SaaS Governance Best Practices for Cloud Customers

cloud security alliance®

The permanent and official location for the SaaS Working Group is https://cloudsecurityalliance.org/research/working-groups/saas-governance/

Acknowledgments

Finishing Initiative Leads

Chris Hughes
Tim Bach
Michael Roza
Anthony Smith
Walter Haydock
Andreas Peter
Andrew Luhrmann
James Underwood
Alistair Cockeram
Saan Vandendriessche

Finishing Contributors

Bryan Solari
Sai Honig
Amit Kandpal
Jessica Shouse
Abhishek Vyas

Finishing Reviewers

Jerich Beason
Kapil Bareja
Or Emanuel
Udith Wickramasuriya
Priya Pandey

Initial Leads and Contributors

Akin Akinbosoye
Yao Sing Tao
J. R. Santos
Mickey Law
Vani Murthy
Zeal Somani
Paul Lanois
Michael Roza

CSA Global Staff
Shamun Mahmud

Table of Contents

1. Introduction

In the context of cloud security, the focus is almost always on securing Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) environments. This is despite the reality that while organizations tend to consume 2-3 IaaS providers, they are often consuming tens to hundreds of SaaS Offerings. The SaaS Governance Best Practice for Cloud Customers is a baseline set of fundamental governance practices for SaaS environments. It enumerates and considers risks during all stages of the SaaS lifecycle, including Evaluation, Adoption, Usage, and Termination.

As organizations continue to adopt SaaS-based applications and solutions, several areas of traditional organizational cybersecurity must be updated to reflect this new operating model.

Internal organizational policies must be updated to reflect key items, such as service level agreements, security and privacy requirements, and operational implications. Organizational operational security activities are impacted, such as responsibilities and tasking as well as implications for mobile devices and remote working employees. Information is an asset and in the SaaS paradigm classification, labeling, and storage requirements must be considered when it comes to external service providers. While SaaS providers handle much of the responsibility in the Shared Responsibility Model, SaaS consumers are still largely responsible for data governance and access control. This means ensuring who has access to what data, what level of permissions, and under what context, especially in a Zero Trust Architecture.

Organizations still have key decisions around encryption key management and operational activities such as vulnerability management and backup and storage. Organizations need to ensure they consider SaaS providers as part of their third-party risk management programs and that incident response and business continuity plans and processes are updated accordingly. This is increasingly true, as SaaS often serves key functions from a business continuity perspective in the remote work paradigm. Even with the shared responsibilities, organizations also still have compliance and regulatory requirements they must meet to protect their stakeholders as well as their reputation and to avoid potential legal consequences.

The SaaS environment ultimately presents a shift in the way organizations handle cybersecurity that introduces a shared responsibility between producers and consumers. Failing to adjust accordingly can have devastating consequences such as disclosing sensitive data, loss of revenue, customer trust, and regulatory consequences.

1.1 Scope

This document:

- Provides a baseline set of SaaS governance best practices for protecting data within SaaS environments
- Enumerates and considers risks according to the SaaS adoption and usage lifecycles
- Provides potential mitigation measures from the SaaS customer's perspective

1.2 Audience

- SaaS Consumers
- SaaS Providers
- SaaS Security Solution Providers
- Cloud Security Professionals
- Legal
- Cybersecurity Executives
- IT Executives
- Risk Managers
- IT Auditors and Compliance
- Third-party Risk Managers

2. Overview

Software as a Service (SaaS) consumers and customers should assess and mitigate information security risks raised by the usage of SaaS services. This document discusses SaaS in the context of NIST 800-145, which defines SaaS as "the capability provided to the consumer through using a provider's applications running on cloud infrastructure." In this context, the consumer does not manage or control the cloud infrastructure, operating systems, associated storage, or even individual applications, except specific configuration settings.

While the domain of cloud adoption and security continues to evolve, not much guidance is available regarding SaaS governance and security. This is despite the reality that organizations are increasingly utilizing SaaS offerings occasionally by different departments in the organization (Shadow IT), to power their critical business processes and functions and often storing sensitive data in SaaS environments.

2.1 Approach

SaaS requires a different security governance mindset. While there are some similarities to the governance of other Shared Responsibility frameworks (i.e., IaaS), the nature of SaaS deployments and management necessitates a unique approach. Proper security and governance due diligence for SaaS must start at a high level–an understanding of the SaaS application's use and capabilities–and proceed down to the details, such as what types of data will be stored in the system and who will have access.

Given the unique complexities of properly governing SaaS application usage combined with the myriad SaaS applications likely deployed, an organization should first seek a framework (such as NIST CSF) that suits the organization's security, business, and regulatory needs. That framework will shape the people, processes, and technology that make up the security architecture.

Following a widely adopted security framework, such as NIST CSF, coupled with the best-practices and recommendations in this document, will help organizations establish SaaS governance and security processes to mitigate risk associated with SaaS usage.

2.2 Structure

This document defines three necessary components of SaaS security: process, platform, and application. Integrated security for SaaS can be realized by gluing process security, platform security, and application security together into a cohesive strategy.

Process security protects the integrity of procedural activities, to ensure the input and output of processes are not easily compromised. These are the managerial aspects, including policies and procedures, to ensure that an organization's processes are consistent.

Platform security deals with the security strength of the platform, the underlying dependencies of a SaaS service. These include the SaaS infrastructure, operating systems, and its potential suppliers.

Application security deals with the security of the SaaS application itself. A SaaS application can only stay secure if it does not contain exploitable vulnerabilities and has implemented hardened configurations aligned with organizational and vendor security best practices, as well as compliance requirements.

In the SaaS model, limited control and visibility is largely restricted to the process and application security components. SaaS consumers do not have control over the platform security components of a SaaS application or the underlying supply chain. These realities emphasize the need for SaaS consumers to have sound process security within their organizations as well as ensure application-level security controls are implemented.

Sector-specific security controls are commonly used to satisfy privacy, governmental, or financial compliance. Examples are FedRAMP, NIST 800-53, HIPAA, and PCI-DSS. These requirements are often vertically focused that apply across three SaaS security areas.

2.3 Lifecycle Considerations

When properly governed, the adoption and usage of SaaS applications in an enterprise environment generally follows three key lifecycles: Evaluation, Adoption, and Usage. The common patterns of these lifecycles are described below.

It is important to note, however, that SaaS application adoption has in all likelihood grown organically at many organizations that today find themselves behind in the monitoring of SaaS applications. In such organizations where a SaaS security and governance program is being put into place after the widespread adoption of SaaS, the Usage lifecycle will be the most relevant.

2.3.1 Evaluation Lifecycle

The Evaluation Lifecycle takes place prior to procurement starting with the identification of a business need that may be solved by a SaaS application. In many organizations, this takes place in the line of business and may or may not involve a centralized procurement organization. The Evaluation Lifecycle is typically composed of 4 steps:

> - Understanding the services users are already leveraging for the use case under consideration
> - Market research
> - Pilot efforts
> - Purchasing decision

If a purchasing decision is made by the organization, the SaaS application will begin to be deployed with the Adoption Lifecycle, described below. While ideally, a representative from the relevant security and compliance organization(s) is present during the evaluation phase, it is critical that such representatives be involved in the adoption phase. As an organization builds a SaaS security and governance program, these organizational “checkpoints” are key integration points into the SaaS lifecycle for security teams.

2.3.2 Adoption Lifecycle

The SaaS Adoption lifecycle is consistent across almost all organizations. It spans the time from which the SaaS application is procured in an initial form (which may sometimes be an expanded pilot program) through full deployment and growth in usage, all the way to potential termination and decommissioning.

The Adoption Lifecycle varies in length–and for large, business-critical SaaS applications may realistically be a steady-state–but is typically composed of four steps:

- **Evaluation:** During the evaluation phase, a cloud consumer evaluates a potential SaaS application for consumption. This typically involves a pilot or proof of concept activity to explore features, functionality, and the ability to meet business needs.
- **Adoption:** The adoption phase of the lifecycle is where the cloud consumer begins to officially adopt the SaaS offering and move beyond a pilot or proof of concept. This may involve moving more sensitive data into the SaaS application as well as rolling it out to additional business units to consume.
- **Routine Use and Expansion:** Routine use and expansion can be thought of as a sustainment phase. At this point the consumer is routinely using the SaaS application for various business functions and has standard operating procedures for its use.
- **Termination:** The termination phase of the lifecycle represents when the cloud consumer has decided to no longer use the SaaS offering. This may be due to various reasons such as cost, security or perhaps no longer meeting business needs. The consumer begins to shut down their SaaS application usage, reduce sensitive data, accounts and more.

2.3.3 Usage Lifecycle

The SaaS Usage Lifecycle helps protect against daily operational risks and security concerns such as least privilege and Identity and Access Management.

The SaaS Usage Lifecycle is composed of four steps:

- **Eligibility:** Should this person or non-person entity be a user of this service?
- **Provisioning:** What needs to be done to add this person to the service and what are their appropriate permissions?
- **Monitoring:** Is this person using documented patterns that are aligned with the usage expected by the consuming organization?
- **Deprovisioning:** How do we remove this person from the service?

The SaaS usage lifecycle maps out how your organization engages the CSP and the SaaS service.

It is important that you understand and monitor the SaaS usage lifecycle in its entirety. It can be very easy to get drawn into focusing all your efforts in optimizing one stage of the life cycle, such as onboarding when doing so won’t help the business to achieve its desired outcomes more easily or quickly.

3. Information Security Policies

SaaS customers should develop a SaaS security strategy and build a security architecture that reflects that strategy. A strong security architecture should include security policies that guide the deployment and maintenance of SaaS applications.

3.1 Policies for Information Security

Policies should be developed regarding governing evaluation, adoption, usage, and termination of SaaS services. Refer to the description of the common SaaS lifecycles above and ensure that your organization has in place comprehensive policy and evaluation controls for each lifecycle phase.

3.1.1 Evaluation

Any decision should be guided by the enterprise architecture requirements and processes. An overall enterprise architecture (evaluation of the products, services, and tools, and the needs they solve) of the environment should be done. This prevents unnecessary duplication of products, services, and tools.

If a need is identified that is not available in the current enterprise architecture, an evaluation of products, services, and tools can begin.

The initial evaluation of a SaaS service will typically allow the business, legal, and security stakeholders to understand the risk of the transaction and proceed accordingly. The critical question is, "Is this a potential fit with our risk profile and enterprise architecture?"

3.1.1.1 Determining Acceptable Risk

When evaluating a SaaS service the first step is to determine what risks would the customer be assuming aligned with their risk appetite. The SaaS application may be hosted in a private, hybrid, or public cloud environment, with the application offered on dedicated or shared resources at application level (single instance, multi-tenanted). As with any cloud product, service, or tool, the Shared Responsibility Model must be understood.

According to ISO/IEC 27001, a risk management approach should be used to manage information security. A SaaS customer should first determine the acceptable risk to the organization from the SaaS service, which forms the baseline of the evaluation stage. Different methods can be used to manage risk, including the international risk management standard ISO 31000.

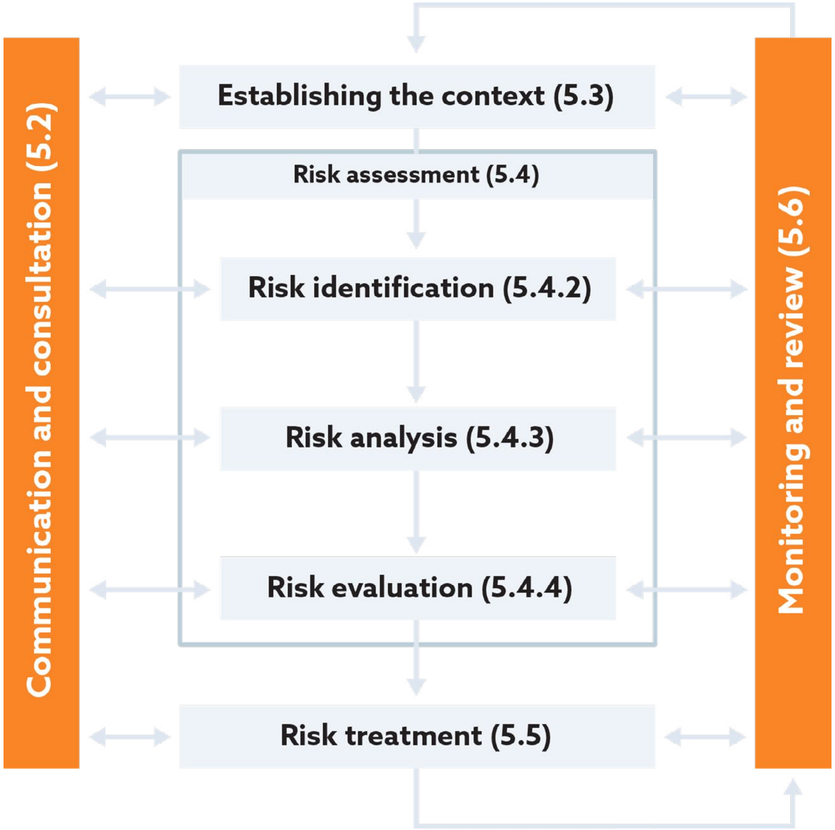
Communication and consultation (5.2)
Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Monitoring and review (5.6)

Figure 1. ISO Risk Management Process, Clause 5: Process

Given an understanding of the organization's risk profile, a SaaS customer should be able to determine if the SaaS service in question could be a potential fit with the organization's risk profile.

