident response handled?
- What is the cloud service provider's fault tolerance capability?
- What is the provider's business model (consumer/enterprise, small business/corporate, etc.)?
- What type of applications will you be hosting? What information will they contain?
- What internal technical standards need to be replicated to the cloud service provider?
- What regulatory requirements need to be applied to the cloud service provider?
- How are encryption keys stored and managed? Who has access to these keys?
- Is anti-virus/anti-malware installed on all servers and workstations, and how is it updated?
- Is security penetration testing performed against the external and internal networks?
- What is the cloud service provider's password policy? Are user access policies and procedures documented, approved and implemented?
- What firewalls, IPS/IDS and Web filtering technologies are in place?
- Are data leakage prevention controls in place at the network, email and end-user computing layers?
- Are baseline security requirements established and applied to the design and implementation of applications, databases, systems and network infrastructure and information processing?
- Are existing wireless networks encrypted with WPAv2, and are these networks isolated from the internal networks?
- Is two-factor authentication required for remote administration of all networking and infrastructure devices?

Continued from page 4

still a very good standard to use as a reference tool. It does not provide a governance structure and is fairly high level, but it provides some input on managing third parties. It also contains a decent self-assessment and is free to download.

- **CSA.** Finally, while not a standard or framework, the latest entrant into the risk governance universe is the Cloud Security Alliance, a not-for-profit organization with a mission to promote best practices for providing cloud computing security assurance. The CSA provides a "Cloud Controls Matrix," as well as mapping tools to other standards and frameworks (including ISO, COBIT, PCI, etc.). The CSA is a relatively new resource, but one that should be in every IT manager's risk assessment toolbox.

Home

Editor's Note

Risk Management Frameworks for Cloud Security

Information Security, Compliance and the Cloud

Keep on Top of Cloud SLAs

CLOUD PROVIDER DUE DILIGENCE

Regardless of whether you use one or more standards or frameworks, there are some basic risk management principles that must be followed when managing outsourced cloud service providers. The essential elements of third-party due diligence are fairly straightforward. These include:

- Third-party reviews (SSAE 16, PCI certification, etc.)
- Documentation on the provider's information security and business continuity programs
- Financial and insurance information
- References and independent research
- Vendor history (service interruptions, security breaches, legal or regulatory issues, etc.)

It is critical not just to acquire this information, but also to conduct a detailed review and analysis of it (see page 5). Any information that raises issues or concerns should be addressed promptly with the CSP.

While there is an almost infinite number of questions that can be asked of

any CSP, ultimately all of the due diligence comes down to answering two key questions:

- How do you know the cloud provider can support your operation, and up to your service-level expectations?
- How do you know the provider can protect your data?

Acquiring enough governance and technical information to answer both of these questions satisfactorily is the key to CSP management. If any other IT or risk management frameworks help in this management process, then they also may be worth considering as part of your overall risk management program. —*Eric Holmquist*

Information Security, Compliance and the Cloud

To say that information security and compliance professionals are sometimes at odds with each other is a bit of an understatement. Despite IT industry guidance about the value of network security and compliance teams working together, quite a bit of friction can occur. The root cause, most often, has to do with the fundamental disconnect between how the two disciplines prioritize specific efforts, including individual technology controls.

Understanding why this friction crops up isn't difficult. Information security professionals focus on risk management (i.e., keeping technology-related risk within acceptable parameters), so they concentrate on deploying controls with the potential to significantly lower overall technological risk. Compliance professionals, by contrast, need to ensure that technology controls fully address regulatory compliance requirements.

From the compliance professional's point of view, failing to implement a required control is a risk in and of itself.

From the compliance professional's point of view, failing to implement a required control is a risk in and of itself. Disagreement between the information security and compliance camps comes when there is disparity between how a given control fulfills one function but not the other. For example, a control required by regulatory mandates sometimes provides little in the way of overall technological risk reduction, and a control with practical risk reduction doesn't always meet a regulatory objective.

This prioritization gap has been difficult to rectify. Organizations sometimes try to align the information security and compliance functions via

governance, risk and compliance unification efforts. Very often, however, these integrated functions tend to drift back toward a more independent dichotomy.

Recent changes in the way organizations purchase IT services—specifically, the adoption of provider-supplied services through cloud technologies—help redefine the relationship between info security and compliance teams. This can harmonize the working relationship between each department's resources through necessity. By the same token, when that necessity is ignored and contentious relationships persist, it can become a recipe for security and compliance concern.

The use of cloud requires high-level coordination between compliance and technical security teams.

The use of cloud—especially multitenant, provider-supplied technology services—requires high-level coordination between compliance and technical security teams. Why? A significant percentage of cloud security controls in this context are provider-supplied resources. As a result, these controls require input from both disciplines to be managed and evaluated effectively.

FORGING AN ALLIANCE

A primary goal of compliance professionals is to validate vendor-implemented controls and deem them sufficient to meet regulatory mandates. To do so, they almost certainly need to draw upon technical insights from information security stakeholders. Not only are information security teams (usually) more technically focused than their compliance counterparts, but they are also intimately familiar with the organization's internal technical security controls.

