

# Recommendations for Using a Customer Controlled Key Store



The permanent and official location for Cloud Security Alliance Cloud Key Management research is <https://cloudsecurityalliance.org/group/CKM>.

© 2022 Cloud Security Alliance – All Rights Reserved. You may download, store, display on your computer, view, print, and link to the Cloud Security Alliance at <https://cloudsecurityalliance.org> subject to the following: (a) the draft may be used solely for your personal, informational, non-commercial use; (b) the draft may not be modified or altered in any way; (c) the draft may not be redistributed; and (d) the trademark, copyright or other notices may not be removed. You may quote portions of the draft as permitted by the Fair Use provisions of the United States Copyright Act, provided that you attribute the portions to the Cloud Security Alliance.

# Acknowledgments

## Initiative Lead

Paul Rich

## Lead Authors

Michael Born

Paul Rich

## Contributing Authors

Iain Beveridge

Marina Bregkou

Vani Murthy

Michael Roza

## Reviewers

Diego Fernandez Vazquez

Ankur Gargi

Shamik Kacker

Brynna Nery

Alex Rebo

Jai Singla

Katalin Szenes

Mike White

## CSA Staff

Marina Bregkou

Claire Lehnert

Stephen Lumpe

# Table of Contents

Acknowledgments .....	3
1. Introduction .....	5
1.1 Purpose .....	6
1.2 Scope .....	7
1.3 Target Audience .....	7
2. Introduction to the Customer Controlled Key Store (CCKS) .....	8
3. Choosing a CCKS Provider or Supporting Cloud Service Provider (CSP) .....	9
3.1 Technical Considerations .....	9
3.1.1 Hardware Security Module (HSM) Backed Keys.....	9
3.1.2 General Technical Considerations.....	10
3.2 Operational Considerations .....	12
3.3 Regulatory Considerations .....	13
3.4 Legal Considerations .....	15
3.5 Financial Considerations .....	19
4. Planning a CCKS.....	20
4.1 Technical Considerations .....	20
4.1.1 Identity and Access Management .....	20
4.1.2 Shared Responsibilities .....	23
4.1.3 Separation of Duties (SOD) .....	24
4.1.4 General Technical Considerations .....	26
4.2 Operational Considerations .....	29
4.3 Regulatory Considerations.....	31
4.4 Legal Considerations .....	31
4.5 Financial Considerations .....	32
5. Deploying a CCKS.....	33
5.1 Technical Considerations .....	33
5.2 Operational Considerations .....	35
5.3 Regulatory Considerations .....	36
5.4 Legal Considerations.....	36
5.5 Financial Considerations .....	37
6. Conclusion .....	38
7. References.....	39
Appendix A: Acronyms .....	41
Appendix B: Glossary .....	42

# 1. Introduction

Before reading this document, readers are encouraged to review [Key Management in Cloud Services: Understanding Encryption's Desired Outcomes and Limitations](#), which provides the foundation for the choice of Cloud Key Management Service (KMS) patterns and general guidance for using KMS, whether the KMS is native to a cloud platform, external, self-operated, or yet another cloud service. This document does not cover the pros and cons of this pattern and its advantages and disadvantages relative to other cloud KMS patterns. Organizations seeking to establish a risk/benefit analysis using this pattern should refer to the same link.

Prior documents in this series have covered patterns where a cloud customer leverages a cloud provider's KMS related to that same cloud provider's other services. The Customer Controlled Key Store (CCKS) pattern (see figure 1) addresses the scenario where a customer chooses to use a cloud service and selects a KMS that is external to the cloud provider operating the service. Furthermore, this pattern is distinct in that no key wrapping/unwrapping is carried out by the Cloud Service Provider (CSP), payloads being encrypted prior to being uploaded.

An example of using a CCKS with a cloud service is that of a data backup and/or archival system where the customer manages the KMS and encrypts all data prior to transmitting it to the cloud service. A second example of this pattern is a Cloud Encryption Gateway, or a tokenization/data masking solution where an on-prem HSM/KMS encrypts before it goes to the cloud and only decrypts once it is pulled back into the enterprise domain.

The foundational document mentioned above<sup>1</sup> defines the CCKS pattern as follows:

The External Key Management System uses a cloud service where the KMS is hosted entirely external to the cloud service, either wholly on the customer's premises, fully hosted by a third party chosen by the customer, or a combination of the two. Hardware may be the property of the consumer or the cloud provider but is provisioned solely for use by the consumer. A cloud provider may support a dedicated cloud HSM service offering or co-location model where the consumer hardware (or virtual appliance) is hosted in the same facility where the cloud provider has a presence. The consumer manages all aspects of the KMS and typically agrees to service-level agreement considerations in the event the KMS is the source of a service incident. **The CSPs can perform no key wrapping or unwrapping to archive total data privacy from the cloud provider.**

The motivation for using this pattern can include:

- Control of some or all facets of key management. This could be a key ceremony, rolling/renewal, or algorithm choice.
- Elimination of the ability of a cloud service to process customer data in plaintext, potentially exposing the customer's data to third parties.
- A desire to simplify operational complexity, security, and cost by reducing the number of KMS instances.

---

<sup>1</sup> <https://cloudsecurityalliance.org/artifacts/recommendations-for-adopting-a-cloud-native-key-management-service/>

- Regulatory or contractual obligations for key management systems, standards, or operations.
- Vendor lock-in, when using IaaS or PaaS.

It is essential to recognize that choosing the CCKS pattern may not achieve the goal that is motivating the choice of pattern. For example, a customer choosing this pattern because of a motivation to control encryption algorithm selection may find that there are still encryption algorithms used in cloud service operations that are outside the ability to control with CCKS.<sup>2</sup> Likewise, a customer motivated by the desire to eliminate the ability of a cloud service to process customer data in plaintext may find it impossible to use the cloud service in a productive way because of features that require plaintext computation.<sup>3</sup>

Because this pattern deals specifically with the integration of systems - a chosen KMS and one or more public cloud selected services - recommendations are provided concerning the integration dynamic. Recommendations will focus on the integration dynamic of the CCKS pattern and are exclusively relative only to one of the participating systems.

## 1.1 Purpose

The purpose of this document is to provide general guidance for using a KMS that is a dependency of a cloud service but is not hosted within that cloud service. It is fundamentally an integration pattern, and therefore the guidance is scoped to the integration dynamics of using a CCKS with one or more public cloud services. The guidance will provide recommendations for choosing, planning, and deploying a KMS *for this pattern* and encompasses technical, operational, legal, regulatory, and financial considerations. The goal is to optimize security, operational and business agility, and cost.

The **Customer Controlled Key Store** pattern is distinct from the **Cloud-Native KMS** pattern, where the keys and KMS reside in the cloud provider infrastructure throughout their lifecycle. The Cloud-Native KMS uses the **External Key Origin pattern**, where keys may be generated outside the cloud provider then imported into the Cloud KMS for use. Both of these patterns were covered in detail in earlier CSA publications. The recommendations for both of those prior patterns have considerably more focus on the capabilities and design of the KMS, for the following reasons:

- Cloud-Native KMS services are much newer than legacy enterprise KMS products and may not be as mature across technical, operational, regulatory, and financial domains.
- Organizations with a long history of operating enterprise KMS products may be unfamiliar with cloud KMS services and their differences with legacy enterprise KMS products.
- Newer organizations may be “born in the cloud”, entirely unfamiliar with Key Management Systems, and highly motivated to stay “cloud-native”.

Using a CCKS presents the customer with many challenges. The greatest of these is establishing the rationale for choosing this pattern and ensuring that the choice is well thought out and defensible. This pattern typically has a higher cost and complexity than using the Cloud-Native KMS pattern or Cloud-Native KMS using External Key Origin pattern.

<sup>2</sup> For example, a cloud provider may use its own encryption keys for replication of data between data centers.

<sup>3</sup> This would be the case for SaaS, since SaaS requires the ability to compute with plaintext.

This document provides guidance on how to assess and implement cloud key management services concerning an organization's needs for key management. It is the customer's responsibility to use encryption keys (or other artifacts, such as secrets) to follow encryption best practices.

## 1.2 Scope

This paper addresses the Customer Controlled Key Store pattern previously described as the "Cloud Native using External KMS" pattern.

Coverage includes mainstream business and Information technology (IT) usage of hybrid and cloud technologies. We will not address more specialized patterns such as high-assurance military, or intelligence community scenarios, as the recommendations made in this document should benefit organizations of any kind.

## 1.3 Target Audience

The audience for this document includes program and project managers, requirements or business analysts, architects, systems integrators, cloud customers, developers, as well as security and compliance staff concerned with the selection of, as well as the secure and reliable implementation and operation of KMSes that will be used with cloud services.

The primary use of this document is as an aide to the program or project manager that leads an organization through the lifecycle stages covered in this document. The goal is to provide explicit content that conveys enough explanation so that the project manager can identify how to map the considerations to their organization.