One way of determining the risk profile of a SaaS service can be determined by understanding the usage context of the SaaS service taking the following considerations into account:

- Data:
  - What data will be stored in the process or be exposed to a SaaS application?
  - What are the direct costs (costs to notify impacted individuals, costs to shareholders if the stock drops, mass exodus to competitors, loss of profit) and indirect costs (reputational harm and missed future sales, increase in cyber insurance cost, termination of key staff), and hidden costs (the cost of pivoting staff to respond, the cost to fortify breach points) to the business if the confidentiality or integrity of data stored in this SaaS application are compromised?
- Processes:
  - Does this service affect core or critical business processes?
  - What organizational policies and processes would need to be revised if the SaaS service is utilized?
- Requirements:
  - What business requirements, laws, and regulations are relevant to this service?

At this stage, the following aspects should be evaluated on how they affect the risk profile of the SaaS customer:

- The SaaS provider
- The SaaS service
- The SaaS providers suppliers
- The usage of the SaaS service
- The SaaS customer's capabilities for applying continuous monitoring and posture management to the SaaS provider in question to mitigate risks

The most common risk profiling method available is the classic CIA classification:

- Confidentiality
- Integrity
- Availability of information

With CIA, applications and databases are risk-scored per your requirements.

Once the risk footprint has been established you can start calculating the risk the SaaS application poses.

There are many ways to calculate risk and developing a risk profiling framework depends on organizational need and type of industry.

It pays to keep in mind that by transferring activities to a CSP, the SaaS customer itself is **not outsourcing its accountability** to the CSP. The SaaS customer must always keep in mind that the risk owner is responsible for accepting the risk of adopting a SaaS service. While there is a sharing of responsibility between the CSP and the consumer, and the presence of agreements such as Service Level Agreements (SLA)'s, the consumer ultimately still owns the risk.

3.1.1.2 Security and Privacy Requirements

Once a baseline risk level is established, many cloud service customers engage in the security and privacy due diligence process. It is common for cloud service customers to send assessment questionnaires or Request for Information (RFI)'s to the cloud provider for completion.

These questionnaires inquire about internal security controls the customer wants to see in place with the CSP, and typically address regulatory requirement concerns around security and privacy.

Self-assessment schemes such as the CSA STAR Consensus Assessment Initiative Questionnaire or third-party assessments (such as SOC2 or FedRAMP) help CSPs inform potential customers about SaaS provider security capabilities and existing practices.

The self-assessments or third-party reports also inquire about the cloud provider's use and disclosure of personal information or where personal information will be processed. These items also inquire whether the cloud provider will be using the information for its own purposes or disclosing it to third parties (for example, disclosures to third-party advertisers).

It is also important to note the location of data since there may be data sovereignty requirements.

Some of the key categories of third-party assessments evaluated are:

> - Certifications and Standards
> - Data Protection
> - Access Control
> - Auditability
> - Disaster Recovery and Business Continuity
> - Legal and Privacy
> - Vulnerability and Exploits

3.1.1.3 Communicating Requirements

The responses in these questionnaires or reports further allow customers to refine their risk assessment and feed into the contracting phase of the cloud transaction. To reinforce their risk assessment and due diligence process, and as part of their supplier management, many cloud customers create standard data security and privacy schedules or clauses to include in their cloud contracts.

The purpose of these schedules or clauses are many and can have significant consequences. One purpose is to address regulatory issues such as maintaining data in a specific region. Another is to create a mechanism to hold a cloud vendor to reasonable security standards. These schedules or clauses may also establish incident response obligations and transfer the risk of loss for data breaches or privacy violations caused by the cloud provider. They may also require responses to issues, such as data breaches, in a specified time and in a specified manner and include the right to audit, and the right to perform periodic monitoring and controlling activities.

In addition, It is essential to understand the relevant jurisdictions as well as regulatory frameworks where the contract would be enforced or governed between the CSP and Consumer. As an example: in case you are looking for a SaaS platform to store or process employee or customer PIIs and GDPR is applicable, then you would need to see if the CSP stores data on the EU/EEA region or a country which provides adequate protection. If not, you would need to see the applicable legal framework of the country where data would store and also ensure that the CSP has adequate protection and as well as supplementary technical controls to safeguard the data as per Schrems II judgment issued by the Court of Justice of the European Union (CJEU).

The overall goal is to attempt to contractually create a seamless relationship with the cloud provider and reduce the risk for the customer as much as possible.

The contracting process for vendor management programs is sometimes further refined to allow customers to have pre-established “fallback” positions for certain terms during negotiations with cloud providers. This may include how data and other items are transferred (e.g., prevent vendor lock-in) if it is decided that the relationship should end. It is not unusual for both a customer’s legal team and security team to be involved in the negotiation of these terms.

3.1.1.4 Internal Controls

Customers should develop a SaaS security strategy and build a security architecture that reflects that strategy. SaaS customers should bear in mind the portion of the Cloud Shared Responsibility Model that they are responsible for. Namely, that the SaaS customer, not the SaaS provider, is ultimately responsible for the secure configuration, management, and usage of the SaaS platform within designed limits.

Threat modeling and threat profiling are key in developing the SaaS security strategy. Cloud Security Alliance has published Cloud Threat Modeling to "provide crucial guidance to help identify threat modeling security objectives, set the scope of assessments, decompose systems, identify threats, identify design vulnerabilities, develop mitigations and controls, and communicate a call-to-action".

Like with types of technology, cloud or otherwise, effective risk management and security controls for the use of SaaS platforms requires the SaaS customer to put in place a multi-pronged security strategy appropriate to the risk level and classification of the SaaS application determined earlier in this process. This strategy likely includes such elements as:

- Understand applicable Cloud Service Customer related security controls and configurations which can be applied on the SaaS platform (SSO, MFA, role assignments, team/group segregations, exporting logs or integrating with security monitoring solutions, IP restrictions, etc.) and employ them
- Regular review of SaaS usage and appropriateness
- Penetration testing with regards to the business logic or processes managed or deployed out of the SaaS application or platform
- Continuous security posture monitoring of the configuration of the SaaS application compared to the approved/expected configuration specific to the organization
- Continuous monitoring of audit, event, or other change/activity logs generated by the SaaS application, ideally in an environment that can correlate these logs with other SaaS and non-SaaS applications
- Continuous monitoring of access to critical data and/or processes in the SaaS application

3.1.1.5 Service Terms

The failure to negotiate robust incident response and security and forensic assessment rights can also pose risk.

If a SaaS provider suffers a breach that impacts the customer's information but does not have a contractual duty to provide notice of the breach, remediate, and cooperate, then the SaaS customer may not be able to reduce its legal risk and comply with regulatory obligations. Regional laws and obligations to notify may vary; therefore, retaining an expert cyber attorney during the procurement and contract phase is important.

Contractual Controls to consider:

- Service-level management
    - Service provider SLA vs. organization's SLA requirements (should address resource and support aspects)
    - Business continuity promises: RPO, RTO vs. MTD of the organization
    - Incident handling and escalation
- Availability of backups
- Legal concerns
    - Legal and regulatory requirements
    - Jurisdictional authority, legal requirements of CSP and SaaS service
    - Indemnity: relocation of jurisdiction, M&A
- Notifications: security, privacy, compliance changes, and events
- Termination rights and process
    - Data portability (in case you are migrating to another platform, then data export options need to be considered)
    - Data deletion, timelines, and written notification of successful deletion
    - Exit strategy in the event of termination of outsourcing agreement

3.1.1.6 Affected data

One significant risk that a shift to cloud computing presents is a loss of absolute control over data that has been transferred to the cloud and network availability outsourced to the cloud.

For instance, in a more traditional IT setting, organizations have the ability to assess and adjust their systems so they are compliant with applicable regulations and standards. This may include requirements with regards to data residency based on the location of the organization or its customers.

Since many SaaS providers use infrastructure as a service provider located in multiple jurisdictions, the use of SaaS services without taking these requirements into consideration can present an increased risk to compliance.

A SaaS customer should be able to answer the following questions:

- What jurisdictions does the SaaS provider operate in?
- What regulatory requirements are applicable?
- What data will be transferred to the SaaS service?
- What data will the SaaS service have access to?
- What reliance will we have on the SaaS service on our data?
- What are the legal obligations of the CSP? For example, payment providers would need to retain some data per their legal obligations to comply with Anit-Money Laundering (AML).
- What would the SaaS provider do if a government or military entity requests access to data?

For example, if only non-sensitive records are being stored in the SaaS application, as opposed to sensitive data (e.g. social security numbers or financial account data), less supplier scrutiny may be appropriate.

Controls:

- Confidentiality requirements are driven by data value
- Data classification requirements (e.g., HIPAA, PCI)
- Data and metadata control: ownership, processing, licensing
- Data location and sovereignty
- Availability requirements and data mobility

3.1.1.7 Privacy

When utilizing a SaaS provider, it is important for customers to ensure that they understand the privacy implications of storing data in that provider. SaaS customers should understand if there are any allowable uses of data they store in the SaaS application by the provider (e.g. machine learning, anonymous dataset evaluation, etc.). Those uses, if any, meet the SaaS customer's regulatory and audit requirements.

The ever-changing regulatory landscape itself increases the risks of privacy-related compliance or data residency violations, complicating the deployment of SaaS applications for some customers and certain types of data. Concerns abroad about U.S. SaaS providers housing European citizens' data increase this potential risk.

Controls:

- Role of the SaaS customer vs. the role of the SaaS service?
  - Controller (PII of customers or staff)
  - Processor (PII supplied by a controller)
- Privacy policy: Rights of the SaaS provider to data on their service
- Breach obligations and responsibilities
- PII data inventory, visibility
- Consent management

3.1.1.8 Steps for performing a detailed risk assessment

1. Identify assets
2. Identify threats
3. Identify vulnerabilities
4. Develop metrics
5. Consider historical breach data
6. Calculate cost
7. Perform fluid risk-to-asset tracking

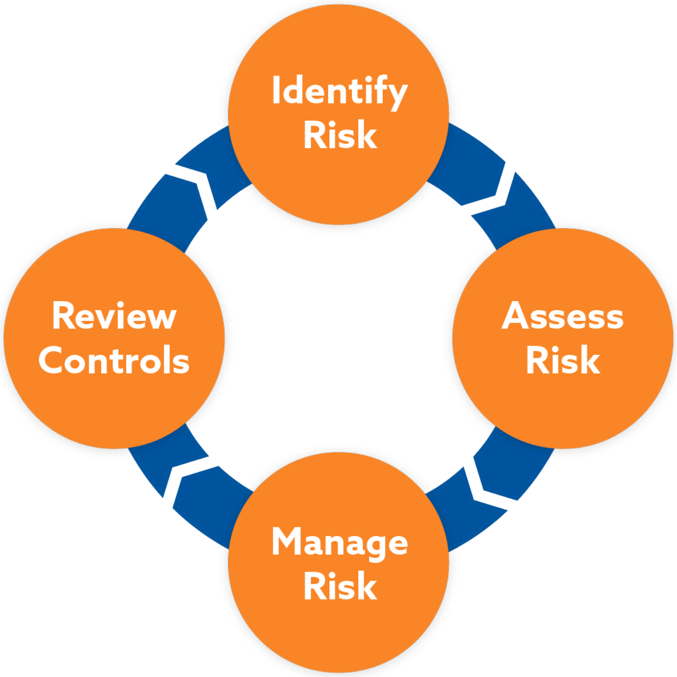

Figure 2. Risk assessment cycle

3.1.1.9 Identify Risk

Identify Risk areas that could pose a hindrance to business objectives:

- Loss of data, financial information, intellectual property/competitive advantage
- Regulatory, legal mandates
- Company reputation
- Threats, vulnerabilities, attacks
- Incident management
- Technological complexity:
  - Personnel expertise
  - Financial commitments
- Third-party supplier
- Third-party audit, SOC 2 report, STAR Registry, etc.
- Human error

3.1.1.10 Assess Risk

- Qualitative/Quantitative Risk Assessment
- Governance Risk Compliance (GRC)
- Risk Tolerance/Appetite

3.1.1.11 Manage Risk

- Implement physical, technical, and/or administrative controls per risk tolerance
- Transfer risk to third party
- Accept risk

3.1.1.12 Review Controls

- Internal/external audits
- Risk analysis

To identify risk, a detailed risk assessment on the SaaS service and CSP is a must.

Risk assessments should be conducted before placing company assets into the CSP's cloud. The level of detail given to the risk assessment will vary depending on the environment. For example, one might decide to start off using a CSP under a limited use-case (i.e., sandbox, developing software, testing CSP features, controls, etc.). Under this scenario, a 'minimal risk assessment' may be performed. If the CSP's tools and features satisfy the CSC's business objectives, then a more detailed risk assessment should be done before the application moves to production.

When deciding to perform a SaaS risk assessment, three areas should be closely examined: a) the SaaS provider; b) the SaaS provider's management practices; and c) the technical security considerations of the SaaS application. This table lists areas of concern to consider.

Provider	Practices	Application
What certification(s) does the CSP possess?	What control measures does the CSP employ to restrict data to/from different regions/zones logically?	Are application/privileged accounts centrally managed (e.g., via IAM, RBAC, or account management tool)?
Has the CSP undergone a third-party assessment or audit? Can the CSP provide a SOC II report (or an equivalent)?	What backup/restore services does the CSP provide (e.g., for the application, data, VM)?	Is a secure channel in place (e.g., for the secure transfer of passwords, certificates, data)?
Is CSC data stored on-premises with the CSP, or does the CSP have a contract with a third-party supplier (for "ping power pipe")?	What is the CSP's Incident Management process? How are incidents classified?	Is SSO/SAML/MFA used for secure authentication?

