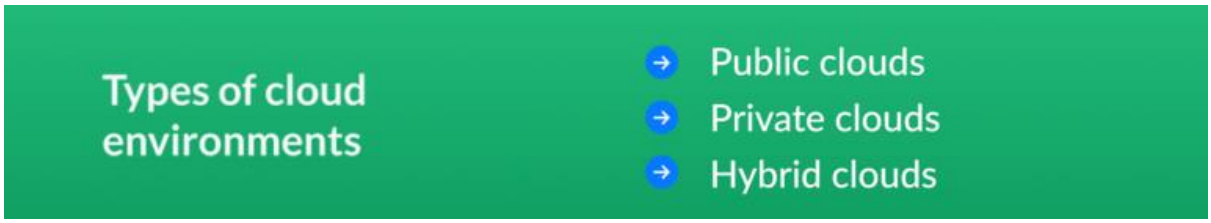
Cloud Security Fundamentals

Cloud security, also known as cloud computing security, is a collection of security measures designed to protect cloud-based infrastructure, applications, and data. These measures ensure user and device authentication, data and resource access control, and data privacy protection. They also support regulatory data compliance. Cloud security is employed in cloud environments to protect a company's data from distributed denial of service (DDoS) attacks, malware, hackers, and unauthorized user access or use.

When you're looking for cloud-based security, you'll find three main types of cloud environments to choose from. The top options on the market include public clouds, private clouds, and hybrid clouds.

Types of Cloud Environments



1. **Public Clouds**
   Public cloud services are hosted by third-party cloud service providers. A company doesn't have to set up anything to use the cloud, since the provider handles it all. Usually, clients can access a provider's web services via web browsers. Security features, such as access control, identity management, and authentication, are crucial to public clouds.
2. **Private Clouds**
   Private clouds are typically more secure than public clouds, as they're usually dedicated to a single group or user and rely on that group or user's firewall. The isolated nature of these clouds helps them stay secure from outside attacks since they're only accessible by one organization. However, they still face security challenges from some threats, such as social engineering and breaches. These clouds can also be difficult to scale as your company's needs expand.

3. **Hybrid Clouds**
   Hybrid clouds combine the scalability of public clouds with the greater control over resources that private clouds offer. These clouds connect multiple environments, such as a private cloud and a public cloud, that can scale more easily based on demand. Successful hybrid clouds allow users to access all their environments in a single integrated content management platform.

Strategies to Achieve Cloud Security

Cloud security is a complex interaction of technologies, controls, processes, and policies that is highly personalized to each organization's unique requirements.

1. **Identity and Access Management:** All companies should have an Identity and Access Management (IAM) system to control access to information. An IAM combines multi-factor authentication and user access policies, helping you control who has access to your applications and data, what they can access, and what they can do to your data.
2. **Physical Security:** It is a combination of measures to prevent direct access and disruption of hardware housed in your cloud provider's data center. Physical security includes controlling direct access with security doors, uninterrupted power supplies, CCTV, alarms, air and particle filtration, fire protection, and more.
3. **Threat Intelligence, Monitoring, and Prevention:** Threat Intelligence, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) form the backbone of cloud security. Threat Intelligence and IDS tools deliver functionality to identify attackers who are currently targeting your systems or will be a future threat. IPS tools implement functionality to mitigate an attack and alert you to its occurrence so you can also respond.
4. **Encryption:** Using cloud technology, you are sending data to and from the cloud provider's platform, often storing it within their infrastructure. Encryption is another layer of cloud security to protect your data assets, by encoding them when at rest and in transit. This ensures the data is near impossible to decipher without a decryption key that only you have access to.
5. **Cloud Vulnerability and Penetration Testing:** Another practice to maintain and improve cloud security is vulnerability and penetration testing. These practices involve you – or your provider – attacking your own cloud infrastructure to identify any potential weaknesses or exploits. You can then implement solutions to patch these vulnerabilities and improve your security stance.
6. **Micro-Segmentation:** Micro-segmentation is increasingly common in implementing cloud security. It is the practice of dividing your cloud deployment into distinct security segments, right down to the individual workload level. By

isolating individual workloads, you can apply flexible security policies to minimize any damage an attacker could cause, should they gain access.

7. **Next-Generation Firewalls:** Next-Generation firewalls are another piece of the cloud security puzzle. They protect your workloads using traditional firewall functionality and newer advanced features. Traditional firewall protection includes packet filtering, stateful inspection, proxying, IP blocking, domain name blocking, and port blocking. Next-generation firewalls add in an intrusion prevention system, deep packet inspection, application control, and analysis of encrypted traffic to provide comprehensive threat detection and prevention.

