**19SFC162- CLOUD SECURITY MODULE 4 NOTES**

**1.Examine the key features of Data Center Operations with its diagram**

**Characteristics of DataCenters:**



* **Data integrity:** Data integrity refers to mechanisms, such as error correction codes or parity bits, which ensure that data is stored and retrieved exactly as it was received.
* **Availability:** Availability of information as and when required should be ensured.  Unavailability of information can severely affect business operations, lead to substantial financial losses, and damage the reputation of an organization.
* **Security:** Policies and procedures should be established, and control measures should be implemented to prevent unauthorized access to and alteration of information.

[Where do we store DATA and INFORMATION ?](http://www.tsmtutorials.com/2016/06/storing-information.html)

* **Scalability:** Organizations may need to deploy additional resources such as compute systems, new applications, and databases to meet the growing requirements. Data center resources should scale to meet the changing requirements, without interrupting business operations.
* **Capacity:** Data center operations require adequate resources to efficiently store and process large and increasing amounts of data. When capacity requirements increase, additional capacity should be provided either without interrupting the availability or with minimal disruption. Capacity may be managed by adding new resources or by reallocating existing resources.
* **Performance:** Data center components should provide optimal performance based on the required service levels.
* **Manageability:** A data center should provide easy, flexible, and integrated management of all its components. Efficient manageability can be achieved through automation for reducing manual intervention in common, repeatable tasks.

**Managing a Datacenter**

Any Datacenter should be properly managed by the organisation to make the business running without disruptions. The activities carried out to ensure the efficient functioning of a data center can be broadly categorized under the following key management processes.

* **Planning:** It is a process of estimating the amount of IT resources required to support business operations and meet the changing resource requirements. Planning leverages the data collected during monitoring and enables improving the overall utilization and performance of resources. It also enables estimation of future resource requirements. Data center managers also determine the impact of incidents and devise contingency plans to resolve them.

[Introduction to the key Storage Management Operations](http://www.tsmtutorials.com/2016/09/Storage-Management-Operations-overview.html)

* **Provisioning:** It is the process of configuring and allocating the resources that are required to carry out business operations. For example, servers are provisioned to run applications and storage capacity is provisioned to a server. Provisioning primarily includes resource management activities to meet capacity, availability, performance, and security requirements.
* **Monitoring:** It is a continuous process of gathering information on various resources in the data center. The process involves monitoring parameters such as configuration, availability, capacity, performance, and security of resources.
* **Maintenance:** It is a set of standard repeatable activities for operating the data center. It involves ensuring the proper functioning of resources and resolving incidents such as malfunctions, outages, and equipment loss. It also involves handling identified problems or issues within the data center and incorporating changes to prevent future problem occurrence.
* **Reporting:** It is a process of collating and presenting the monitored parameters such as resource performance, capacity, and utilization of resources. Reporting enables data center managers to analyze and improve the utilization of data center resources and identify problems. It also helps in establishing business justifications and chargeback of costs associated with data center operations.

**2.Investigate the various issues of Security challenge**

Cloud computing in its many forms, has proven to be a powerful, effective set of technologies which can provide even the smallest enterprise with significant benefits.

However, cloud computing does not come without its own challenges, including those that are security related. Below you will find an overview of the key security challenges faced by cloud computing adopters.

**Lack of Visibility and Control**

Relating to both public and hybrid cloud environments, the loss of overall service visibility and the associated lack of control can be a problem.

Whether you’re dealing with public or hybrid cloud environments, a loss of visibility in the cloud can mean a loss of control over several aspects of IT management and data security. Where legacy style in-house infrastructure was entirely under the control of the company, cloud services delivered by third-party providers don’t offer the same level of granularity with regards to administration and management.

When it comes to visualizing potential security vulnerabilities, this lack of visibility can lead to a business failing to identify potential risks. In some sectors, such as media, cloud adoption is as [low as 17%](https://www.forbes.com/sites/louiscolumbus/2017/04/23/2017-state-of-cloud-adoption-and-security/#2ff59b131848), which has been blamed on this lack of visibility and control.

**Data Breaches and Downtime**

Despite the fact that generally speaking, enterprise-grade cloud services are more secure than legacy architecture, there is still a potential cost in the form of data breaches and downtime. With public and private cloud offerings, resolving these types of problems is in the hands of the third-party provider. Consequently, the business has very little control over how long critical business systems may be offline, as well as how well the breach is managed.

In the [12th annual Cost of Data Breach Study](https://www-03.ibm.com/security/uk-en/data-breach/), sponsored by IBM, it was found that the global cost of data breaches amounted to $3.62 million, so we can see how this particular issue is a major one with regard to cloud adoption.

**Vendor Lock-In**

For companies that come to rely heavily on public and hybrid cloud platforms, there is a danger that they become forced to continue with a specific third-party vendor simply to retain operational capacity. If critical business applications are locked into a single vendor, it can be very difficult to make tactical decisions such as moving to a new vendor. In effect, the vendor is being provided with the leverage it needs to force the customer into an unfavourable contract.

Logicworks recently [performed a survey](https://www.cio.com/article/2925773/cloud-security/cloud-security-transparency-is-crucial-for-service-providers.html) that found showed that some 78% of IT decision makers blame the fear of vendor lock-in as a primary reason for their organization failing to gain maximum value from cloud computing.

**Compliance Complexity**

In sectors such as healthcare and finance, where legislative requirements with regard to storage of private data are heavy, achieving full compliance whilst using public or private cloud offerings can be more complex.

Many enterprises attempt to gain compliance by using a cloud vendor that is deemed fully compliant. Indeed, data shows that [some 51% of firms in the USA](http://www.enterprisefeatures.com/privacy-and-data-security-in-the-cloud-statistics/) rely on nothing more than a statement of compliance from their cloud vendor as confirmation that all legislative requirements have been met.

But what happens when at a later stage, it is found that the vendor is not actually fully compliant? The client company could find itself facing non-compliance, with very little control over how the problem can be resolved.

**A Lack of Transparency**

When a business buys in third-party cloud services as either a public or hybrid cloud offering, it is likely they will not be provided with a full service description, detailing exactly how the platform works, and the security processes the vendor operates.

This lack of service transparency makes it hard for customers to intelligently evaluate whether their data is being stored and processed securely at all times. Surveys have shown that [around 75% of IT managers](https://www.cio.com/article/2925773/cloud-security/cloud-security-transparency-is-crucial-for-service-providers.html) are only marginally confident that company data is being stored securely by their cloud vendor.

**Insecure Interfaces and APIs**

Cloud vendors provide their customers with a range of Application Programming Interfaces (APIs), which the customer uses to manage the cloud service.

Unfortunately, not every API is entirely secure. They may have been deemed to be initially, and then at a later stage be found to be insecure in some way. This problem is compounded when the client company has built its own application layer on top of these APIs. The security vulnerability will then exist in the customer’s own application. This could be an internal application, or even a public facing application potentially exposing private data.

**Insufficient Due Diligence**

For companies that lack the internal resources to fully evaluate the implications of cloud adoption, then the risk of deploying a platform that is ineffective and even insecure is real.

Responsibility for specific issues of data security needs to be fully defined before any deployment. Failing to do so could lead to a situation where there is no clearly defined way to deal with potential risks and solve current security vulnerabilities.

**Shared Technology Vulnerabilities**

Using public or hybrid cloud offerings can expose a business to security vulnerabilities caused by other users of the same cloud infrastructure.

The onus is upon the cloud vendor to see that this does not happen, yet no vendor is perfect. It is always possible that a security vulnerability caused by another user in the same cloud will affect every user.

**Other Potential Threats**

Alongside the potential security vulnerabilities relating directly to the cloud service, there are also a number of external threats which could cause an issue. Some of these are:

* **Man in the Middle attacks** – where a third party manages to become a relay of data between a source and a destination. If this is achieved, the data being transmitted can be altered.
* **Distributed Denial of Service** – a DDoS attack attempts to knock a resource offline by flooding it with too much traffic.
* **Account or Service Traffic Hijacking** – a successful attack of this kind could provide an intruder with passwords or other access keys which allow them access to secure data.