## 2. Introduction to the Customer Controlled Key Store (CCKS)

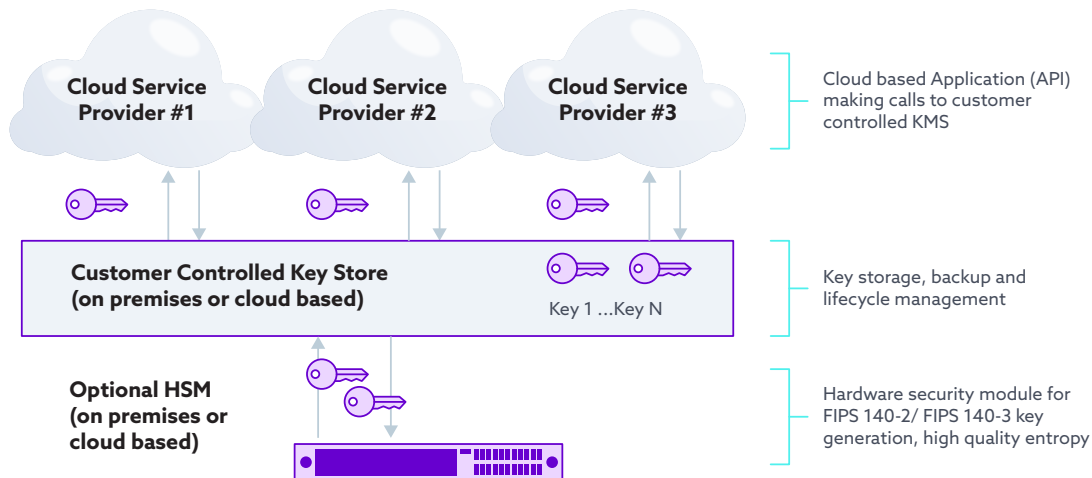


Figure 1: Leveraging the services of a Cloud-Native KMS and importing key(s) from an external source.

In the cloud, KMS patterns identified in the CSA paper "Key Management when using Cloud Services"<sup>4</sup>, the *Customer Controlled Key Store* pattern reflects the scenario where:

- A customer has chosen to use a public cloud service
- The cloud service leverages the functions of a KMS
- The customer chooses to use a KMS neither owned nor controlled by the cloud service.

The scenarios that will be covered for this pattern are:

- Choosing a CCKS
- Planning a CCKS
- Deploying/implementing a CCKS

Within each of the above scenarios, the following considerations are addressed:

1. Technical considerations - architecture, functional, scale, availability, security, etc.
2. Operational considerations - APIs, change management, logging, security, etc.
3. Regulatory considerations - provider certifications
4. Legal considerations - contractual
5. Financial considerations - total cost of ownership

A CCKS is relatively new to the world of cloud computing, so the set of available best practices is very small.<sup>5</sup> Therefore, the guidance combines best practices from experience with traditional Key Management Systems, cloud services in general, and Cloud-Native Key Management Systems.

<sup>4</sup> <https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/>

<sup>5</sup> Reader feedback is welcomed and can be submitted via <https://circle.cloudsecurityalliance.org/home>.



## 3. Choosing a CCKS Provider or Supporting Cloud Service Provider (CSP)

When choosing a Cloud Service Provider (CSP) to support a CCKS or CCKS provider, the organization should create a list of the aforementioned technical, operational, legal, regulatory, and financial requirements that the provider must meet. It is unusual to find significant differences in the legal, regulatory, and financial economic aspects of Cloud Service Providers (CSPs), so the technical and operational considerations are the main differentiating factors.

### 3.1 Technical Considerations

The following technical considerations will help determine whether a particular Customer Controlled Key Store provider or Cloud Service Provider offering provides the functionality needed by your organization to support a Customer Controlled Key Store. Note that PCI DSS, along with GLBA/FFIEC<sup>6</sup> and FISMA, requires NIST-certified AES encryption and FIPS 140-2 & 140-3 compliant key management using an HSM.

#### 3.1.1 Hardware Security Module (HSM) Backed Keys

Choosing a Customer Controlled Key Store	
Consideration	Justification/Rationale
Is the Customer Controlled Key Store capable of protecting keys using a Hardware Security Module (HSM)?	HSM-backed keys help meet compliance requirements such as FIPS 140-2 & 140-3 levels 2 <sup>7</sup> and above, or provide additional physical security of keys <sup>8</sup> .
Where will the HSMs run?	When choosing the HSM source there are a few options i) On-premises HSM, ii) HSM provided by CSP, iii) HSM as a service provided by a third party. Each of these options presents their own set of challenges, complexity, and security implications.

6 Gramm-Leach-Bliley Act / Federal Financial Institutions Examinations Council (GLBA/FFIEC).

7 For additional information see <https://csrc.nist.gov/publications/detail/fips/140/2/final> and <https://csrc.nist.gov/publications/detail/fips/140/3/final>

8 To verify if the components of a CCKS are validated to meet FIPS cryptographic standards the Cryptographic Module Validation Program (CMVP)# provides the necessary information.

### 3.1.2 General Technical Considerations

Choosing a Customer Controlled Key Store	
Consideration	Justification/Rationale
Has the organization defined a standard integration framework for integrating with a CSP?	Depending upon the chosen integration framework, certain CSPs may or may not be able to integrate with the CCKS or may offer limited integration with the CCKS.
Does the CSP support the CCKS product?	<p>Certain CSPs may have limited support for this pattern and limited support for specific KMS products.</p> <p>CSPs may only provide specific HSM configurations that may or may not meet the organization's needs.</p> <ul style="list-style-type: none"><li>• If the CSP doesn't explicitly support the choice of CCKS, the CSP may not honor specific contractual commitments such as availability or recovery objectives.</li><li>• In a multi-CSP scenario, it may be necessary that all CSPs the organization uses support the chosen CCKS.</li></ul>
Does the CSP supporting a CCKS provides the ability to migrate to one of the other Cloud KMS patterns?	The flexibility to move to a more or less complex cloud KMS pattern may be required when the customer's needs change. <sup>9</sup>
Does the CCKS offer labeling functionality for keys and secrets (e.g., tags, metadata, etc.) or does the CSP provide this capability by interfacing with the CCKS via an API?	<ul style="list-style-type: none"><li>• The capability to label keys allows an inventory-based system to understand the key's usage and allows for potential internal processes to take action on the keys.</li><li>• Labeling keys would be helpful in the event of key exposure. For example, If application X is exposed, having all keys used in application X tagged allows for easy identification and automation to replace those keys.</li></ul>
Does the CCKS offer an API for accessing or managing the KMS?	Additional application security controls may be necessary to properly protect the API.
Does the CCKS enforce secure transport using NIST standards and CISA recommendations?	Ensuring proper (secure/latest version) TLS protocols are used in the CCKS when accessing the KMS, keys, or secrets, to help protect that information in transit.

<sup>9</sup> For more information about migrating to one of the other KMS patterns, please see <https://cloudsecurityalliance.org/artifacts/key-management-when-using-cloud-services/>

If the CCKS is a public cloud service, does it support granular network access control to limit inbound traffic to its administrative end points?	In many scenarios, only certain IP ranges relevant to the organization will need access to the CCKS. The capability to limit inbound network access to those IPs increases the security of that KMS against access from malicious actors. This is a form of attack surface reduction.
Does the CCKS support cryptographic keys and secret life-span and expiration settings?	Any keys used within cloud services may increase the likelihood of key exposure the longer the key is used. Having a key expiration or rotation capability allows for the regeneration of keys, thus ensuring that any exposure of keys is limited in timeframe and impact.
Does the CCKS offer the capability to back up, restore individual keys and secrets, and transfer them once backed up?	<p>Cryptographic keys used in data encryption are critical not only to encrypt the data but also to decrypt the data. Should a cryptographic key be lost or destroyed, the data protected using that key is no longer accessible. Having the capability to back up keys protects that data. Backup copies of keys should be protected with controls as strong as the controls used for online keys using either an alternate KMS or a Key Escrow system.</p> <p>When backing up keys, the organization should consider where the backups will be placed to ensure the integrity and confidentiality of the backup. Using another KMS or a Key Escrow system serving as a backup solution allows for a greater capability to 'failover' in the event of a disaster, as part of the organization's business continuity plan and disaster recovery plan.</p>
Does the CCKS offer geographic redundancy that maps to the planned geographic/availability dynamics of the planned cloud service(s)?	This geographic redundancy may be necessary as part of the organization's disaster recovery processes and any limitations in geographic redundancy must be considered when choosing a CCKS provider.
Does the CCKS or CSP supporting the CCKS offer the capability to set a mandatory retention period for content before deletion (i.e., 'recycle bin' or 'soft delete')?	Soft delete provides recovery capability if a key is accidentally or maliciously deleted from the KMS.
Does the CCKS provide reporting functionality - providing a dashboard of operational activities?	Having the capability to review operational activities in the KMS in an easy-to-view manner assists the organization in understanding and anticipating costs.

Does the CCKS integrate into asset management systems, e.g., CMDB, so it, along with the keys it creates, can be tracked as assets?	Cryptographic keys, being an integral part of an organization's security, should have the capability to be tracked as an asset. Ensuring their operation, availability, and lifecycle (creation, renewal, destruction, etc.) is essential to the health of the cryptographic functions.
Can the CCKS support just-in-time access?	Ensuring proper access to the KMS is foundational to the security of the cryptographic keys within.  Just-in-time (JIT) access is the capability to provide access when needed, avoiding the use of persistent highly-privileged accounts. JIT access can be manually or automatically approved through policy actions.

## 3.2 Operational Considerations

The choice of a CCKS provider can significantly impact your organization's existing technology, people, and processes. Integrating the KMS into your overall architecture, processes, and procedures can be daunting. Given that the CCKS is either new or replacing an incumbent in the architecture, ensuring appropriate implementation or uplift ensures timely and consistent access to your organizational data is maintained. The following operational considerations will help determine whether your organization can support a particular KMS and whether the CSP supports the chosen KMS.