Cloud Security Benefits

Security in cloud computing is crucial to any company looking to keep its applications and data protected from bad actors. Maintaining a strong cloud security posture helps organizations achieve the now widely recognized benefits of cloud computing. Cloud security comes with its own advantages as well, helping you achieve lower upfront costs, reduced ongoing operational and administrative costs, easier scaling, increased reliability and availability, and improved DDoS protection.

Here are the top security benefits of cloud computing:

1. Lower upfront costs

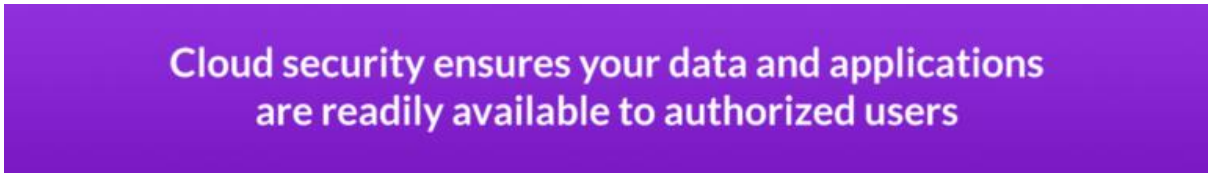
One of the biggest advantages of using cloud computing is that you don't need to pay for dedicated hardware. Not having to invest in dedicated hardware helps you initially save a significant amount of money and can also help you upgrade your security. CSPs will handle your security needs proactively once you've hired them. This helps you save on costs and reduce the risks associated with having to hire an internal security team to safeguard dedicated hardware.

2. Reduced ongoing operational and administrative expenses

Cloud security can also lower your ongoing administrative and operational expenses. A CSP will handle all your security needs for you, removing the need to pay for staff to provide manual security updates and configurations. You can also enjoy greater security, as the CSP will have expert staff able to handle any of your security issues for you.

3. Increased reliability and availability

You need a secure way to immediately access your data. Cloud security ensures your data and applications are readily available to authorized users. You'll always have a reliable method to access your cloud applications and information, helping you quickly take action on any potential security issues.

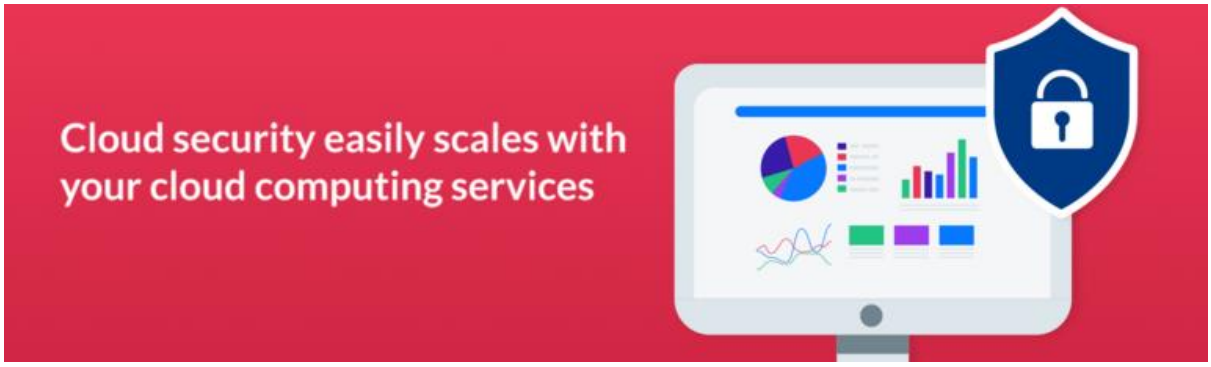


4. Centralized security

Cloud computing gives you a centralized location for data and applications, with many endpoints and devices requiring security. Security for cloud computing centrally manages all your applications, devices, and data to ensure everything is protected. The centralized location allows cloud security companies to more easily perform tasks, such as implementing disaster recovery plans, streamlining network event monitoring, and enhancing web filtering.

5. Greater ease of scaling

Cloud computing allows you to scale with new demands, providing more applications and data storage whenever you need it. Cloud security easily scales with your cloud computing services. When your needs change, the centralized nature of cloud security allows you to easily integrate new applications and other features without sacrificing your data's safety. Cloud security can also scale during high traffic periods, providing more security when you upgrade your cloud solution and scaling down when traffic decreases.



6. Improved DDoS protection

Distributed Denial of Service (DDoS) attacks are some of the biggest threats to cloud computing. These attacks aim a lot of traffic at servers at once to cause harm. Cloud security protects your servers from these attacks by monitoring and dispersing them.

Privacy and Security in Cloud

Data Privacy

One of the main concerns regarding the security and privacy in cloud computing is the protection of data.

Millions of users have stored up their important data on these clouds, which is what makes it riskier to secure every bit of information. In cloud computing, data is

distributed in different storage devices and machines including PCs, servers and different mobile devices such as smartphones and wireless sensor networks. If the security and privacy in cloud computing is neglected, then the private information of each user is at risk, allowing easy cyber breaches to hack into the system and exploit any users' private storage data.

