WHITE PAPER

MITIGATING RISK IN THE CLOUD

Effective cloud computing requires that organizations know the risks and take the appropriate steps to address them.

Executive Summary

Many organizations have adopted cloud computing solutions, but often this adoption has not involved full-fledged risk management methodologies. Instead, cloud providers are trusted to take care of security. Or they simply activate security controls that are widely considered best practices for the cloud.

This can leave entities without an understanding of the risks they are accepting. It can also increase the likelihood that adverse events will disrupt cloud operations.

But this situation isn't inescapable. Organizations can address the risks inherent in cloud computing. An excellent first step is to review the categories of risk most relevant to cloud technologies. Next, IT managers can take actionable risk management steps and implement technical, operational and management controls.

Table of Contents

SHARE THIS WHITE PAPER

The Situation

A wide variety of organizations have adopted cloud computing. It offers numerous benefits, including flexibility, scalability and rapid provisioning. However, some IT shops, even those that have adopted some cloud technologies, are reluctant to increase their cloud adoption.

For many organizations, security concerns dampen IT leaders' enthusiasm for cloud solutions. Fortunately, an increased understanding of cloud security characteristics and the maturation of cloud security products and services have mitigated these concerns.

While security is an important consideration for those looking to deploy cloud technologies, it is far from the only one. IT leaders most also be concerned about privacy, availability and reliability (including disaster recovery and business continuity), scalability, compatibility and standardization, as well as commercial viability.

Cloud solutions have evolved significantly in recent years. As these technologies have matured, many enterprises have addressed their concerns. But legitimate issues remain.

To deal with these issues, IT leaders should consider a change in their approach. Rather than addressing cloud risk by deploying a sequence of standard best-practice controls, IT chiefs should perform a full-fledged risk assessment and make conscious decisions to handle the residual risk that existing controls do not eliminate.

They need to see risk management is a core business activity, regardless of where IT infrastructure is located – either on-premises data center or in the cloud. The well-run organization maximizes risk analysis, avoiding toxic risks while accepting manageable ones and thereby maximizing operations.

How Risky Is the Cloud?

Security is a clear example of cloud risk. In the early days of cloud computing, IT leaders had serious concerns about the security of cloud computing itself. For example, many were worried that vulnerabilities in cloud-based virtualization software would be easily exploited to bypass the protection and isolation that virtualization provides. This would grant access to sensitive data, such as personally identifiable information (PII), financial information or medical records.

However, these potential weaknesses of virtualization software simply haven't affected enterprises that have deployed cloud solutions. Time after time, studies have shown that exploitation of virtualization is not a major factor in successful breaches.

For example, the Verizon *2014 Data Breach Investigations Report* details many types of common attacks based on the percentage of successful compromises caused by each attack type. However, virtualization exploitation isn't mentioned among them.

As organizations have grown more comfortable with cloud security, they have shed their reluctance to use cloud solutions. A recent IDG survey indicated that 73 percent of technology decision-makers felt "very or somewhat confident" in the security of information assets in cloud environments.

Risk Mitigation in the Cloud

Efforts to address risk in the cloud should be based on standard risk management methodologies. Although the details of particular methodologies differ, each has the same core components:

- To determine the organization's needs (such as key security requirements)
- To assess risk
- To select and implement controls to mitigate those risks
- To assess the controls and identify any shortcomings
- To monitor the controls to ensure that they are functioning effectively

Following a risk management methodology almost always provides a better, more cost-effective solution than simply implementing the best practice controls that conventional wisdom dictates.

Each cloud implementation faces a unique combination of risks. A "one-size-fits-all" solution makes no sense when each organization has its own risk profile to handle.

This is not to say that best practice controls are not necessary. In fact, they are often the foundation of mitigating risk. However, best practice controls often set a minimum benchmark for risk mitigation, and additional controls, as well as other enhancements, are often necessary to achieve the desired level of risk mitigation.

The best approach to mitigate risks in the cloud is to take an information-centric approach to risk management in general and risk mitigation in particular. For many years, security experts focused on safeguarding systems (for example, securing the operating system and applications).