Provider	Practices	Application
What level of support is provided to the CSC for troubleshooting, maintenance, etc.?	Are VM images, servers, and databases regularly patched? What is the CSP's antivirus management process?	Will applications/storage accounts be public facing?
What are the CSP's SLA's/ OLA's?	How are encryption keys managed, stored, etc.? Who has access to them?	Is the application/software licensed for the cloud?
Has the CSP provided a list of all third-party suppliers that will support this SaaS? If so, does the CSP employ background checks, and NDAs?	What logging/SIEM event threat detection tools are provided to the customer?	Is the software/data subject to any regulatory/privacy requirements?
Which standards and regulatory requirements, can the CSP adhere to? What standard(s) (i.e., ISO, NIST, CIS, PCI, HIPAA, GDPR) does the CSP map their baseline controls?	What IDS/IPS tools does the CSP provide?	What software development process/tools are required for the development/ maintenance of the application (i.e., DevSecOps, GitHub., SDLC)? What tools/ applications does the CSP use to support this effort?
Is the CSPs underlying architecture designed/ developed utilizing industry-best practices or standards?	Does the CSP provide VM-hardened images? How are they managed/enforced?	What APIs are required in support of the application? What help can the CSP provide?
Does the CSP utilize/provide automated tools, scripts of its cloud resources (e.g., VMs, IaC, auto-remediation)?	Does the CSP offer controls to prevent unauthorized exfiltration of data?	Does the CSP support vulnerability/Pen testing (if necessary) for the application?

To be clear, the above risk evaluation is specific to the security of the SaaS provider and the underlying architecture and implementation of the SaaS application that will be used. It is *not* a replacement for continuous security monitoring and risk review of the SaaS customer's implementation and usage of the SaaS application.

To correctly manage SaaS risks, it must be understood and viewed through various lenses. Only then can one have some level of assurance that SaaS risks have been appropriately identified, evaluated, and mitigated. Risk assessments should not be viewed as a "one and done" exercise. Cloud risks are fluid and should be conducted at regular cadences and whenever there is a significant change.

It is up to the SaaS customer to understand the requirements for their solution and then ensure those requirements are understood and can be met by the SaaS provider. Suppose the SaaS provider does not offer a particular service/control that is required for your application/industry; in such a case, it is the responsibility of the SaaS customer to mitigate the gap or choose not to use the provider in question.

3.1.1.13 Cloud provider vetting best practices

- Treat third-party technical services as an asset in your organization.
- Establish a risk-based approach to third-party assessments.
- Develop third-party assessments based on input from key stakeholders across the organization.
- Ensure business owner engagement.
- Periodically review the highest risk vendors.
- Publish the list of sanctioned vendors/apps.
- Require sanctioned vendor/app use without business justification and approval.
- Consider requiring the use of pre-approved vendors across the organization.
- Encourage or mandate the use of compliant suppliers.

3.1.1.14 Develop policies and procedures

To securely deploy and utilize SaaS applications, it is critical for the SaaS customer to develop internal policies and procedures for continuous assessment and monitoring of their implementation and usage of the SaaS application. Regular risk reviews and assessments as described earlier in this section target the SaaS provider's technology, practices, and certifications; it is equally important, if not more so, for the SaaS customer to have monitoring and assessment methodologies in place targeting their configuration and real-world usage of the SaaS application.

Such policies should, at minimum, include:

- Account management procedures
- Centralized identity management procedures
- Data and system access requirements, i.e., approving any grants of significant access and requiring additional authentication for such accounts
- Acceptable use policy against service abuse
- Integrated user lifecycles in context with business processes
- Data classification and labeling
- Integration into existing service level, incident and vulnerability management processes
- Integration into existing governance mechanisms, creating/uplifting where required, i.e., change control

As with other security programs, it is not acceptable to view the monitoring of SaaS application configuration, data classification, and data access as a point-in-time exercise. SaaS, even more so than other cloud technologies, changes rapidly and can be quickly reconfigured. SaaS customer administrators can substantially change the security posture of a SaaS application with a single inadvertent command or button-click, further highlighting the need for a continuous monitoring program.

3.1.1.15 Configuration and Security Posture Management

Critical SaaS applications, as defined by metrics such as the sensitivity of data stored in the system or the potential disruption to the business if compromised, must be continuously monitored. Such monitoring capabilities, preferably automated, should run frequently and be able to be run on an ad-hoc basis after major changes; ideally, they should also be able to run against sandbox or pre-production environments to validate configuration changes before they are made live in a production SaaS environment.

At minimum, the SaaS customer's posture management program for critical SaaS applications should take into account:

- Configuration baseline for system settings, especially settings relevant to:
  - Identity
  - Authentication and system access, including MFA, SSO, and geographic or IP restrictions
  - Password policies
  - Session controls
  - Platform-provided DLP and audit capabilities
  - Platform-provided encryption and BYOK capabilities
- Installed and approved third-party plugins, integrations, and OAuth or other cloud-to-cloud connections
- Assignment of users to Roles, Profiles, Groups, Teams and any entity in the SaaS application that can grant additional access or capabilities
- Configuration of access granting elements and the effective access this coffers upon users
- Administrative action and authorization logs that may indicate sensitive or privileged actions
- Correlation of actions across key SaaS applications or environments
- User access to key types of data or records, and determination of read access (confidentiality) vs. write access (integrity)
- Offboarding procedures

Configuration Management in this section refers to 'configuration control.' NIST 800-53, CM-2 states, *"Baseline configurations serve as a basis for future builds, releases, or changes to systems and include security and privacy control implementations, operational procedures, information about system components, network topology, and logical placement of components in the system architecture. Maintaining baseline configurations requires creating new baselines as organizational systems change over time. Baseline configurations of systems reflect the current enterprise architecture."*

One of the benefits of the cloud is that it facilitates the rapid development of new capabilities, applications, and services for software developers. In major SaaS applications today, this can frequently include the creation and deployment of little or no-code applications that control critical business processes. These integrations, workflows, and applications can be quickly deployed and modified by users with permission to do so. The potential impact of such permissions is thus even greater to the business, and it is important to be able to monitor and alert upon incorrect assignment or usage of such capabilities.

Additionally, the rapid configurability of SaaS applications and the prevalence of cloud app marketplaces on many SaaS platforms can allow users to quickly extend the SaaS platform with third-party (not developed by either the SaaS customer or the SaaS provider) applications. While powerful, this can also introduce vulnerabilities that are otherwise hidden from vendor risk assessment and procurement programs. It is thus critical that security organizations have monitoring and alerting capabilities in place to detect unauthorized connection of third-party applications to approved SaaS platforms.

With the SaaS echosystems connecting one SaaS platform with one or many others, it is essential to understand the permissions and the integration properly prior to integrating. If sufficient integration information is not available, then you might have to do the integration in a lower or sandbox environment.

Let's take an example where you would need to integrate your marketing automation platform (MAP) with your Customer Relationship Management (CRM) platform to feed MAP data to CRM. In this scenario, you would need to consider and follow from where to where the data would be flowing. Is it from MAP to CRM, or CRM to MAP? In this case, it would be MAP to CRM.

Then you would need to check if the CRM has a pre-vetted marketplace integration. Usually Marketplace integrations are somewhat safer.

After that, you would check on the best practice guidelines or reach out to the support personnel to get those best practices, if it doesn't exist.

Lastly, you would need to analyze how to ensure least privileges and adhere to data minimization principles.

Also, it's essential to understand how to remove the connection as well.

Let's take another example where a user would be integrating their Google account with a third-party application. The user would need to mainly see what the permissions and scopes the third-party application would get, and what would the actions that the application would be able to perform on behalf of the user. Then make a judgment call based on the risk appetite of the organization. Users would probably need to get support from the security experts on this and they also might want to know how to revoke third-party access as well.

When developing security posture management policies and rules, SaaS customers can utilize industry-wide best practices (i.e., the CIS Benchmark for Microsoft 365), work with SaaS Security Posture Management vendors who have developed baseline security policies through research, or undertake an internal effort to identify best practices and requirements specific to the organization. Frequently, the most comprehensive policies will be developed through a combination of these options.

3.1.1.16 Data Security

SaaS customers should monitor access to sensitive data stored in the SaaS application in a similar fashion to monitoring put in place for system configuration and security posture. Again due to the inherent flexibility and configurability of the SaaS applications, the access that users have to data may be quickly changed. Thus it is, as with other parts of SaaS security monitoring, critical to treat monitoring access to data as a continuous process and not a point-in-time exercise.

As part of any data security and access monitoring solution, SaaS customers should undergo an effort at regular intervals (or using automated platform features) to classify data by sensitivity level, type of data, and so on. This classification, whether maintained in an external system or on the SaaS platform itself, will be crucial in designing a data security policy and monitoring the actual state against it.

Other considerations with regards to data security, that likely can be monitored as part of security posture monitoring but should be clearly defined nonetheless, include:

- Configuration of (and user access to) data export functionality and data backup functionality
- Inventory of assets, ownership, and responsibilities
- Limitations on internal and external sharing and monitoring of system configuration to match that policy
- Cryptographic controls and requirements, and monitoring of the system to ensure it is configured as intended

Another class of security solutions that can be applied to SaaS applications are Data Loss Prevention (DLP) solutions. DLP solutions frequently sit in-line with access paths to data or are provided as built-in SaaS application features. Data loss prevention helps to provide a higher level of information protection. It can prevent the transfer or exfiltration of certain types of documents. DLP solutions also have a relationship to data classification. First, you need to classify your data and documents where the DLP solution would be able to understand the classification and monitor accordingly (e.g., PII, PCI).

DLPs mainly operate based on keywords, phrases, and metadata. Upon a DLP logic match, it can perform one or more actions such as inform the user, alert the administrators, block the transmission, remove attachments and documents, redact sensitive data, and retain a copy of the data for inspection/forensics purposes. SaaS providers typically provide mechanisms or APIs for their customers to automate this process. When there are a considerable amount of SaaS systems being utilized, customers would go for a DLP solution which has integrations with SaaS platforms for seamless administration.

3.1.1.17 User awareness and training

- Develop best practices guidelines for secure usage of this service
- Enforce data classification and labeling
- User awareness on what are security incidents for this service and how to report them
- Add coaching policies whenever feasible (i.e., user gets a prompt to access the sanctioned service for a category or log a justification for the usage of an alternate one)
- Promote a no-repercussion atmosphere for candid reports

3.1.1.18 Insider threats

- Leaving employees could share SaaS data with their personal accounts. This could allow for the exfiltration of company data
- Employees overexpose sensitive data internally (finance and engineering can consume each other's information)
- Sensitive data is being shared with the wrong third party
- No segregation of duties
- Improper platform configuration leading to data exposure (i.e., S3 buckets containing sensitive data are publicly exposed)
- Employees are allowed to take data dumps of systems which would allow them leaking or taking those data away when they are resigning.

3.1.1.19 External threats

- Third-party collaborators have access to your company data forever
- Your vendors share your company data with their vendors, who were never gone through a third-party risk assessment by you
- Third-party collaborators with your company data with their personal accounts which in most cases don't have multifactor authentication set up
- Third-party vendors or their subcontractors or suppliers are not bound by a regulatory entity to safeguard data

3.1.2 Usage

- Acceptable use
- Administration
- Governance

3.1.2.1 Periodic service/supplier reviews

- Monitor service terms and conditions for changes archive versions
- Validity of security assurances
- Ongoing security performance

CSP supplier management is challenging.

3.1.2.2 Alerts

- Monitor suspicious logins and data access
- Monitor service usage and abuse
- Monitor service attributes for SLA compliance
- Monitor any anomalies in logins and access
- Monitor any risky organization wide settings change
- Monitor abnormal access to data

Service terms and conditions can change overnight resulting in loss of control. Therefore, continuously monitor the attributes of the service using automated tooling.

Monitor configuration changes and alerts, if necessary.

3.1.2.3 Usage visibility

- Authentication logs with login, user location
- Access logs
- Audit logs
- Account provisioning and de-provisioning logs

3.1.2.4 Continuously evaluate and reduce the attack surface

- Monitor basic attributes of service for a sanity check
- Review controls to reduce attack vectors
- Monitor potential internal failure points

3.1.2.5 Configuration management

- Monitor configuration changes and alerts if necessary

3.1.2.6 Data

- Monitor access to sensitive data, systems, and fields
- Monitor administrative actions
- Enable auditing
- Monitoring of valid backups

Ensure that backups of data are performed and even more important, test the backups by performing or requesting a restore.

3.1.3 Termination

Termination of SaaS usage requires coordination and planned execution.

One of the most important yet frequently overlooked risks of SaaS services lies in the contracts offered by CSPs.

Organizations have traditionally worked with their legal departments to negotiate service provider contract terms to be less “vendor-friendly” and to mitigate any losses caused by service providers by holding the providers financially responsible. But cloud providers haven’t been willing to offer the usual indemnification, limitations of liability, or other terms — particularly pertaining to privacy and data security.

The most prevalent reasons CSPs cite are that these additional duties and obligations threaten the lower-priced model for cloud computing and, since CSPs don't know what their customers are storing on the cloud, they can't be held liable for segregating and securing customer data. However, the CSPs must provide the means for the customer to accomplish this.

Unfavorable terms in cloud agreements may increase the risk for cloud service customers.

Cloud service customers may also want to contractually limit the subcontractors that a CSP utilizes to store or process the customer's data. Without these limitations, a customer may find that its data is actually two or three hops removed from the primary CSP.

3.1.3.1 Internal processes

- Notify all users of service termination
- Disable all API access
- Guidelines on replacement or data extraction
- Extract data for future usage or migration to new service
- Where to store and who is responsible?
- Ensure all integrations/data flows into other systems is understood

3.1.3.2 Data retention

- Destruction of backups and residual data/metadata (e.g., system logs, audit logs, access logs, search indices)
- Data retention timeframe should satisfy data classification requirements
- Exporting and removal of financial information
- Exporting of usage and other reports

3.1.3.3 Return of assets

- Export of data/metadata (e.g., audit logs, access logs, backups)
- Comply with data location requirements
- Acceptable data formats
- Delivery time, method, accessible for how long

3.1.3.4 Decommission service-specific attachments

- Service-specific monitoring
- Security monitoring of service

3.1.3.5 Service management

- Removal of all integrations with service
- Ensure decommissioning of service
- Ensure closure of the contract

3.2 Review of the Policies for Information Security

Since technology changes frequently, a regular cycle of reviewing policies is necessary. Additional acceptable controls may be required since the last version. This would also require that the SaaS operations still meet the minimum required standards that are set by the organization.