Choosing a Customer Controlled Key Store	
Consideration	Justification/Rationale
Does the CCKS or CSP supporting the CCKS provide an SDK/API that can help to automate routine processes?	Automation of routine operations minimizes human interaction and produces reliable and repeatable results. An SDK/API provides an interface to achieve this. This can then be leveraged as part of robust, auditable, and consistent application development.
Does the CCKS provide a user interface for efficient management and operational tasks?	A user interface will centralize administration, management, and operational tasks by providing useful dashboards displaying key management metrics.
Does the CCKS provider's staff require access to the KMS as part of the provider's duties?	As part of operating in a public cloud, it is expected that the cloud provider will need to perform operations on infrastructure backing many of the Platform-as-a-Service (PaaS) solutions or Infrastructure-as-a-Service (IaaS) solutions such as a KMS. As part of those operations, the cloud provider personnel may, at times, require access to the infrastructure housing the KMS.  Some organizations may have concerns about the risk of exposure to cryptographic material or the use of persistent and highly privileged credentials. Organizations with these concerns should review the terms of service with the cloud provider to assess these risks.

Can some or all operations be required to use two-person integrity or Separation of Duties?	Requiring two or more persons to complete operations helps protect against malicious insiders and mistakes.
Does the CCKS integrate with existing security controls such as a Security Information Event Management (SIEM) Platform for security monitoring?	The operations and activities within a KMS are sensitive and should be appropriately monitored to ensure no undue or malicious access or use.
Does the CCKS provide usage and deployment options with a level of complexity within the organization's operational capabilities?	This pattern comes with the risk of additional complexity to operate and each organization will need to weigh the additional complexity against the benefits of using this pattern accordingly.

### 3.3 Regulatory Considerations

Regulations and regulatory agencies typically do not specify prescriptive implementation details for technology. Encryption is where regulators typically refrain from specifying operational requirements. Regulators seek to guide or constrain behavior and outcomes, not technology. In fact, constraining technology can be counterproductive to regulators' intentions because it can hamper an organization's ability to innovate in ways that advance the regulators' objectives - usually risk reduction, improved privacy, and more robust security. Suppose technology constraints are included in regulatory language. In that case, it is to set a minimum acceptable value<sup>10</sup> or compel the use of a technology,<sup>11</sup> but not the specific implementation of that technology.

Regarding compliance with a regulation, the CSP can assert compliance, but it is ultimately the customer's responsibility to ensure compliance to applicable regulations. Stated differently, a CSP can violate or support your compliance with a regulation, but it cannot guarantee your compliance, only that of its own systems and processes. For this reason, the customer needs to know what regulatory regimes<sup>12</sup> it is subject to, and ensure that the cloud KMS does not violate any of those regimes.

Organizations with a global footprint may need to be cognizant of varying country-specific mandates, such as those requiring key escrow schemes. In addition, some country-specific regulations require long-term storage and recovery of cryptographic keys. For example, German tax regulations require storing tax-related documentation for 6-10 years.

<sup>10</sup> For example, the number of bits of entropy in an encryption key.

<sup>11</sup> For example, the use of encryption with certain data specified by the Payment Card Industry Security Standards Council, or the requirement to use encryption for data-in-transit.

<sup>12</sup> An example of this is ISO 27001. A customer of Microsoft Azure, for example, can obtain all Microsoft cloud service certifications for ISO 27001 at the Microsoft Service Trust Portal or via public Microsoft documentation.

In the realm of Key Management Systems, few regulatory bodies have promulgated guidance or constraints. Known instances include:

In the USA, the Defense Information Systems Agency (DISA) publishes the Cloud Computing Security Requirements Guide Version 1, Release 4 (January 2022) (commonly referred to as the DISA SRG), which in Section 5.11 *“Encryption of Data-at-Rest in Commercial Cloud Storage,”* constrains the use of cloud KMS services as follows:

*“Mission systems at all impact levels must have the capability for DoD data to be encrypted at rest with exclusive DoD control of encryption keys and key management.<sup>13</sup> Some Cloud Service Offerings (CSOs) may facilitate this by providing a hardware security module (HSM) or offering customers dedicated HSM devices as a service. CSOs not providing such a capability may require mission owners to use encryption hardware/software on the DISN or a cloud encryption service that provides DoD control of keys and key management. Some CSOs may offer a KMS service that can suffice the management of customer keys by the customer while preventing CSP access to the keys. It is recommended that NSA evaluate such CSP KMS services.”*

The Bank of Israel (Supervisor of Banks) promulgated Memorandum 15LM2087 on 29/06/2015, constraining key management with cloud services as follows: *“Cryptographic keys must be stored in the corporation banking and not at the cloud service provider.”*

The European Data Protection Board published [“Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data”](#), including both compliant and non-compliant implementation recommendations that leverage encryption and key management. This document is relevant for the recommendations where key management is the focus of the proposed implementation.

The CCKS pattern is appropriate for addressing regulatory regimes recommending customers retain control over key management operations. However, customers remain responsible for ensuring compliance.

It is also worth noting that regulators have not typically created constraints on using particular technologies, including KMS products and services. As a general rule, regulators avoid technology recommendations because they do not concern themselves with *how* regulation is complied with, but focus only on *whether* a regulation is complied with.

---

<sup>13</sup> Note, however, that DISA SRG Section 5.11 includes a provision for exceptions to this constraint: “For cloud applications where encrypting DAR with DoD key control is not possible, Mission Owners must perform a risk analysis with relevant data owners before transferring data into a CSO.” <https://dl.dod.cyber.mil/wp-content/uploads/cloud/SRG/index.html#5.11EncryptionofData-at-RestinCommercialCloudStorage>

## 3.4 Legal Considerations

When choosing a CCKS, legal considerations fall into two categories: (1) the acceptability of the warranties and representations in the contract, and (2) the likely outcome of any legal demand or lawsuit brought against the cloud service provider supporting the CCKS. Major cloud providers tend to have very similar contract provisions regarding legal demands and are well-written. When using smaller cloud providers, it can be helpful to compare contract provisions against those of a major cloud provider.

The following table lists considerations when a customer chooses a cloud service as the external KMS.

Choosing a Customer Controlled Key Store	
Consideration	Justification/Rationale
Is it possible for encryption keys to be exposed to third parties without the customer's consent?	If the use of CCKS is to prevent exposure of encryption keys to third parties then the customer should expect that the contract confirms this expectation. It is especially important to ensure that the customer contract with CCSK and the service CSP includes the facets of key management where this expectation needs to be met. It should also cover the exception areas where this expectation cannot be met. The contract should also cover regulatory or contractual obligations for key management systems, standards, or operations.
Does the contract describe the physical and logical security measures taken to protect the service and its contents?	The contracts with CCSK and the service CSP's should address integrating a chosen KMS and one or more chosen public cloud-selected services. It should clearly state the purpose for which the integration will be used with specific use cases. It should describe the responsibilities of both the cloud service provider/s and the tenant and identify what physical and logical security measures are taken to protect the service and its contents. Customers should expect physical measures to include secure facilities with man-traps, biometric authentication, video and audio surveillance, fail-secure mechanisms, and armed guards, if warranted by physical location. Logical security measures should be appropriate for a company of the cloud provider's size and sophistication, considering the sensitivity of stored data.

Does the contract include retention policies?	<p>Representations regarding the maximum time that the provider will retain customer content (keys, key policies, etc.) once the customer has (a) deleted the content within the service; (b) ceased to continue the customer-provider relationship. These policies should ideally include default data destruction timelines and specify whether the deletion process meets any necessary "secure" requirements (e.g., disk shredding or multiple overwrites).</p> <p>In case of accidental or malicious deletion from KMS, the contract should provide the capability to recover the key, it should designate roles who are allowed to make recovery requests, it should also define a time period during which recovery requests can be made. (Example: Recovery requests for keys beyond the data retention time will not be processed.) This clause should be included in the customer contracts with both the CCSK and the service CSP.</p>
Does the contract define acceptable parameters for customers performing penetration testing or similar activities?	<p>The contract should inform customers of what penetration testing is allowed, if any, and any limitations in the customer's actions if a customer is in scope for regulatory compliance like FedRAMP, the contract should include a clause that covers likely attack scenarios such as credentialed and non-credentialed attacks, simulations, social engineering, tenant to tenant attacks, attack on endpoints such as mobile applications, etc. as required for customer compliance. The contract should also include scenarios using backdoors and covert channels, which may be outside the customer FedRAMP boundary but part of CSP infrastructure that support other tenants. The contract should mention any CSP or CCKS provider roles supporting the customer, who would need to participate in pen testing (including roles that provide support for multiple tenants).</p>
Does the contract define and describe any regional availability, including service partitioning?	<p>Contract should describe clearly, any expectations from cloud customers, CCSK and service CSP. For example, the contract should include the geographical location where customers (or their users) have acquired and are able to use the CSP or CCSK services. The contract should also describe limitations on customers such as limitations on re-selling the service to their own customers or making use of the CSP or CCSK service outside of the designated geography.</p> <p>Contracts including referenced documentation should include language representing the geographic characteristics of the service that may impact the customer's operations, as well as any warranties regarding geographic boundaries. For example, the contract should state any geofencing that results from using any feature of the service that intends to accomplish that goal. The customer should also note whether the contract including referenced documentation allows for cross-border transfers, which should be further addressed in a DPA.</p>