**3.Characterize the steps to Implement Five Principal Characteristics of Cloud Computing**

**1. Resources Pooling**

It means that the [**Cloud provider**](https://data-flair.training/blogs/cloud-service-providers-companies/) pulled the computing resources to provide services to multiple customers with the help of a multi-tenant model. There are different physical and virtual resources assigned and reassigned which depends on the demand of the customer. The customer generally has no control or information over the location of the provided resources but is able to specify location at a higher level of abstraction

**2. On-Demand Self-Service**

It is one of the important and valuable features of Cloud Computing as the user can continuously monitor the server uptime, capabilities, and allotted network storage. With this feature, the user can also monitor the computing capabilities.

**3. Easy Maintenance**

The servers are easily maintained and the downtime is very low and even in some cases, there is no downtime. Cloud Computing comes up with an update every time by gradually making it better. The updates are more compatible with the devices and perform faster than older ones along with the bugs which are fixed.

**4. Large Network Access**

The user can access the data of the cloud or upload the data to the cloud from anywhere just with the help of a device and an internet connection. These capabilities are available all over the network and accessed with the help of internet.

**5. Availability**

The capabilities of the Cloud can be modified as per the use and can be extended a lot. It analyzes the storage usage and allows the user to buy extra [**Cloud storage**](https://data-flair.training/blogs/cloud-storage-tutorial/) if needed for a very small amount.

**6. Automatic System**

Cloud computing automatically analyzes the data needed and supports a metering capability at some level of services. We can monitor, control, and report the usage. It will provide transparency for the host as well as the customer.

**7. Economical**

It is the one-time investment as the company (host) has to buy the storage and a small part of it can be provided to the many companies which save the host from monthly or yearly costs. Only the amount which is spent is on the basic maintenance and a few more expenses which are very less.

**8. Security**

[**Cloud Security**](https://data-flair.training/blogs/cloud-security/), is one of the best features of cloud computing. It creates a snapshot of the data stored so that the data may not get lost even if one of the servers gets damaged. The data is stored within the storage devices, which cannot be hacked and utilized by any other person. The storage service is quick and reliable.

**9. Pay as you go**

In cloud computing, the user has to pay only for the service or the space they have utilized. There is no hidden or extra charge which is to be paid. The service is economical and most of the time some space is allotted for free.

**10. Measured Service**

Cloud Computing resources used to monitor and the company uses it for recording. This resource utilization is analyzed by supporting charge-per-use capabilities. This means that the resource usages which can be either virtual server instances that are running in the cloud are getting monitored measured and reported by the service provider. The model pay as you go is variable based on actual consumption of the manufacturing organization.

**4.Classify the various Data center Security Recommendations**

Data is a commodity that requires an active **data center security strategy** to manage it properly. A single breach in the system will cause havoc for a company and has long-term effects.

Are your critical workloads isolated from outside [cyber security threats](https://phoenixnap.com/blog/cyber-security-attack-types)? That’s the first guarantee you’ll want to know if your company uses (or plans to use) hosted services.

Breaches into trusted data centers tend to happen more often. The public notices when news breaks about advanced persistent threat (APT) attacks succeeding.

To stop this trend, service providers need to adopt a Zero Trust Model. From the physical structure to the networked racks, each component is designed with this in mind.

**Zero Trust Architecture**

The Zero Trust Model treats every transaction, movement, or iteration of data as suspicious. It’s one of the latest intrusion detection methods.

The system tracks network behavior, and data flows from a command center in real time. It checks anyone extracting data from the system and alerts staff or revokes rights from accounts an anomaly is detected.

**Security Layers and Redundancies of Data Centers**

Keeping your data safe requires security controls, and system checks built layer by layer into the structure of a data center. From the physical building itself, the software systems, and the personnel involved in daily tasks.

You can separate the layers into a physical or digital.

**Data Center Physical Security Standards**

**Location**

Assessing whether a data center is secure starts with the location.

A trusted Data Center’s design will take into account:

* Geological activity in the region
* High-risk industries in the area
* Any risk of flooding
* Other risks of force majeure

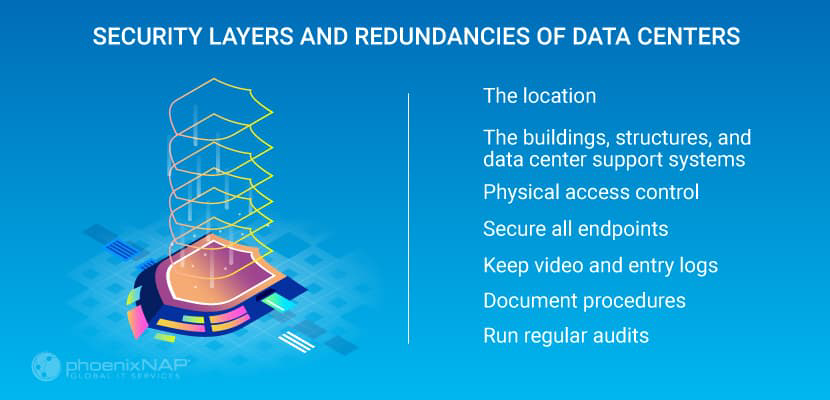
You can prevent some of the risks listed above by having barriers or extra redundancies in the physical design. Due to the harmful effects, these events would have on the operations of the data center; it’s best to avoid them altogether.

**The Buildings, Structures, and Data Center Support Systems**

The design of the structures that make up the data center needs to reduce any access control risks. The fencing around the perimeter, the thickness, and material of the building’s walls, and the number of entrances it has. All these affect the security of the data center.

Some key factors will also include:

* Server cabinets fitted with a lock.
* Buildings need more than one supplier for both telecom services and electricity.
* Extra [power backup systems like UPS and generators](https://phoenixnap.com/blog/data-center-power) are critical infrastructure.
* The use of mantraps. This involves having an airlock between two separate doors, with authentication required for both doors
* Take into account future expansion within the same boundary
* Separate support systems from the white spaces allow authorized staff members to perform their tasks. It also stops maintenance and service technicians from gaining unsupervised entry.

****

**Physical Access Control**

Controlling the movement of visitors and staff around the data center is crucial. If you have biometric scanners on all doors – and log who had access to what and when – it’ll help to investigate any potential breach in the future.

Fire escapes and evacuation routes should only allow people to exit the building. There should not be any outdoor handles, preventing re-entry. Opening any safety door should sound an alarm.

All vehicle entry points should use reinforced bollards to guard against vehicular attacks.

**Secure All Endpoints**

Any device, be it a server, tablet, smartphone or a laptop connected to a data center network is an endpoint.

Data centers give out rack and cage space to clients whose security standards may be dubious. If the customer doesn’t secure the server correctly, the entire data center might be at risk. Attackers are going to try to take advantage of unsecured devices connected to the internet.

For example, most customers want remote access to the power distribution unit (PDU), so they could remotely reboot their servers. Security is a significant concern in such use cases. It is up to facility providers to be aware of and secure all devices connected to the internet.

**Maintain Video and Entry Logs**

All logs, including video surveillance footage and entry logs, should be kept on file for a minimum of three months. Some breaches are identified when it is already too late, but records help identify vulnerable systems and entry points.

**Document Security Procedures**

Having strict, well-defined and documented procedures is of paramount importance. Something as simple as a regular delivery needs to well planned to its core details. Do not leave anything open for interpretation.

**Run Regular Security Audits**

Audits may range from daily security checkups, and physical walkthroughs to quarterly PCI and [SOC audits](https://phoenixnap.com/blog/soc-2-audit-compliance).

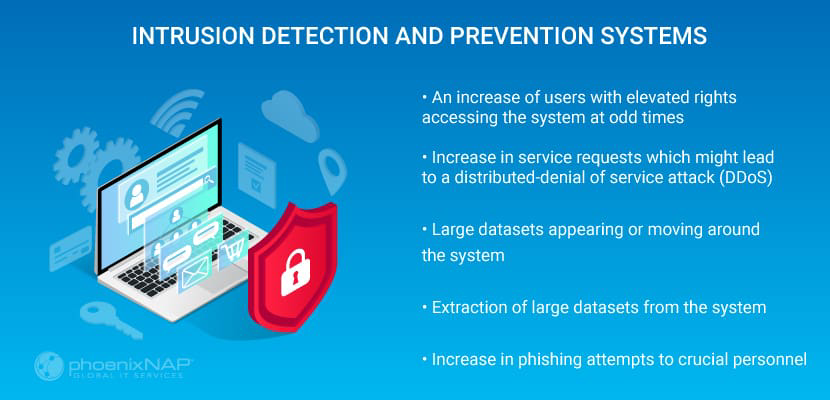
Physical audits are necessary to validate that the actual conditions conform to reported data.