But in recent years, experts have shifted to a more information-centric view, where the focus is on safeguarding information. The underlying system still needs to be safeguarded. The challenge for security administrators is to protect the information itself, which requires a strategy to be tailored to each situation and environment.

33% of cloud services were vulnerable to the Heartbleed bug when it was discovered, which put user data, passwords and private keys at risk.

SOURCE: Skyhigh Networks, *Cloud Adoption and Risk Report*, 2014

Functional Areas for Risk Mitigation

The Booz & Company report, *Eyes Wide Open: Mitigating Risk in Cloud Computing*, categorizes cloud risk mitigation by several functional areas:

- **Security and privacy** – Security is a top concern for cloud deployments. Cloud security demands that the confidentiality and integrity of data stored and processed within the cloud, as well as the data transferred to and from the cloud, be protected. Privacy concerns are closely linked to security, with the focus of privacy falling squarely on data that contains or is linked to personally identifiable information.

- **Availability and reliability** – The enterprise also must ensure that cloud services (such as applications) and data are accessible by authorized users at all times. For many organizations, any loss of availability or reliability has a direct impact on the bottom line, such as lost business opportunities or lost productivity.

  Disaster recovery and business continuity planning play a major role in availability and reliability considerations in the cloud. Some cloud users erroneously believe that "cloud" equals "reliable," but in reality, clouds do have failures from time to time. Organizations with concerns about availability and reliability for their services and data must conduct disaster recovery and business continuity planning and implement the plans they establish. These plans can include steps such as providing redundancy by duplicating cloud resources in a geographically and logically separate cloud.

- **Scalability** – Not every application is designed to work optimally in a cloud environment. Although clouds themselves offer a high level of scalability, individual applications may not. For example, an application may perform extensive data transfers for all transactions, causing a performance bottleneck and incurring high service charges.

  Achieving scalability within the cloud may necessitate redesigning and rewriting portions of in-house applications, or acquiring new versions of commercial applications, to eliminate or reduce the behavior that causes scalability concerns. Another aspect of cloud scalability is being prepared for immediate provisioning of resources as needed, as well as rapid deprovisioning when resources are no longer needed. In general, reducing scalability risks can improve performance and reduce costs for cloud implementations.

- **Compatibility and standardization** – At one time, organizations held significant, well-founded concerns about vendor lock-in with cloud deployments. For example, an organization might have to write an application to interact with a particular cloud provider's unique application programming interfaces (APIs). Should that organization want to move its application to a different cloud in the future, it would have to rewrite those portions of the application to use a different cloud provider's unique API.

  Fortunately, complaints from customers have driven many cloud providers to drop their use of unique APIs. Still, IT shops are cautioned to avoid clouds that require extensive application customization. Instead, they should seek out clouds that take a more standardized approach to interoperability.

- **Commercial viability** – Enterprises also must address the risk they face in achieving a return on their investment in cloud resources. Many users believe that cloud service invariably provides great cost savings for organizations, but in reality, cloud solutions can be more expensive than standard technologies under some circumstances.

  Cloud resources must be managed like every other IT resource, especially if cloud provisioning is not centrally managed and controlled, allowing users from throughout the enterprise to acquire cloud resources on demand. Some applications may not be designed with cloud infrastructures in mind, so their behavior may consume significant cloud resources and thus be correspondingly costly.

Types of Risk in the Cloud

As IT shops consider the cloud, they must address a variety of risks.

Policy and Organizational Risks – In addition to the risk of vendor lock-in through the use of proprietary interfaces, organizations face challenges such as complying with various regulations, even though applications and data have been migrated from a traditional data center to a cloud environment.

Cloud Service Failure – IT shops also must deal with the risk of a cloud service failure and be prepared to mitigate these risks (for example, through disaster recovery and business continuity planning). A final type of risk to consider is the loss of business reputation. For example, a cloud security breach could result in damage to the reputation of organizations using that cloud.