Some solution providers like CASB provide ongoing assessment and scoring of SaaS services and provide the functionality to set up alerts and access policies based on these dynamic scores.

4. Organization of Information Security

4.1 Internal Organization

4.1.1 Information Security Roles and Responsibilities

Even though many view SaaS as an outsourced responsibility, it is imperative that the Role and Responsibility (R&R) between the Cloud Service Customer (CSC) and Cloud Service Provider (CSP) is clearly understood. When the CSC does their due care and due diligence before contracting with a potential CSP, it will help alleviate assumptions and misunderstandings. It will also help identify the distinction between CSP and CSC of liability. One could argue that knowing what the CSP is NOT responsible is more telling than what they are responsible for.

Having a good understanding of how 'R&R' is divided between CSP and CSC (as described in the 'Shared Responsibility Model') will bring to light that there are many aspects of control that the CSC will not have control. It is generally understood that the CSC is responsible for how access is granted to their application/data for most SaaS implementations. At the same time, the CSP is responsible for everything else (i.e., the SaaS customer cannot mitigate known VM vulnerabilities because it is not under their control). The CSC thereby entrusts most security and maintenance activities to the CSP.

There are functions of the SaaS solution for which the CSC is responsible. The CSC must embrace the challenge, take the time to understand the risk, and then reduce the risk to a commensurate level. Consider the case where a SaaS application accepts a weak TLS cipher (e.g., TLS 1.2). The customer could prohibit using the old version and force the application only to accept TLS 1.3. Another example could be requiring the use of Active Directory to authenticate users.

That being said, the SaaS customer will need a combination of both administrative and technical controls to protect its assets and resources from the security and operational risks that arise from the reliance on the SaaS platform. The table lists controls that the CSC should have in place. Please keep in mind that the actual technical controls will vary by CSP.

Technical Control	Administrative Control
System Application account for security audit/ logging	User/System authorization
Multifactor Authentication (MFA) for privileged accounts	User/system authorization
System monitoring of privileged accounts	Yearly attestation by account owner of all privileged accounts

Technical Control	Administrative Control
Identity and Access Management (IAM) Tool for all accounts	Identified ownership of encryption keys
Secured repository of encryption keys, digital certificates, etc.	Inventory tracking of all CC resources/assets
Secure communication channel (e.g., HTTPS, SSH, TLS, SFTP)	Approvals from Network/Architectural team
A single "pane of glass" into all cloud resources/assets (e.g., SIEM, log integration)	• User authorization • Metrics • Compliance reporting
Vulnerability Management Patch Management Remediation/Fixes	Classification of vulnerabilities Notification of vulnerability
Incident Management Tools	Alignment between CSP/CSC on how incidents are identified, communicated and managed
Risk Management Evaluation Tool (which could include): • Vulnerability Scanning • Threat Model • Penetration Test	• Risk Management Approval/Review • Key Risk Indicators • Communicate findings to relevant stakeholders • Knowledge transfer

Note: Please refer to CSA's Enterprise Architecture – CCM Shared Responsibility Model for a detailed listing of shared responsibilities between CSC and CSP.

4.1.2 Segregation of Duties

Controls must be in place to enforce the security principle of Segregation of Duties (SoD). In its simplest terms, Segregation of Duties assures that critical tasks require two or more persons/entities to be completed; the objective is to prevent fraud/collusion.

If one were to refer to the NIST 800-145 definition of 'Cloud Computing,' it lists "on-demand self-service" as an essential cloud characteristic. "On-demand self-service" means "a consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction." In other words, the 'on-demand self-service' cloud characteristic allows the CC to spin up cloud resources and assets very rapidly and easily without requiring much technical expertise from the end user. This also means enforcing SoD can become very complex and out of control very easily.

Cloud resources created/spun up by the user or application can come in various forms (such as user/system/application account IDs, roles, and groups). The customer must understand what those resources can access (inside/outside the cloud perimeter), the privileges associated with those IDs, and then take appropriate measures to ensure those accounts have the minimum level of privileges to perform certain tasks. Failure to do so could lead to the possibility of an account having access to resources for which it was not intended. Risks associated with not having SoD controls are unauthorized disclosure of confidential/privacy information, data loss, loss of integrity, and so on.

4.1.3 Contact with Authorities

Even though the CSP may own the majority of tasks associated with maintaining the Cloud solution, the CSC is still accountable for everything that happens in the cloud. This is because the CSC agreed to the 'Terms & Conditions', services provided, and limitations provided by the CSP when they signed the contract.

The CSC should have a documented process that identifies key stakeholders to be notified in the event of an incident or change in SLA/OLA (Service Level Agreement/Operating Level Agreement). The CSC shares this with the CSP, so they know whom to contact (in an incident). These stakeholders should be keenly aware of their business objectives/deliverables and compliance/regulatory requirements.

4.1.4 Contact with Special Interest Groups

Risks to cloud security can change by the day and are almost impossible to keep track of. It is highly recommended that an organization identify specific personnel/teams tasked with establishing/maintaining contact with special interest groups. These special interest groups typically keep track of new or 'zero day' vulnerabilities, and they may also share possible fixes to some of these vulnerabilities. Having a relationship with special interest groups could save a company time (when it comes time to discover a fix). Another benefit is that a company can pick the particular interest group most relevant to their needs (e.g., by industry, technology, regulation). Finally, these special interest groups can also provide the latest information related to emerging trends, privacy, threats, vulnerabilities, and remediation.

4.2 Mobile Devices and Teleworking

4.2.1 Mobile Device Policy

COVID-19 has had an impact that no one could have predicted. Numerous companies had to scramble to offer work-from-home solutions to keep their operations running.

The SaaS service provides mobile device access through a web frontend catered to mobile devices or a SaaS service-specific application installed on mobile devices. Such devices could be in the form of personal/corporate-issued laptops, personal/corporate-issued cell phones, or tablets. No one knows for sure if there will be a return to normal pre-COVID. Therefore, policies, procedures, and guidelines must be developed to facilitate secure continuous operations.

The CSC must identify risk(s) associated with allowing mobile devices to access corporate resources. Below is a sample of areas that should be considered:

- Who can access corporate resources?
- Does access extend to only internal employees, or can contractors and third-party suppliers have access?
- What corporate resources can be accessible by everyone?
- What corporate resources should be restricted to contractors/third-party suppliers?
- How should access be granted–VPN, soft token, MFA?
- Should personal devices be allowed to access corporate resources?
- If personal devices are allowed, how can we ensure corporate resources are protected from malware, phishing, spoofing attacks, and so on?
- Once an employee/contractor is granted access, how can we ensure they can only access resources for which they were given explicit permissions?
- How should access be monitored/logged?
- How do we ensure company confidential/secret information is not stolen/transferred offsite (or to an unauthorized person or competitor)?
- If an employee decides to leave the company, what measures should be in place to ensure our company data does not leave with that employee?

Aside from the technical controls that the CSC must consider, below are some administrative controls to consider as well (non-exhaustive):

- Security Awareness training
- Acceptable Use Policy
- Data Classification Standard/Policy
- Handling of Confidential/Secret Data
- Media handling
- Use of removable media
- Encryption (of company-issued devices)
- Physical controls (for company-issued devices)
- Data retention/destruction

5. Asset Management

To benefit from a SaaS service, the SaaS customer would need to provide certain data to be processed on the SaaS service. Therefore, management of data is extremely important for a SaaS customer.

5.1 Responsibility for Assets

5.1.1 Inventory of Assets

A SaaS customer should be able to answer the following questions:

- What data will be transferred to the SaaS service?
- How will the data be transferred?
- What data will the SaaS service have access to?
- What is our reliance on the SaaS service for our data?
- Are there any geolocation requirements for the data, such as regulatory or client service requirements?
- How many SaaS applications are being used in the organization as a whole; is there shadow SaaS?
- Can the CSC identify resources that are no longer being used? Having unused (but active) resources available can quickly add up one's operational expenditures.
- Can the CSC readily identify all cloud-hosted resources? The CSC should also have a corporate, centralized repository that documents ownership and responsibility for the asset. Also, the CSC should develop a corporate-wide tagging policy and schema. Tagging allows the CSC to facilitate accurate tracking of cloud-hosted resources and can support corporate security governance initiatives because it allows one to categorize cloud resources by geo-location, sensitivity, legal mandates, cost optimization as well as other numerous attributes.

5.1.2 Discovery of Assets

A process and ideally a solution should be in place to continually discover and identify the usage of SaaS by users in the organization. This can be achieved one of four different ways.

- Through a procedural methods in which all potential purchase and acquisition of SaaS is brought to IT and security prior to use
- Through the analysis and evaluation of logs from firewalls, web gateways, and CASBs
- Through the usage of a SaaS Security Posture Management solutions
- Through the analysis of expense reports and financial records for line items relating to SaaS

5.1.3 Ownership of Assets

A SaaS customer should be able to answer the following questions:

> - Who is responsible for what data is located on the SaaS service?
> - Who is the SaaS administrator?

5.1.4 Acceptable Use of Assets

There are two parts to this:

> - What is the SaaS provider allowed to do with our data? Metadata?
> - What are our users allowed to do with data on the SaaS service?

Data and metadata control: ownership, processing, licensing.

6. Access Control

6.1 Business Requirements of Access Control

6.1.1 Access Control Policy

- Evaluate whether a person needs access to resources
- Identify business requirements and role
- Information clearance based on data classification
- Approval by security review and data owner (sponsor)

Users in organizations are typically granted access to applications based on historical events or by cloning the access rights of their peers.

Therefore it is important to evaluate whether a person genuinely needs access to a service and to identify the business requirements and establish roles.

6.2 User Access Management

Properly managing and architecturing Identity and Access Management (IAM) is essential to protect cloud resources. When onboarding a platform it is essential to think on security and business requirements so that proper user grouping, segregations and required privileges are being assigned to users as per their job role or business requirement. Having proper IAM practices would enforce least privileges and segregation of duties.

6.2.1 User Registration and Deregistration

6.2.1.1 User access provisioning

- User training on best practices
- Awareness of acceptable use, relevant policies, and procedures
- Create an account according to user access baseline
- Should be part of the overall joiners, movers, and leavers process
- Adhere to least privilege by leveraging role-based access whenever feasible
- Billing party: group or sponsor based on usage?
- Identify and set resource limits

Always follow the concept of least privilege and identify and set resource limits.

6.2.2 Management of Privileged Access Rights

- Justification should be sought for privileged access to ensure it is required.
- Consider the use of just-in-time access, elevating privileges only when required, and reverting back to non-privileged access
- The number of users who require privileged access should be kept to a minimum

6.2.3 Management of Secret Authentication Information

- Break glass access should only be used for very specific purposes, and credentials stored with the appropriate level of security e.g. Kay Vault

6.2.4 Review of User Access Rights

- Access rights should be regularly reviewed to ensure appropriateness, in line with changes in the business

6.2.5 Removal or Adjustment of Access Rights

- Ensure immediate account termination
- Halt's resource billing related to accounts
- Audit logs and access logs must be kept in line with business policy
- Security review if necessary
- Update account termination logs and inventory

Ensure audit logs are reviewed and retained, in line with security policy.

And finally, ensure billing is halted when resources are no longer used. Do this in an automated fashion and try to eliminate any manual actions.

6.2.6 Monitoring of User Access

- Set monitoring alerts based on the basic usage profile
- Alert on suspicious login (e.g., location, time) and data access (e.g., batch access)
- Adherence to password policies
- Data loss prevention monitoring
- Set up alerts and monitor suspicious behavior and logins differentiating external/contractor activity from internal employees activities
- Leverage API-based solutions to monitor Data at rest

6.3 System and Application Access Control

6.3.1 Information Access Restriction

- Information stored in the SaaS application should only be accessible by authenticated users from approved devices that adhere to business security policies of the SaaS consumer. If this is not feasible given the nature of the application (e.g. collaboration application with external, there are other solutions like Reverse Proxy which may be helpful in providing the required granular access control.

> - API based solutions can be leveraged for securing data at rest and enforcing appropriate sharing and DLP policies (i.e., any document with PII if shared with an external domain will automatically revert to access to internal users only). Given that the SaaS application is available over the public internet, where possible the scope of access should be limited to only approved IP ranges/locations
> - Should information held in the SaaS application require downloading (once accessed), appropriate security controls should be deployed, to ensure that the information is being downloaded to an approved device that adheres to business security policies.
> - It is important to be able to distinguish between sanctioned and unsanctioned instances of the SaaS applications and apply the usage policies accordingly.
> - Any API-based access to any third party needs to be approved only after appropriate checks and revoked once the business requirement is met.
> - Should the SaaS provider need to access SaaS consumer data, they should be notified, and evaluate the request, and have the ability to approve/deny the request.

6.3.2 Secure Log-on Procedures

> - Basic authentication should not be enabled, this is inherently insecure.
> - Where possible, the SaaS application should use the Identity Provider (IdP) of the business, enabling Single Sign-On (SSO) to securely log on
> - Where SSO is not possible, the SaaS application should enforce passwords to be complex and undisclosed (i.e., validate against https://haveibeenpwned.com/). This password should not be the same as the corporate password.
> - Given that the SaaS application is available over the public internet, to ensure the user is who they claim to be, multifactor authentication should be deployed
> - Users should only log onto the SaaS application from approved devices that adhere to business security policies
> - If secure log-on fails, any password reset procedure should be self-service

6.3.3 Password Management System

> - Where possible, the SaaS application should not have to manage passwords, and leverage the business iDP instead to authenticate users through SSO
> - Where local authentication is used, passwords should follow guidelines set out by OWASP

Passwords should also be stored in a Key Vault or similar security device to protect confidentiality, integrity, and availability.