The following are four key considerations for users to keep in mind regarding data privacy:

a. **Control Over Personal Information:** Users should be aware of the types of personal information they share with cloud service providers, such as email addresses, passwords, contact details, and payment information. It's essential for users to understand how their data is collected, stored, and processed by cloud services, and to have control over who can access their information. Users should review privacy settings and permissions for their accounts to manage what data is shared with the cloud service provider and third-party applications.
b. **Data Encryption and Security Measures:** Users should look for cloud service providers that offer strong encryption and security measures to protect their data from unauthorized access and breaches. It's important to use secure passwords and enable additional security features like two-factor authentication (2FA) to add an extra layer of protection to their accounts. Users should be cautious about sharing sensitive information over unsecured networks and ensure they are accessing cloud services via encrypted connections (e.g., HTTPS).
c. **Awareness of Data Handling Practices:** Users should understand the data handling practices of cloud service providers, including how long their data is retained, who has access to it, and how it is used for advertising or analytics purposes. It's essential for users to read and understand the terms of service and privacy policies of cloud providers to ensure they are comfortable with how their data will be treated. Users should be vigilant about phishing scams and other social engineering tactics used to trick them into revealing personal information or compromising their accounts.
d. **Compliance with Privacy Regulations:** Users should be aware of privacy regulations and laws that apply to the collection and processing of their data, such as the General Data Protection Regulation (GDPR) in the European Union or the California Consumer Privacy Act (CCPA) in the United States. It's important for users to understand their rights regarding their personal data, including the right to access, correct, or delete their information held by cloud service providers. Users should choose cloud service providers that are transparent about their privacy practices and comply with applicable privacy regulations to ensure their data is handled responsibly.

Data Security

The cloud computing environment has various functions— some of the major ones involve data storage and computing.

The easy accessibility to the cloud functions allows users to effortlessly work on their computing tasks and access their data simply via any internet connection. The data protection and its security regarding stored information of individual users, is the reason why many consumers use the cloud so much and that is exactly why it has prospered through its use of trustful functions.

Because of its efficient and continuous use, the cloud has become a very important tool for large scale purposes, such as for business and companies to prosper and on the lower scales where it is used by almost every individual as a necessary part of their everyday life. What's even great about it that aside from being easily accessible, it can provide quality and high-performance computational services at extremely cheap rates.

It makes sense why a lot of people are fond of using it and are willing to trust the cloud system with their valuable information. But a data breach may break this trust. That is why it is extremely crucial that the security and privacy in cloud computing must create a solid line of defense against these cyber-attacks.

The 4 pillars of Cloud Security

The four pillars of any security program are authorization, logging, confidentiality, and integrity.

a. **Authorization.** Simply put, you have to determine who has access to what. You want to make sure that employees have the authority they need to do their job, but not so much authority that they could become a security risk if their credentials are compromised.

b. **Logging.** Keeping tabs on the actions of users creates an audit trail that can be reviewed when something goes wrong. That trail can also help identify patterns that reveal security flaws and gaps, or system compromises.

c. **Confidentiality.** Making sure data is viewed or shared with only authorized parties is important, not only for maintaining the confidence of customers and stakeholders, but, in many cases, because it's required by law. Failure to obey those laws can result in stiff fines and penalties.

d. **Integrity.** Just as you don't want your data to be seen or shared by unauthorized individuals, you don't want data you're responsible for to be

> accidentally or maliciously modified. One way to preserve the integrity of data is to encrypt it. Encryption makes it difficult to tamper with data because a set of keys is needed to decrypt it. Those keys are usually stored securely and access to them is limited.

5 Tips to Keep Your Data Secure on the Cloud

Here are five data privacy protection tips to help you tackle the issue of cloud privacy:

1. Avoid storing sensitive information in the cloud.

Many recommendations across the 'Net sound like this: "Don't keep your information on the cloud." Fair enough, but it's the same as if you asked, "How not to get my house burned down?" and the answer would be, "Do not have a house." The logic is solid, but a better way to translate such advice is, "avoid storing sensitive information on the cloud." So if you have a choice you should opt for keeping your crucial information away from virtual world or use appropriate solutions.

2. Read the user agreement to find out how your cloud service storage works.

If you are not sure what cloud storage to choose or if you have any questions as for how that or another cloud service works you can read the user agreement of the service you are planning to sign up for. There is no doubt it's hard and boring but you really need to face those text volumes. The document which traditionally suffers from insufficient attention may contain essential information you are looking for.