Technical Risks – Organizations that deploy cloud solutions also face technical risks such as resource exhaustion, which can occur when not managing cloud resources effectively and not preparing to automatically provision additional resources when needed. Resource exhaustion can cause degradation of services and, in some cases, a failure to provide services at all.

Interception of Data – Another technical risk is the interception of data in transit to or from a cloud. This is easily remedied by ensuring that all data transmissions are strongly encrypted and that the endpoints for any data transmission are strongly authenticated to ensure that they are legitimate.

Distributed Denial-of-Service Attacks – DDoS attacks represent another technical risk that must be addressed. Although the cloud provider and their Internet service providers are typically responsible for dealing with DDoS attacks, customers should discuss DDoS with cloud providers to ensure that the proper controls are in place to mitigate a DDoS attack rapidly should it occur. Similarly, service availability is a category of technical risk that must be addressed through scalability, availability and reliability facets.

Legal Risks – Organizations must consider the legal risks of the cloud. A critical risk that must be confronted is maintaining compliance with regulations such as the Health Insurance Portability and Accountability Act (HIPAA) or the Payment Card Industry Data Security Standard (PCI DSS). Many organizations find it difficult or even impossible to achieve compliance while using cloud architecture. IT leaders should thoroughly research any applicable regulations before planning a cloud migration.

Changes in Jurisdiction – Organizations may face varying requirements if different cloud servers are located in different geographic locations, each of which has its own set of laws (including, federal, state and local). In some cases, it may be necessary to limit the geographic locations in which cloud workloads can be placed to avoid the legal requirements of certain jurisdictions.

Data Privacy – This also poses a legal risk. For example, some cloud providers state in their contracts that they have the right to monitor customer data in the cloud and harvest information from it, then sell this information to third parties.

Actionable Risk Mitigation Steps

Organizations can pursue risk management (and risk mitigation) in many frameworks, with differences in the details but the same underlying principles. Risk mitigation typically is incorporated into the broader risk management processes. These steps can be extracted from the risk management process and considered as their own risk mitigation process.

STEP 1: Examine the business context. This refers to assessing the types of services and data handled,(for example, personnel records, credit card numbers or prescriptions), then considering the threats against these services and data. IT leaders face numerous questions when analyzing these threats for each service and data set, such as:

- What individuals or groups would have the greatest interest in obtaining unauthorized access to the service or data?
- Why would these parties want to obtain access to the service or data? What would they do with the service or data once they gained access to it? For example, might they commit identity theft with stolen information or reuse intellectual property?
- How likely is it that a party seeking unauthorized access (such as a well-funded competitor or a disgruntled ex-employee) would succeed in compromising the service or data?

This step includes implementing the basic management and operational security controls for services and data. These controls include security policies and associated procedures, service-level agreements (SLAs), basic audit controls and other forms of governance.

STEP 2: Review application security. Assessing the security of applications is a critical step in risk mitigation. It's important to determine what features an application offers for mitigating risk. IT managers also should consider how robust these features are. For example, if an application encrypts data at rest to protect its confidentiality, what encryption algorithm and key length are used, and how strong are the algorithm and key combination?

Security Considerations for Custom Applications

Most risk mitigation steps are based on the assumption that an application is an existing commercial product. However, IT managers often find much greater opportunities for mitigating risk when an application is being developed specifically for the organization. In these cases, risk management should be integrated throughout the application's development lifecycle, starting with the identification of risk-related requirements during the design phase.

This allows risks to be identified and quantified before the application is even created, giving developers a much greater opportunity to mitigate uncertainty through the design of the application. This is generally much more cost-effective than trying to mitigate the same risks after development of the application has been completed. The earlier in the process that risk management can be incorporated the better.

If an application is not designed to meet strong security requirements, it may need to be retrofitted or overlaid with additional security controls, such as a virtual private network (VPN) tunnel to "wrap" unsecured network protocols transiting unprotected networks. Further, IT staff may use the features of an operating system to mitigate application risks, such as having the OS perform backups of application data to ensure its availability.

