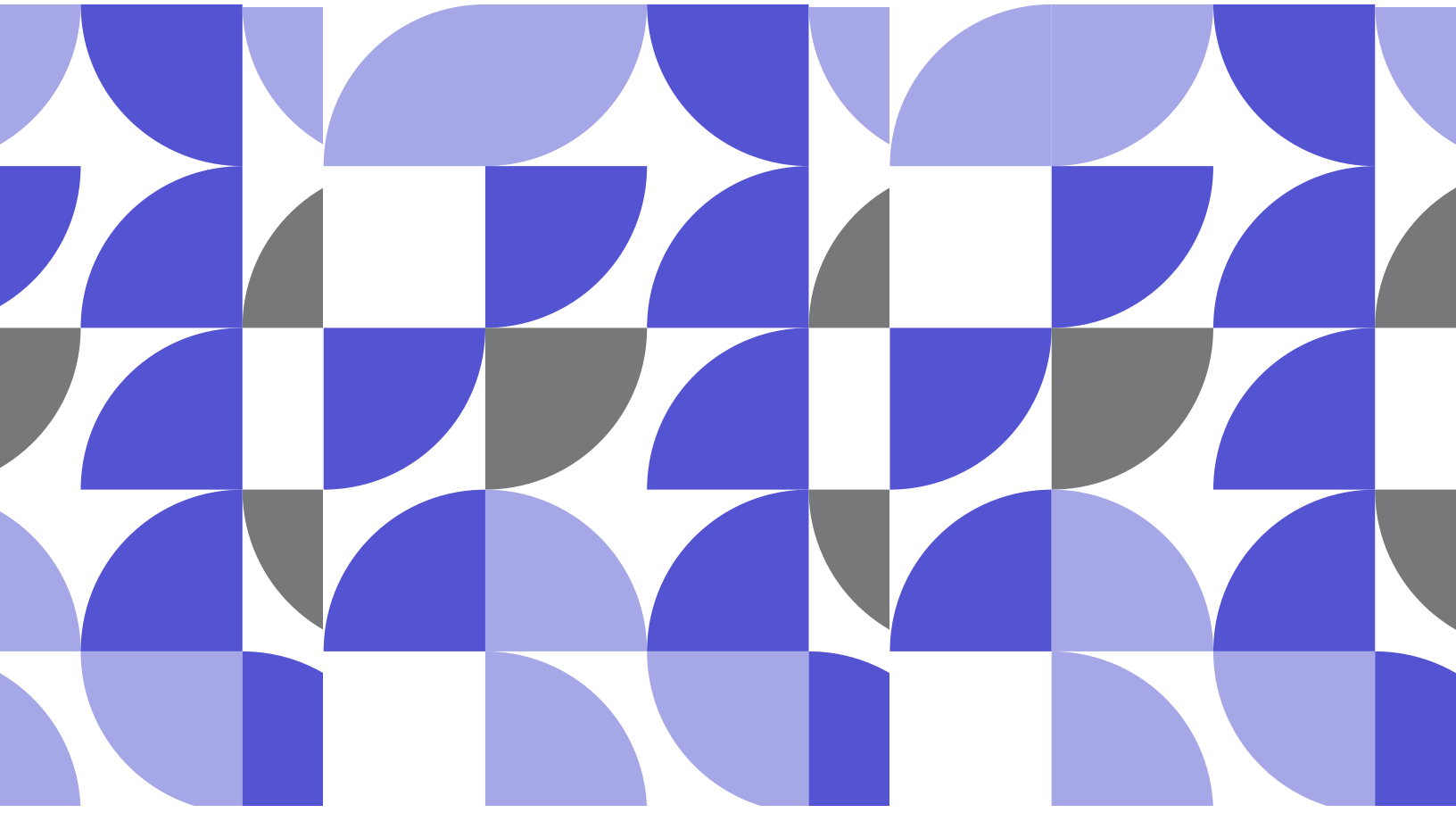
ARE YOU SHARING THE RESPONSIBILITY?