3. Be serious about passwords.

You must have heard this warning a hundred times already, but yet most people do not follow it. Did you know that 90 percent of all passwords can be cracked within seconds? Indeed, a great part of all the sad stories about someone's account getting broken is caused by an easy-to-create-and-remember password. Moreover, doubling your email password for other services you use (your Facebook account, your cloud storage account) is a real trap as all your login information and forgotten passwords always arrive to your email.

4. Encrypt.

Encryption is, so far, the best way you can protect your data. Generally, encryption works as follows: You have a file you want to move to a cloud you use certain software with which you create a password for that file, you move that password-protected file to the cloud and no one is ever able to see the content of the file not knowing the password.

5. Use an encrypted cloud service.

There are some cloud services that provide local encryption and decryption of your files in addition to storage and backup. It means that the service takes care of both encrypting your files on your own computer and storing them safely on the cloud. Therefore, there is a bigger chance that this time no one — including service providers or server administrators — will have access to your files (the so called "zero-knowledge" privacy).

Identity Management and Access control

Identity and access management (IAM) is a collective term that covers products, processes, and policies used to manage user identities and regulate user access within an organization.

"Access" and "user" are two vital IAM concepts. "Access" refers to actions permitted to be done by a user (like view, create, or change a file). "Users" could be employees, partners, suppliers, contractors, or customers. Furthermore, employees can be further segmented based on their roles.

3 Key Tasks of IAM:

- **Identify** : Establishing a unique digital identity for each user within an organization is critical. IAM systems ensure accurate recognition of individuals in various systems.
- **Authenticate** : Verifying the identity of users through secure methods like passwords, biometrics, or security tokens helps prevent unauthorized access.
- **Authorize**: Once authenticated, IAM systems determine the resources and areas a user is permitted to access, effectively controlling their abilities within the organization's network.

Components of an IAM framework:

- **User database**: The cornerstone of IAM is a repository containing sensitive data regarding users' identities and associated access permissions, safeguarded by stringent security protocols.

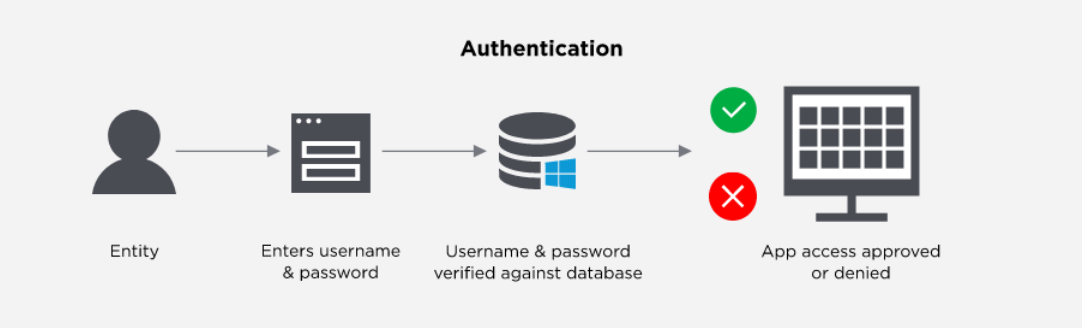
- **Management tools**: There are tools for creating, monitoring, modifying, and deleting access privileges. IAM tools facilitate the dynamic administration of access privileges, enabling IT administrators to easily onboard, monitor, and revoke user access as necessary.

- **Audit Systems**: Comprehensive systems for reviewing and recording login and access patterns, playing a pivotal role in oversight and compliance endeavors within the organization is essential.

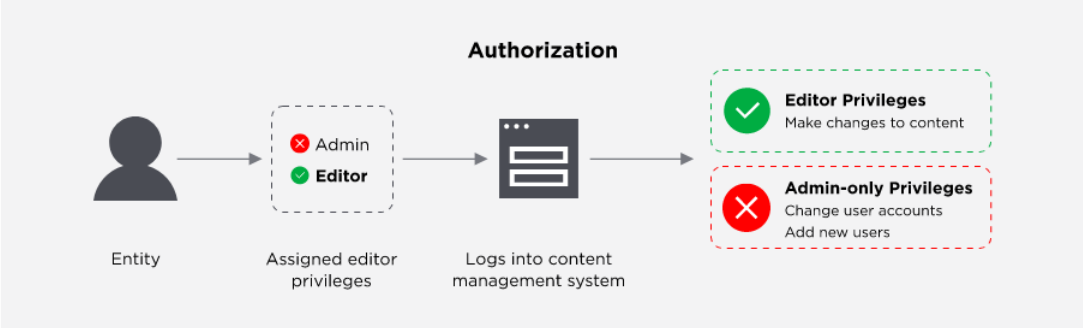
How Does IAM Work?

Identity management solutions generally perform two tasks:

Authentication: IAM confirms that the user, software, or hardware is who they say they are by authenticating their credentials against a database. IAM cloud identity tools are more secure and flexible than traditional username and password solutions.