**Digital Layers of Security in a Data Center**

As well as all the physical controls, software, and networks make up the rest of the security and access models for a trusted data center.

There are layers of digital protection that aim to prevent security threats from gaining access.

**Intrusion Detection and Prevention Systems**

****

This system checks for advanced persistent threats (APT). It focuses on finding those that have succeeded in gaining access to the data center. APTs are typically sponsored attacks, and the hackers will have a specific goal in mind for the data they have collected.

Detecting this kind of attack requires real-time monitoring of the network and system activity for any unusual events.

Unusual events could include:

* An increase of users with elevated rights accessing the system at odd times
* Increase in service requests which might lead to a distributed-denial of service attack (DDoS)
* Large datasets appearing or moving around the system
* Extraction of large datasets from the system
* Increase in phishing attempts to crucial personnel

To deal with this kind of attack, intrusion detection, and prevention systems (IDPS) use baselines of normal system states. Any abnormal activity gets a response. IDP now use artificial neural networks or machine learning technologies to find these activities.

**Security Best Practices for Building Management Systems**

Building management systems (BMS) have grown in line with other data center technologies. They can now manage every facet of a building’s systems. That includes access control, airflow, fire alarm systems, and ambient temperature.

A modern BMS comes equipped with many connected devices. They send data or receive instructions from a decentralized control system. The devices themselves may be a risk, as well as the networks they use. Anything that has an IP address is hackable.

**Secure Building Management Systems**

Security professionals know that the easiest way to take a data center off the map is by attacking its building management systems.

Manufacturers may not have security in mind when designing these devices, so patches are necessary. Something as insignificant as a sprinkler system can destroy hundreds of servers if set off by a cyber-attack.

**Segment the System**

Segmenting the building management systems from the main network is no longer optional. What’s more, even with such precautionary measures attackers can find a way to breach the primary data network.

During the infamous Target data breach, the building management system was on a physically separate network. However, that only slowed down the attackers as they eventually jumped from one network to another.

Which leads us to another critical point – monitor lateral movement.

**Lateral Movement**

Lateral movement is a set of techniques attackers use to move around devices and networks and gain higher privileges. Once attackers infiltrate a system, they map all devices and apps in an attempt to identify vulnerable components.

If the threat is not detected early on, attackers may gain privileged access and, ultimately, wreak havoc. Monitoring for lateral movement limits the time data center security threats are active inside the system.

Even with these extra controls, it is still possible that unknown access points can exist within the BMS.

**Secure at the Network Level**

The increased use of virtualization-based infrastructure has brought about a new level of security challenges. To this end, data centers are adopting a network level approach to security.

Network-level encryption is the use of cryptography at the network data-transfer layer, which is in charge of connectivity and routing between endpoints. The encryption is active during data transfer, and this type of encryption works independently from any other encryption, making it a standalone solution.

**Network Segmentation**

It is good practice to segment network traffic at the software level. This means classifying all traffic into different segments based on endpoint identity. Each segment is isolated from all other, thus acting as an independent subnet.

Network segmentation simplifies policy enforcing. Furthermore, it contains any potential threats in a single subnet, preventing it from attacking other devices and networks.

**Virtual Firewalls**

Although the data center will have a physical firewall as part of its security system, it may also have a virtual firewall for its customers. Virtual firewalls watch upstream network activity outside of the data center’s physical network. This helps in finding packet injections early without using essential firewall resources.

Virtual firewalls can be part of a [hypervisor](https://phoenixnap.com/kb/what-is-hypervisor-type-1-2) or live on their own virtualized machines in a bridged mode.

**Traditional Threat Protection Solutions**

Well-known threat protection solutions include:

* Virtualized private networks and encrypted communications
* Content, packet, network, spam, and virus filtering
* Traffic or netflow analyzers and isolators

The combination of these technologies will help make sure that data is safe while remaining accessible to the owners.

**Data Center Security Standards**

There is a trend in making data services safer and standardizing the security for data centers. In support of this, the [Uptime Institute](https://uptimeinstitute.com/tiers) published the Tier Classification System for data centers.

The classification system sets standards for data center’s’ controls that ensure availability. As security can affect the uptime of the system, it forms part of their [Tier Classification](https://phoenixnap.com/blog/data-center-tiers-classification) Standard.

There are four 4 tiers defined by the system. Each tier maps to a business need that depends on what kind of data is being stored and managed.

**Tiers 1 & 2**

Seen as tactical services, Tier 1 and 2 will only have some of the security features listed in this article. They are low cost and used by companies who do not want real-time access to their data and who won’t suffer financially due to a temporary system failure.

They are mainly used for offsite data storage.

**Tiers 3 & 4**

These tiers have higher levels of security. They have built-in redundancies that ensure uptime and access. Providing mission critical services for companies who know the cost of damage to a reputation a break in service creates.

These real-time data processing facilities provide the highest standards of security.

**Take Data Center Security Seriously**

More and more companies are moving their critical workloads and services to hosted servers and cloud computing infrastructure. Data centers are prime targets for bad actors.

Measuring your service providers against the best practices presented in this article is essential.

Don’t wait for the next major breach to occur before you take action to protect your data. No company wants to be the next Target or Equifax.

**5.Identify the necessary steps in Encryption for Confidentiality and Integrity**

**Data security in cloud computing**

With all the high-profile data breaches in the headlines over the last couple years, many people wonder if they can trust their data if it lives in the cloud.  Of course, anytime you use an Internet or Phone based app, data is accessed from Cloud infrastructure.  The conversation of data security in the cloud explains how the actual web or mobile app provider is accountable for the data protection, regardless of the Cloud platform.

The burden of protection and accountability is assumed by the software architecture team within the company that builds and manages critical data.  To ensure a high level of accountability, there are many regulatory measures that must be implemented within the IT operation.  The main framework is known as the CIA Triad - where data must maintain a specific level of Confidentiality, Integrity and Availability.  This blog highlights some of the practices companies leverage to maintain these measures.

A common misconception in Cloud computing is that data is not secure when hosted on 3rd party hardware.  While there have been numerous stories in the [headlines exposing data breaches](https://www.hackread.com/2018s-biggest-security-breaches-what-to-worry-in-2019/), the truth is that Cloud computing can be even more secure as opposed to when you host it in your own environment.  Regardless of the hardware and Cloud infrastructure, the software that a company delivers must maintain validated checks and balances to prove that data is safe.

**Keeping Cloud Computing Confidential**

Encryption is the means for which data privacy is protected and insured, modern encryption technologies are very mature.  V[endors that provide cloud storage have security measures](http://www.idexcel.com/blog/data-security-challenges-in-cloud-computing/) built into the platform that help protect the data. One example of this is having encryption on the data “at rest,” something a traditional file system would not have without additional software.  This means that data in encrypted, while sitting on a server, and no one in the outside world can make heads or tails from it.

When using Cloud apps, in theory, your data should be protected from unauthorized access.  This is because the online software provider uses encrypted data and enforces security controls over the infrastructure. There may also be situations where you want to make data available to certain personnel under certain circumstances – providers must be able to do this securely.  In the business world, all Cloud providers are [subject to the compliance](https://www.datamation.com/cloud-computing/data-security-in-cloud-computing.html) regulations that are dictated by their customers.  If they enter into an agreement, they must able to validate that secure measures are followed, and all breaches or losses must be disclosed.

Data breaches inevitably result in [diminished trust by customers](https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/). In one of the largest breaches of payment card data ever, cyber-criminals stole over 40 million customer credit and debit card numbers from Target. The breach led customers to stray away from Target stores and led to a loss of business for the company, which ultimately impacted the company’s revenue.  It is important to note that Target was collecting their customer's data and storing it within their own environments.  They were not able to uncover the vulnerabilities that led to the breach.

When companies scale their environment to the size of an enterprise like Target (or other high profile breaches), they must have a solid foundation with layers of management and software.  A critical cyber security operation should be managed 24x7x365 with human eyeballs and have data coming from as many points as possible.