Key Practices for SaaS Application End Users Ultimate Protection



October 2024

CSaaS SIG
An IT ISAC Community

PRODUCT OF THE
IT-ISAC Critical SaaS Special Interest Group (CSaaS SIG)

CONTRIBUTORS

David B. Cross
Deepen Desai
Jeffrey DiMuro
James Dolph
Ashlyn Jimenez
Chris Niggel
Kaitlyn Palatucci
Dhaval Parekh
Akshay Shetty

INFORMATION TECHNOLOGY - INFORMATION SHARING AND ANALYSIS CENTER (IT-ISAC)

Founded in 2000, the Information Technology - Information Sharing and Analysis Center (IT-ISAC) is a non-profit organization that augments member companies' internal capabilities by providing them access to curated cyber threat analysis, an intelligence management platform, and a trusted forum to engage with senior analysts from peer companies.

CRITICAL SaaS SPECIAL INTEREST GROUP (CSaaS SIG)

The Critical SaaS Special Interest Group (CSaaS SIG) is part of the IT-ISAC and serves as a forum for CSaaS companies to collaborate on a collective defense strategy to improve the security and operational resiliency of their services and share intelligence information with the industry. It enables companies who are essential to the internet to share cyber threat intelligence and effective security practices. The SIG holds a weekly analysts meeting and is designed for security managers, analysts, and IT executives from Critical SaaS companies.

INTRODUCTION

When it comes to security, clarity is key - ambiguity only increases risk. However, determining whether it is the customer or provider who is responsible for what can be a confusing topic in terms of managing software applications, especially in the context of cloud-hosted services. There is often uncertainty over where the line is drawn between the provider's role in administering security and the customer's duty in managing and securing their data. The assumption may persist that critical SaaS (CSaaS) providers bear the brunt of the responsibility when it comes to all security measures; from identity management to data security and incident response – but this is simply not the case in many instances, and such assumptions can lead to overall confusion, vulnerabilities, and loss of customer data.

Enter the **Shared Responsibility Model**: a framework that helps delineate exactly who does what and when in these provider/customer partnerships. The Shared Responsibility Model places the onus for developing and maintaining security and compliance measures on both the CSaaS provider and the customer and helps establish who needs to keep track of what – including maintaining security components and application features. Each entity is responsible for fulfilling its designated roles and must clearly understand "who does what." Both groups should actively communicate and collaborate to ensure all aspects of security are effectively managed. Some roles are split between the customer and the provider; others are solely the responsibility of one or the other.

Understanding the Shared Responsibility Model is imperative for effectively securing your information in a critical SaaS (CSaaS) environment. As you navigate implementation, you will want to be sure you understand what your team's security role is in its entirety to close any possible gaps. In a general sense, providers are typically in charge of monitoring and responding to security threats pertaining to the cloud itself, as well as any related infrastructure; meanwhile, the customer must manage the security of their own stored data and other information. However, these are broad strokes – talking directly with your provider about specifics is the best way to know where your responsibility lies, and that requires asking the right questions.

The following paper highlights the key security practices that should be outlined within a Shared Responsibility Model for a cloud-specific hosted application environment and provides a guideline to follow when discussing security responsibilities with your CSaaS provider. Written in collaboration by the Information Technology - Information Sharing and Analysis Center's CSaaS Special Interest Group (SIG), this paper aims to help customers begin a dialogue with their providers so that they may better understand their role in the CSaaS security environment more thoroughly, dispel misconceptions and conclusion, and foster a better and more secure relationship between provider and customer.

1 IDENTITY ACCESS MANAGEMENT

Protection starts with identity and access management (IAM), two crucial elements that ensure the right individuals have the appropriate access at the right times and for the right reasons. Proper IAM provides a strong preliminary layer of protection for an organization.

Identity management focuses on identifying and managing users, while access management focuses on controlling and monitoring their access. The Identity Defined Security Alliance (IDSA) noted in their 2023 Trends in Securing Digital Identities report that identity-related incidents are rising, with 90% of organizations reporting an incident within the last 12 months. This shows that attackers aren't just breaking in but logging in – cementing how important it is for customers to understand which IAM controls they are responsible for when implementing new technology and services.

Authentication Mechanisms - Mandatory MFA

In an ideal environment, new applications would ensure all users are protected by mandatory multi-factor authentication (MFA) that is hardware-backed and phishing-resistant. For increased protection, following Fast IDentity Online or FIDO is recommended. FIDO is a set of standards that use public key cryptography, unique to the system they are used on, and a phishing-resilient option for protecting your accounts and information.

New applications are not always ideal environments, so ask yourself or your provider the following questions to ensure maximum security:

ASK THESE ?