<p>Does the contract specify when and how changes to the service are performed?</p> <p>Does the contract include any provision for the customer to control changes or the timing of changes?</p>	<p>All cloud services are constantly evolving-the code itself is likely taking changes on a daily basis - but service changes that impact the customer should require at least reasonable notice. Ideally, the contract represents that a customer has the option to delay the implementation of a service-impacting change for some period of time (up to 60 days, for example) if a change is scheduled for a particularly business-critical time. Additionally, the contract should spell out terms under which the provider may deprecate a feature and what remedies are available to the customer if any.</p> <p>Contracts should have time period validity and any contractual changes like any other organizational changes and need to go through change management policy and procedures of the organizations. This should be clearly stated in the customer contracts with both CCSK and service CSP. These contractual changes could be triggered by any of the parties involved in the contract such as CCSK or service CSP or the customer and each of these parties would have their own change management policy. Any contractual changes should go through a workflow requiring approvals from designated roles mentioned in the contract.</p>
<p>Does the contract define and specify Service Level Agreement guarantees and penalties, including Recovery Point Objective (RPO) and Recovery Time Objective (RTO)?</p>	<p>The contract should spell out the provider's Service Level Agreement commitments, including any penalties and conditions of penalties (e.g., the customer remains a customer; the customer can show harm, etc.). The service should have Recovery Point Objective (RPO) and Recovery Time Objective (RTO) identified as a representation, and it is beneficial for the provider to identify what conditions are necessary for identifying RPO and RTO starting points.</p> <p>Both RPO and RTO are critical for defining availability goals for the customers and would directly result in coming up with the customer cost. Inability for the service CSP or CCSK to meet the RPO, RTO designated in the SLA could result in financial liability. Any changes to the RPO, RTO should go through the change management workflow with appropriate approvals.</p>
<p>Does the contract include representations regarding the screening of employers, contractors, and third parties?</p>	<p>The contract should represent that all personnel have been examined for criminal background, previous civil law findings of a character nature, any required drug testing, nationality, and any other personal attributes required by the customer. The contract should also describe the frequency with which background checks are performed. Only a few specialized roles may require periodic background checks.</p> <p>Contracts should cover specific background check requirements as required by their regulatory or their customer's compliance needs. For example, certain government regulations may require additional screening for personnel in order to be able to access government data. Regulatory compliance may require screening for suppliers, contractors, etc. Any changes to the background checking requirement in the contractual language should go through standard change management policy and must go through the approval workflow process.</p>

Does the contract define and describe the CSP's incident and breach notification policy?	<p>A contract should define and describe incident and breach notification policy and indicate when and how the CSP or CCSK will notify their customer that their data may have been exposed in a security breach. A security breach in the CSP infrastructure or a breach in another customer's application might have an adverse impact.</p> <p>Customers should ensure that the KMS provider's policies and incident response commitments meet the customer's requirements. Consider that breaches of a KMS can have widespread effects and can be difficult to remedy quickly, so it may be prudent to consider asking for reduced notification time. Customers may also wish to specify that even <i>suspected</i> incidents be reported as swiftly as possible owing to the sensitivity of a KMS.</p>
Does the contract define and describe termination rights?	<p>A contract should have a start date and a termination date. A contract should also provide early termination rights for customers under certain reasons. A few examples of valid reasons for contract termination could be: There is a risk of vendor lock in where it is not feasible for customers to terminate existing contracts and move to other cloud service providers. Another reason where customers can terminate contracts is where CSP or CCKS has a breach in their platform and the customer loses trust in their services. Other reasons could be when the CSP or CCKS becomes insolvent or changes the terms of their service without the agreement of the customers. Customers should ensure that termination does not infringe upon any representations already established in the contract.</p>
Does the contract include Indemnification and Limitation of Liability?	<p>In a contract, if a mistake made by one of the parties causes damages, they are liable for these damages. A contract should contain indemnification clauses to compensate the losses due to the other party. Limitation of liability caps the extent of damage by preventing one of the members in the party to file a lawsuit against another party by pre-setting an amount. This is similar to insurance.</p> <p>These "purely legal" concerns are essential components of any business contract. They should be carefully reviewed in the context of the sensitivity and relative importance of a Cloud-Native KMS using EKO. Legal should always review these sections to ensure that the contract supports claims made by the cloud provider's marketing and sales departments.</p>
Does the CSP or CCKS allow customers or a third party to audit the CSP or CCKS?	<p>If a customer has a regulatory obligation to audit outsourcing partners then the customer must ensure that a cloud KMS will permit direct or third party audits. It is not common for a customer to be able to directly audit their CSP or CCKS. Instead, CSP or CCKS can undergo a third party audit by an independent assessor and share the certification report with their customers. Example of an audit certification report, is SOC2 type 2 report on how well the controls are operating in the CSP organization.</p>

Both technical and legal staff should rigorously examine the terms to ensure a thorough understanding and address all concerns or outstanding issues before committing. In general, large and well-established cloud service providers will have similar contract language. However, variances do exist, and some may be of particular importance to any single customer.

The primary legal aspect to consider is the contractual representations and warranties made by the provider. Of nearly equal importance is the ability of a CSP to pay damages or survive a lawsuit—representations, warranties, and indemnification rights are less valuable if a CSP is underinsured or an asset-poor startup. Customers should attempt to discover any litigation the CSP has been a party to and determine if the circumstances and outcome of litigation are a cause for concern.

## 3.5 Financial Considerations

This pattern typically has a higher cost and complexity than using the **Cloud-Native KMS** or **Cloud-Native KMS using External Key Origin** patterns. Cloud-Native key stores usually have zero cost and often require no implementation work or operational support, as these are all the cloud provider's responsibility. Even for Cloud-Native KMS using External Key Origin, the implementation and operational cost can be minimal because only root keys, of which there are orders of magnitude fewer than other types of keys, are generated and archived. The only ongoing operational activities are to safeguard archived root keys and generate new root keys when needed. Contrast this with implementing and operating a full KMS where operational staffing is typically needed 24x7, high availability demands typically require geographically distributed KMS stores, and key management extends to all keys generated. The overall cost is generally driven by operational demands, particularly the retention of technical expertise necessary to administer and operate the KMS functions.

The higher cost and complexity are motivations to ensure a very strong rationale and solid logic for choosing this model.

Choosing a Customer Controlled Key Store	
Consideration	Justification/Rationale
To estimate the cost of the cloud service(s) used with the CCKS, customers must understand the provider's pricing model.	Cloud providers may categorize external KMS support as a premium feature and charge higher transaction rates. Customers should clearly understand not only the specific services/features to be consumed but the volume of transactions expected to achieve a reasonable degree of precision for budgeting.
A fundamental characteristic of this pattern is the requirement for integration of cloud services with systems that are external to the service.	Integration implies creating a "bridge" between two islands, and this can incur costs for skills acquisition and training, computer language/API mismatch requiring either porting existing code or creating a translation layer.

## 4. Planning a CCKS

After choosing a KMS product and a cloud provider to interface with the CCKS, the next logical step is to plan the deployment. Many technical, operational, legal, regulatory, and financial concerns must be addressed in this step. The outcome of this step should be a list of requirements that the user or organization will use when deploying the CCKS.

### 4.1 Technical Considerations

When planning to deploy a CCKS, organizations have several categories of technical considerations.

#### 4.1.1 Identity and Access Management

Identity and Access Management (IAM) is a fundamental component of any commercial information technology system and significantly contributes to an overall security posture. It is the foundation of any secure and fully compliant public cloud architecture.

IAM systems serve as mechanisms that can reduce risks associated with cloud environments as they serve as a cornerstone of authorization which is essential for upholding the least privilege principle. Many organizations provide IAM systems to secure the information by controlling the permission of each user access request, called "need to know (n2n)" or per-info classification. It's critical to plan how to govern the control and data-plane access to resources. Any design for IAM must meet regulatory, security, and operational requirements.

The primary and unique mechanism for controlling access to a KMS key is the resource policy which is also unique for each KMS. Access control mechanisms, on the other hand, can be used in combination with the resource policy to control access to a KMS key when it comes to defining IAM policies.

This way, the user will be able to manage all of their permissions in IAM for their own IAM identities, and as long as it is defined so in the resource policy, they may also be allowed access to the KMS key by using it.

An IAM policy can control access to any KMS operation and multiple KMS keys, while providing operation permissions to several related services.

The Identity and Access Management (IAM) procedure includes IAM and resource policies together. The KMS key resource policies must include the account permission for using IAM policies.

In IAM policy statements that control access to KMS keys, it is necessary to use the least privileged principle. IAM principals are provided only with the permissions they need, on only the KMS keys they must use or manage.

In general, IAM is critical for helping companies strengthen their security postures while reducing the likelihood and impact of cyberattacks. Organizations can protect their data from external and internal threats by verifying and authenticating user identity, limiting user access, and monitoring activity.

The body of IAM requirements may vary from organization to organization, but there are common design considerations and recommendations to consider like:

- User identification, verification, and authentication
- User and access management
- Security practices to protect company data and assets
- Activity tracking and monitoring
- Compliance auditing
- Multifactor authentication (MFA)
- Monitor activity and workflow.

The CSP supporting the customer controlled key store should offer several secure options for authenticating to the KMS.