Please keep in mind that a password is a ‘credential’. For the sake of this discussion, ‘credentials’ can come in the form of encryption keys, digital certificates, and/or tokens. If the CSC cannot manage their keys, then it is highly advisable that they utilize a Key Vault or similar security solution to enforce confidentiality, integrity, and availability.

6.3.4 Use of Privileged Utility Programs/Third-Party Plugins

- Basic authentication should not be allowed programmatically
- Identity of the caller should be verified via mTLS
- Token-based authentication (OAuth 2.0) flows are preferred
- SaaS API should only be available across specified IP ranges
- Establish Secure Vault and store privileged credentials in an encrypted format
- API's keys should be stored securely, and only transmitted over HTTPS
- The SaaS Application should have the capability to revoke access keys and token grants
- Identities used for privileged program access should be regularly reviewed
- Review consent granted by users to third-party apps
- Monitor activity made by third-party apps

6.3.5 Access Control to Program Source Code

- Access to source code should be restricted the SaaS provider
- Access control for development pipelines/environments that produce the source code should also be restricted to the SaaS provider
- The source code should not provide backdoor access to other programs or systems which are not in the control of the SaaS provider or part of the provision to the SaaS consumer
- Any source code created by the SaaS consumer should only be accessible by them, along with any backups created
- The CSC should document a process that describes what security gates are to be implemented, as well as which event(s) would trigger a security review when using a CI/CD pipeline. A security gate is a security policy that assesses the security risks of software code. All software code must be reviewed and approved before the software is moved to the next phase

7. Encryption and Key Management

7.1 Security of Data in SaaS Environments

One of the most critical aspects to consider when using SaaS services is the security of the data being stored within that service. In this operating model, the vendor takes on much of the responsibility for the application's security. However as recognized by the Shared Responsibility Model, data is the responsibility of the cloud consumer.

To ensure that data is secure while being transferred to and stored with the SaaS provider, encryption of the data, and the management of the encryption keys therein, is an area that customers should be considering when engaging these vendors. Any time data is moved from a secure internal location, there is a risk to the customer organization of accidental or malicious exposure of said data. Ensuring proper encryption and key management means that even if improper access to the data did occur, it would be unusable without first decrypting it.

This section reviews the steps a customer organization can take to ensure that data stored with SaaS providers are adequately encrypted using well-managed encryption keys.

7.1.1 Shared Responsibility Model

While using a SaaS service shifts some of the responsibilities for managing and maintaining applications from the customer organization to the vendor, some responsibilities will remain with the customer. These responsibilities include the governance and security of the data in the SaaS service and access models therein.

	Responsibility	SaaS	PaaS	IaaS	On-Prem
Responsibility always retained by the customer	**Information and data**	🔵	🔵	🔵	🔵
	Devices (Mobile and PCs)	🔵	🔵	🔵	🔵
	Accounts and identities	🔵	🔵	🔵	🔵
Responsibility varies by type	**Identity and directory infrastructure**	🟠🔵	🟠🔵	🔵	🔵
	Applications	🟠	🟠🔵	🔵	🔵
	Network controls	🟠	🟠🔵	🔵	🔵
	Operating system	🟠	🟠	🔵	🔵
Responsibility transfers to cloud provider	**Physical hosts**	🟠	🟠	🟠	🔵
	Physical network	🟠	🟠	🟠	🔵
	Physical datacenter	🟠	🟠	🟠	🔵

🟠 Microsoft is responsible 🔵 Customer is responsible 🟠🔵 Shared responsibility

7.2 Encrypting Data Shared with SaaS Providers

As noted above, any time data is moved from a secure internal location, there is a risk of accidental or malicious exposure. Possibly the best way of mitigating this risk is to ensure the encryption of data as it's transmitted to or from the SaaS provider, as well as while stored in the SaaS provider's systems. This includes ensuring proper encryption within the application and physical resources, which are SaaS providers' responsibilities.

7.2.1 Questions and Areas to Consider

The level of encryption needed and the locations where it is needed depends on understanding the data being transferred and the SaaS provider's practices. Below are some questions that should be considered when determining the level of protection your data needs.

7.2.1.1 Questions for Vendor

- Does the vendor offer granular controls for sharing data (e.g., share only internally, share with select partners, share with everyone, etc.)
- Does the SaaS provider offer encryption of data while in-transit?
- Does the SaaS provider offer encryption of data while at-rest?
- Does the SaaS provider support end-to-end encryption?
- What encryption algorithms and transport protocols does the SaaS provider support?
- Does the SaaS provider offer unique encryption keys per customer (single-tenancy)?
- Does the SaaS provider have documentation on their key management procedures?
- Does the SaaS provider allow the use of customer-managed encryption keys?
- Does the SaaS provider have a capability to identify and/or mask sensitive data?
- Does the SaaS provider allow pseudonymisation or redact when production data is needed to be replicated to a sandbox environment?
- Does the SaaS provider provide a mechanism for users to tag sensitive data or fields?

7.2.1.2 Internal Questions

- Does the data being uploaded to the SaaS provider include any sensitive details?
  - Sensitive data can include things like Personally Identifiable Information (PII) or other elements defined by your data privacy and compliance needs.
- What is the impact to the customer organization should the data become exposed?
- Do you feel confident in your organization's key management practices?
- Does the internal process support end-to-end encryption?

7.2.2 Encryption In-Transit

Data is considered 'in-transit' when it moves from one location to another, and this includes data being transferred from the customer organization to the SaaS provider or vice versa. Data security is at its strongest when multiple inter-operable layers are configured; thus, while data is in-transit, security is typically considered lower as fewer layers are available to protect the data.

To secure data while in-transit, it's recommended to ensure the usage of secure cryptographic network protocols in all data transfers. When writing, the best cryptographic network protocols to use are Transport Layer Security (TLS) version 1.2 or higher (with a preference on TLS 1.3). At a high level, the TLS protocol uses a combination of symmetric encryption (where the same key is used to encrypt and decrypt the data) and asymmetric encryption (where a mathematically related public and private key are used to encrypt and decrypt the data). This combination of encryption methods enhances the confidentiality and integrity of the data being transmitted.

The use of TLS 1.3 removes some steps from TLS 1.2 for performance without sacrificing security aspects. The TLS handshake and key exchange processes for TLS 1.2 and 1.3 operate as in the examples:

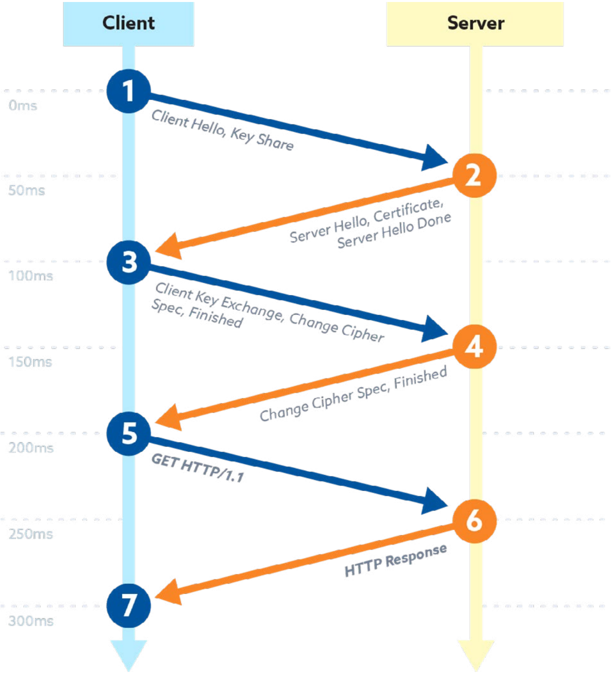
Client
Server
0ms
50ms
100ms
150ms
200ms
250ms
300ms
1
Client Hello, Key Share
2
Server Hello, Certificate, Server Hello Done
3
Client Key Exchange, Change Cipher Spec, Finished
4
Change Cipher Spec, Finished
5
GET HTTP/1.1
6
HTTP Response
7

Figure 3. TLS 1.2 (Full Handshake)

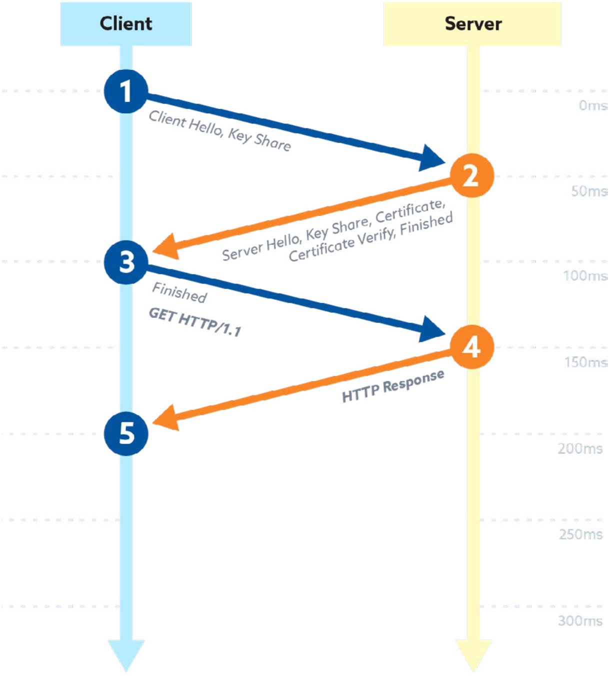

Figure 4. TLS 1.3 (Full Handshake)

7.2.3 Encryption At-Rest

Data is considered 'at-rest' if it's not moving within an application, network, or system. If not adequately protected, during this 'at-rest' period, an attacker with improper access to the SaaS provider's hosting facility can expose the data publicly or use it for profit. Encrypting this data while at-rest ensures that it cannot be used even if the hardware storing the data is stolen.

Data can also be encrypted in the application itself, ensuring only the SaaS consumer is able to see their data (as they are the only ones that can decrypt it), providing a boundary in a multi-tenanted SaaS provider environment.

The type and strength of the encryption depend on the data classification. If the stored data is considered public, it may not require as stringent encryption as data that is classified as sensitive. As such, the customer organization should review the following aspects before storing data with the SaaS provider:

> - Business Impact Analysis (BIA) for exposure of data
>   - To determine if data needs to be encrypted at rest, the organization should perform a BIA to understand the impact should that data become public.
>   - Additionally, other security components from the CSP, such as access management, should be considered to determine the risk of data exposure.
> - Availability of encryption at-rest services
>   - Not all SaaS providers will offer encryption of data at-rest as a free service. Understand what licensing model is required to receive encryption at-rest.
> - Availability of encryption of backup data at-rest
>   - While many SaaS providers will offer a form of encryption at-rest, this does not always apply to data backups. Ensure that the actively stored data and all backups are encrypted while at-rest.
> - The use of full-disk vs. file-based encryption methods
>   - Understand the type of at-rest encryption offered. For example, using a full-disk method, while a reasonable control, is primarily used to provide protection when a disk or system is stolen.
>   - As a far more common scenario, the use of file-based encryption will protect individual files and data from being stolen in the case of inappropriate access.
> - The encryption algorithm and key-length used to encrypt data-at-rest
>   - Ensure the encryption method for data-at-rest and meets the CSC's needs. NIST 800-57 Part 1: Recommendation for Key Management (Table 2 for reference) details encryption strength based on the algorithm and key length.

7.3 Customer-Managed vs. Vendor-Managed Encryption Keys

Generally, it is more secure to use customer-managed encryption keys than those provided by the vendor. However, whether or not to use vendor-managed encryption keys depends on two factors. First, does the vendor allow the use of customer-managed keys? Not all vendors provide the capability to use your encryption keys. Second, does the data stored with the vendor warrant the level of risk mitigation provided by using your keys, or is the risk of using vendor-managed keys acceptable?

As an example, the level of risk from using vendor-managed encryption keys can depend on answers to the below questions:

> - Does the vendor provide info on how encryption keys are created and managed?
>   - In most scenarios, vendors will not share the details behind the creation and lifecycle management of encryption keys within their environment.
>   - To gain a level of comfort with the vendor's key creation and management practices, it's recommended to request documentation on how data is encrypted in-transit and in-use in their systems.
> - How sensitive is the data being stored within the vendor's systems?
>   - For example, data classified as public may result in little to no risk in using their encryption keys.

- Does your organization have a good encryption key management practice?
  - In addition to the security of the vendor, the protection afforded through key management also relies on your organization's capability to protect key material. If your organization is immature in its practices as compared to the vendor, it may be in your best interest to use the vendor-managed keys.

7.4 The Future State of Encryption and Key Management

Areas for future consideration:

- Hardware Security Module as a Service (HSMaaS)
  - Sometimes also known as 'Cloud HSM', this is a method of creating and managing cryptographic keys through a SaaS-provided HSM offering.
  - Still growing in popularity, but FIPS validated HSMaaS providers such as Fortanix, Microsoft, and others are increasing in usage.
- Privacy-Enhancing Cryptography (PEC) methods
  - A set of techniques that are used to minimize the amount of personal or sensitive data collected by systems while still maintaining functionality.
  - In an effort to maintain generalized services, SaaS providers may not support the use of PEC techniques as they require more customization and interaction with user systems to achieve results.
  - NIST has provided blog posts and a project to review PEC techniques, as well as to create standards and requirements around them.
- Homomorphic Encryption
  - Involves encryption of data while in-use while still allowing operations on the data through a bit-level encryption/decryption. Very slow compared to traditional methods.
  - Documentation for requirements on PEC methods, including homomorphic encryption, are still in development by organizations such as ISO and NIST with leadership through an open consortium.
- 'Confidential Computing' or secure enclaves
  - The use of hardware-enabled features to secure cloud data while in-use by isolating and processing the data from other concurrent workloads.
  - NIST has draft documentation available providing further information on confidential computing technologies for cloud and edge computing.
- Post-Quantum Cryptography (PQC) methods
  - Likely still 8+ years out at least
  - The NIST Internal Report (IR) 8105 from 2016 called out that quantum computers capable of breaking 2,000 bit RSA in a matter of hours could exist by 2030.
  - NIST, and other organizations, have projects and efforts underway to create standards for post-quantum encryption with some having public calls for submissions and feedback.