**Maintaining Data Integrity in the Cloud**

Data integrity can be [defined as protecting data](https://pdfs.semanticscholar.org/2760/46ac1e0fa92763a1444a8097bf81a79a54f9.pdf) from unauthorized modification or deletion.  An example of this is easily understood if you think about online banking.  If specific administrators have access to bank accounts, how are they held accountable and protect the bank from illegal changes?  There must be a system of permissions and logs that can demonstrate that there is no inappropriate access to customer data.

With cloud computing, there are large amounts of data, coming from many sources.  A Cloud system will deliver the access in its base form, but it is up to the cloud app developer to define means of access.   Authorization is crucial in assuring that only specific entities can interact with data and that there are ways of producing the proof.  In a cloud environment, data integrity must be maintained at all times to avoid any inherent data loss.

**Ensuring Data Availability and Cloud Access**

Cloud and Infrastructure engineers always plan for inevitable network failures and downtime. There are [several architectural concepts](https://www.datamation.com/cloud-computing/data-security-in-cloud-computing.html) that must be takes to insure that data is highly available in a Cloud infrastructure.

[Data availability](https://searchstorage.techtarget.com/definition/data-availability) is a term used by some computer storage manufacturers and storage service providers (SSPs) to describe products and services that ensure that data continues to be available, at a required level of performance, in situations ranging from normal to disastrous.  Within a Server or Storage Network, architects must build out the storage component with redundancy.  Often, they will build in twice the number of drives that would ever be used to make sure there is always 2X the level of availability in case there are failures.

Now with the advent of Public Cloud providers like AWS, subscribers can dictate what region(s) data is stored in. To increase availability data can replicated or backed up across various availability zones and geographic regions.   This is important because it not only helps with compliance but also increases response time/latency on a global scale.

A Cloud platform is a tool that software developers can use to make their product better.  Right out of the box, Public Cloud providers like Microsoft (99.9% availability) and AWS (99.99% availability) deliver availability SLAs (Service Level Agreements) for stored objects. If a web application provider must deliver a better SLA to their clients, it is up to them to engineer redundant/fault tolerant networks to back up, replicate and maintain copies of customer data.

When selecting a Cloud partner, it is important to know where your baseline SLA is so that you can build off it.  Businesses must pay close attention to these SLA definitions because they will share the burden of downtime if there is a loss of data from a cloud provider.  For the typical consumer, SLAs are as big of a concern because the app is usually free.  Consumers must trust that the technology provider is taking these measures and ensuring that your data is safe.

**Air-Tight Security Controls for Cloud Computing Services**

Access control is a security technique that regulates who or what can view or use resources in a computing environment.   Companies that run online applications must comply with regulatory requirements and define access controls in accordance with their verticals.  Practices must be validated with regularly security checks, measures and audits.

[When running a complaint (secure) Cloud operation](https://techbeacon.com/security/how-maintain-security-compliance-cloud), specific measures and practices must be defined on how you manage your infrastructure - this is known as change management.  These reports must outline even the most minute of details such as: defining the specific steps to be taken when making changes on a firewall.

Most employee-related incidents are not malicious however, your greatest threat could be inside your walls.  According to the Ponemon Institute’s *2016* [*Cost of Insider Threats Study*](https://www.observeit.com/ponemon-report-cost-of-insider-threats/), 598 of the 874 insider related incidents in 2016 were caused by careless employees or contractors. It also found 85 incidents due to imposters stealing credentials and 191 were by malicious employees and criminals.

To fight off internal threats, compliant employers must manage their networks responsibly by enforcing company policies that mitigate threats.  For example, they should require intricate passwords and automatically ask for changes every 1-3 months.  2 Factor Authentication can also be implemented to validate every log-in and stop brute force bots.  On a larger scale, the network administrators must have strong visibility with analytical data to see complex, distributed networks (on Cloud Servers and Cloud Storage). They must install, configure and operate sophisticated software that continuously scans the network looking for vulnerabilities, abnormal activity and the movement of large quantities of data.

**Industry Compliance for Cloud Infrastructure**

Compliance is dictating much of the required security measures and it is becoming more and more sophisticated.  Anyone holding European data must follow the guidelines of the recently enforced GDPR (Global Data Protection Regulation) and California has also implemented their own version called CCPA (California Consumer Privacy Act).  HIPAA, HITRUST, SOX, PCI, NIST etc. are all defined regulatory compliance measures that specifically cater to verticals such as Medical Records, Financial Data etc.

The [definition of compliance](https://searchcompliance.techtarget.com/definition/compliance-audit) is either a state of being in accordance with established guidelines or specifications or the process of becoming so. The definition of compliance can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation.  This allows companies the freedom to grow as long as they can [demonstrate that they are defining policies](https://techcrunch.com/2019/04/02/how-to-handle-dark-data-compliance-risk-at-your-company/) and improving their security  practices along that path.  The market generally pushes this agenda as it becomes more challenging to sell a product against competition if your product is not verifiably complaint.

A [compliance audit](https://searchdatamanagement.techtarget.com/definition/compliance) is a comprehensive review of an organization's adherence to regulatory guidelines.  Audit reports evaluate the strength and thoroughness of compliance preparations, security policies, user access controls, and risk management procedures over the course of a compliance audit.  These reports need to be validated and run by a third party that specializes in cyber security and general IT practices.

**6.Illustrate the key points in relation with Encrypting data at rest**

**What is encryption at rest?**

Encryption at Rest is the encoding (encryption) of data when it is persisted. The Encryption at Rest designs in Azure use symmetric encryption to encrypt and decrypt large amounts of data quickly according to a simple conceptual model:

* A symmetric encryption key is used to encrypt data as it is written to storage.
* The same encryption key is used to decrypt that data as it is readied for use in memory.
* Data may be partitioned, and different keys may be used for each partition.
* Keys must be stored in a secure location with identity-based access control and audit policies. Data encryption keys are often encrypted with a key encryption key in Azure Key Vault to further limit access.

In practice, key management and control scenarios, as well as scale and availability assurances, require additional constructs. Microsoft Azure Encryption at Rest concepts and components are described below.

**The purpose of encryption at rest**

Encryption at rest provides data protection for stored data (at rest). Attacks against data at-rest include attempts to obtain physical access to the hardware on which the data is stored, and then compromise the contained data. In such an attack, a server’s hard drive may have been mishandled during maintenance allowing an attacker to remove the hard drive. Later the attacker would put the hard drive into a computer under their control to attempt to access the data.

Encryption at rest is designed to prevent the attacker from accessing the unencrypted data by ensuring the data is encrypted when on disk. If an attacker obtains a hard drive with encrypted data but not the encryption keys, the attacker must defeat the encryption to read the data. This attack is much more complex and resource consuming than accessing unencrypted data on a hard drive. For this reason, encryption at rest is highly recommended and is a high priority requirement for many organizations.

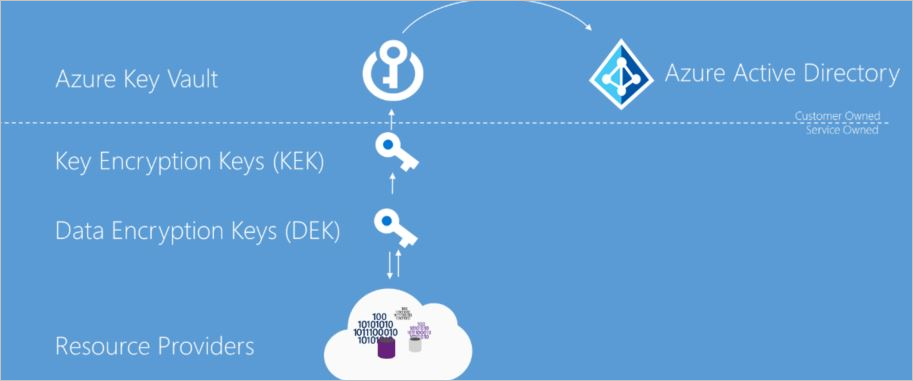
Encryption at rest may also be required by an organization’s need for data governance and compliance efforts. Industry and government regulations such as HIPAA, PCI and FedRAMP, lay out specific safeguards regarding data protection and encryption requirements. Encryption at rest is a mandatory measure required for compliance with some of those regulations.