STEP 3: Construct a data-centric governance plan. Data governance involves the management of data throughout an enterprise, such as performing backups, archiving old data and handling e-discovery requests. A 2013 survey, conducted by Rand Secure Data, determined that nearly half of all organizations didn't have a data governance policy. This can increase the chances that data will be misplaced, making it more susceptible to compromise.

It is important for organizations, particularly those using the cloud, to know where their data is stored and to limit access to the data and the virtual machines on which it resides to authorized individuals only. Technologies such as data loss prevention (DLP) can help to prevent the unwanted proliferation of sensitive data to unauthorized locations.

STEP 4: Test and retest. After a data-centric governance plan has been implemented, IT staff should periodically test it. This includes actions such as verifying the integrity of backups, ensuring that archived data is stored securely and making sure that unnecessary data is destroyed properly.

Further, authorized users must be able to find information on demand, such as that needed to respond to e-discovery requests. Testing should be performed regularly to ensure that these controls function as intended.

Control Options for the Cloud

Organizations have many ways to select security controls for the cloud. The *Cloud Security Alliance Cloud Controls Matrix* (CSA CCM), currently in version 3.0, defines cloud control domains and control identifiers.

It maps each of them to controls from several other security control catalogs, such as the *National Institute of Standards and Technology Special Publication 800-53*, the *Control Objectives for Information and related Technology* (CobiT), HIPAA and PCI DSS. The CSA CCM can be thought of as a meta-catalog for cloud security controls.

The control domains for CSA CCM version 3.0 can be grouped by the type of controls they generally contain: technical, operational or management. Each control domain should be considered based on how it addresses current risks as well as likely future risks.

Technical Control Options

Application and interface security: When it comes to cloud technologies, application security is often overlooked because it largely can't be applied after the fact. It must be incorporated throughout the lifecycle of the application, including its initial planning and design.

Enterprises that try to apply security after an application has been deployed often find it prohibitively expensive to do so. IT leaders who are thinking about migrating their applications to the cloud should already be addressing application and interface security concerns.

Technical, Operational and Management Controls

The National Institute of Standards and Technology developed the concept of having three categories of controls — technical, operational and management. In early versions of *NIST Special Publication 800-53*, these categories were used to distinguish families of controls.

However, the latest version of SP 800-53, Revision 4, no longer uses these distinctions, likely because most of the families include controls from multiple categories. So while a family may fall within a primary category, other controls within that family may fall into a different category. This could lead someone interested in technical controls to overlook the management and operational families, which may also contain technical controls.

Data security and information lifecycle management: This broad control domain covers the protection of data. It includes sanitizing stored data, a goal that many enterprises achieve by encrypting stored data and protecting the secret key from discovery.

Another example involves protecting ecommerce data on public networks. This requires not only confidentiality and integrity protection through the use cryptography, but also nonrepudiation, which requires the use of strong authentication techniques such as multifactor authentication.

Deployment of MFA is an effective tactic to thwart identity-based attacks, such as password theft. But it can be costly and can hamper usability, so organizations considering it for cloud usage should carefully evaluate its effects, both positive and negative.

Data security can also be achieved by the use of DLP solutions. Organizations can deploy host-based and network-based DLP software within the cloud and fine-tune it to stop the unwanted flow of sensitive data.

Encryption and key management: Key management is one of the most challenging aspects of security in any environment, and it can be even more difficult in a cloud implementation. Many compromises involving the use of encryption can be traced back to poor key management practices.

In the cloud, a common mistake is to store encryption keys in the cloud alongside the data that they protect. Should cyberattackers compromise the cloud's security, or should a cloud administrator act maliciously, the keys could be used to decrypt sensitive data stored in the cloud. To thwart this, an enterprise should never store encryption keys in the same place as the data that they protect.

Policies and procedures play an essential role when it comes to key management. For example, keys must be rotated on a regular basis, meaning that they are replaced periodically to reduce the impact of a compromised key as well as the likelihood of success for long-term, brute-force attacks.

Identity and access management: The identity and access management control domain has a variety of controls related to authenticating users, restricting access to only data for which the user is authorized (often referred to as least privilege) and auditing these authentication and access-control decisions.