The user needs to obtain credentials for authenticating their requests in the KMS. Their credentials must include permissions to access the CSP’s resources, its KMS keys and aliases. Permissions are determined by policies: identity-based and resource policies.

To access the KMS keys, users need to secure the relevant resource policies, the IAM policy and access control mechanisms. This way, access may be delegated to other users as well.

Authentication to Customer Controlled Keys	Authentication for the KMS
The customer establishes and maintains their own resource policies.	The CSP offering the KMS establishes and maintains the KMS key policy.
The customer establishes and maintains their IAM policies.	Authentication and authorization processes operate independently of where the key is stored.
The customer establishes and maintains their own access control mechanisms and aliases <sup>14</sup> .	Identity-based and resource policies attached to the keys are used for authentication of users’ requests.

14 An alias is correlated with a customer KMS key. Once updated though, it can be associated with a different customer KMS key.

And here are some design considerations in key operational areas.































Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Does the CCKS or the CSP interfacing with the CCKS support granular and/or custom roles and role assignments?	<ul style="list-style-type: none"><li>• Operating on the 'principle of least privilege', users having only the rights necessary to perform specific actions within the KMS makes for the most secure access model.</li><li>• In some scenarios, there may not be a built-in role that works, and consideration should be given to a custom role in these scenarios. Please refer to the cloud provider or KMS vendor's best practices for custom roles as they are not always possible or a recommended solution.</li></ul>
Does the CCKS or the CSP interfacing with the Customer Controlled Key support integration into existing authentication mechanisms, such as Single Sign-On (SSO) and federation with the organization's identity provider?	If the organization has an existing identity provider, ensuring that authentication occurs using these accounts via federation or SSO can increase security through the already in-use authentication mechanisms from the organization. Customers should not be required to perform password synchronization to a cloud provider, thus creating an exposure and threat to the enterprise.
Does the CCKS or the CSP interfacing with the Customer Controlled Key support the use of separate roles for read/write access?	Separating write access to a privileged role so that a user must escalate to safeguard against accidental changes from the user or malicious changes should the normal user account become exposed.
Does the CSP or CCKS offer notifications of privileged role use and trending/comparison metrics through the organization's identity provider? Are those metrics configurable?	When using Privileged Identity Management (PIM) in this fashion, it is essential to regularly audit the access logs to ensure no undue access.
Does the CCKS or the CSP interfacing with the Customer Controlled Key support the use of conditional access policies through the organization's identity provider for providing access?	<ul style="list-style-type: none"><li>• The use of conditional access policies can increase security by ensuring access is only permitted in certain use cases.</li><li>• An example is that a user must successfully authenticate from an IP within the organization's authorized IP ranges.</li></ul>

Does the CCKS or the CSP interfacing with the Customer Controlled Key support the use of Multifactor Authentication (MFA) for write access through the organization's identity provider?	<ul style="list-style-type: none"> <li>Typically performed at the organization's identity provider instead of the CCKS.</li> <li>Using MFA strengthens security by providing further confidence that the person logging in is the correct and authorized person.</li> </ul>
Does the CCKS or the CSP interfacing with the Customer Controlled Key allow the disablement, or non-use, of non-federated identities from the organization's identity provider?	Managing user credentials within an organization-managed directory service will help centrally enforce the same secure account management policies for user accounts with access to the KMS.
Does the CCKS or the CSP interfacing with the Customer Controlled Key follow a security approach that requires all users to be authenticated and authorized continuously to enforce access control?	This leads to a Zero Trust approach that prevents security breaches by eliminating the implicit trust from the system's architecture. Instead of automatically trusting users inside the network, Zero Trust requires validation at every access point. It protects modern network environments using a multi-layered approach.

## 4.1.2 Shared Responsibilities

Shared responsibilities recognize that while cloud providers are responsible for the security of the cloud, cloud customers are responsible for security in the cloud. However, shared responsibilities vary by service model (IaaS, PaaS, SaaS) and CSP. Regardless of the model or service provider, data and access to that data are, in the end, the customer's responsibility. It is up to the cloud customer to verify shared responsibilities and controls over data (at rest and in transit) and keys in the CCKS.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Are shared responsibilities considered with the Cloud Service's interaction with the CCKS and separation of duties (SOD see 4.1.3)? For example, Key Management and Data Access.	Permissions are assigned to roles based on responsibilities, enabling performance and establishing accountability. Consider separation of duties when assigning roles to protect against error or fraud.
Is the Cloud Service's interaction with the CCKS shared responsibilities, and separation of duties (SOD see 4.1.3) documented in writing in operational policies and procedures and other documentation?	Document responsibilities/SOD in writing to ensure a source for training, operational use, and contractual disputes.

	Areas of Responsibility	SaaS	PaaS	IaaS	On-Prem
Customer's Responsibility	Account, Identity				
	Applications				
	Devices (PC, Portable, Mobile)				
	Information and Data				
	Identity and Directory Infrastructure				
	Network Controls				
Cloud Provider Responsibility	Operating System				
	Physical Infrastructure and Connectivity (network, datacenter, hosts)				




 Cloud Provider
 Customer
 Shared Responsibility

Figure 2: The Shared Responsibility Model

### 4.1.3 Separation of Duties (SOD)

Separating job duties or privilege levels is an Information Security best practice. When planning the deployment of the CCKS, the organization should consider how user roles are separated and whether that will occur across CSP and CSC Key Management System, users, or accounts.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Will your organization need service accounts with specific access to certain keys or secrets?	It is essential to document ALL accounts accessing the CCKS, especially accounts associated with applications accessing the KMS. Thorough documentation helps organizations with timely response to security incidents, separation of duties validation, and other security-related account management tasks for the CCKS.



<p>Will the system allow the HSM managing account to exchange event/log information with the master account?</p>	<p>The exchange of event/log information is necessary to ensure timely response to security incidents, separation of duties validation, and other security-related account management tasks for the CCKS.</p>
<p>Does the CCKS and the interfacing CSP KMS support the assignment of typical roles<sup>15</sup>?</p>	<ul style="list-style-type: none"> <li>• <b>Administrator:</b> Full access to the customer controlled key store. The primary responsible for day-to-day administration. This role has read, write, delete, recover, backup, restore, import/export, update, and purge permissions on keys/secrets.</li> <li>• <b>Break Glass Administrator:</b> Same privileges as the Administrator role. To be used only if the other administrators cannot access their accounts. This role should be time-bound and linked to the user's unique ID.</li> <li>• <b>Auditor:</b> Read access to all keys and secrets within the customer controlled key store. This access should have enough privileges to review necessary metadata or log data associated with key or secrets expiration, key or secret rotation activity, key or secrets import or export activity, key or secret restore or recovery activity, and key or secret purge activity.</li> <li>• <b>Read-Only:</b> Groups, users, or service accounts with the Read-Only access role shall have this role assigned to specific keys or secrets appropriate for their job requirements. This role will allow read-only access to keys or secrets and will not allow users with this role to alter the keys or secrets in any way. Service accounts with this role serve a specific read-only purpose within applications interacting with the CCKS.</li> <li>• <b>Encrypt/Decrypt:</b> Groups, users, or service accounts with this role are allowed to interact with specific keys or secrets within the CCKS. This role may also require that the group, users, or service accounts have read access to the same specific keys or secrets within the KMS. Assigning this role to a service account will fulfill an application that needs to perform encryption/decryption.</li> <li>• <b>Write-Only:</b> Groups, users, or service accounts with Write-Only access will only be able to perform 'write' operations within the KMS. This may be necessary for any applications that would need to write keys/secrets within the CCKS.</li> </ul>

<sup>15</sup> <https://docs.aws.amazon.com/cloudhsm/latest/userguide/manage-hsm-users.html> provides a particular view on segregating duties when managing an HSM.

## 4.1.4 General Technical Considerations

Organizations deploying a CCKS should consider the level of effort required to configure this pattern and integrate the KMS into the organization's information system architecture, including integration with the organization's deployed cloud services that will interact with the KMS.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Are systems accessing the CCKS capable of utilizing web (e.g. Representational state transfer (REST)) protocols?	Each architecture may require additional account management tasks, controls and/or configurations impacting the level of effort needed to support and secure the KMS. Solutions unable to support web protocols will have a larger effort needed to utilize the KMS.
Are staff technically proficient with the chosen CCKS and the Cloud Services interacting with the KMS?	The time to achieve operational readiness will be significantly impacted by the staff's technical proficiency to integrate and operate the CCKS, and each piece of technology or Cloud Service that will interact with the CCKS.
Will documentation and configuration procedures need to be developed prior to deployment?	Allow sufficient time to document configurations, architecture, and any steps to deploy the KMS. This will save time in the future as personnel changes and updates to the KMS or environment are made. In addition, security and compliance audits of the processes and procedures will be simplified if these are properly documented and maintained.
What systems integration work will be required to allow necessary service access to the CCKS?	Other information systems may need to be configured to allow secure access between the organization's Cloud Services, the organization's information systems, and the CCKS.
What systems integration work will be required to monitor and alert on security-related events within the CCKS?	Additional information systems may need to be configured to store security-related event logs, additional connections to support alerting facilities, and other systems to support automated responses to specific events.
How will encryption types, algorithms, and key lengths be determined?	Industry best practices, organization use cases, expected lifespan of encrypted data and compliance requirements, as well as the KMS configuration and the key material it supports, may shift over time. Has any consideration been made for crypto agility and the migration effort to post-quantum (PQ) safe algorithms or composite methods?