In addition to satisfying compliance and regulatory requirements, encryption at rest provides defense-in-depth protection. Microsoft Azure provides a compliant platform for services, applications, and data. It also provides comprehensive facility and physical security, data access control, and auditing. However, it's important to provide additional “overlapping” security measures in case one of the other security measures fails and encryption at rest provides such a security measure

Microsoft is committed to encryption at rest options across cloud services and giving customers control of encryption keys and logs of key use. Additionally, Microsoft is working towards encrypting all customer data at rest by default.

**Azure Encryption at Rest Components**

As described previously, the goal of encryption at rest is that data that is persisted on disk is encrypted with a secret encryption key. To achieve that goal secure key creation, storage, access control, and management of the encryption keys must be provided. Though details may vary, Azure services Encryption at Rest implementations can be described in terms illustrated in the following diagram.



**Azure Key Vault**

The storage location of the encryption keys and access control to those keys is central to an encryption at rest model. The keys need to be highly secured but manageable by specified users and available to specific services. For Azure services, Azure Key Vault is the recommended key storage solution and provides a common management experience across services. Keys are stored and managed in key vaults, and access to a key vault can be given to users or services. Azure Key Vault supports customer creation of keys or import of customer keys for use in customer-managed encryption key scenarios.

**Azure Active Directory**

Permissions to use the keys stored in Azure Key Vault, either to manage or to access them for Encryption at Rest encryption and decryption, can be given to Azure Active Directory accounts.

**Key Hierarchy**

More than one encryption key is used in an encryption at rest implementation. Storing an encryption key in Azure Key Vault ensures secure key access and central management of keys. However, service local access to encryption keys is more efficient for bulk encryption and decryption than interacting with Key Vault for every data operation, allowing for stronger encryption and better performance. Limiting the use of a single encryption key decreases the risk that the key will be compromised and the cost of re-encryption when a key must be replaced. Azure encryptions at rest models use a key hierarchy made up of the following types of keys in order to address all these needs:

* **Data Encryption Key (DEK)** – A symmetric AES256 key used to encrypt a partition or block of data. A single resource may have many partitions and many Data Encryption Keys. Encrypting each block of data with a different key makes crypto analysis attacks more difficult. Access to DEKs is needed by the resource provider or application instance that is encrypting and decrypting a specific block. When a DEK is replaced with a new key only the data in its associated block must be re-encrypted with the new key.
* **Key Encryption Key (KEK)** – An encryption key used to encrypt the Data Encryption Keys. Use of a Key Encryption Key that never leaves Key Vault allows the data encryption keys themselves to be encrypted and controlled. The entity that has access to the KEK may be different than the entity that requires the DEK. An entity may broker access to the DEK to limit the access of each DEK to a specific partition. Since the KEK is required to decrypt the DEKs, the KEK is effectively a single point by which DEKs can be effectively deleted by deletion of the KEK.

The Data Encryption Keys, encrypted with the Key Encryption Keys are stored separately and only an entity with access to the Key Encryption Key can decrypt these Data Encryption Keys. Different models of key storage are supported. We will discuss each model in more detail later in the next section.

**Data Encryption Models**

An understanding of the various encryption models and their pros and cons is essential for understanding how the various resource providers in Azure implement encryption at Rest. These definitions are shared across all resource providers in Azure to ensure common language and taxonomy.

There are three scenarios for server-side encryption:

* Server-side encryption using Service-Managed keys
  + Azure Resource Providers perform the encryption and decryption operations
  + Microsoft manages the keys
  + Full cloud functionality
* Server-side encryption using customer-managed keys in Azure Key Vault
  + Azure Resource Providers perform the encryption and decryption operations
  + Customer controls keys via Azure Key Vault
  + Full cloud functionality
* Server-side encryption using customer-managed keys on customer-controlled hardware
  + Azure Resource Providers perform the encryption and decryption operations
  + Customer controls keys on customer-controlled hardware
  + Full cloud functionality

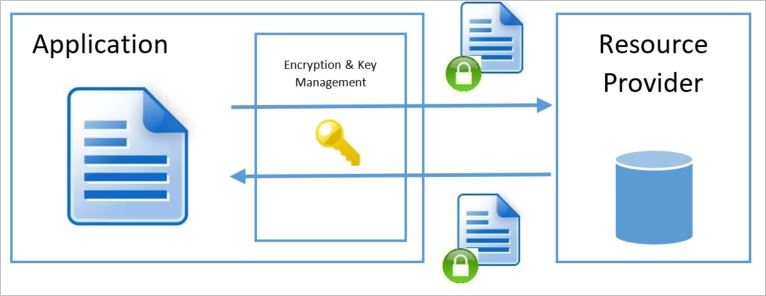
For client-side encryption, consider the following:

* Azure services cannot see decrypted data
* Customers manage and store keys on-premises (or in other secure stores). Keys are not available to Azure services
* Reduced cloud functionality

The supported encryption models in Azure split into two main groups: “Client Encryption” and “Server-side Encryption” as mentioned previously. Independent of the encryption at rest model used, Azure services always recommend the use of a secure transport such as TLS or HTTPS. Therefore, encryption in transport should be addressed by the transport protocol and should not be a major factor in determining which encryption at rest model to use.

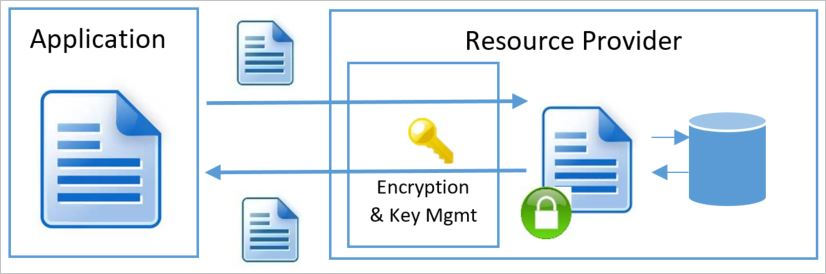
**Client encryption model**

Client Encryption model refers to encryption that is performed outside of the Resource Provider or Azure by the service or calling application. The encryption can be performed by the service application in Azure, or by an application running in the customer data center. In either case, when leveraging this encryption model, the Azure Resource Provider receives an encrypted blob of data without the ability to decrypt the data in any way or have access to the encryption keys. In this model, the key management is done by the calling service/application and is opaque to the Azure service.



**Server-side encryption model**

Server-side Encryption models refer to encryption that is performed by the Azure service. In that model, the Resource Provider performs the encrypt and decrypt operations. For example, Azure Storage may receive data in plain text operations and will perform the encryption and decryption internally. The Resource Provider might use encryption keys that are managed by Microsoft or by the customer depending on the provided configuration.



**Server-side encryption key management models**

Each of the server-side encryption at rest models implies distinctive characteristics of key management. This includes where and how encryption keys are created, and stored as well as the access models and the key rotation procedures.

**Server-side encryption using service-managed keys**

For many customers, the essential requirement is to ensure that the data is encrypted whenever it is at rest. Server-side encryption using service-managed Keys enables this model by allowing customers to mark the specific resource (Storage Account, SQL DB, etc.) for encryption and leaving all key management aspects such as key issuance, rotation, and backup to Microsoft. Most Azure Services that support encryption at rest typically support this model of offloading the management of the encryption keys to Azure. The Azure resource provider creates the keys, places them in secure storage, and retrieves them when needed. This means that the service has full access to the keys and the service has full control over the credential lifecycle management.

Server-side encryption using service-managed keys therefore quickly addresses the need to have encryption at rest with low overhead to the customer. When available a customer typically opens the Azure portal for the target subscription and resource provider and checks a box indicating, they would like the data to be encrypted. In some Resource Managers server-side encryption with service-managed keys is on by default.

Server-side encryption with Microsoft-managed keys does imply the service has full access to store and manage the keys. While some customers may want to manage the keys because they feel they gain greater security, the cost and risk associated with a custom key storage solution should be considered when evaluating this model. In many cases, an organization may determine that resource constraints or risks of an on-premises solution may be greater than the risk of cloud management of the encryption at rest keys. However, this model might not be sufficient for organizations that have requirements to control the creation or lifecycle of the encryption keys or to have different personnel manage a service’s encryption keys than those managing the service (that is, segregation of key management from the overall management model for the service).