8. Operations Security

8.1 Operational Procedures and Responsibilities

8.1.1 Documented Operating Procedures

The flexibility of SaaS products make it necessary to have an understanding of how such products will be used by the organization.

> - Access Control - see Access Control section
> - Change Management
> - Capacity Management
> - Separation of Environments
> - Termination - see Termination section

8.1.2 Change Management

Adding a SaaS product should be thoughtfully considered. The ease with which such products can be added to an organization's ecosystem can cause issues. Therefore, strong change management processes should be put into place. Changes to SaaS products tend to be small and occur frequently. Often, the changes may not be noticeable to the user. However, downstream systems may be affected.

It is important to identify if changes affect the security posture of the organization. Such changes may require the organization to revise other systems. Significant changes, usually, version changes, need to be reviewed and included as part of the change management processes.

Additionally, SaaS products are often considered for use under a specific operating scope. Later changes to the SaaS applications' business function, growth in usage, or change in the complexity of use can lead to a need to revisit the security considerations attached to the use of the SaaS application. It is recommended that administrators review the use of SaaS applications on a regular basis to ensure that the scope of the initial security review matches the current scope of use. This will ensure an up-to-date security model of the SaaS application is maintained.

8.1.3 Capacity Management

The use of SaaS products may have licensing limits on the number of users. Monitoring products may also limit the number of accounts that are overseen or attached. There may be pricing differences based on the number of users or accounts. Consideration needs to be taken to understand needs prior to increases in capacity.

8.1.4 Separation of Development, Testing, and Operational Environments

As with internally developed systems, separation of environments are necessary to prevent production data from leaking out of production-approved systems. SaaS vendors are expected to continually improve their systems. Improvement, upgrades, or updates should be tested in non-production environments with non-production data. SaaS vendors should provide an attestation that, not only, separate environments exist, but also that non-production data resides in these environments.

Additionally, the configuration of these SaaS applications should be continuously evaluated to ensure that a secure environment is being maintained. Identifying misconfigurations in security settings and data access across users and third-party integrations mitigates the risk of a data leak occurring. In environments that support a 'staging to product' workflow, reviews should be conducted in staging environments so as to identify security issues before they impact production environments.

8.2 Protection from Malware

8.2.1 Controls Against Malware

The majority of the responsibility for malware protection rests with the SaaS provider, however, some vectors for malware distribution still exist under the control of the SaaS user/administrator. Examples of these user-controlled vectors include customizable static-file hosting and attachments, which may be uploaded by either employee of the organization using the SaaS application/privileges users, or by the general public if the SaaS application is providing a public-facing portal.

SaaS administrators and their security organizations should conduct typical threat modeling exercises to understand what, if any, content upload capabilities exist in the public-facing functions of their SaaS deployments. Be on the lookout for public-facing content or document upload systems that are intended to store or transmit files that internal or privileged users of the SaaS application will download on corporate devices or otherwise review.

When evaluating their SaaS deployments and configurations, customers should become familiar with the built-in capabilities of the SaaS platforms. Many come with standardized malware and virus scanning capabilities that will flag or block potentially malicious uploads. The configuration of SaaS systems should be evaluated and monitored to (1) minimize the types and amount of externally-controlled content that can be uploaded and (2) ensure that built-in protections and filetype limitations are enabled.

8.3 Backup and High Availability

8.3.1 Information Backup

In most SaaS applications, responsibility for managing data backup, redundancy, and failover in the case of infrastructure or application-layer failures falls on the SaaS provider. This is the logical assignment of responsibility as the SaaS customer will not have direct database access, the ability to create failover instances/replicas, and so on.- The customer's access to data will generally be limited to supported APIs from the SaaS platform, which is a generally inefficient way to create and manage data backups. In the event of a catastrophic data loss event, the SaaS platform provider will be responsible for restoring data. For this reason, information backup is not as critical a consideration when managing SaaS deployments as it would be for IaaS or other deployments where the customer controls the deployment at a lower level.

That said, there are still information backup concerns that SaaS customers should consider. In the event of inadvertent or malicious data deletion that falls within the expected/allowable use parameters of a SaaS application (i.e., a malicious actor deleting data and/or records using supported deletion processes, API endpoints, etc.) the SaaS provider would not be responsible for providing and restoring from backups. As a rule of thumb when managing SaaS applications as a customer. If the platform is operating as designed, even if your configuration was insecure or incorrect, it will not be the SaaS provider's responsibility to remediate an issue.

To mitigate such risks as a SaaS customer, it is first critical to deploy continuous configuration and data access monitoring that can help ensure inadvertent or overly permissive access is not granted to any user that could cause a data loss event. This may include managing data access such that users are properly granted least privilege as well as monitoring system configurations to ensure that soft-deletion/data retention settings allow easy recovery of data. Finally, SaaS customers should consider whether additional, off-platform API-based data backup solutions will provide additional redundancy for critical data if the SaaS provider does not already offer "rollback" or "backup" solutions on platform.

Along with backing up data, the CSC should implement a snapshot strategy. NIST Standard 800-125 defines a snapshot as *"... a record of the state of a running image, generally captured as the differences between an image and the current state. For example, a snapshot would record changes within virtual storage, virtual memory, network connections, and other state-related data. Snapshots allow the guest OS to be suspended and subsequently resumed without having to shut down or reboot the guest OS. Many, but not all, virtualization systems can take snapshots."* A benefit of snapshots is that they can be used to restore an image/data quicker than performing a restore from a backup.

8.3.1.1 High Availability

Many SaaS providers have SLAs and OLAs defined in their contract with the SaaS customer, often backed by service credits, should they not be able to meet the contractual requirement. That said, the SaaS customer may have an option to choose the different redundancy options, given their requirements of the SaaS application. It should not be assumed that just because it is SaaS, it will always be available, and available options should be explored, taking into consideration the business impact on an availability issue with the SaaS application.

8.4 Logging and Monitoring

8.4.1 Event Logging

Event and access logging for SaaS deployments present a markedly different set of challenges when compared to more traditional logging considerations security teams may be used to from Infrastructure, IaaS, PaaS, or Application logging. From the point of view of a security organization that is consuming SaaS application logging, significant limitations exist due to the fact that the security organization will not have access to the underlying logs of the hardware or software running the SaaS application. Security teams monitoring usage and management of SaaS applications are, by definition, limited to consuming logs that are made available to them by the SaaS provider.

In rare cases, more verbose and/or more raw (closer to the application source) logs may be available for an additional cost from the SaaS provider via a manual request process, but due to the lag time, process cost, and financial cost involved with such options, they cannot reasonably be considered part of a best practice SaaS log monitoring program.

Adding to the complexity for security organizations monitoring SaaS application security, there is no industry standard, accepted format for SaaS application log output. A common action like a user login may look markedly different in terms of log message format and content between different SaaS applications, presenting challenges to the security organization that wishes to correlate logs and activity across SaaS applications.

Timeliness of log delivery can also present challenges to security organizations hoping to use SaaS event logs as a means of incident detection. Log entries will not be available to the SaaS application user until after they have been processed by the SaaS provider and made available in an API or other delivery facility for automated end-user access. Depending on the SaaS provider, the stated SLA from event occurrence to event log availability can be anywhere from a few minutes to 24 hours.

These complexities present challenges to using SaaS event logs as the only mechanism for monitoring the security and activity in a SaaS application, but by no means remove the value of monitoring SaaS event logs as part of a holistic SaaS security solution. Security organizations consuming SaaS event logs should ensure the following capabilities are developed or deployed:

- The retrieval of SaaS logs from the SaaS application/provider should be automated at a high frequency

- SaaS logs should first be normalized to a common format across SaaS applications before being delivered to a SIEM or other log storage solution. This allows security teams to effectively monitor activity across SaaS applications
- Event, audit, activity, and other log entries that include user information such as usernames or User IDs should be normalized to a corporate identity such that events by the same person in different usernames/user accounts in varied SaaS applications can be correlated
- The expected, average, and maximum delay between action and log entry availability for each SaaS application should be documented and understood by security operations teams who will be using the log system

8.4.2 Protection of Log Information

8.4.2.1 Administrator and operator logs

Many SaaS applications, especially those with significant complexity, have a separate logging or auditing facility to monitor system-level configuration changes made by highly privileged users. This system may be called an "Audit Trail," "Setup Log," or similar. In many cases, this will be a logically separate data structure than the standard access and event logs, and may require a different API or access method to retrieve.

These logs are critical to access as part of a SaaS event monitoring program as they represent privileged, authenticated actions that may materially impact the security posture of the SaaS application. All of the best practices outlined in the "Event Logging" section of this document should be followed for this subset of logs.

Additionally, security teams monitoring SaaS applications should familiarize themselves with the action types that would be most concerning in this set of logs and consider deploying security automation technology that can monitor these logs and alert security teams to security-impacting changes made by privileged users (i.e., SaaS administrators). Monitoring for these pre-defined 'high risk' activities across the SaaS ecosystem is intended to reduce the meantime to detection, which can help reduce the damage associated with a SaaS data leak.

8.5 Technical Vulnerability Management

Identify SaaS application owners, and bridge these owners to a security function. In most organizations, SaaS security falls into the responsibility of the enterprise security silo. However, some organizations define SaaS security as application security or third-party risk issues. No matter who owns this responsibility, it is critical to identify the owners of the SaaS applications, understand the business use case of each SaaS application, and then define responsibilities for vulnerability management.

Controlling security across SaaS applications can be a significant challenge. For example, a SaaS customer may not be able to mitigate known vulnerabilities of a SaaS application if the issue occurs within the SaaS providers' infrastructure. However, the predominant majority of SaaS security issues (and cloud security issues for that matter) occur within the confines of the customer's shared responsibility. These shared responsibilities include managing settings and configurations of the SaaS application to ensure they fall in line with security best practices. Reviewing the configurations against policies mirrored to standards like NIST CSF, ISO 27001, or NIST 800-53 is a strong practice to reduce the risk of a non-compliant or insecurely configured environment.

Consider the case when a SaaS application accepts a weak TLS cipher. The customer's policy could enforce all its users to use a more resilient cipher on connections to this SaaS, thereby mitigating this vulnerability until it is ultimately resolved. Additionally, consider a scenario where an administrator has turned a critical security protection mechanism off (like xss protection) in order to provide their users a more seamless experience. In this scenario, the administrator should be alerted by a continuous monitoring mechanism of this misconfiguration, and remediate the issue.

8.5.1 Management of Technical Vulnerabilities

SaaS security is only improved most effectively through cross-functional collaboration across IT application owners, enterprise security teams, and technology leadership. IT application owners must own the remediation of the issue, while security must own the triage and follow up to ensure remediation occurs within the unique SLA's agreed upon within the organization. It is critical that the organization align to the company's accepted SLA's and follow them as with any other security domain.

As detailed in the Cloud Security Alliance blog post "Building a SaaS Security Program: A Quick Start Guide", "understanding which SaaS applications belong to which teams is important because once you've identified the issues, you'll need to chat with the correct business app team to fix them. It's inevitable that some of your most pressing security issues may exist in business-critical SaaS workflows.

As a result, your triage team will need to act quickly to inventory all security vulnerabilities, map them to owners, and make severity-based decisions about the risk of each finding so they can fix the issues that matter most first."

8.6 Information Systems Audit Considerations

8.6.1 Information Systems Audit Controls

A SaaS provider may not be under the customer's information systems audit controls. However, a customer is required (usually by regulation) to have the assurance that the SaaS provider has acceptable controls in place. This may be through a self-attestation or a third-party attestation.

Though self-attestation may be the minimum required review by law, it is also the least reliable method of understanding if security controls in place are operating effectively. Similarly, it is vital that diligent reviews of third-party reviews are read thoroughly, with a keen focus on the:

- Scope of the assessment - The reader may glean that there are fourth parties engaged, who are not included in the scope of the assessment, including additional IaaS, PaaS, SaaS, or other 4th-party solutions. If this is the case, it will be material to understand the Vendor Management/Third-Party Risk policies, inventory, and scope and depth of assessments conducted.
- Testing and reporting methodology - The choice to forego onsite reviews and choosing to rely on a third-party assessment (ISO27001, SOC2 Type II) should be considered and evaluated by a skilled and thorough reviewer, preferably with industry-recognized credentials, and ideally with solid experience implementing defense-in-depth strategies.
    - The third-party assessment should give the reader confidence that SaaS technology and security personnel were interviewed, documents were read, and samples were gathered and tested.
    - The expertise of the assessor may also be inferred in the reporting language. A simple restatement of the control language with "no exceptions noted" coupled with a non-existent or lackadaisical testing methodology should be discarded.

This may be accomplished by including clauses in contracts requiring the SaaS provider to follow specific acceptable standards (e.g., CSA's CCM, FedRamp, NIST, ISO) and providing an attestation to those standards and regular review of artifacts demonstrating the efficacy of the control.

Cloud Security Alliance provides auditing guidelines based on Cloud Controls Matrix (CCM) version 4. These guidelines are intended to facilitate and guide a CCM audit. Auditors are provided with a set of assessment guidelines per CCMv4.0 control specification with an objective to improve the controls' implementation auditability and help organizations to more efficiently achieve compliance. These guidelines are neither exhaustive nor prescriptive in nature. They represent a generic guide in form of recommendations for assessment. Auditors will need to customize the descriptions, procedures, risks, controls, and documentation and tailor these to the audit work programs for the organization and service(s) in the scope of the assessment, in order to address the specific objectives of an audit.