Does your test environment have the same features as production, and does your organization have sufficient application representation to test business-critical features?	Consider the level of effort needed to properly configure and test network and application access to the KMS from the perspective of each environment and system.
Does your deployment architecture consider multi-cloud deployments (i.e., multiple cloud service providers leveraging the same CCKS)?	For operational/resilience/business continuity or cost reasons you may need to consider the key store interoperating with multiple cloud service providers. You should be mindful of the differing tool sets used by the CSPs and ensure your staff are familiar with and have documented the interaction and accessibility for each CSP.
Have you considered what measures are required to ensure the cryptographic key provenance, usage, backup, longevity, and overall lifecycle management. as well as data sensitivity /level of protection required?	Key management is more than just creating a key and making it usable. Consider the factors when deploying at scale. Do you have the ability to determine why the key exists, and its role?
Have you specific latency needs which need to be validated prior to deploying in an operational environment?	Some solutions require low latency (<50ms) to ensure your deployment can meet the specified latency to meet organizational SLA.
Have you considered the location of your CCKS and whether decentralization might offer a more robust, resilient deployment?	Generally, consideration should be made for a distributed Customer Key Store as opposed to a centralized key store to offer resilience and reduce the attack surface.
HSM upgrade	When using on-premises HSMs, it is important to consider the maintenance and firmware upgrade of the device. Over the life of the HSM it will most likely require infrequent updates to apply new features or patches. Ensure you have a plan in place for this maintenance process and test it prior to deployment.

Organizations should determine KMS deployment model requirements.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
What capacity planning needs to occur, and does the CCKS service provider offer capacity planning tools and documentation?	The organization may need to deploy a KMS solution in multiple geographical regions, and may need to increase bandwidth to account for additional traffic between information systems and the KMS, and may need to monitor the additional potential performance impact to the organization's network.
What automatic scaling capability is needed, and does the cloud provider or CCKS offer native configuration options for this purpose? Organizations should consider the CCKS capabilities when determining configuration requirements. For example, auto-scaling, clustering, and back-ups.	Additional cloud services, information systems, or configuration steps may be necessary for performing these tasks according to the organization's requirements.

Organizations should establish what CCKS provider documentation and support will be available during deployment.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Is sufficient documentation available to troubleshoot issues that might arise during deployment?	A lack of documentation or outdated documentation may dramatically increase the time teams need to troubleshoot technical challenges arising during deployment.
Will technical or engineering support be available from the KMS provider during the deployment process?	Additional costs may be associated with technical support from the KMS provider. Data privacy is a consideration when relying on the KMS support of the provider.

## 4.2 Operational Considerations

During planning a CCKS, deployment is where most operational considerations will be made. Ensuring that proper processes and procedures are in place prior to the deployment is the best way to ensure the adoption and success of the CCKS solution. Consider how an organization plans to use the KMS because different uses of encryption keys (or other KMS features, such as storage of blobs, passwords, or connection strings) will have different levels of sensitivity to service outages. The below operational considerations provide guidance and reviews for users and organizations while planning a CCKS solution.

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
How will users request objects, as well as access to objects, in the CCKS?	Consider initial operational access needs during deployment and then ongoing self-service needs, so that the operations team will not end up handling all provisioning of KMS resources, which could be costly and slow.
What security monitoring needs to be configured on the CCKS during deployment?	Examples of security controls that may require read access to the CCKS include controls such as centralized logging, privileged access management, and cloud security posture management.
How will access to the keys and secrets in the Customer Controlled Key Store work in the event of an outage?	In an outage of the organization's information systems, cloud service provider, KMS, or backing authentication services, users and organizations should prepare business continuity plans for how applications would continue to function without connectivity to the CCKS.
What personnel will monitor stored log data for potentially malicious activity?	The operational roles and responsibilities should be identified with runbooks or processes in place for actions to take on detected security events in the CCKS.
How will the organization manage roles while maintaining the principle of least privilege?	Maintaining the principle of least privilege becomes a challenging exercise when provisioning user accounts without a proper plan or set of documented procedures to efficiently manage user roles and their level of access to the KMS.
How will the organization assign roles to maintain separation of duties?	Without a set of documented procedures in place to help guide how user access to the KMS is provisioned, whether through Role Based Access Control (RBAC) via directory service (cloud, on-prem, or hybrid), or within the KMS privilege assignment functionality itself, maintaining a separation of duties between user accounts becomes nearly impossible.

How will the organization handle new account provisioning, stale account deprovisioning, and periodic role audits?	Similar to information system access, the organization will need to periodically review accounts with KMS access and make a business determination whether that access is still needed. Maintaining policies and procedures with this information will help set the expectation for personnel responsible for performing these actions and ensuring they have the privileges necessary to do so within the KMS.
Does the CCKS offer the capability to log, monitor, and alert based on registrant activities (e.g., read, write, edit, delete, update, etc.)?	As part of a mature security program, logging, monitoring, and alerting on activity within the KMS helps track down whether the alerting activity was performed by malicious users or as part of planned maintenance. Another benefit of logging this activity is in the event of an accidental change made to the KMS. The more information captured, the more likely the organization will be able to revert any unintended changes.
Does the CCKS offer the capability to implement robust disaster recovery functionality?	Not all service providers or vendors can maintain a healthy level of service offering for their KMS product which introduces some level of risk associated with getting locked into a specific KMS. Having the ability to implement robust disaster recovery functionality helps an organization avoid getting locked into one service provider or vendor and provides the organization a way of recovering from an incident within the CCKS.
Does the CCKS provider enable high availability within their KMS product to prevent outages?	This functionality enables an organization to continue operating the KMS in the event of an outage as part of business continuity. For example, an active-active cluster may be appropriate where any changes in one node of the cluster are automatically reflected in all nodes of the cluster.
How will the organization handle upgrades and patches to the CCKS?	Upgrades and patches should be designed in the the process and procedures and where possible without taking the CCKS offline to minimize disruption to the production environment
Does the CCKS have SSH disabled by default?	Ensure your CCKS has SSH access disabled by default, preventing key snooping or clear-text data snooping.
How will your organization security harden the CCKS environment?	The CCKS environment should be configured at time of deployment to ensure it is hardened, locking down access rights and closing any unused communications ports reducing the overall attack surface.

## 4.3 Regulatory Considerations

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
What regulators, if any, need to be notified of your organization's use of cloud services that interact with the CCKS?	<p>For regulated businesses, notification of the use of public cloud services may be required before production usage. Not doing so can result in penalties or fines.</p> <p>Depending upon the size of the organization, different tiers of the CCKS may be needed to meet different regulatory requirements per business unit.</p>
Is your organization mandated to hold customer data (e.g., transaction data, invoices, tax related information etc.) for a long duration?	If encrypted data and therefore associated cryptographic keys need to be retained and managed by your organization for 10 or more years, then a CCKS may lend itself to more convenient long term support than one of the alternative patterns.

## 4.4 Legal Considerations

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
Where will the signed service contract with the CPS or CCKS vendor be stored, and who will need access?	Ensuring the organization has stored a copy of the signed contract ensures that any legal counsel used by the organization can examine the terms and conditions in a dispute with the cloud service provider or KMS vendor. Assume that it is impossible to anticipate every person or role that will want access to the contract and err on the side of making it available broadly within the organization on a read-only basis.
What is the process for all non-legal personnel to raise concerns to legal counsel regarding changes in design and/or operation of the CCKS or Cloud Services interacting with the CCKS?	Should a concern arise that is suspected of having legal ramifications, a process should exist whereby non-legal staff can raise a concern to legal counsel for evaluation.
If changes to the contract occur, how will they be captured and reconciled with any operational impact?	Because contract changes can impact operational considerations (e.g., service level guarantees, disaster recovery dynamics), it is important to capture contract changes and ensure operational personnel are kept apprised of any changes.

## 4.5 Financial Considerations

Planning a Customer Controlled Key Store	
Consideration	Justification/Rationale
What steps are taken to prepare the organization to handle billing from the CCKS vendor or the cloud provider hosting services that interact with the CCKS?	The organization must avoid having services disabled or deprovisioned due to lack of payment of an invoice. Additionally, suppose the organization is performing chargeback of some kind to internal consumers of the service. In that case, the steps to prepare for this billing model must be taken before initiating production.
What steps are being taken to audit the CSP's invoices to ensure that unexpected costs are not being incurred due to a lack of oversight?	It is entirely possible that unexpected transaction volumes occur due to misconfiguration or poor application design, resulting in a potentially enormous discrepancy between the expected and actual invoice for services. Someone must be accountable to ensure that the delta between expected and actual costs can be accounted for and addressed, if necessary.



## 5. Deploying a CCKS

With the deployment of the CCKS planned out, the next step is to perform the processes required to set up the KMS, to set up any cloud services or information systems that will interact with the KMS, and to start utilizing its services. In this scenario, the financial and operational concerns come to fruition as costs are started against a user or organization as resources get deployed and initiated. Additionally, legal and regulatory matters become a reality as data starts to populate.

### 5.1 Technical Considerations

The following technical considerations guide users during a CCKS solution deployment for a user or organization. The primary focus for the user or organization should be on ensuring proper access models are in place and that secure operation of the KMS solution can occur without impacting business functions.