- Who is responsible for setting up authentication in your tenancy/subscription?
- How is user enrollment in MFA implemented?
- Can you enable re-authentication or increased authentication when anomalies occur?
- What MFA methods do you support?
- Are you able to deploy and enforce MFA for administrators at a minimum?

Zero Trust Architecture

Zero trust models are an extension of the concept of least privilege. Users should have access to the data they need to perform their tasks, but no more. Operating under a zero trust architecture (ZTA) maintains that users should not be trusted by default. Companies can enhance security by ensuring access requests are authenticated, authorized, and available. Through ZTA, with continuous verification of access requests, there is a reduction in the risk of unauthorized users/access and movement within the network.

Your CSaaS provider protects the underlying infrastructure, ensures security standards are met, and complies with product regulatory requirements for their applications. As the consumer, asking the following questions around ZTA are important:

ASK THESE ?

- Does the new application integrate with your centralized identity management system?
- What monitoring tools, services, or analytics are offered by the vendor?
- What type of access does the application support?
  - Conditional access
  - Location-aware based access
  - Device specific access
- Does the application support the Continuous Access Evaluation Protocol, the Shared Signals Framework, or the new Interoperability Profiling for Secure Identity in the Enterprise (IPSIE) standard?

Role-Based Access

Role-based access control (RBAC) regulates user access established by their roles and needs to perform their jobs. For example, an organization can have identified roles such as “Administrator”, “Manager”, or “Support” – each role will determine the user's permissions and access rights to resources, applications, and more. In larger companies, RBAC helps to assign and modify roles easily instead of having to configure the permissions of each individual user, saving time and resources. Additionally, through RBAC, companies can enforce the principle of least privilege (PoLP), allowing users to access only what is necessary; this enhances security and simplifies user permissions management.

In larger companies, RBAC helps to assign and modify roles easily instead of having to configure the permissions of each individual user, saving time and resources. Additionally, through RBAC, companies can enforce the principle of least privilege (PoLP), allowing users to access only what is necessary; this enhances security and simplifies user permissions management.

RBAC is not a one-size-fits-all approach, and consumers are responsible for managing their roles and access in most cases. To make sure that is possible, consumers should consider asking the following:

ASK THESE ?

- How is RBAC implemented and monitored within the application?
- Is the RBAC integrated into the organization’s HR applications to terminate access when employment has ended?
- Will this new application give you the depth of control you need to implement your organization’s policies?
- Can you define custom roles and permissions as needed?
  - If yes, is there an extra cost?
  - Are there limitations?
- If applicable, can you define and enforce segregation of duties based on roles?
- How does reporting of RBAC work for the application?
- Do you have audit and compliance analysis and reporting with the RBAC policies and implementation?

Identity and access management is a critical safety component in all SaaS environments that relies on the responsibility of both the provider and the consumer. As a consumer, you know your team and what their access needs are best; however, by working together through collaboration and communication with providers, you can implement a secure approach to IAM. We encourage consumers to ensure MFA enablement, institute or continue with ZTA, maintain up-to-date user access policies, and continuously audit access rights. Remember, not every user needs to be a VIP.

2 LOGGING AND MONITORING

Logging and monitoring make up the next pieces of the protection puzzle. Though these are two unique security practices, they must be implemented in concert – logging is an important first step that allows monitoring to take place. Together they allow organizations to keep track of various information, from application performance tracking to identification of who has accessed what data and when.

Monitoring can be key to detecting cyber threat activity – it can help organizations catch suspicious activity before it progresses, as well as mitigate cyber attacks in progress and provide details on how extensive the breach may be.

Effective logging and monitoring protocol involves the following steps:

1. Defining and implementing application and identity log management policies based on compliance requirements and best practices.
2. Actively monitoring logs for anomalies, security events, and performance issues.
3. Securing access to logging and monitoring platforms with strong authentication mechanisms and regular access privilege reviews.
4. Collecting and retaining logs for not only security risks, but also audit and regulatory retention requirements (when appropriate).

Despite these guidelines, it can often be confusing to determine who – the customer or the provider – is responsible for configuring logs, collecting logs, retaining logs, analyzing logs, and monitoring logs for anomalies in the specific application or environment. This area should be explicitly defined and understood before implementation and onboarding.