**Key access**

When Server-side encryption with service-managed keys is used, the key creation, storage, and service access are all managed by the service. Typically, the foundational Azure resource providers will store the Data Encryption Keys in a store that is close to the data and quickly available and accessible while the Key Encryption Keys are stored in a secure internal store.

**Advantages**

* Simple setup
* Microsoft manages key rotation, backup, and redundancy
* Customer does not have the cost associated with implementation or the risk of a custom key management scheme.

**Disadvantages**

* No customer control over the encryption keys (key specification, lifecycle, revocation, etc.)
* No ability to segregate key management from overall management model for the service

**Server-side encryption using customer-managed keys in Azure Key Vault**

For scenarios where the requirement is to encrypt the data at rest and control the encryption keys customers can use server-side encryption using customer-managed Keys in Key Vault. Some services may store only the root Key Encryption Key in Azure Key Vault and store the encrypted Data Encryption Key in an internal location closer to the data. In that scenario customers can bring their own keys to Key Vault (BYOK – Bring Your Own Key), or generate new ones, and use them to encrypt the desired resources. While the Resource Provider performs the encryption and decryption operations, it uses the configured key encryption key as the root key for all encryption operations.

Loss of key encryption keys means loss of data. For this reason, keys should not be deleted. Keys should be backed up whenever created or rotated. [Soft-Delete](https://docs.microsoft.com/azure/key-vault/key-vault-ovw-soft-delete) should be enabled on any vault storing key encryption keys. Instead of deleting a key, set enabled to false or set the expiry date.

**Key Access**

The server-side encryption model with customer-managed keys in Azure Key Vault involves the service accessing the keys to encrypt and decrypt as needed. Encryption at rest keys are made accessible to a service through an access control policy. This policy grants the service identity access to receive the key. An Azure service running on behalf of an associated subscription can be configured with an identity in that subscription. The service can perform Azure Active Directory authentication and receive an authentication token identifying itself as that service acting on behalf of the subscription. That token can then be presented to Key Vault to obtain a key it has been given access to.

For operations using encryption keys, a service identity can be granted access to any of the following operations: decrypt, encrypt, unwrapKey, wrapKey, verify, sign, get, list, update, create, import, delete, backup, and restore.

To obtain a key for use in encrypting or decrypting data at rest the service identity that the Resource Manager service instance will run as must have UnwrapKey (to get the key for decryption) and WrapKey (to insert a key into key vault when creating a new key).

**Note**

For more detail on Key Vault authorization see the secure your key vault page in the [**Azure Key Vault documentation**](https://docs.microsoft.com/en-us/azure/key-vault/key-vault-secure-your-key-vault).

**Advantages**

* Full control over the keys used – encryption keys are managed in the customer’s Key Vault under the customer’s control.
* Ability to encrypt multiple services to one master
* Can segregate key management from overall management model for the service
* Can define service and key location across regions

**Disadvantages**

* Customer has full responsibility for key access management
* Customer has full responsibility for key lifecycle management
* Additional Setup & configuration overhead

**Server-side encryption using customer-managed keys in customer-controlled hardware**

Some Azure services enable the Host Your Own Key (HYOK) key management model. This management mode is useful in scenarios where there is a need to encrypt the data at rest and manage the keys in a proprietary repository outside of Microsoft’s control. In this model, the service must retrieve the key from an external site. Performance and availability guarantees are impacted, and configuration is more complex. Additionally, since the service does have access to the DEK during the encryption and decryption operations the overall security guarantees of this model are similar to when the keys are customer-managed in Azure Key Vault. As a result, this model is not appropriate for most organizations unless they have specific key management requirements. Due to these limitations, most Azure Services do not support server-side encryption using server-managed keys in customer-controlled hardware.

**Key Access**

When server-side encryption using service-managed keys in customer-controlled hardware is used the keys are maintained on a system configured by the customer. Azure services that support this model provide a means of establishing a secure connection to a customer supplied key store.

**Advantages**

* Full control over the root key used – encryption keys are managed by a customer provided store
* Ability to encrypt multiple services to one master
* Can segregate key management from overall management model for the service
* Can define service and key location across regions

**Disadvantages**

* Full responsibility for key storage, security, performance, and availability
* Full responsibility for key access management
* Full responsibility for key lifecycle management
* Significant setup, configuration, and ongoing maintenance costs
* Increased dependency on network availability between the customer datacenter and Azure datacenters.

**7.Draw the architecture of Encryption and Key Management in cloud security**

**Key Management**

As organizations move increasing amounts of sensitive data to their IaaS, PaaS, SaaS and cloud services provider environments, strong encryption key management is more essential than ever. Separating data from keys is required by many compliance mandates and meets security best practices outlined by the [Cloud Security Alliance](https://cloudsecurityalliance.org/group/cloud-controls-matrix/), among others.

Thales eSecurity provides robust, scalable cloud encryption key management solutions that align with any cloud strategy and help ensure that the enterprise controls its own data. Our partnerships include all major players in cloud computing, and continue to grow as enterprises increase their adoption of the cloud.

* [Challenges](https://www.thalesesecurity.com/solutions/use-case/cloud-security/key-management#tab1)
* [Solutions](https://www.thalesesecurity.com/solutions/use-case/cloud-security/key-management#tab2)
* [Benefits](https://www.thalesesecurity.com/solutions/use-case/cloud-security/key-management#tab3)

**Secure Key Management for Traditional Cloud Data**

Enterprises enjoy numerous benefits from offloading workloads to traditional cloud services providers, such as co-location services, managed services providers and others, but still need to ensure the security of their data. Some cloud providers permit "bring your own" encryption, while others offer encryption natively. While the data encryption may occur in the cloud provider's environment, customers must maintain control of the keys that secure their data.

**Secure Key Management for SaaS Data**

[Gartner](http://www.gartner.com/newsroom/id/3188817) reports that enterprises now spend tens of billions of dollars on software-as-a-service offerings, with continued growth expected. While some SaaS providers have added encryption to their increasingly powerful applications, ensuring the security of sensitive data is ultimately the customer's responsibility. This includes key management in compliance with data security and privacy mandates.

**Secure Key Management for Public Cloud Data**

When using public cloud services such as AWS, Microsoft Azure or others, some enterprises will send encrypted data to the cloud, while others may utilize the encryption offered by the cloud provider. Whichever security key management process applies to your enterprise, controlling the encryption keys is critical to maintaining control of your data.

**SOLUTIONS**

**Key Management Solutions for Traditional Cloud Services**

Thales eSecurity partners with leading cloud services providers to support enterprise data encryption strategies. Whether you leverage a [Vormetric Data Security Manager](https://www.thalesesecurity.com/products/data-encryption/vormetric-data-security-manager) deployed in the provider's environment or you deploy your own DSM, we work with CSPs to ensure you have control over the encryption keys.

**Key Management Solutions for SaaS**

Thales eSecurity offers the [CipherTrust Cloud Key Manager](https://www.thalesesecurity.com/products/key-management/ciphertrust-cloud-key-manager) for a growing number of SaaS solutions including Microsoft Office365 and for [Salesforce.com users of Salesforce Shield Platform Encryption.](https://www.salesforce.com/products/platform/products/shield/) Many other SaaS providers utilize [Vormetric Transparent Encryption](https://www.thalesesecurity.com/products/data-encryption/vormetric-transparent-encryption), which can provide a unique key per customer. We work to partner with other leading SaaS providers to enable them first to encrypt sensitive data and then enable customers to bring their own keys to enhance regulatory compliance.

**Key Management Solutions for Public Cloud Services**

To alleviate concerns about unauthorized access to encryption keys, as well as potential compliance violations, Thales eSecurity offers the CipherTrust Cloud Key Manager for comprehensive, web-based key lifecycle management. CipherTrust Cloud Key Manager leverages Bring Your Own Key (BYOK) APIs offered by public cloud providers such as Amazon Web Services, Microsoft Azure and Salesforce.com.

For protection beyond vendor-provided encryption and external key management, you can bring your own encryption (BYOE) and manage your own keys with Vormetric Transparent Encryption agents protecting data in the cloud and the [Vormetric Data Security Manager](https://www.thalesesecurity.com/products/data-encryption/vormetric-data-security-manager) operating on your premises or in the cloud.