Deploying a Customer Controlled Key Store	
Consideration	Justification/Rationale
Is it warranted to have multiple instances of the CCKS to ensure separation of development, test, and production uses?	It can be beneficial for an organization to deploy and maintain multiple instances of a CCKS and associated cloud service. This will enable testing of changes, upgrades, environmental hardening and DR scenarios in a non-production environment prior to roll out in a production environment.
Have you considered deploying HSMs (either on-premises, HSM as a Service, or natively provisioned by the CSP) in conjunction with your CCKM deployment?	<p>It is industry best practice to use a FIPS 140-2 or 140-3 Level 2 (or greater) HSM for the generation and protection of cryptographic keys. For virtualized KMS appliances, an integration with an HSM should be considered to leverage the rich entropy source provided for the creation of cryptographic keys.</p> <p>The option to use an HSM-backed key is often configurable during key creation processes in the KMS.</p>
Should the cryptographic keys be configured for automatic renewal with the CCKS?	Outages resulting from expired keys are all-too-common. Customers should consider using their KMS key lifecycle management tools with automated renewal/ key rotation and backup features, if available.

<p>Does the CCKS need to be restricted from public Internet access, or is specific access needed between the CCKS and cloud services that interact with the KMS?</p>	<p>A customer may have a requirement where all access to the KMS originates from the customer's network or associated cloud infrastructure, typically done via some form of Virtual Private Network (VPN) connection with the CSP. This can also extend to blanket restrictions based on geographic (as represented by IP address space) location. Regardless of the kind of access needed, organizations are advised to use the principle of least privilege when assigning network access to the KMS and are encouraged to deploy strong network segmentation controls around the KMS.</p>
<p>What configuration settings need to be enacted to reflect the organization's policy regarding key recovery following deletion?</p>	<ul style="list-style-type: none"> <li>• Some KMS solutions will offer the ability to enable a soft delete or versioning of keys at the point of KMS creation.</li> <li>• If this is required, it should be considered during, or prior to, the deployment of the KMS as it cannot be enabled after in some cases.</li> </ul>
<p>Does the CCKS need to be deployed in a specific geographic location or do the cloud services interacting with the CCKS need to be deployed in a specific geographic location?</p>	<ul style="list-style-type: none"> <li>• Cloud providers may allow the selection of a geographic location when a resource is created.</li> <li>• Resources may be optimized to operate in certain regions for technical reasons such as connectivity to other resources or operational reasons such as disaster recovery.</li> </ul>

## 5.2 Operational Considerations

The below operational considerations guide users and organizations during the deployment of a CCKS solution. The operational aspects of deploying this pattern are driven mainly by the need to ensure access, proper monitoring, and associated processes and procedures.

Deploying a Customer Controlled Key Store	
Consideration	Justification/Rationale
If there were two-person-integrity steps that needed certification, have you completed those?	Any key-ceremony steps that have not been completed are potential compliance violations and may undermine the legitimacy of the KMS.
Have owners of all dependencies signed off?	Without sign-off from dependencies (e.g., SIEM, identity management, monitoring, HelpDesk), the decision to move to production implies the acceptance of significant risks.
Have all (planned) supported KMS activities been tested end-to-end in both the CCKS and with the CSP interfacing with the CCKS?	Without standard change-management practices, the organization accepts the risk that the service may fail to deliver services/features as advertised.
Has logging been confirmed functional and calibrated for production use?	It is possible that prior to production use, that logging configuration was set at a reduced or increased verbosity for testing and validation. So, confirming that the desired logging level is set for production addresses the risk of too much or too little detail being collected.
Has monitoring been tested?	Once integrated, the KMS is an instrumental component of an application providing access to keys used by an application and, as such, may benefit from monitoring for service availability and connectivity.
Have disaster recovery scenarios been tested and validated with expectations?	Once integrated, the KMS is an instrumental component of an application providing access to keys used by an application. In the event of a service outage, this could mean downtime to an application that can't access keys. Without plans for how the application will function in an outage, you may experience unexpected downtime.
Has cryptographic key backup been tested and verified?	Ensuring that backup keys are created and stored for disaster recovery/key ESCROW purposes.

Has all network access between information systems, cloud services, and the CCKS been thoroughly tested to be sure the security and segmentation controls have been implemented effectively?	Given the complexity of this pattern, thorough testing of all network access to and from the KMS along with thorough testing of all network security controls is necessary to assure access to the KMS is limited appropriately.
Has the CCKS environment been security hardened?	It is important to ensure all unused ports are locked down, least privileged access set and separation of duties established for access management where appropriate.
Have contingency plans been documented and tested to cater for attrition of personnel, loss of credentials etc.	It is important to test for the scenario where personnel leave the department/ organization and test for credentials, passwords or physical tokens, smart cards etc.

## 5.3 Regulatory Considerations

Deploying a Customer Controlled Key Store	
Consideration	Justification/Rationale
Does your organization maintain compliance documentation that should reflect the usage of the CCKS and any cloud services that interact with the KMS?	Ensure that any required documentation is complete before using the CCKS in production.
Are you prepared for an audit where the CCKS or cloud services interacting with the CCKS might be in scope?	Ensure that audit processes and documentation reflect the use of the CCKS or cloud services interacting with the CCKS before using the services in production.

## 5.4 Legal Considerations

Deploying a Customer Controlled Key Store	
Consideration	Justification/Rationale
What steps have been taken to ensure that the organization has archived a signed contract with the vendor offering the CCKS solution or CSP?	If there is a dispute regarding contractual obligations, the customer will want to produce a valid contract. The customer's Legal department should store a copy of the agreement and all licensing terms.

## 5.5 Financial Considerations

Deploying a Customer Controlled Key Store	
Consideration	Justification/Rationale
Has the accountability for the cost of completing deployment been determined, and is the billing routing planned accordingly?	Completing the deployment steps to enable a CCKS solution is going to incur some one-time and/or unusual charges. Prepare your CFO staff to see new charges appearing, and ensure that the charges you are seeing are expected.
What is the review process to examine the initial and potentially ongoing charges for validity against expectations?	Although the CCKS may incur an annual cost, or one-time cost, an organization may catch a software process that is performing unexpected, high-volume transactions through your billing rather than monitoring settings, so have a technical staff member review billing statements for at least several months after deployment has completed getting a sense of normal operations and charges. This should be done until monthly charges settle into a predictable pattern, at which point triggers may be used to alert of unusual charges.
What process is in place to handle new business units, applications, or other types of customers that begin utilizing the CCKS solution?	Without an intake process to support a charge-back model, the billing for services will likely not be appropriately allocated, possibly resulting in intra-organizational churn and conflict.

## 6. Conclusion

The CCKS pattern is seeing increased adoption and cloud providers are increasing the scenarios where external key stores are supported. Though generally more costly and challenging to operate, this pattern can enable a greater degree of assurance regarding customer data privacy in relationships with CSPs because some implementations allow for all encrypt and decrypt operations to occur outside the cloud service where customer data is stored and processed. However, it is critical to note that any implementation that aims to provide total data privacy (from the cloud provider) is inherently limited to non-SaaS scenarios because SaaS requires the ability to compute over customer data. Organizations may still find the valuable pattern useful for SaaS as a risk management measure that targets compliance measures, including regulatory obligations.

Organizations adopting this pattern need to be very cognizant of the assumption of security and availability risks, relative to the use of the Cloud Native KMS and Cloud KMS with External Key Origin patterns. Choosing this pattern requires a commitment to staffing and skills that are much more extensive and costly.

## 7. References

[AWS Key Management Service Developer Guide, 2022].	AWS. (2022). Identity and access management for AWS Key Management Service. <a href="https://docs.aws.amazon.com/kms/latest/developerguide/security-iam.html">https://docs.aws.amazon.com/kms/latest/developerguide/security-iam.html</a>
[AWS Key Management Service Developer Guide, 2022].	AWS. (2022). Using IAM policies with AWS KMS. <a href="https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html">https://docs.aws.amazon.com/kms/latest/developerguide/iam-policies.html</a>
[Authentication and access control for AWS KMS, 2022]	AWS. (2022). Authentication and access control for AWS KMS. <a href="https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html">https://docs.aws.amazon.com/kms/latest/developerguide/control-access.html</a>
[AWS Key Management Service FAQs, 2022]	AWS. (2022). Key Management Service FAQs. <a href="https://aws.amazon.com/kms/faqs/">https://aws.amazon.com/kms/faqs/</a>
[AWS Key Management Service. About Aliases, 2022]	AWS. (2022). Key Management Service. About Aliases. <a href="https://docs.aws.amazon.com/kms/latest/developerguide/alias-about.html">https://docs.aws.amazon.com/kms/latest/developerguide/alias-about.html</a>
[IBM DataPower Gateway, 2022]	IBM. (2022). DataPower Gateway. Creating Key Aliases. <a href="https://www.ibm.com/docs/en/datapower-gateway/10.0.1?topic=certificates-creating-key-aliases">https://www.ibm.com/docs/en/datapower-gateway/10.0.1?topic=certificates-creating-key-aliases</a>
[IBM Security Key Lifecycle Manager for z/OS, 2021]	IBM. (2021). Security Key Lifecycle Manager for z/OS. Generating Keys and Aliases for Encryption on LTO Ultrium 4 and LTO Ultrium 5. <a href="https://www.ibm.com/docs/en/sklmfz/1.1.0?topic=isklmzk-generating-keys-aliases-encryption-lto-ultrium-lto-ultrium">https://www.ibm.com/docs/en/sklmfz/1.1.0?topic=isklmzk-generating-keys-aliases-encryption-lto-ultrium-lto-ultrium</a>
[ISACA, 2019]	ISACA. (2019). COBIT Framework: Governance and Management Objectives ISBN 978-1-60420-728-6, Copyright © 2018 ISACA Information Systems Audit and Control Association 1700 E. Golf Road, Suite 400, Schaumburg IL 60173 USA;
[NIST, 2018]	National Institute of Standards and Technology. (2018). Framework for Improving Critical Infrastructure Cybersecurity version 1.1.
[NIST SP 800 57 Part 2, 2019]	NIST SP 800-57 Part 2 Rev. 1. (2019). Recommendation for Key Management: Part 2: Best Practices for Key Management Organizations. <a href="https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final">https://csrc.nist.gov/publications/detail/sp/800-57-part-2/rev-1/final</a>