Authorization: Identity access management systems grant only the appropriate level of access. Instead of a username and password allowing access to an entire software suite, IAM allows for narrow slices of access to be portioned out, i.e. editor, viewer, and commenter in a content management system.



Examples of Identity and Access Management

Here are simple examples of IAM at work.

- When a user enters his login credentials, his identity would be checked against a database to verify if the entered credentials match the ones stored in the database. For example, when a contributor logs into a content management system, he's allowed to post his work. However, he's not allowed to make changes to other users' works.
- A production operator can view an online work procedure but may not be allowed to modify it. On the other hand, a supervisor may have the power not

only to view but also to modify the file or create a new one. If there's no IAM in place, anyone can modify the document, and this could lead to disastrous effects.

- A team leader needs to approve their team members' timesheets. Once they log into the timesheet portal, they can view all timesheets and approve or reject them as required. However, they cannot approve or reject their own timesheet, which only their manager or supervisor can do.

Role-Based Access

Many IAM systems use role-based access control (RBAC). Under this approach, there are **predefined job roles with specific sets of access privileges**. Take HR employees as an RBAC example. If one HR officer is in charge of training, it makes little sense if that officer is given access to payroll and salary files.

Single Sign-On: Some IAM systems implement **Single Sign-On** (SSO). With SSO, users only need to verify themselves one time. They would then be given access to all systems without the need to log separately into each system.

Multi-Factor Authentication: Whenever extra steps are required for authentication, it's either a **two-factor authentication** (2FA) or **multi-factor authentication** (MFA). This authentication process combines something the user knows (like a password) with something the user has (like a security token or OTP) or something that's part of the user's body (like biometrics).

Benefits of Identity and Access Management

Here's a look at a few of the primary benefits and why identity and access management are important.

- **IAM enhances security.** This is perhaps the most important benefit organizations can get from IAM. By controlling user access, companies can eliminate instances of data breaches, identity theft, and illegal access to confidential information. IAM can prevent the spread of compromised login credentials, avoid unauthorized entry to the organization's network, and provide protection against ransomware, hacking, phishing, and other kinds of cyber attacks.
- **IAM streamlines IT workload.** Whenever a security policy gets updated, all access privileges across the organization can be changed in one sweep. IAM can also reduce the number of tickets sent to the IT helpdesk regarding password resets. Some systems even have automation set for tedious IT tasks.
- **IAM helps in compliance.** With IAM, companies can quickly meet the requirements of industry regulations (like HIPAA and GDPR) or implement IAM best practices.

- **IAM allows collaboration and enhances productivity.** Companies can provide outsiders (like customers, suppliers, and visitors) access to their networks without jeopardizing security.
- **IAM improves user experience.** There's no need to enter multiple passwords to access multiple systems under SSO. If biometrics or smart cards are used, users may have no more need to remember complex passwords.

https://digitalguardian.com/blog/what-identity-and-access-management-iam

Cloud Computing Security Challenges

There is no doubt that Cloud Computing provides various Advantages but there are also some security issues in cloud computing. Below are some Security Issues in Cloud Computing:

Data Loss

Data Loss is one of the issues faced in Cloud Computing. This is also known as Data Leakage. As we know that our sensitive data is in the hands of somebody else, and we don't have full control over our database. So if the security of cloud service is to break by hackers then it may be possible that hackers will get access to our sensitive data or personal files.

Interference of Hackers and Insecure API's

As we know if we are talking about the cloud and its services it means we are talking about the Internet. Also, we know that the easiest way to communicate with Cloud is using API. So it is important to protect the Interface's and API's which are used by an external user. But also in cloud computing, few services are available in the public domain. An API is the vulnerable part of Cloud Computing because it may be possible that these services are accessed by some third parties. So it may be possible that with the help of these services hackers can easily hack or harm our data.

User Account Hijacking

Account Hijacking is the most serious security issue in Cloud Computing. If somehow the Account of User or an Organization is hijacked by Hacker, the hacker has full authority to perform Unauthorized Activities.

Changing Service Provider

Vendor lock In is also an important Security issue in Cloud Computing. Many organizations will face different problems while shifting from one vendor to another. For example, An Organization wants to shift from AWS Cloud to Google Cloud Services then they ace various problem's like shifting of all data, also both cloud services have different techniques and functions, so they also face problems regarding that. Also, it may be possible that the charges of AWS are different from Google Cloud, etc.

Lack of Skill

While shifting to another service provider with an extra feature, one needs to know how to use the feature. So, it requires a skilled person to work with cloud computing

Denial of Service (DoS) attack

This type of attack occurs when the system receives too much traffic. Mostly DoS attacks occur in large organizations such as the banking sector, government sector, etc. When a DoS attack occurs data is lost. So in order to recover data, it requires a great amount of money as well as time to handle it.