This means that the information security department is best equipped to understand the technical challenges when operating those controls post-deployment. These professionals are also more likely to understand the potential integration issues (including possible gaps in control coverage) that can

occur when internal processes, applications and systems start to directly interact with vendor-managed ones.

Correspondingly, IT security personnel need to draw on compliance team members' skill sets to understand the risk dynamics of a vendor-hosted environment. It is the compliance team that has the processes, methodologies and subject matter expertise to properly audit sufficiency, scope and coverage. Because compliance team members have this audit and data collection expertise, they are (or at least have the capability to be) the eyes and ears of risk management relative to the vendor-managed services and controls.

It's important for organizations to recognize that both teams have a role to play in evaluating cloud deployment from a security and compliance standpoint. The same is true for monitoring activities post-deployment. In situations where the information security and compliance teams are already working well together on a consistent basis, a tighter working relationship will happen naturally. But in situations where they are either completely independent or where they don't see eye to eye, it's imperative that a closer-knit relationship be formed. If the two teams don't communicate or otherwise work together, both technical risk and compliance risk come into play.

IT security personnel need to draw on compliance team members' skill sets to understand the risk dynamics of a vendor-hosted environment.

In those situations where there isn't an already-established close working relationship between security and compliance, a few productive measures can go a long way toward starting one. One approach is the designation of a cloud "tiger team"—a multidisciplinary team that incorporates stakeholders from across the organization (including security and compliance) when considering and implementing cloud deployment. As team members work closely together, they solidify relationships that tend to carry over into other business processes.

A modified version of the team approach that incorporates direct

partnership between information security and compliance (without the rest of the multidisciplinary team) can work, but requires an internal champion in one or both of the disciplines. Alternatively, standardization and toolset sharing for tracking vendor compliance can also be helpful, assuming you can get to a consensus on what the tool should be and how it will be used.

When all else fails, a "top-down" approach or, put simply, a directive from senior management outlining joint ownership of tasks, is better than nothing. But because this approach doesn't start demonstrating the value of this cooperation, it can be more brittle than relationships that evolve themselves.

Whichever route organizations take to remove the information security and compliance disconnect, it is vital to the success of any cloud deployment, as well as many other organizational functions. If the two functions don't work together when it comes to cloud deployment, risk and compliance concerns will abound. —*Ed Moyle*

Keep on Top of Cloud SLAs

If you want to make IT and compliance professionals laugh, try suggesting that the importance of service-level agreements is overblown when it comes to cloud services. Take a spin around the Web, or read some blogs, and it becomes apparent that leaders from top cloud service providers believe IT executives put too much emphasis on cloud service-level agreements (SLAs). These providers often claim that IT customers fret more about potential outages than about mastering the details of how the technology will be applied to and benefit their business.

Recognizing the business value of one's cloud service doesn't diminish the value of an SLA.

Recognizing the business value of one's cloud service doesn't, however, diminish the value of an SLA, many experts insist. As more cloud offerings enter the market and find their way into not just IT departments but business units across the enterprise, proponents of cloud SLAs say that getting base-level parameters in writing—from uptime expectations to incident notification—is a must for risk management purposes.

Don Peterson, Merced College's director of IT, takes the SLA very seriously. He recently oversaw the implementation of cloud-based storage to support the data security and compliance demands of the California college's nearly 18,000 students, staff and faculty.

"We wouldn't even think about [using cloud technology] without an SLA," Peterson said. "It's the ground rules."

Arlis Brotner, Peterson's network manager who researched and proposed that Merced turn to the cloud for storage, said base-level expectations,

especially from a security and compliance standpoint, have to be explicitly stated in writing. "It's not just about downtime; it's about response time, how quickly we report it and how they respond to it—that's critical to have," he said.

Otherwise, you're essentially left in the dark when it comes to cloud use. Unlike with on-premises technology, there is no one to turn to with questions or with blame when there are security or compliance issues.

As it turned out, Peterson and Brotner were fortunate to forge a good relationship with their cloud storage vendor, which didn't balk at an SLA that included some finer points. "We needed it to really spell out how they were protecting our data, the redundancy, that it was encrypted in transit and in storage, all those things," Peterson said. "Some SLAs aren't quite so granular as that, but we needed that. It protects us and it protects the vendor."

EMBRACING CLOUD STORAGE AND TRUSTING SECURITY

Peterson and Brotner also became more comfortable with cloud security when their own research found that information would be stored in more than one location, and would be encrypted in transit and in storage.

"That helped, because you always worry about your data not physically being 'here,'" Peterson said. "It's probably safer in the cloud than it is here because we don't encrypt on disk here, but they do in the cloud ... so it just seems to me it's safer. I wouldn't have said that before, but now, seeing this [solution], I can say that."