[NIST SP 800 57 part 1, 2020]	SP 800-57 Part 1 Revision 5. (2020). Recommendation for Key Management: Part 1 – General. NIST Publishes Special Publication (SP) 800-57 Part 1
[NIST 800:38b, 2005]	NIST 800:38b. (2005). Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication. NIST SP 800-38B - NIST Page
AWS Cloud KMS	AWS Key Management Service (KMS) <a href="https://aws.amazon.com/kms/">https://aws.amazon.com/kms/</a> Importing key material in AWS Key Management Service (AWS KMS) <a href="https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys.html">https://docs.aws.amazon.com/kms/latest/developerguide/importing-keys.html</a>
Google Cloud	Cloud Key Management <a href="https://cloud.google.com/security-key-management">https://cloud.google.com/security-key-management</a> Customer-Supplied Encryption Keys <a href="https://cloud.google.com/security/encryption/customer-supplied-encryption-keys">https://cloud.google.com/security/encryption/customer-supplied-encryption-keys</a> Key Import <a href="https://cloud.google.com/kms/docs/key-import">https://cloud.google.com/kms/docs/key-import</a>
Microsoft Key Vault	Key Vault <a href="https://azure.microsoft.com/en-us/services/key-vault/">https://azure.microsoft.com/en-us/services/key-vault/</a> Import HSM-protected keys to Key Vault (BYOK) <a href="https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-byok">https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys-byok</a>
[Cloud Security Alliance, 2020]	CSA. (2020). Cloud Key Management Working Group. Key Management when using Cloud Services. <a href="https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/">https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/</a>
[Cloud Security Alliance, 2021]	Cloud Security Alliance. (2021). Cloud Key Management Working Group. Recommendations for Adopting a Cloud-Native KMS. <a href="https://cloudsecurityalliance.org/artifacts/recommendations-for-adopting-a-cloud-native-key-management-service/">https://cloudsecurityalliance.org/artifacts/recommendations-for-adopting-a-cloud-native-key-management-service/</a>
[NIST FIPS 140-3, 2019]	NIST FIPS 140-3 Security Requirements for Cryptographic Modules. (2019). <a href="https://csrc.nist.gov/publications/detail/fips/140/3/final">https://csrc.nist.gov/publications/detail/fips/140/3/final</a>



# Appendix A: Acronyms

Acronyms and abbreviations used in this paper are defined below.

<b>API</b>	Application Programming Interface
<b>AES</b>	Advanced Encryption Standard
<b>BYOK</b>	Bring Your Own Key
<b>CCKS</b>	Customer Controlled Key Store
<b>CCPA</b>	California Consumer Privacy Act
<b>CFO</b>	Chief Financial Officer
<b>CKMS</b>	Cloud Key Management Systems
<b>CMDB</b>	Configuration Management Database
<b>CMVP</b>	Cryptographic Module Validation Program
<b>CSC</b>	Cloud Service Customer
<b>CSO</b>	Cloud Service Offering
<b>CSP</b>	Cloud Service Provider
<b>DAR</b>	Data-at-Rest
<b>DISA SRG</b>	Defense Information Systems Agency Security Requirements Guide
<b>DOD/DoD</b>	Department of Defense
<b>EKO</b>	External Key Origin(ation)
<b>FFIEC</b>	Federal Financial Institutions Examination Council
<b>FIPS</b>	Federal Information Processing Standards
<b>FISMA</b>	Federal Information Security Management Act
<b>GDPR</b>	General Data Protection Regulation
<b>GLBA</b>	The Gramm-Leach-Bliley Act
<b>HSM</b>	Hardware Security Module
<b>IAM</b>	Identity Access Management
<b>IP</b>	Internet Protocol
<b>ISO</b>	International Organization for Standardization
<b>IT</b>	Information Technology
<b>KMS</b>	Key Management System/Key Management Server
<b>MFA</b>	Multifactor authentication
<b>NSA</b>	National Security Agency
<b>NIST</b>	National Institute of Standards and Technology
<b>PIM</b>	Privileged Identity Management
<b>PQ</b>	Post-Quantum
<b>RBAC</b>	Role-Based Access Control
<b>REST</b>	Representational State Transfer
<b>RPO</b>	Recovery Point Objective
<b>RTO</b>	Recovery Time Objective
<b>SDK</b>	Software Development Kit
<b>SIEM</b>	Security Information Event Management
<b>SLA</b>	Service-Level Agreement
<b>SOD</b>	Separation of Duties
<b>SSO</b>	Single Sign-On
<b>TLS</b>	Transport Layer Security
<b>VPN</b>	Virtual Private Network

# Appendix B: Glossary

Selected definitions for terms used in this paper are defined below.

## Alias

The **meaning** of **ALIAS**: otherwise known as —used to indicate an additional name that a person sometimes uses. ([Merriam-Webster dictionary](https://www.merriam-webster.com/dictionary/alias))

In cloud computing or programming languages it is an easier-to-understand or more significant name for a defined data object.

In key management, it is a string of characters. An added layer of security that supplies an indirect reference, or alias, to a file that contains a private key. It is a label for a specific key within a keystore. In this pattern's case an alias is created in order to be corresponded to a KMS key.

## Cloud-Native

Systems and applications are designed, developed, and deployed to (and for) the cloud to maximize cloud computing concepts, and architectural advantages, including speed, scalability, resiliency, and agility.

## External Key Origination

Refers to the generation of cryptographic keys outside of a cloud KMS and subsequently importing the key(s) to a cloud KMS.

## Cloud-Native KMS with an External Key Origination

Reflects the pattern where a customer has chosen to use a [public] cloud-hosted KMS that is designed and operated as a multi-tenant cloud service, including hardware-based key protection, and has also chosen to use one or more keys from an external source.<sup>16</sup>

## Cloud-Native CCKS

A KMS controlled by a customer of a cloud service. The cloud service has no control over the KMS.

## Cloud-Native KMS

Reflects the pattern where the KMS is built and owned by the same provider that delivers the cloud service the customer consumes, and all components of the KMS are in the cloud.<sup>17</sup>

## Break Glass Administrator

Provides the user immediate access to an account that they may not normally be authorized to access. This method is generally used for highest-level system accounts, such as root accounts for Unix or SYS/SA for a database.

These accounts are highly privileged and the break glass method limits them by the password time duration. The goal is to control and reduce the account's usage to that which is absolutely necessary to complete a certain task.

## Hardware Security Modules (HSMs)

Hardened, tamper-resistant hardware devices that strengthen encryption practices by generating keys, encrypting and decrypting data, and creating and verifying digital signatures.

[https://csrc.nist.gov/glossary/term/hardware\\_security\\_module\\_hsm](https://csrc.nist.gov/glossary/term/hardware_security_module_hsm)

<sup>16</sup> See <https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/> for the reasons a customer may choose an external key source, as well as the pros and cons of choosing this model.

<sup>17</sup> See <https://cloudsecurityalliance.org/artifacts/key-management-in-cloud-services/> page 12

## **Security information and event management (SIEM)**

This technology supports threat detection, and compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources. The core capabilities are a broad scope of log event collection and management, the ability to analyze log events and other data across disparate sources, and operational capabilities (such as incident management, dashboards, and reporting).  
<https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem>

## **Separation (Segregation) of Duties (SOD)**

Segregation of Duties is a fundamental building block of sustainable risk management and internal controls. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department.  
<https://www.aicpa.org/interestareas/informationtechnology/resources/value-strategy-through-segregation-of-duties.html>

## **Shared Responsibility**

The customer security team maintains some responsibilities for security as you move applications, data, containers, and workloads to the cloud. At the same time, the provider takes some responsibility, but not all. Defining the line between customer responsibilities and providers is imperative for reducing the risk of introducing vulnerabilities into your public, hybrid, and multi-cloud environments.  
<https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/>

## **Identity and Access Management (IAM)**

IAM is the information security process of protecting how users and devices are identified in a system and can access resources based on these identities.

Identity and access management (IAM) is the discipline that enables the right individuals to access the right resources at the right times for the right reasons.

IAM addresses the mission-critical need to ensure appropriate access to resources across increasingly heterogeneous technology environments and to meet increasingly rigorous compliance requirements. IAM is a crucial undertaking for any enterprise. It is increasingly business-aligned, and it requires business skills, not just technical expertise.

Enterprises that develop mature IAM capabilities can reduce their identity management costs and, more importantly, become significantly more agile in supporting new business initiatives.  
<https://www.gartner.com/en/information-technology/glossary/identity-and-access-management-iam>