**BENEFITS**

**Security and Regulatory Compliance**

Whatever cloud strategy you leverage - traditional, SaaS, public or hybrid - Thales eSecurity helps you separate the keys from the data to ensure compliance with regulations and standards such as PCI DSS, HIPAA and others.

**Gain Privileged User Access Controls and Security Intelligence**

Gain distinct advantages when you bring your own encryption (BYOE) to public cloud providers:

* Granular access controls that prevent risk of data loss due to compromised privileged user credentials.
* Detailed security management logs that specify which processes and users have accessed protected data.

Learn more at [Vormetric Transparent Encryption](https://www.thalesesecurity.com/products/data-encryption/vormetric-transparent-encryption)

**Efficient and Convenient Key Management**

A web interface to the CipherTrust Cloud Key Manager gives you control of your sensitive data in SaaS, IaaS and PaaS environments.

**Maintain the Flexibility to Change CSPs**

With Thales eSecurity's easy-to-use key management, enterprises can more easily move their data to other cloud environments. When you control your sensitive data in the cloud, you can rapidly change infrastructure providers as business requirements change.

**8.Categorize various process in development of Key Management Lifecycle**

**Importance of Key Lifecycle Management**

The most important aspect to consider is what the key is used for. One should always be careful not to use any key for different purposes. Here an important distinction is made between data keys (used to encrypt data) and key-encryption-keys (KEKs), which are used entirely to protect other keys. Keys are, fundamentally, used for encryption - but encryption often acts as a very cunning proxy for other uses such as authentication and signing (you can prove who you are based on ownership of a key).

**Determination of the key’s operational lifetime and key strength**

Once a key is generated, the key-management system should control the sequence of states that a key progresses over its lifecycle, and allow an authorized administrator to handle them when necessary. The [National Institute of Standards and Technology (NIST)](http://www.nist.gov/public_affairs/nandyou.cfm) provides strict guidelines for most aspects of the life cycle of cryptographic keys and has also defined some standards on how a crypto period is determined for each key. A crypto period is the operational life of a key, and is determined by a number of factors based on:

* The sensitivity of the data or keys to be protected
* How much data or how many keys are being protected

From this information, the operational life of the key can be determined, along with the key length (which is proportional to the cryptographic strength of the system). The algorithm (and, therefore, the key type) is determined by the purpose of the key; for example, DSA is applicable to a signing purpose only whereas RSA is appropriate for both signing and encryption. NIST specifies cryptographic algorithms that have withstood the test of time.

**The occasional need to change a key state based on unexpected circumstances**

There are instances when it is necessary for an authorized administrator to make changes to the key's parameters which cause a change in its state during a life-cycle. (Some of these can still be automatically taken care of through the key-management system.)

* Whether the key or associated data or encrypted key is suspected of compromise
* Change in vendor support of product or need to replace product
* Technological advances that make it possible to attack where it was previously infeasible
* Change of ownership where a change of keys is associated with a change in assignment of liability
* Regulatory requirements, contractual requirements, or policy (crypto-period) that mandates a maximum operational life

**Description of the basic phases of a key life cycle**

The following paragraphs examine the phases of a key lifecycle and how a key management solution should operate during these phases. Note that every [key-management solution](https://www.cryptomathic.com/products/key-management) is different, so not all of them will use the same phases. Some are not used at all, and other phases can be added, such pre-activation, activation, and post-activation.

**Generation**

Keys can be generated through a [key management system](https://www.cryptomathic.com/products/key-management/crypto-key-management-system), hardware security module (HSM) or by a trusted third party(TTP), which should use a cryptographically secure true random number generator (TRNG) for seeds.The keys, along with all their attributes, will then be stored in the key storage database (which must be encrypted by a master key). Attributes include items like name, activation date, size, and instance. A key can be activated upon its creation or set to be activated automatically or manually at a later time.

Each key should have a key strength (generally measured in number of bits) associated with it that can provide adequate protection for the entire useful lifetime of the protected data along with the ability to withstand attacks during this lifetime. The different key lengths will depend on the algorithm that uses it. A standard cryptographic algorithm is recommended that has been thoroughly evaluated and tested.

***Backup and Storage***

In order to retrieve a key that has been lost during its use (for example due to equipment failure or forgotten passwords), a secure backup copy should be made available. Backup keys can be stored in a protected form on external media (CD, USB drive, etc.) or by using an existing traditional backup solution (local or networked). When a [symmetric key or an asymmetric](http://resources.infosecinstitute.com/symmetric-asymmetric-encryption/) private key is being backed up, it must be encrypted before being stored.

**Distribution and Loading**

The objective of the deployment and loading phase is to install the new key into a secure cryptographic device, either manually or electronically. This is the most critical phase for key security and should only be performed by authorized personnel in case of manual installation. For manual distribution, which is by far the most common method of shared key distribution in the payments space, key encryption keys (KEKs) must be distributed and loaded in key shares to avoid the full key being viewed in the clear. Once the KEK is installed, data keys can then be shared securely since they can be encrypted (also known as wrapped, in this context). Best practice key management standards (such as PCI DSS) are now mandating that - as well as encrypting the key material - the key usage needs to be equally secured (e.g. PIN block encryption/decryption). While this is a very secure, well-known and established method of key distribution - it is labor intensive and it does not scale well (you need a new KEK for every point that you share a key with); for larger scale key deployments (e.g. managing keys for an entire secure web server farm), asymmetric key distribution techniques are really the only feasible way. In this case, the initial step of sharing a KEK using key shares is displaced by the simple technique of deploying a public key. Keys can then be transmitted securely as long as the public key (or its fingerprint) gets adequately authenticated.

Cryptomathic CKMS - Automated Key and Certificate Distribution

**Normal Use and Replacement**

The key management system should allow an activated key to be retrieved by authorized systems and users e.g. for encryption or decryption processes, or MAC generation and verification. It should also seamlessly manage current and past instances of the encryption key.

The key manager will replace a key automatically through a previously established schedule (according to the key's expiration date or crypto-period) or if it is suspected of compromise (which might be achieved manually by an authorized administrator.) When replacing keys, the intent is to bring a replacement key into active use by the system, and typically to also re-encrypt  all stored data under the new key (for example if the key was used for S/MIME or Encrypting File System) but if the new key has to be used for new sessions such as TLS then old data doesn’t need to be secured by the new key. Replacing keys can be difficult because it necessitates additional procedures and protocols, which may include correspondence with third parties in public-key systems.

The timing for expiration depends on the strength of the key (key length) and how long the protected data or key will be valid. In common practice, keys expire and are replaced in a time-frame shorter than the calculated life span of the key. As a key is replaced, the old key is not totally removed, but remains archived so is retrievable under special circumstances (e.g., settling disputes involving repudiation).

**Archival**

Archival refers to offline long-term storage for keys that are no longer in operation. These keys usually have data associated with them that may be needed for future reference, such as long term storage of emails. There may also be associated data in other external systems.

When archiving a key, it must be encrypted to add security. As recommended in the Creation and Deployment phases, it may be useful to encrypt a symmetric key with the public key of an asymmetric key pair so that the person/entity holding the corresponding private key can only decrypt it. Sometimes (depending on the key’s deployment scenario), archival is the last phase in the life process, and never moves on to deletion or destruction.

An archived key cannot be used for cryptographic requests. In certain cases the key can continue to be used to e.g. decrypt data previously encrypted with it, like old backups, but even that can be restricted. An archived key can, if needed, be reactivated by an administrator. Before a key is archived, it should be proven that no data is still being secured with the old key.

**End of Key's Life-cycle**

The last phase is the end of the key's life-cycle, where all of its instances, or just certain instances, are completely removed, and recovery of that key may be possible, depending on the method used. The end of life for a key should only occur after an adequately long Archival phase, and after adequate analysis to ensure that loss of the key will not correspond to loss of data or other keys.

There are three methods of removing a key from operation:

* *Key destruction:* This method removes an instance of a key in one of the permissible key forms at a specific location. Information may still exist at the location from which the key may be feasibly reconstructed for subsequent use.
* *Key deletion:* This method removes an instance of a key, and also any information from which the key may be reconstructed, from its operational storage/use location. Instances of this key may continue to exist at other locations (e.g., for archival purposes).
* *Key termination:* All instances and information of the key are completely removed from all locations, making it impossible to regenerate or reconstruct the key (other than through a restore from a backup image).