Ethics in Cloud Computing

Ethics in cloud computing play a pivotal role in shaping the responsible and equitable use of cloud technologies in today's digital landscape. As organizations increasingly rely on cloud services for data storage, processing, and collaboration, ethical considerations regarding data privacy, security, vendor lock-in, and interoperability have come to the forefront. Cloud computing raises complex ethical dilemmas related to the protection of user privacy, the fair treatment of data, and the societal impact of technological advancements. Understanding and addressing these ethical challenges are essential for fostering trust, ensuring accountability, and promoting the ethical use of cloud technologies. In this context, exploring the ethical principles and considerations inherent in cloud computing is paramount to navigating the evolving landscape of digital ethics and responsible technology adoption.

Ethical Principles:

Ethical principles provide guidelines for individuals and organizations to conduct themselves with integrity, honesty, fairness, and respect for others, guiding moral decision-making and behavior.

Data privacy and Security:

Sensitive data must be protected, respecting user privacy rights, and implementing robust security measures to prevent unauthorized access and data breaches.

Vendor Lock-in and Interoperability:

Vendor lock-in refers to the situation where a user becomes dependent on a particular vendor's products or services, limiting their ability to switch to alternatives. Interoperability, on the other hand, refers to the ability of systems or components to work together seamlessly, promoting flexibility and preventing vendor lock-in.

Environmental Impact:

The environmental impact of ethics in cloud computing emphasizes the importance of adopting sustainable practices and minimizing energy consumption, carbon emissions, and resource utilization to mitigate the environmental footprint of cloud infrastructure and operations.

Social and Economic Equity

The social and economic equity aspect of ethics in cloud computing underscores the need to address digital inequalities, promote access to technology, and ensure fair distribution of resources to bridge the digital divide and promote inclusivity in cloud adoption.

Professional Responsibility and Ethical Decision-Making:

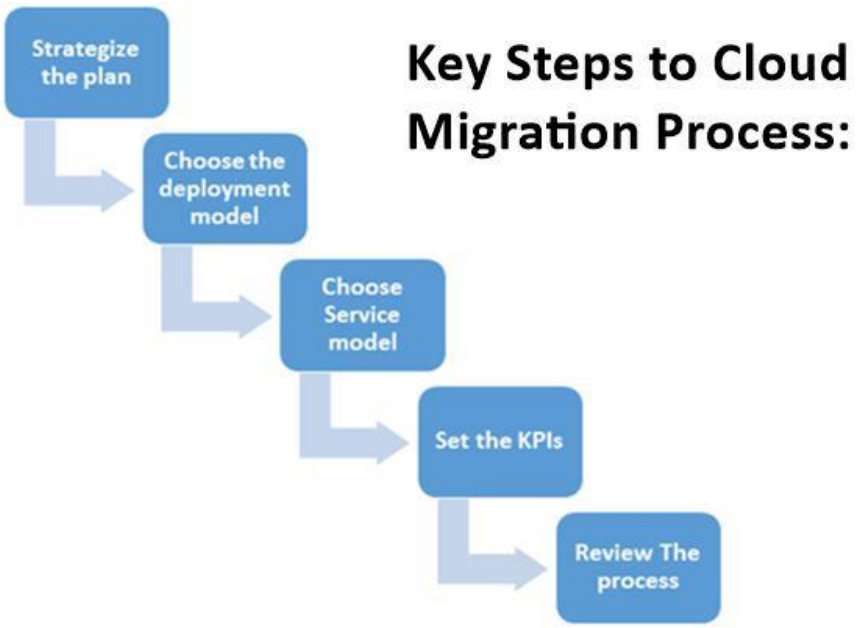
Professional responsibility and ethical decision-making in cloud computing require one to uphold integrity, transparency, and accountability in their actions, prioritize the privacy and security of data, and navigate ethical dilemmas with ethical frameworks and considerations to ensure the ethical use of cloud technologies and services.

Cloud Migration

Cloud migration is the process of moving applications, databases and other business elements from the local server to the cloud server. A cloud migration happens when a company moves some or all of its data center capabilities into the cloud, usually to run on the cloud-based infrastructure provided by a cloud service provider such as AWS, Google Cloud, or Azure.

Cloud Migration Process

https://www.knowledgenile.com/blogs/cloud-migration-process/



- **Strategize the Plan for Cloud Migration**

As a first step to move to the cloud, you will need to understand the requirements and devise a plan to make the shift.

You need to have clarity on which data and what operations you are going to move to the cloud and you need to have a specialist or consultant who has done it before to make this shift smooth and successful.

You also need to decide whether your applications fall under the lift-and-shift category where you need to move them as they are or if you need to make modifications to the data and/or applications to get the best out of cloud platforms.

