CAPINTECH

Security in a Cloud Computing Environment

By Allison Davis, Partner

Cloud computing can offer a number of benefits to nonprofit organizations, including cost savings and flexibility. With the move to a remote workforce, most organizations are now using the cloud in some manner.

If your organization uses a cloud computing environment, it's important to understand the inherent security risks and take steps to reduce them.

A Look at the Risks

The Federal Financial Institutions Examination Council (FFIEC) recently released a statement on security in a cloud computing environment that serves as a helpful resource. The FFIEC consists of five governing regulators: the Federal Reserve, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau.

While these members work together to provide guidance for federally supervised financial institutions, the technology-related guidance they release is often relevant to all organizations. And this statement is no different. All organizations — regardless of industry, size, or complexity — can benefit from the takeaways from this statement, which we'll discuss here.

What constitutes a cloud environment?

Organizations can implement cloud environments in various ways to fit their needs. The way certain risks are mitigated and the level of control you may have evolves with the environment. That's why it's important to start by understanding the type of cloud solution your organization is using so you can manage and secure it properly.

The National Institute of Standards and Technology (NIST) identifies three types of cloud environments: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

	SaaS	PaaS	IaaS
Overview	An application is hosted on the vendor's infrastructure and used by the organization	Applications developed or acquired by the organization are run on the vendor-managed infrastructure	Software and applications are deployed on the vendor's infrastructure, but the organization manages the majority of the infrastructure components
Example	QuickBooks Online	QuickBooks runs on a server that is hosted and managed by a vendor	QuickBooks runs on the client's server hosted at a data center where the client leases equipment

> Failure to understand the type of cloud environment your organization is using and your resulting roles and responsibilities may result in increased risk, failures, and potential for breaches.

An organization's requirements and responsibilities become more expansive as it migrates from SaaS environments to IaaS environments. Typically, more technical internal staff is required to support PaaS and IaaS environments.

Organization Requirements	SaaS	PaaS	IaaS
Management of application settings, user access, identity management, and risk management of the cloud service provider relationship	√	√	√
Provisioning and configuration of infrastructure resources; development, deployment, and administration of applications; establishment of controls for operations, applications, operating systems, data, and data storage		√	√
Management of system software, operating systems, and applications			√

The inverse is true for vendor requirements. Vendors supporting SaaS often maintain more responsibilities as they move from IaaS environments to PaaS and SaaS environments.

Vendor Requirements	SaaS	PaaS	IaaS
Implementation of physical security of hardware and network infrastructure, environmental controls (e.g., heating, cooling, and fire suppression), data communications, and management of hypervisors (software, firmware, or hardware that creates and runs virtual machines)	√	√	√
Management of underlying infrastructure and platform (network, servers, operating systems, storage, etc.)	√	√	
Application development and infrastructure maintenance	√		

Most organizations have some form of SaaS in use. However, PaaS and IaaS environments are becoming increasingly common with the rise in the use of data center services such as Amazon Web Services and Microsoft Azure. It's important to note that these responsibilities can still be unique to the implementation and your organization should review contracts in detail to ensure management understands your organization's level of responsibility.

Who bears the responsibility?

One of the most important takeaways from the FFIEC statement is the reiteration of an organization's responsibility when it comes to cloud computing relationships. The statement notes that "management should not assume that effective security and resilience contracts exist simply because the technology systems are operating in a cloud computing environment."

Many organizations believe that when they outsource portions of their network, systems, applications, and infrastructure they no longer bear the responsibility for ensuring the confidentiality, integrity, privacy, and availability of those systems and the data within.

However, your organization is ultimately responsible for the security of your systems and data and for understanding and mitigating the potential risks that arise with the relationship — regardless of the type of environment implemented. Failure to understand the type of cloud environment your organization is using and your resulting roles and responsibilities may result in increased risk, failures, and potential for breaches.

How do we mitigate risks?

The FFIEC guidance outlines numerous risk management controls, which become applicable depending on the increasing level of responsibility your organization has as it migrates from SaaS to IaaS platforms. Implementing controls is not "one size fits all," however. You should use adequate procedures to prevent, detect, identify, and respond to issues associated with your cloud environment.

Here are some of the most relevant controls necessary, regardless of the type of cloud environment you are using:

- **Establish proper governance** so cloud computing strategies are implemented into your organization's overall strategic planning and risk management processes.
- **Create procedures for initial due diligence and ongoing monitoring of your providers**. Security-related controls are relevant in all situations, whether those controls are electronic, physical, or both. The controls should be vetted to ensure they are adequate to mitigate relevant risks. In addition, business continuity and disaster recovery may become critical and it's important for you to understand what your vendor is doing to ensure the availability of your data.
- **Evaluate contracts thoroughly** to ensure they clearly identify the roles and responsibilities of your organization and your vendor. Additional stipulations related to confidentiality, information security, subcontractor use, data ownership, data location, and breach response may also become relevant, depending on the situation.
- **Inventory the assets in the cloud environment.** For SaaS environments, these assets may just be the data that is stored; however, you may need to account for additional assets as you move into PaaS and IaaS environments. It is critical for you to know what is maintained at these cloud providers so you can ensure it is properly secured and managed.
- **Establish strong access management and security controls to your applications**. For all environments, you manage who has access to the system and infrastructure. In a SaaS environment, it likely just relates to managing access and rights to the application itself. However, when you move to the other platforms, you have other layers of access to manage (e.g., access to the servers or network equipment). In addition, regardless of the platform you usually retain the rights to configure password, lockout, inactivity timeouts, and multi-factor authentication (MFA) settings. Conservative settings can reduce the risk of unauthorized access to your applications.
- **Incorporate your cloud solutions into your business continuity, disaster recovery, and incident response plans.** Just because your system or infrastructure is in the cloud does not mean that the chance for an incident or disaster goes away. What if the vendor's hosting location goes down for an extended period due to ransomware, a monumental national disaster (e.g., Hurricanes Katrina and Sandy), or a cyberattack? How long could you reasonably operate without your cloud environment — eight hours, a few days, several weeks? You could be significantly affected. Therefore, planning proactively for cloud computing challenges and this type of downtime and for timely response to an issue can increase the likelihood of continuance of operations and proper handling of the incident.
- **Train your end users**. End users can often be your weakest link. If your end users still fall for phishing attempts, install malware, or disclose sensitive information, it can negate the many layers of controls you have implemented. Ensure all your end users are adequately trained on current cybersecurity threats and what they can do to mitigate the risks and reduce the impact.

Finally, as you move to PaaS and IaaS environments, ensure you know your responsibilities related to general security practices of the infrastructure. Anti-malware and patch management, system configuration, data encryption, data backups and configurations of critical infrastructure, vulnerability management, and incident identification and response may be your responsibility.

Even when the systems and infrastructure are not hosted at your location, improper management by you or your vendor could result in a compromise to your hosted systems and data. Keep in mind that this may also apply to employees' home office environments, as cloud systems are often used in remote work.

Please contact us at cybersecurity@capincrouse.com with questions or for help assessing the security of your organization's cloud computing environment.

About the Author

Allison Davis, Partner
CapinTech
adavis@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor and senior manager, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinTech

Capin Technology, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintechnology.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.