**The importance of monitoring keys during their life-cycle**

The key-management system should be able to handle all of the transitions between phases of a life-cycle, and should be capable of monitoring and keeping track of these workflows.

There are certain aspects to monitoring that should be considered:

* It is important to monitor for unauthorized administrative access to the system to ensure that unapproved key management operations are not performed.
* The computer processor may be under significant load. When combined with an overloaded cryptographic service, the results could be serious, including data corruption or unavailability.
* Monitoring the key's life-cycle is also important to ensure that the key has been created and deployed properly.

**9.Investigate various features of Cloud Encryption Standards**

Ninety-seven percent of all organizations use some form of cloud technology.1 To protect data stored in the cloud, organizations must have a strong cloud data policy and be proactive in implementing best practices for protecting cloud data. One of the most important security safeguards for protecting cloud data is encryption.

Cloud service providers (CSPs) and third-party cloud security software vendors offer an array of tools for securing cloud data, applications, and network connectivity. However, cloud customers are always responsible for protecting their data and who can access it.

While all data should be protected, not all data needs the extra safeguards that cloud encryption provides. Sensitive cloud data is absolutely essential to protect, as it may contain intellectual property or financial information and may be subject to various regulations and mandated compliance. For this category of cloud data, the highest level of security is needed, especially in the face of potential theft, ransom, or data destruction.

When protecting critical data (as opposed to applications), two security practices stand out: protecting *access* to that data, and protection of the *data itself*. Access controls can be as simple as password authentication and should be used only in non-critical applications. Multi-factor authentication and user entity behavior analytics (UEBA) offer significantly improved protection but are only protecting against unwanted access. Therefore, encryption of sensitive data is a critical defense against data theft. Encrypted data—even if stolen—is useless to third parties without the encryption keys to decipher it.

Best practices for cloud encryption involve the following steps:

1. Formulate a cloud encryption policy
2. Define what data needs encryption, and when
3. Identify where that data resides
4. Implement encryption solutions and key management

**Formulating a cloud encryption policy**

Depending on the industry, organizations may need to formulate and publish their data encryption policy. The policy should detail specifically what data is subject to encryption and how it protects the organization and its adherence to regulations. Another important component of the policy is key management—who holds the keys for deciphering data, and how are the keys protected against theft or loss.

Organizations should follow four simple steps in determining how and when to use encryption in the cloud:

1. What data needs encryption?
2. When does data need encryption?
3. Where should cloud encryption be deployed?
4. Who should hold the encryption keys?

**What data needs encryption?**

Not all data needs encryption. Non-sensitive data that is already backed up, or data for non-critical operations may not be candidates for encryption. In addition, cost of encryption should be considered. Running encryption in the cloud uses cloud computing resources while data is encrypted and decrypted on virtual servers, and each instance of this compute power adds to customer costs. Therefore, organizations should carefully determine what data really needs encryption by considering the following questions:

* Does the data fall under regulatory compliance requirements, such as health records (HIPAA), financial data (PCI, SOX), privacy acts (GDPR), or other legal or contractual obligations?
* Is the data personally identifiable information?
* Does the data contain sensitive intellectual property?
* Is the data essential to the operation of the organization?

Other factors may vary by organization. Typically, about 20% of data in the cloud can be categorized as sensitive to most organizations.2

**When does data need encryption?**

Most data is not static. Records are updated, new data is added, and files and datasets are often transmitted to and from remote locations or between users and the cloud. Encrypting data at rest—data saved on disk or other media—is essential. However, data that moves between clouds or workloads and off-site—data in motion or in transit—is also vulnerable. Therefore, encryption of the most sensitive data when in motion (transmission security) should also be considered. If large amounts of sensitive data are transmitted, it is definitely a candidate for data-in-motion encryption.

**Where should encryption be deployed?**

Cloud encryption can be deployed:

* **On the storage media and/or through the operating system (OS).** Most major operating systems and large storage vendors offer data-at-rest encryption. Amazon Web Services, Microsoft Azure, and Google Cloud all provide data-at-rest encryption.
* **In the cloud application.** Many software-as-a-service (SaaS) application vendors provide de facto or optional encryption of data. However, organizations are then “locked in” to the vendor's encryption technology.
* **In transit over the network.** Although virtual private network (VPN) and Internet Protocol Security (IPSec) connectivity provide excellent data-in-motion protection at low or no cost, they may affect network performance. These technologies require certificate management, thereby adding another layer of complexity.
* **Cloud security service software.** As a part of their increasingly comprehensive protection services, third-party security software companies offer encryption technologies. For example, [McAfee MVISION Cloud](https://www.mcafee.com/enterprise/en-us/products/mvision-cloud.html) can apply encryption to cloud services and work with device-level encryption to apply the same policies.

**Who should hold the encryption keys?**

Some CSPs offer a choice—they manage the encryption keys for their cloud customers, or they allow the customer to manage them. Key management is critical—loss of keys or unsecure key management can put critical data at risk. Therefore, organizations should weigh the extra cost of CSP-managed keys versus the risk of not having direct management of these essential security controls. Full regulatory compliance may tip the scales in favor of the organization holding and managing its keys.

Regardless of who holds the keys, organizations should make certain that key access is through multi-factor identification and that key storage is itself secure and backed up in case of hardware failure. Moreover, it is recommended that organizations securely keep keys on storage separate from their data.

**10.Classify various Recommendations of cloud encryption standards**

**Cloud Encryption: Challenges and Recommendations**

With the expansion of mobile applications, customers should consider having their service provider or a third-party proxy provider manage the encryption keys rather than the company's own IT department, suggests Manny Landrón, senior manager of security and compliance at Citrix. The problem companies run into, he says, is that if data is encrypted before being uploaded to a cloud storage provider and that data is then needed on a mobile or remote device that does not already have the decryption key, the resulting download will be useless, encrypted data. This becomes exacerbated when a company tries to share data with a business partner, but does not want the partner to have direct access to decryption keys.

Key rotation and destruction also becomes more complex when a company is managing its own keys for what can entail millions of files, he notes. A third-party proxy provider can add a layer of protection by keeping the keys separate from the encrypted data at a cloud provider, but this also adds another layer of complexity, as well as the additional cost of a second third-party provider for the company.

Landrón cautions companies to ask their providers and potential SaaS partners what protocols they use for transmitting data. The Secure Socket Layer (SSL) approach, which had been the standard for years, has fallen out of favor since the discovery in 2014 of the POODLE (Padding Oracle On Downgraded Legacy Encryption) attack, a man-in-the-middle exploit that effectively was designed into the SSL code.

Implementing TLS rather than SSL eliminates the vulnerability, but some legacy systems running older operating systems, such as Windows XP, are unable to implement TLS. As a result, some retailers still have some servers running SSL to support these older systems, even though there is the possibility of confidential data being compromised. The only way to eliminate the risk entirely is to disable SSL entirely either on the client system or the server which gets rid of the problem but also makes the servers inaccessible to systems that only have SSL capabilities.

Beyond key management, the largest issue SMBs must grapple with is believing that a cloud provider is better at protecting sensitive data than they are and is as vested in protecting the company's data as is the data's owner, says Jeff Cherrington, VP of product management at Prime Factors, a cloud security vendor.

Cloud providers are not subject to the same data breach disclosure laws as are banks, federal agencies, and other entities, he points out, and breaches that do occur might not be widely publicized or associated with cloud providers. However, the organization that owns the data is responsible, even when the cause of the data breach lies with the cloud hosting organization. If such a data breach is publicized, the negative attention will be focused more on the data owner than on the cloud computing provider. It is, ultimately, the obligation of the enterprise to protect its data, wherever and however it is processed. This is why the [Cloud Security Alliance](https://cloudsecurityalliance.org/), in its Security Guidance for Critical Areas of Focus in Cloud Computing, recommends that sensitive data should be:

* Encrypted for data privacy with approved algorithms and long, random keys;
* Encrypted before it passes from the enterprise to the cloud provider;
* Should remain encrypted in transit, at rest, and in use;
* The cloud provider and its staff should never have access to decryption keys.

"This last stipulation can be the most challenging for SMBs, depending on their use of cloud,"

**PREPARED BY**

**SRINIVASAN.L,Sr.AP,ISE/NHCE**