The ability to perform such audits is especially important for cloud computing. In some cloud environments, enterprises find it challenging to get reliable audit data and to prevent audit data from inadvertently being accessed by other cloud customers or the cloud service provider itself.

One possible solution to work around this problem is to have each application perform its own auditing. This would take the place of relying on the underlying operating systems to perform auditing on behalf of the applications.

Infrastructure and virtualization security: Virtualization security is a major component of cloud security. This is because of cloud's heavy dependence on operating system and hardware virtualization technologies. Virtualization security covers a wide variety of topics, ranging from ensuring the integrity of virtual machine images to hardening the operating systems within virtual machine images and restricting access to hypervisor management functions.

Another critically important aspect of infrastructure and virtualization security is ensuring that a cloud deployment has sufficient resources. A lack of resources can cause the degradation or outright failure of services.

Interoperability and portability: One interoperability control requires the use of open and published APIs, which also helps to prevent cloud vendor lock-in. Other controls involve using standard network protocols, virtualization platforms and virtual machine image formats for cloud communication, processing and storage.

Mobile security: This domain has many controls related to bring-your-own-device (BYOD) security and other elements of securing mobile devices themselves, such as establishing password policies for device authentication. But these controls are not particularly relevant to cloud security.

Supply chain management: Several controls in the supply chain management domain are directly related to establishing supply chain agreements and performing supply chain management reviews of partner organizations. However, this domain is broader, including some controls such as validating inputs received from cloud-based supply chain partners and sharing security incident reporting information with supply chain partners and others.

Operational and Management Control Options

Audit assurance and compliance: One control for audit assurance and compliance — maintaining a current inventory of all legal, statutory and regulatory compliance obligations involving an organization's data or infrastructure (including virtual infrastructure) — is of particular interest for cloud environments. The control specifically calls out geographic location as one of the factors to be considered, underscoring the complex issues that public clouds can introduce when data is stored or processed in different legal jurisdictions.

Business continuity management and operational resilience: This domain includes controls that relate to performing business continuity testing in production cloud environments, which can present significant hazards. Because clouds are intentionally designed to be reliable and have a great deal of redundancy, many IT managers find it surprisingly tricky to conduct true business continuity testing in production.

Other controls in this domain involve typical data center controls, such as providing physical security and documenting basic system and security administration tasks and features. The domain also includes typical business continuity controls, such as business continuity policy and procedure creation.

Change control and configuration management: Change control can be tricky in a dynamic cloud environment, because it includes changes to underlying infrastructure components. In a cloud environment, such components may change frequently. IT leaders should understand and accept this. They also must mitigate threats above the infrastructure level so that infrastructure changes do not adversely affect cloud data and application security.

Data center security: This domain includes a variety of controls related to the basics of data center security, such as establishing physical security perimeters and establishing policies and procedures related to physical security within the data center. IT managers involved in cloud environments should pay particular attention to controls related to "ingress and egress to secure areas," which restrict who can access secured systems.

Most cloud environments generally do not provide dedicated hosts for particular customers, and in most situations customers have no need to physically access hosts – all access should be virtual. IT managers should know the physical security policies and ensure that unauthorized parties cannot physically access the organization's resources.

Governance and risk management: Risk management and governance are often overlooked when it comes to cloud technologies. This domain has a wide range of controls that involve performing periodic risk assessments as well as engaging in efforts to mitigate risk.

Shadow IT

Shadow IT describes IT solutions used without the approval or knowledge of an organization's IT department. All too often, cloud solutions become shadow IT solutions, with individuals, departments or other groups within an organization making their own arrangements for cloud-based hosting of data and applications.

Many users find it surprisingly easy to make such arrangements and to gain access to enterprise applications — sometimes in a matter of minutes. This ease can tempt users to circumvent the organization's IT staff and procedural controls and acquire their own cloud-based solutions.

The major problem with this scenario is that risk management professionals are typically not involved in the acquisition, deployment and maintenance of these solutions. Thus, these risks are not identified, assessed and mitigated using a standard methodology, and the organization is essentially assuming these risks without knowledge of doing so.