- **Choose the Cloud Deployment Model**

Choosing the cloud deployment model is one of the most crucial processes of cloud migration. You can either opt for a single cloud environment or a multi-cloud environment.

Furthermore, you'll need to choose the deployment model for which is best suited for your organization. You can either go for a **private cloud or public cloud**. You may also go for a hybrid cloud model where you can keep some of the operations on your private cloud and keep the rest on the public cloud platform. In a multi-cloud platform, you can use different cloud service providers for different operations and at different stages.

- **Choose your Service model**

In the next step, you need to finalize the type of service model required for different operations. These service models are Platform-as-a-Service, Software-as-a-Service, and Infrastructure-as-a-Service.

- ✓ **Infrastructure-as-a-Service:** It is the form of cloud computing that can be accessed throughout the network with the of storage and compute capabilities.
- ✓ **Platform-as-a-Service:** These services have platforms on which the web-based applications can be built, such as web apps, data servers, and many other security concerning operations**.**
- ✓ **Software-as-a-Service:** These include centrally stored, subscription-based user applications catered as a service.

- **Set the KPIs**

These are the metrics you need to understand as to how your cloud service should operate. These KPIs normally include parameters such as user experience, app performance, and infrastructure parameters.

- **Move your Data to the Cloud and Review the Process with KPIs**

Once you have finalized all the steps necessary to make the cloud migration, you can make the shift to the cloud. After a previously set deadline passes, make sure to check whether all the requirements are getting fulfilled with the help of KPIs.

Challenges of Cloud Migration

There are certain challenges companies need to face while shifting to the cloud. We are enlisting a few of them below.

Cost

Even though increased productivity and efficiency reduce the overall cost in the long term, you need to invest capital upfront while switching to the cloud.

To reduce this problem, you can opt for a hybrid cloud platform wherein you can keep some of the operations on your end and rest on the public cloud. You can move your operations to the cloud gradually.

Lack of Skillset

For most organizations, skilled employees with cloud technology are not in abundance. The demand for skilled professionals is more than the available resources.

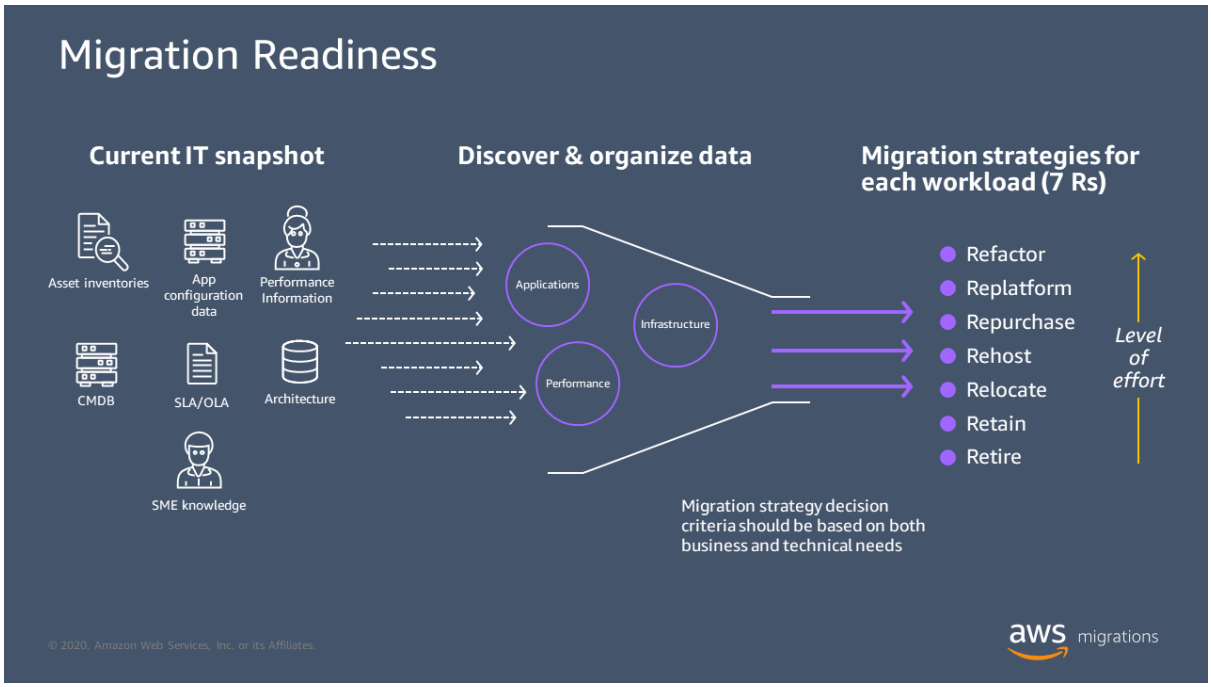
Companies can reduce this challenge by developing initiatives such as on the job training and in-house training processes.