So, what are Peterson and Brotner now comfortable entrusting to the cloud? Brotner said that information includes individuals' files from home directories, spreadsheets, Word documents, Access databases, images used between departments or within departments, SQL database backups, virtual machine backups and email archives. IT also is looking to add direct-to-cache storage, which would allow users to access archived data on their own, an action that is currently carried out by IT on request.

Cloud gateways (and their accompanying SLAs) might be another answer for those still hesitant about moving data operations to the cloud. In an

August 2012 report, Forrester Research analyst Andrew Reichman asserted that issues holding back cloud-based storage solutions from broader adoption in the enterprise could be addressed through agreements with gateway providers.

Reichman identified latency, uncertainty about accessing data across the WAN, difficulty coding to cloud providers' application programming interfaces (APIs) and the risk of data leaks as enterprise organizations' chief cloud storage concerns. In response, the market is seeing a growing number of cloud gateway vendors. Most gateways provide data caching for frequently accessed data; WAN optimization; API integration; protocol translation; and data encryption, protection, synchronization and deduplication.

THE CLOUD SLA BILL OF RIGHTS

The importance of cloud SLAs and setting ground rules for cloud risk management are more important than ever, according to analyst group Constellation Research Inc. The San Francisco-based firm recently released The Enterprise Cloud Buyers Bill of Rights. Focused on Software as a Service (SaaS), the document includes 55 "basic rights" that organizations should demand over the life of a cloud service.

Constellation Principal Analyst and CEO R "Ray" Wang said that with the majority of enterprise software now being consumed via SaaS or cloud deployment, companies need to apply the same rigor and expectations in adopting and negotiating these contracts as for on-premises software. Just in terms of customer experience, for example, three "critical rights" must be met: quality guarantees and remuneration, ownership of and access to data with no questions asked, and ongoing financial and risk management transparency.

Those rights go well beyond the ones demanded by the IT department. As Wang states, the relationship between the vendor and the "client" today often includes not just IT but the chief marketing officer and other business executives, including compliance officers. Going from on-premises software to the cloud is a chance for a clean slate for the IT department—not only in

building a trusted relationship with the vendor but also in building a strong partnership with the business units that are served by the cloud.

The security issues and legal concerns inherent in cloud computing are complex, to be sure, said analyst Robert Desisto at Stamford, Conn.-based Gartner Inc. But there are some things that should be simple and straightforward. For example, some cloud applications are less mission-critical than others, and their lack of availability might not harm a company, he said. But even for these less-critical business apps, buyers must insist on reaching a written agreement on performance expectations.

"The bottom line is, if vendors are so confident about their performance, why not put it down on paper? What is the resistance?" he said. "The resistance is they don't want to have the liability out there that they won't be able to perform as advertised."

Desisto won't get any argument about that from Walter Weir. In 2012, the University of Nebraska CIO and his IT team carried out a cloud migration that moved 13,000 staff and faculty members from an on-premises system to a cloud-based system. For him, those more specific details about business value were covered in a request for proposals. But, he said, that didn't diminish the importance of the cloud SLA.

"There's an understanding that stuff happens and nobody's going to go gunning for anybody unless it's drastic," Weir said. "But you still want some degree of confidence that your partnership will be driven, managed and evaluated on the vendor's ability to live up to this agreement." —*Karen Goulart*

ERIC HOLMQUIST is the managing director for enterprise risk management at Accume Partners, and has more than 30 years of experience in the financial services industry. He has authored *Right-Sizing ORM: Scaling Operational Risk Management for the Small and Medium-sized Market*, and is a contributing author to *Operational Risk 2.0 and The Advanced Measurement Approach to Operational Risk*. Write to him at editor@searchcompliance.com.

ED MOYLE is a founding partner at New Hampshire-based information security and compliance consulting firm SecurityCurve. Moyle previously worked as a senior manager with Computer Task Group Inc.'s global security practice and, prior to that, served as a vice president and information security officer at Merrill Lynch Investment Managers. Write to him at editor@searchcompliance.com.

KAREN GOULART is features writer for SearchCIO.com and SearchCIO-Midmarket.com. She covers CIO strategies for cloud computing and virtualization, the data center and business application trends. Write to her at kgoulart@techtarget.com.

TechTarget

Risk Management for Cloud Computing is a SearchCompliance.com e-publication.

Rachel Lebeaux
Managing Editor

Scot Petersen
Editorial Director

Ben Cole
Associate Editor

Eric Holmquist, Ed Moyle
Contributing Writers

Karen Goulart
Features Writer

Linda Koury
Director of Online Design

Corey Strader
Director of Product Management
cstrader@techtarget.com

TechTarget
275 Grove Street, Newton, MA 02466
www.techtarget.com

About TechTarget: TechTarget publishes media for information technology professionals. More than 100 focused websites enable quick access to a deep store of news, advice and analysis about the technologies, products and processes crucial to your job. Our live and virtual events give you direct access to independent expert commentary and advice. At IT Knowledge Exchange, our social community, you can get advice and share solutions with peers and experts.