9. Network Security Management

Governance of network security or controls related to data flow security within the context of consumption of SaaS services has been broken down into two distinct domains; Controls owned and operated by the SaaS provider and controls that a SaaS consumer may need to consider.

The critical network controls across both domains may be summarized as encryption of data in transit, authorization to specified resources, and data transfer control.

The Zero Trust Network Access and Secure Access Service Edge approach to network security are covered here.

9.1 SaaS Provider Network Controls

Service consumers should confirm with the SaaS provider that valid TLS certificates are utilized for external connections and the internal protection of microservices. The Certificate should be from a well-known, trusted Certificate Authority, and not self-signed.

In addition, the service consumer should seek to confirm the extent that encryption is utilized between discrete service components within the SaaS platform.

SaaS providers may control network data flow through Zero Trust Network Access policies on a least privileged basis. SaaS providers may utilize network flow anomaly detection capabilities as a detective control.

9.2 SaaS Consumer Network Controls

Service consumers should consider the following network security controls when evaluating the security posture and risks associated with a SaaS provider.

As connections to SaaS providers may traverse the public internet, protecting data in transit via encryption such as TLS 1.2+ is critical security control.

Access to SaaS services may create opportunities for a bad actor to undertake data exfiltration by uploading data to an account uncontrolled by the SaaS consumer. Using Cloud Access Security Brokers (CASB) and tenancy channel authentication controls to control this risk.

Data Loss Prevention (DLP) controls should also be considered; these may be deployed at the network, or other layers, depending on access to payload data.

Service consumers should consider availability requirements when architecting network connectivity with SaaS providers, for example, redundant internet circuits and capacity planning.

SaaS consumers should consider controlling DNS traffic with Protective DNS (often a SaaS-based service).

Modern network architectures may leverage the disaggregation of outbound internet access, resulting in local branch internet breakout. SaaS consumers must consider applying the controls as mentioned above where customers consume SaaS services directly.

A Secure Access Service Edge (SASE) model may facilitate this control posture by acting as a policy enforcement point between the SaaS consumer and provider.

10. Supplier Relationships

10.1 Information Security in Supplier Relationships

SaaS products are almost always built on top of third-party services, including those managed and maintained directly by the supplier as well as fourth-party IaaS, PaaS, and SaaS offerings. Unlike in traditional customer-managed software deployments, it is often difficult for SaaS consumers to understand the complete set of dependencies upon which the product in question relies. Thus, it is critical for those operating SaaS products to build a comprehensive model of the technologies upon which their business operations depend.

As with traditional customer-managed software deployments, developing software bills of material (SBOM) for SaaS offerings, also known as SaaSBOMs, can provide such a model. The existing standard CycloneDX can facilitate the creation of SBOMs that incorporate SaaS components. Evaluation of these representations can allow organizations to identify known vulnerabilities in their technology supply chain and allow for more rapid remediation of them.

In addition to developing and maintaining a real-time picture of the components comprising a given SaaS product, organizations should develop internal risk management policies for using them. Similarly, organizations should negotiate contractual terms with CSPs to ensure the security of the offering. Finally, external certification regimes can assist in risk management analyses and decisions, but organizations using SaaS services should not rely solely upon them.

10.1.1 Information Security Policy for Supplier Relationships

All enterprises relying on others to facilitate any part of their business operations - essentially every company in the modern economy - should have a third-party risk management policy in place. In addition to third parties with which organizations have direct relationships, these external parties will themselves have a network of relationships and dependencies with fourth parties, necessitating a third-party risk management policy.

This policy should address SaaS products in addition to other technologies upon which the organization depends. At a minimum, such a policy should identify a(n):

> - Single accountable role or position within the organization for each relationship with a third party (and all of its inherent fourth party risk).
> - Requirement that this individual provides a written assessment regarding the criticality of the business operations that depend on the third party's product or service, preferably in quantitative terms.
> - Methodology for evaluating the likelihood that an incident will impact such a third party and the impact such an incident will have on the organization's business operations, considering the criticality identified above. This can include, but is not limited to, the use of the following:
>   - External audits and security reviews (see certified assurance section for details)

> - Security scoring/rating vendor tools
> - Direct technical due diligence, including audits conducted by the customer organization, penetration testing, or the use of automated scanning tools against the provider's product or infrastructure
>
> - Established risk threshold, based on the above, which, if the third party exceeds this, will trigger a requirement for remedial action either on the part of the third party (mandated contractually), the organization itself (through some set of compensating controls), or both
> - Single accountable role or position within the organization with the authority to accept risk exceeding the threshold mentioned above, along with a transparent process for documenting and justifying such risk acceptance

10.1.2 Addressing Security Within Supplier Agreements

Agreements with suppliers should require various measures to ensure their SaaS products' secure and reliable operation. SaaS providers can represent organizations of varying sizes and levels of complexity, and their offerings may be of varying levels of importance to the organization. Thus, it may be necessary to tailor agreements to individual suppliers. Such contracts can include:

> - Service level agreements (SLA) for not only the product's availability (also known as "uptime") but also the confidentiality and integrity of the underlying data. For example, to ensure appropriately aligned incentives, an organization might require a vendor to agree to pay a predetermined fee for every record of a particular type exposed or corrupted by a malicious actor.
> - Requirements that the organization undergo - and provide the results of - external verification processes, such as audits, penetration tests, and so on.
> - Requirements to resolve or identify mitigations for vulnerabilities identified by the organization, but in the supplier's products, within a given timeframe based on an objective risk scoring system.
> - Requirements that the supplier notifies the organization within a specific time period if the supplier identifies a vulnerability for which the organization can apply compensating controls to reduce its severity or likelihood of exploitation.
> - Requirements that the supplier cooperates with the organization in investigating and remediating incidents that have impacted or might impact the confidentiality, integrity, or availability of the organization's data.
> - Requirements that supplier notify of new data center locations and right to decline undesirable locations

Organizations negotiating with suppliers should carefully focus their risk management efforts and avoid adding gratuitous terms to contracts. For example, a requirement that the supplier notify an organization of *any* vulnerability identified in its networks, systems, or software would likely lead to a flurry of alerts that will prove essentially useless for driving action.

10.1.2.1 External certifications

External certifications result when a trusted external organization attests that a provider meets specific requirements. Such certifications can assist when making risk assessments of CSPs and can help to clarify what a provider claims regarding its controls versus the actual reality of its security posture. With that said, reviewing external attestations should be a supplement to - not a replacement for - a comprehensive extensive third-party risk management program.

Not all certifications and audit reports are the same, nor do the same report types cover the same scopes. A certification such as ISO/IEC 27001 demonstrates that a CSP has established a baseline for information security management, following a prescribed set of controls.

A SOC 2 attestation, however, is based on the auditor's assessment of the provider's ability to comply with the controls that the provider establishes. Unlike ISO/IEC 27001, however, a SOC 2 report is not a "certification," per se. Given the Trust Services Criteria under examination (chosen by the provider), the auditor will issue one of four types of opinions regarding whether the provider meets the requirements of these criteria. The auditor's report will also note any exceptions identified to the controls the provider has claimed to have implemented. Many vendors will claim they are "SOC 2 compliant," which is not a possible outcome from an audit. In case of you are reviewing a SOC 2 Report, make sure to check:

> - Which TSP criteria (Security, Confidentiality, Availability, Processing integrity and Privacy) was considered.
> - What is the report type
>   - SOC 2 Type 1 - States service organization's system and the design of controls based on TSC. The report describes the current system(s) and controls in place reviews conducted on documents around these controls. Design consideration of all administrative, technical and logical controls are validated for a specific point of time.
>   - SOC 2 Type 2 - States service organization's system has designed and applied relevant controls and whether those controls are effective or not. SOC 2 Type 2 audits are conducted by collecting evidence and analyzing them for a period of a minimum of six months to see if the systems and control in place are functioning as described by the management of the service organization. Usually SOC 2 Type 2 reports are shared with a MNDA.
>   - SOC 3 - This is a publicly shareable report which is similar to SOC2 Type 2 report.
> - Make sure to read the independent auditor's comments section. The auditor would state which areas were non-compliant. This would give an idea on whether the SaaS provider practices what they state on policies and procedures.

Regardless of which report(s) of the CSP you review, *it is vital to pay close attention to the scope and business entity subject to the certification or attestation*. The scope should cover the SaaS services you are considering or using, and the business entity should be that with which you will be signing a contract. For example, some vendors will provide the SOC 2 attestation report for the IaaS provider upon which their service operates, rather than one which reviews their internal controls. While helpful in analyzing the fourth-party risk, such a report is not a replacement for reviewing the provider itself.

Similarly, reviewing the report is necessary to determine whether it covers the entire offering your organization will rely on, not just the data center that houses the application.

Below is a non-comprehensive list of assurance reports, certifications, and attestations that SaaS customers can use when evaluating the security of a CSP:

- Comprehensive
    - American Institute of Certified Public Accountants (AICPA) - SOC 2
    - International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) - 27001
    - HITRUST - Common Security Framework (CSF)
- Government-sponsored
    - United States - FedRAMP
    - Singapore - SS584
    - European Union - General Data Protection Regulation
- Cloud security-focused
    - Cloud Security Alliance - STAR
    - ISO/IEC - 27017
- Financial transaction-focused
    - BSI Kitemark - Secure Digital Transactions
    - Payment Card Industry - DSS
- Privacy-focused
    - ISO/IEC - 27018

11. Incident Management

11.1 Management of Cloud-Homed Information Security Incidents

Many organizations uphold a cloud-first strategy. Although it is often a more business-driven decision, these organizations must be aware that foundational information security processes and procedures must be reviewed, adapted, and adopted accordingly. One of these key documents is the security or cyber incident response (IR) plan. As part of sound security governance, the existing IR process and procedures should be reviewed to incorporate all Cloud Computing Service & Deployment models leveraged by the business.

For more detailed information on cloud incident response and the respective phases, it is strongly recommended to review CSA's Cloud Incident Response Framework.

11.2 Software-as-a-Service Incident Response Responsibilities and Procedures

As often misperceived within the industry, shifting digital information assets to the cloud doesn't entirely shift the responsibility (although exceptions can exist via explicit contractual agreements in the context of a managed service contract) or accountability. In the end, the owner of the assets (and the data residing on them) is entirely responsible for managing them with due care - appropriate to the exposed risks. From the three flavors of Cloud Computing Service models, the Software-as-a-Service model offers the most "done-for-you" compared to the others (i.e., PaaS and IaaS). As mentioned in CSA's Security Guidance v4, p. 20 - with SaaS, the cloud provider is responsible for the security of nearly all layers. The cloud service customer (CSC) can only manage the identity and access to the application (incl. client devices), the information clearance of the application, and, depending on the provider, some data encryption settings (i.e., Bring your own key). The CSC has no control over virtualization, networking, and perimeter security. Please refer to the image Shared Responsibility Model by the Centre for Internet Security:

Responsibility	On-Prem	IaaS	PaaS	SaaS	FaaS
Data classification and accountability	🟠	🟠	🟠	🟠	🟠
Client and end-point protection	🟠	🟠	🟠	🟠🔵	🟠🔵
Identity and access management	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Application-level controls	🟠	🟠	🟠🔵	🟠🔵	🟠🔵
Network controls	🟠	🟠🔵	🔵	🔵	🔵
Host infrastructure	🟠	🟠🔵	🔵	🔵	🔵
Physical security	🟠	🔵	🔵	🔵	🔵

🟠 Cloud Customer is responsible 🔵 Cloud Provider is responsible 🟠🔵 Shared responsibility

As some technological responsibility is shifted in this model, it is thus essential to have clear, contractual agreements with the Cloud Service Provider that match the enterprise security requirements and standard baselines. The CSC could leverage the CSA Consensus Assessment Initiative Questionnaire during the procurement phase to facilitate this discussion. As mentioned before, the CSC remains accountable to safeguard the enterprise information and assets, no matter the context. Responsibility can be transferred, but accountability can't.

Customer's Incident response plans must be updated to incorporate these technological limitations and maintain a register of critical CSPs contact points. Service Level Agreements for security and non-security incidents must be agreed with via contractual agreements.

11.3 Phase 1: Preparation

As outlined in the referenced CSA Cloud Incident Response framework, the level of preparedness is directly linked to how an organization reacts to a (cyber) security event. In terms of SaaS-services, it is imperative to have a solid understanding of the corporate (sanctioned) SaaS-landscape. Every SaaS service should be vetted during the procurement process and include reliable third-party risk analysis aligned to the corporate risk appetite and regulatory and industry compliance requirements. Any identified risk that is not under direct (technical) control by the CSC must be assessed and, if needed, contractually mitigated.

It is paramount for the CSC to understand the importance of this service in terms of supply chain risk and the continuity of the business objectives (assessed to confidentiality, integrity, and availability). Next to this, for any procured SaaS service, a list of critical stakeholders contacts (business, technical (IT/IT security) must be documented and added to the central enterprise asset database and be known to incident responders (or any other member of CSIRT).

By preference, SaaS-specific playbooks must be drafted to match with threat/abuse scenarios applicable to this service model. Draft communication can be prepared to inform corporate (internal/external) stakeholders if a SaaS provider is breached. Statements could be issued to notify customers/partners proactively, even if the impact is not yet clear or fully completed. Having centrally stored parameters or tags (i.e., CMDB) per SaaS service will be beneficial in deciding what type of communication should be performed (i.e., Does the tenant manage personal customer data or not?).