Platform / Infrastructure Monitoring

Infrastructure monitoring involves looking at the performance of an application's infrastructure – all of the different components that make up its backend. This includes logging the health of the technology it takes to keep the application running, such as servers, operating systems, databases, and more. These logs are then analyzed for patterns and potential issues to ensure operations continue running smoothly and that no anomalies would impact operations.

Often, the onus of platform monitoring is placed on the provider, as customers may not have clear visibility into the application's backend. However, you can validate those assumptions by asking these clarifying questions:

ASK THESE ?

- Is your vendor monitoring their infrastructure for security events and demonstrating it with audit evidence?
- Is the vendor performing penetration tests of the SaaS platform and infrastructure and providing pen test results reports similar to the application tests?
- What is the service level agreement of this application, and how will you be notified if an event occurs that impacts your data?

Application Monitoring

Application monitoring analyzes log data, network traffic, and more, allowing an organization to identify anomalies such as bugs and breaches. Point-in-time monitoring captures information at particular moments; continuous monitoring provides a more holistic view of how the application is operating and where any vulnerabilities may be, as well as a more precise snapshot of when and how an incident may have occurred.

Application monitoring is crucial to maintaining an organization's security, and it's a collaborative process – which makes it all the more important to ensure you and your provider are both on the same page regarding responsibilities so nothing slips through the cracks.

Be sure to ask the following questions:

ASK THESE ?

- What kinds of logs are created by the application, and how long are they retained for?
- Who identifies security events within the application, such as potentially risky administrator actions?
  - Will the vendor monitor your users for anomalous activity? If not, what tools and resources do they provide to you?
  - Do the logs capture enough data on risky activities to enable you to act?
- Who is responsible for detecting risks to your organization, including:
  - General Abuse?
  - Data Loss / Extraction?
  - Ransomware / Encryption?
- Have the correct teams within your organization been brought into the purchasing and deployment conversations to ensure there is someone who can perform this monitoring?

Ultimately, consumers are responsible for leveraging the insights gained from logging and monitoring to take appropriate actions. This includes promptly investigating and responding to security incidents, identifying areas for performance optimization, and continuously improving their overall security posture based on the information provided by the logging and monitoring solutions.

3 DATA SECURITY

Your data is important – and in a world where data leaks happen regularly to even the largest and most secure organizations, keeping that data safe and secure is all the more paramount. But when data lives within a CSaaS application, who ensures the information stays under lock and key?

While the CSaaS provider typically takes responsibility for securing infrastructure, the customer is often responsible for securing their own data and user access.

Many SaaS vendors have what's known as "Complementary User Entity Controls," or a "Customer Responsibility Matrix" – in other words, these are controls that the customer must implement on their end and take responsibility for. These tools help define how you, as a customer, must configure a service to have it operate to a specific compliance framework, such as PCI, SOC2 Type II, or FedRAMP.

However, even if your vendor does not have a Customer Responsibility Matrix, it's still recommended to talk with them to understand what tools they give you to protect data. Explore the following questions with your provider:

ASK THESE ?

- Is all data encrypted in transit and at rest?
- Are there options to self-manage encryption keys (BYOK)? If there are, does this impact functionality, availability, or other service level agreements (SLAs)?
- Does the application support TLS inspection or integration with secure access edge (SASE) tools to ensure consistent policy enforcement?
- What is expected from the vendor when new threats are identified?
- Will the settings in our application be automatically changed, or will our administrator need to make updates?
- How will those recommendations be communicated to us?

Penetration Testing

An application is only as secure as how rigorously it's tested. Penetration testing, or pen testing, involves allowing an expert or a program to look for vulnerabilities by attempting to breach your system. This purposeful simulated attack allows organizations to see exactly where they need to beef up security. Penetration testing may also be performed as part of a compliance program, such as PCI-DSS, SOC2, and ISO 27001, so you may be able to request and view tests performed by vendors with these certifications or attestations.

When it comes to using cloud infrastructure, penetration testing can be a significant challenge. If your organization must complete pen testing due to a compliance requirement, it's important to know what your options are, and what cooperation can be expected from your vendor. Talk to your vendor to understand how they support security control testing and if it is appropriate for your use-case.

ASK THESE ?

- What testing is performed by the vendor and at what cadence?
  - Will the results be available to you?
- When an organization adds customization, PaaS extensions or additional software to a public cloud SaaS application or service, the organization (customer) is typically responsible for all elements of the security development lifecycle (SDL), including threat modeling, SAST, scanning and regular penetration testing. Has this been built into your security program?