Unwillingness of Employees

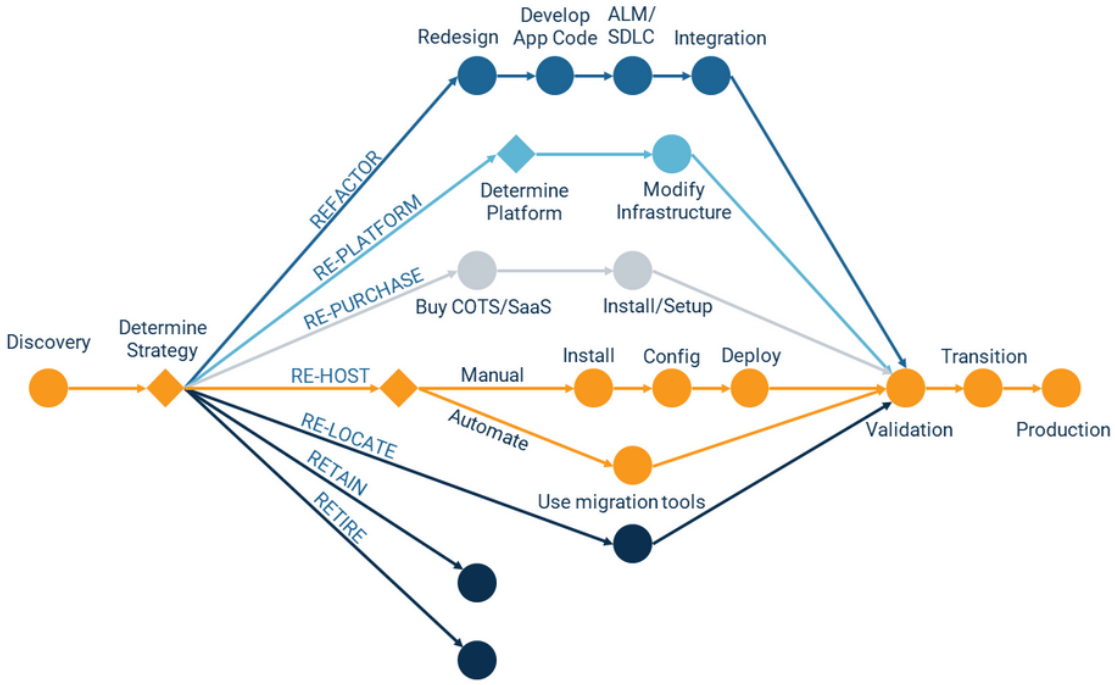
Even though the repetitive nature of the operations is going reduce by opting to cloud, many employees still find the processes to be confusing. This may change with time, but companies need to take initiatives and explain the benefits of making the switch to the cloud.

Seven common migration strategies (7 R's) for moving applications to the cloud:

These strategies are built upon the 5 Rs that Gartner identified in 2011 and consist of the following:



An understanding across all the applications in your portfolio is an important step for determining individual migration strategies, the subsequent migration plan and business case. Here are the seven most commonly used strategies.
https://www.polarseven.com/post/7rs-cloud-migration-strategies



- **Refactor/re-architect** – Move an application and modify its architecture by taking full advantage of cloud-native features to improve agility, performance, and scalability. This typically involves porting the operating system and database. Example: Migrate your on-premises Oracle database to the Amazon Aurora PostgreSQL-Compatible Edition.
- **Replatform (lift and reshape)** – Move an application to the cloud, and introduce some level of optimization to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Amazon Relational Database Service (Amazon RDS) for Oracle in the AWS Cloud.
- **Repurchase (drop and shop)** – Switch to a different product, typically by moving from a traditional license to a SaaS model. Example: Migrate your customer relationship management (CRM) system to Salesforce.com.
- **Rehost (lift and shift)** – Move an application to the cloud without making any changes to take advantage of cloud capabilities. Example: Migrate your on-premises Oracle database to Oracle on an EC2 instance in the AWS Cloud.
- **Relocate (hypervisor-level lift and shift)** – Move infrastructure to the cloud without purchasing new hardware, rewriting applications, or modifying your existing operations. This migration scenario is specific to VMware Cloud on AWS, which supports virtual machine (VM) compatibility and workload portability between your on-premises environment and AWS. You can use the VMware Cloud Foundation technologies from your on-premises data centers when you

migrate your infrastructure to VMware Cloud on AWS. Example: Relocate the hypervisor hosting your Oracle database to VMware Cloud on AWS.

- **Retain (revisit)** – Keep applications in your source environment. These might include applications that require major refactoring, and you want to postpone that work until a later time, and legacy applications that you want to retain, because there's no business justification for migrating them.
- **Retire** – Decommission or remove applications that are no longer needed in your source environment.