11.4 Phase 2: Detection and Analysis

As the customer (CSC) is only responsible for securing the data and the access to the data, most of the incidents in such SaaS-context will be detected by CSP-owned systems. However, the CSC should closely monitor unauthorized access by leveraging identity provider signals and SaaS-service access logs. The CSC is entirely responsible for detecting data exfiltration or reconnaissance activities (i.e., using honey tokens). CSCs must, for this reason, always aim to integrate any SaaS-service with a corporate identity platform - including multifactor authentication. Next to this, the alerting coming from CSPs should be combined with the standard CSC incident response process. Preferably this is automated by automatically ingesting alerts and assigning the proper priority - directly influenced by the business criticality of the SaaS-service. If the CSP supports it, logs should be offloaded to the CSC SIEM or IDS solution.

Independent of the latter, it remains critical to leverage the established SaaS CSP stakeholder contracts to invoke the agreed cyber clauses in the agreement and get the necessary support to analyze any potential breach of confidentiality, integrity, or availability. Lastly, the involvement of the CSP will be crucial for forensic investigation.

11.5 Phase 3: Containment, Eradication, and Recovery

As with all previous phases, the CSC is restricted in response actions. The CSC will only be able to: limit access to its tenant-based on originating IP (Allowlist note: not all SaaS-providers support this), revoke user or account access (incl. oAuth permissions, key rotations, multifactor tokens, etc.), and rotate data-at-rest encryption keys, and so on.

In terms of recovery, it is crucial to request the necessary support from the CSP to invoke the CSC data backup and recovery plan. This can be led by the CSC leveraging third-party backup tools or by requesting the CSP to support restoring tenant data.

11.6 Phase 4: Post-Mortem

Never let a serious crisis go to waste; taking a step back and reviewing the lessons learned is the critical final step of a sound IRP. Review the incident to determine what elements in the plan could be improved. It can be technical or even administrative (i.e., missing contractual agreements with the SaaS-provider or missing steps in the process). Key questions could be:

> - Did we detect the event in time, or can we improve? (metrics and logs)
> - Did we get the necessary support from the vendor? (contractual/SLA)
> - Did we inform our stakeholders in due time (compliance and communication)

The outcome of this after-action report should flow back directly as lessons-learned into Phase 1 and help prepare the CSC to manage (SaaS) incidents better. Ideally, the post-incident analysis should not just consolidate timelines and events but also be a learning process. An excellent example of this, although not strictly security-focused, is the "how we got here" or "howie" process originally co-created by Jeli, Netflix, Slack, and Adaptive Capacity labs.

Alternatively, it must be evaluated if some post-incident information could benefit peers or other CSPs. An option is to release an announcement message to your stakeholders (see an example of a Google Cloud outage of 16/11/2021) or leverage CSA's Cloud Cyber Incident Sharing Center (CloudCISC). Please refer to the CSA Cloud Incident Response Framework, chapter 6, to guide information sharing and coordination.

12. Compliance

12.1 Compliance with Security Policies and Standards

The use of SaaS applications to store and process sensitive data must be evaluated against all relevant internal and external applicable compliance standards and security policies in the same manner, and with the same rigor, as all other corporate systems. Notably, this means that SaaS applications should be categorized and assessed based on the types and sensitivity of data contained within them as well as other relevant risk factors such as: number of records at risk, organizational reliance, and continuity.

At a minimum, compliance organizations must understand, document, and monitor:

- The relevant classifications of data within a SaaS application
- The type(s) of users who have access to the SaaS application broadly
- The type(s) of users who have access to which classifications of data within the SaaS application
- The access controls in place within the SaaS application
- Any audit capabilities made available by the SaaS application
- Any applicable compliance assessments or attestations for compliant frameworks relevant for the SaaS consumer

It is especially important to note any SaaS applications in use that both contain sensitive and/or compliance-relevant data *and* expose a portal or other entry point to external (non-employee/non-privileged) users. These SaaS applications require extra scrutiny and monitoring as a misconfiguration can result in the highest criticality deviation from compliance requirements. For example, a data leak to the anonymous internet or unauthorized users.

While at many organizations compliance evaluation and attestation for SaaS applications frequently takes place on an as-needed basis - usually quarterly or annually - it is a better practice to put in place an automated, continuous monitoring system that can fulfill both security and compliance needs. The up-front effort to set up a continuous monitoring system is, generally speaking, equal to the effort needed to validate compliance for a single compliance cycle. A continuous monitoring system both reduces effort in future compliance cycles and reduces the amount of time a system might remain out of compliance, making it a worthwhile long-term investment. It also facilitates near real-time compliance assurance, rather than traditional snapshot-in-time assessment activities.

Deployment of such a continuous monitoring solution will generally require:

- Identifying which SaaS applications are relevant and in scope for each compliance framework
- Identifying which user groups or cohorts in each relevant SaaS application are in scope or of compliance concern
- Mapping SaaS application-specific settings and access controls required for relevant compliance frameworks to the elements of those frameworks they satisfy
- Utilizing software-based tooling to facilitate the automated continuous monitoring and reporting activities of the SaaS applications

Once these efforts are completed and a continuous monitoring solution is in place, ensuring that SaaS applications and their data remain in compliance with all relevant internal standards and external compliance frameworks becomes a mostly automated process. This continuous monitoring can be used to generate artifacts as required, which validate that the SaaS applications are in compliance and that they have been compliant over a given period of time.

Requesting custom retention times is best negotiated in the contract phase. If a SaaS solution is procured to complete a custom task, when can the processed data be permanently deleted from the SaaS solution? If the SaaS solution has a legal obligation to retain data, can processed data be transferred at intervals to offline storage? Significant risk reduction can be achieved by requesting a custom retention time.

12.2 Compliance with Legal and Contractual Requirements

12.2.1 Identification of Applicable Legislation and Contractual Requirements

See "Addressing Security Within Supplier Agreements" in the "Supplier Relationships" section.

12.2.2 Intellectual Property Rights

Cloud customers must review and understand the CSP's 'Terms and Conditions' for usage of their platform. In some instances, the CSP may reserve the right to have access to customer data. The CSP may also contract with third-party vendors for certain tasks. This could also lead to the possibility of an outside company accessing the cloud customer's data.

12.3 Information Security Reviews

Utilizing continuous monitoring tooling and practices as discussed above, can facilitate information security review activities of the organization's SaaS consumption. These reviews can consist of activities such as compliance evaluation, adherence to organizational and industry security best practices, and the implementation of sufficient security hygiene. Information security reviews should also involve activities to evaluate the organization's SaaS inventory, identifying potentially unsanctioned SaaS usage.

13. CASB Functionality and Way Forward

The Cloud Access Security Broker category is one of the key categories to emerge with the proliferation of SaaS services with a focus on visibility, monitoring, and control of shadow IT i.e. services being used that are not sanctioned and hence not secured by the company IT department. These consist of the main functionalities below:

- Risk Insights: The initial use case was analyzing customer egress device logs along with proprietary data about risks associated with individual cloud services to share insights like:
    - The total number of cloud services in a customer environment;
    - Percentage of services that are high-risk (e.g., application categories like Remote desktop control, collaborations applications, and so on);
    - Amount of data getting uploaded into high-risk cloud services;
    - Any cloud subscriptions obtained by leveraging organizations company credit card to determine the unsanctioned application being purchased.

This visibility was unprecedented for business decision-makers. The next question, of course, was about controlling the now visible risk.

- API: This mode leverages APIs for additional visibility and control. Common use cases, for example, are listing the top users that are downloading the maximum amount of data, revoking access for any external parties for a certain subset of the company data, etc. All the policy actions taken in this mode are near-real-time
- Inline: This mode provides the most comprehensive coverage by actually steering the application traffic to CASB cloud, decoding the traffic pattern to detect specific activities like uploads, downloads, and so on, applying granular policies instead of the traditional allow or block policy. A common example would be a policy only allowing downloads with no data protection policy violations for cloud applications with medium risk.

Another related category to emerge is SaaS Security Posture Management (SSPM) which simplifies and automates configuration management of SaaS applications by continuously monitoring SaaS applications against pre-built policy profiles that map to industry standards such as CIS or NIST. Misconfigurations are quickly alerted and users can even automatically remediate issues before they are exploited.

These categories continue to evolve and converge into a new category called Secure Services Edge (SSE). The detailed analysis of this evolution is outside the scope of this paper but this is something that Cloud and SaaS security practitioners should keep track of on an ongoing basis.

14. Conclusion

It's clear that the utilization of SaaS is only accelerating. With this acceleration, there are widespread impacts being made to the way organizations operate and utilize cloud offerings. That said, unlike traditional cloud security, the nuances of SaaS warrant some additional attention and addressing. This includes how organizations handle information security policies, access management, and access control. Considerations around encryption and key management become paramount as the data is no longer under the control of the consumer. Network security decisions can have ramifications for both how the consumer accesses SaaS services and the potential connectivity from the provider to the SaaS consumers organizational environment, whether on-premise or in the cloud. SaaS also represents a complex supply chain, often consisting of not just SaaS vendors but also underlying cloud or hosting providers. Incident Management and Business Continuity practices must be revisited to account for the increased role that SaaS offerings play in business operations.

While SaaS offers tremendous opportunities for organizations to change the way they operate, consume innovative capabilities and offload many of the operational burdens associated with both creating and maintaining applications, it isn't without its concerns. Failing to address these concerns can increase the potential risk and ramifications of security incidents associated with the consumption of SaaS.

15. References

Cloud Security Alliance. (n.d.). *Security, Trust, Assurance and Risk (STAR)*. CSA. Retrieved May 20, 2022, from https://cloudsecurityalliance.org/star/

Cloud Security Alliance. (2017, July 26). *Security Guidance for Critical Areas of Focus in Cloud Computing v4.0*. CSA. https://cloudsecurityalliance.org/artifacts/security-guidance-v4/

Cloud Security Alliance. (2021a, May 4). *Cloud Incident Response Framework*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-incident-response-framework/

Cloud Security Alliance. (2021b, June 7). *Cloud Controls Matrix and CAIQ v4*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/

Cloud Security Alliance. (2021c, June 7). *STAR Level 1: Security Questionnaire (CAIQ v4)*. CSA. https://cloudsecurityalliance.org/artifacts/star-level-1-security-questionnaire-caiq-v4/

Cloud Security Alliance. (2021d, July 29). *Cloud Threat Modeling*. CSA. https://cloudsecurityalliance.org/artifacts/cloud-threat-modeling/

Cloud Security Alliance. (2021e, December 8). *CCMv4.0 Auditing Guidelines*. CSA. https://cloudsecurityalliance.org/artifacts/ccm-v4-0-auditing-guidelines

International Standards Organization. (2020, December 16). *ISO/IEC 27001:2013*. ISO. Retrieved May 20, 2022, from https://www.iso.org/standard/54534.html

International Standards Organization. (2021, April 15). *ISO/IEC 27002:2013*. ISO. https://www.iso.org/standard/54533.html

International Standards Organization. (2022a, February 4). *ISO 31000:2018*. ISO. https://www.iso.org/standard/65694.html

International Standards Organization. (2022b, May 4). *ISO/IEC 27000:2018*. ISO. https://www.iso.org/standard/73906.html

16. Definitions

Cloud access security brokers (CASBs). On-premises, or cloud-based security policy enforcement points, placed between cloud service consumers and cloud service providers to combine and interject enterprise security policies as the cloud-based resources are accessed. CASBs consolidate multiple types of security policy enforcement. Example security policies include authentication, single sign-on, authorization, credential mapping, device profiling, encryption, tokenization, logging, alerting, malware detection/prevention, and so on.[1]

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (i.e., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[2]

Software Bill of Materials. A formal record containing the details and supply chain relationships of various components used in building software. Software developers and vendors often create products by assembling existing open source and commercial software components. The SBOM enumerates these components in a product.[3]

SaaS Security Posture Management (SSPM). Provides automated continuous monitoring of cloud-based SaaS applications like Slack, Salesforce, and Microsoft 365 to minimize risky configurations, prevent configuration drift, and help security and IT teams to ensure compliance.

Secure Service Edge (SSE). Secures access to the web, cloud services, and private applications. Capabilities include access control, threat protection, data security, security monitoring, and acceptable use control enforced by network-based and API-based integration. SSE is primarily delivered as a cloud-based service and may include on-premises or agent-based components.

[1] https://www.gartner.com/en/information-technology/glossary/cloud-access-security-brokers-casbs

[2] https://csrc.nist.gov/glossary/term/software_as_a_service

[3] https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

17. Acronyms

AICPA - American Institute of Certified Public Accountants

API - Application Interface

CASB - Cloud Access Security Broker

CIA - Confidentiality, Integrity, Availability

CCM - Cloud Control Matrix

CSA CCM - Cloud Security Alliance Cloud Control Matrix

CSA STAR - Cloud Security Alliance Security, Trust, Assurance, and Risk

CSC - Cloud Service Customer

CSP - Cloud Service Provider

DLP - Data Loss Prevention

FedRAMP - Federal Risk and Authorization Management Program

HIPAA - Health Insurance Portability and Accountability Act

HITRUST - Health Information Trust Alliance

IaaS - Infrastructure as a Service

IEC - International Electrotechnical Commission

ISMS - Information Security Management System

ISO - International Organization for Standardization

NIST - National Institute of Standards and Technology

MTD - Maximum Tolerable Downtime

OTP - One-Time Password

PaaS - Platform as a Service

PCI - Payment Card Industry

PII - Personal Identifiable Information

RFI - Request for Information

RPO - Recovery Time Objective

RTO - Recovery Point Objective

SaaS - Software as a Service

SASE - Secure Access Service Edge

SBOM - Software Bill of Materials

SIEM - Security Information and Event Management

SLA - Service-Level Agreement

SOC 1 - Service Organization Control 1

SOC 2 - Service Organization Control 2

SSE - Secure Service Edge

SSPM - SaaS Security Posture Management

TLS - Transport Layer Security

VM - Virtual Machine

ZTNA - Zero Trust Network Architecture