Data Protection Regulations

Depending on your geographical location or industry, your organization may need to comply with data protection regulations such as GDPR or HIPAA. These regulations outline what can and cannot be done with customer data and what rights customers have over their data privacy.

Complying with these regulations is a shared responsibility between your vendor and you. Be sure to regularly validate policies and requirements with your infrastructure or software provider so you know exactly what data is being stored within the application, how it is being used, how you can access and remove it if necessary, and more.

ASK THESE ?

- Does your vendor implementation comply with the regulations that apply to you, or is there another tier of service that you must purchase?
- Does the vendor have 3rd party audit or compliance attestation reports that you can periodically review and validate?

4 INCIDENT RESPONSE

The ultimate goal of incident response is to minimize the overall impact of a security breach, efficiently restore operations, and ideally prevent future attacks. The three key components of incident response are: detect, respond, and recover.[1]

As a customer, even with a tried-and-true incident response (and plan in place), the waters can get murky if a security event impacts you and a provider. It is important to understand the defined shared security model in this area and ask your provider what happens in incident response scenarios. Define clear ownership, expectations, and SLAs from the onset to ensure a speedy response and recovery. Incident response should be defined and communicated within your Managed Service Agreement. One best practice is to conduct joint annual tabletop or playbook exercises with your critical providers for training and assessment readiness.

Detect

When proper security measures and tools are implemented for detection and response, team members can monitor systems and networks for signs of unusual activity and potential threats. Incident response teams should understand how to communicate and document threats clearly and effectively to third-party vendors and providers. It is important to record details, including affected systems, initial findings, and evidence.

ASK THESE ?

- At what point of detection will the provider communicate an incident?
  - How will your provider communicate an incident or breach?
- As a customer, if you have an incident that could impact the provider, who should you communicate it to?

[1] *Formal incident response programs should be built upon a 4-step IR process, as defined by NIST (Protection, Detection & Analysis, Containment, Eradication, & Recovery, and Post-Incident Actions). However the simplification here is sufficient for the purposes of discussion.*

Respond

Once an incident is confirmed, it is time for containment from a short- and long-term perspective. This can include isolating networks, implementing patches, or other steps. Containment swiftly moves into overall threat removal by eliminating or correcting the root cause.

ASK THESE ?

- What is the provider's incident response plan? Ask for a copy to share with your teams.
  - Does the plan include contact strategies to ensure collaboration and free flow of information in the case of an event?

Recover

After containing a security event, you will need to recover quickly and provide services to your customers in order to stay solvent. The affected systems or data should be reinstated through recovery, and services should be restored to normal operations.

ASK THESE ?

- What is the provider's service level agreement for recovery from an incident?
- Will there be a root cause analysis?
  - When will it be shared?

Communication and understanding between consumer and provider are key to incident response. When and if an attack occurs, you will not have time to figure out who is responsible for what and how to communicate. Spend the time needed and ask the imperative questions when establishing your agreement to ensure that the focus after a breach can return to getting operations back up and running with minimal disruption.

5 BACKUP AND DISASTER RECOVERY

Backup and disaster recovery are not identical and should not be considered synonymous. Most cloud vendors provide disaster recovery - they guarantee the service will be available quickly after an event. When reviewing disaster recovery plans, there are two key metrics to consider: recovery time objective (RTO) and recovery point objective (RPO). RTO measures “acceptable” downtime for an organization, while RPO measures how much data can be lost during a disaster event. Extended outages can trigger regulatory reporting requirements for some organizations, so it is important to ensure that RTO and RPO guarantees align with your business needs.

A vendor’s disaster recovery strategy may not allow you to restore specific settings, policies, or pieces of data if they have been damaged by an attacker or an accident. This would be covered by a Data Backup program. It is important to clearly understand if and how the vendor is backing up your data and to create policies and procedures to fill in the gaps.

Just like the incident response previously discussed, your managed service agreement should clearly define and predetermine the roles and responsibilities of backup and disaster recovery. To best understand your responsibilities as a customer and to properly prepare, we recommend asking the following questions:

ASK THESE ?