Specifically, five categories of risks often arise including:

1. Data security risks
2. Company name and brand risks
3. Compliance risks
4. Business continuity risks
5. Financial risks – spiraling costs

Human resources: Most of the controls in this domain are related to personnel, such as performing background checks and having training and awareness programs for all users. A few of the controls relate specifically to the use of mobile devices in cloud environments and the concerns about them being used in accordance with the organization's policies. This often boils down to being concerned about unauthorized data transfers and storage. Thus, the use of DLP software within the cloud may be warranted to reduce risk related to mobile device use.

Security incident management, e-discovery and cloud forensics: Many entities that have implemented a public cloud solution may find that this complicates their efforts to perform e-discovery and forensics activities. Different portions of a single cloud may reside in different legal jurisdictions, and data and applications may move freely from place to place for optimization purposes.

When an incident occurs, the data and applications may have resided in a completely different jurisdiction than where it will sit in the future. In some cases, different sets of data and applications may even be split among jurisdictions. E-discovery and forensics may involve exhaustively checking all the places where the data and applications may have resided for information such as copies of the data or records of data and application usage.

Threat and vulnerability management: Only a few controls are relevant to the threat and vulnerability management domain. They involve using anti-virus or other anti-malware software; detecting software flaw and security configuration vulnerabilities and remediating them; and stopping unauthorized mobile code from running.

Organizations may deploy special versions of anti-virus software, intrusion detection systems and other controls for stopping malware, malicious mobile code and other attacks from executing on virtualized cloud systems. Patch and vulnerability management can be tricky, because cloud workloads can be migrated from operating system to operating system, so the vulnerabilities may change from moment to moment.

Cloud Roadmap: Recommendations

Key considerations for cloud:

- Launch first with services that don't pose unacceptable risks to the organization, aren't business critical and where complexity of implementation is low – i.e., storage, office productivity.
- Tap a cross-section of your stakeholders for a thoughtful analysis of benefits and costs, and then select a cloud strategy consistent with an IT service fulfillment model.
- Leverage users' consumer experience: Familiarity will maximize success of cloud adoption.

Source: *CDW 2013 State of the Cloud Report*

CDW: A Cloud Partner That Gets Security

Keeping pace with cloud computing security isn't a luxury, it's a necessity. As a leading provider of technology solutions for business, government, education and healthcare, CDW can get you to the cloud, integrate your new solution seamlessly with existing solutions and even manage your new cloud solution day to day, all while putting plans in place to enhance security and mitigate identified risks.

CDW provides the risk management methodologies to secure data, maximize continuity of operations and put disaster recovery plans in place. A risk assessment performed by CDW, or under our guidance, can help reveal vulnerabilities and prioritize their handling by risk, cost and impact.

Our cloud client executives use the power of the cloud to boost productivity, regulate IT costs, enhance flexibility and drive innovation. And we offer a cloud portfolio that includes more than 200 high-profile products spanning 36 categories.

Let us help you with the entire cloud-computing lifecycle, from selecting which cloud models are best for your organization to simplifying the challenging process of moving applications and data from your existing infrastructure to the cloud.

The CDW approach to customer service includes:

- An initial discovery session to understand your goals, requirements and budget
- An assessment review of your existing environment and definition of project requirements
- Detailed manufacturer evaluations, recommendations, future environment design and proof of concept
- Procurement, configuration and deployment of a cloud solution
- Telephone support, as well as product lifecycle support

To learn more about CDW's cloud computing solutions, contact your CDW account manager, call 800.800.4239 or visit CDW.com/cloud

SHARE THIS WHITE PAPER

The information is provided for informational purposes. It is believed to be accurate but could contain errors. CDW does not intend to make any warranties, express or implied, about the products, services, or information that is discussed. CDW®, CDW·G® and The Right Technology. Right Away® are registered trademarks of CDW LLC. PEOPLE WHO GET IT™ is a trademark of CDW LLC.

Together we strive for perfection. ISO 9001:2000 certified

PEOPLE WHO GET IT™