- What is the vendor’s disaster recovery strategy?
- How quickly will services be available?
  - Does that fit your risk profile (RPO and RTO)?
- What happens if data is damaged within our tenant?
  - Can the vendor repair that?
- Are the vendor’s backups immutable?
  - Can the backups be damaged in a ransomware event?
- How long is data stored, including backups?
  - Is this aligned with any of your regulatory requirements?

6 OPERATIONAL AND CYBER RESILIENCY

Whether a disruption occurs internally or externally, it is important that both providers and customers can anticipate, prevent, respond, and adapt in a way that minimizes any impact on services or data security. Service continuity is maintained through clear communication and trust in the other parties' ability to respond and handle potential disruptions, including well-established disaster recovery plans and processes.

As all organizations are different in size, scope, and security needs, it's essential for each team to take an aerial view of what steps they have in place for if and when a disruption occurs – and what steps should be put in place if there are gaps. It is, however, a shared responsibility between the vendors and their customers to ensure appropriate cyber and operational resiliency measures are secured.

To help clarify roles and expectations, here are some questions that can be asked to yourself and your provider:

ASK THESE ?

- Do you have a disaster recovery (DR) and business continuity plan (BCP) for your critical services?
  - How often are these BCP/DR plans tested?
- What are the service level agreements (SLAs) specific to DR that are provided by your critical services vendor?
- Does your critical services product have DR support built-in?
  - Does it provide customers with the ability to test DR?
- What procedures are in place for reporting and responding to operational disruptions?
- How are service outages or availability details communicated to the customers?
  - Are there post-outage review processes in place?

Although some exploratory questions with your provider may already be covered when discussing incident response or data security responsibility, we also encourage customers to review those answers through an operational resiliency lens.

6 POLICY STANDARDS AND APPLICATION GOVERNANCE

A strong security policy is essential for outlining the standards and strategies that must be followed to protect against cyber threats and to mitigate incidents, breaches, and vulnerabilities if they do occur. Govern is the first core function outlined in NIST's Cybersecurity Framework 2.0 and is an organization's risk management expectations and policy – driving and monitoring their overall cybersecurity strategy.

Security policies often cover a wide variety of topics, including determining roles and responsibilities within – and outside – of an organization when it comes to handling any number of operational activities. The shared service model doesn't end with the delineation between vendor and customer; it's also important to define who is responsible for what actions within your own company.

Part of an organization's policy may involve application governance – a structure that outlines and manages the deployment and use of outside applications, such as SaaS. Implementing a new application takes cross-organizational collaboration: Information Technology, Information Security, Governance & Risk, and other teams may all play roles, working together to ensure the application not only runs as it should but it meets policy requirements.

Ask questions internally early in the process to ensure that all teams have an appropriate amount of resources dedicated to the management of an application. In addition, test or development tenants can create opportunities to leak data. Understand who is accountable for the security of the system, as everyone is responsible in some way for collaborating to ensure compliance.

The following are some best practices to ask yourself and your team when implementing a new application:

ASK THESE ?

- What policies are in place across your environments and does everyone have access to these policies?
  - Ensure consistent policies are deployed across all environments, including:
    - Maintaining all environments (test, staging, development) with the same security controls
    - Enforced data masking
    - Regular patching and updates
    - Consistent access controls
    - Consistent adherence to hardening standards
- Is ownership of the cloud application assigned to a role? Does this include responsibility for risk acceptance?
- Who in your organization is responsible for validating the vendor's controls are in place? *Typically this is performed by a third-party risk, GRC or internal audit group.*
- Have you built a proactive culture between IT, Engineering, DevOps, and Security executives to encourage users to utilize approved cloud vendors?

SUMMARY

Every organization is different, and it is not possible to create a definitive list of questions you may need answered to create your own Shared Responsibility Model, but we hope that this document creates a foundation for you to build upon. It is important to first start by examining your application cloud provider's documentation, attestations, and best practices to have a meaningful dialogue on where gaps or misunderstandings may exist in the shared security responsibility framework. We believe that information sharing, whether it be between customers and vendors, or between all of us as security and IT professionals, is a key tool in our defense against attackers. We encourage you to participate with the IT-ISAC or find a sharing center for your industry at the National Council of ISACs.

IT ISAC
FOUNDED 2000

CSaaS SIG
An IT ISAC Community

Questions? Interest in joining IT-ISAC and the CSaaS SIG?
Email us at csaas@it-isac.org.

IT-ISAC.ORG