Cloud Security

Cloud Security Challenges

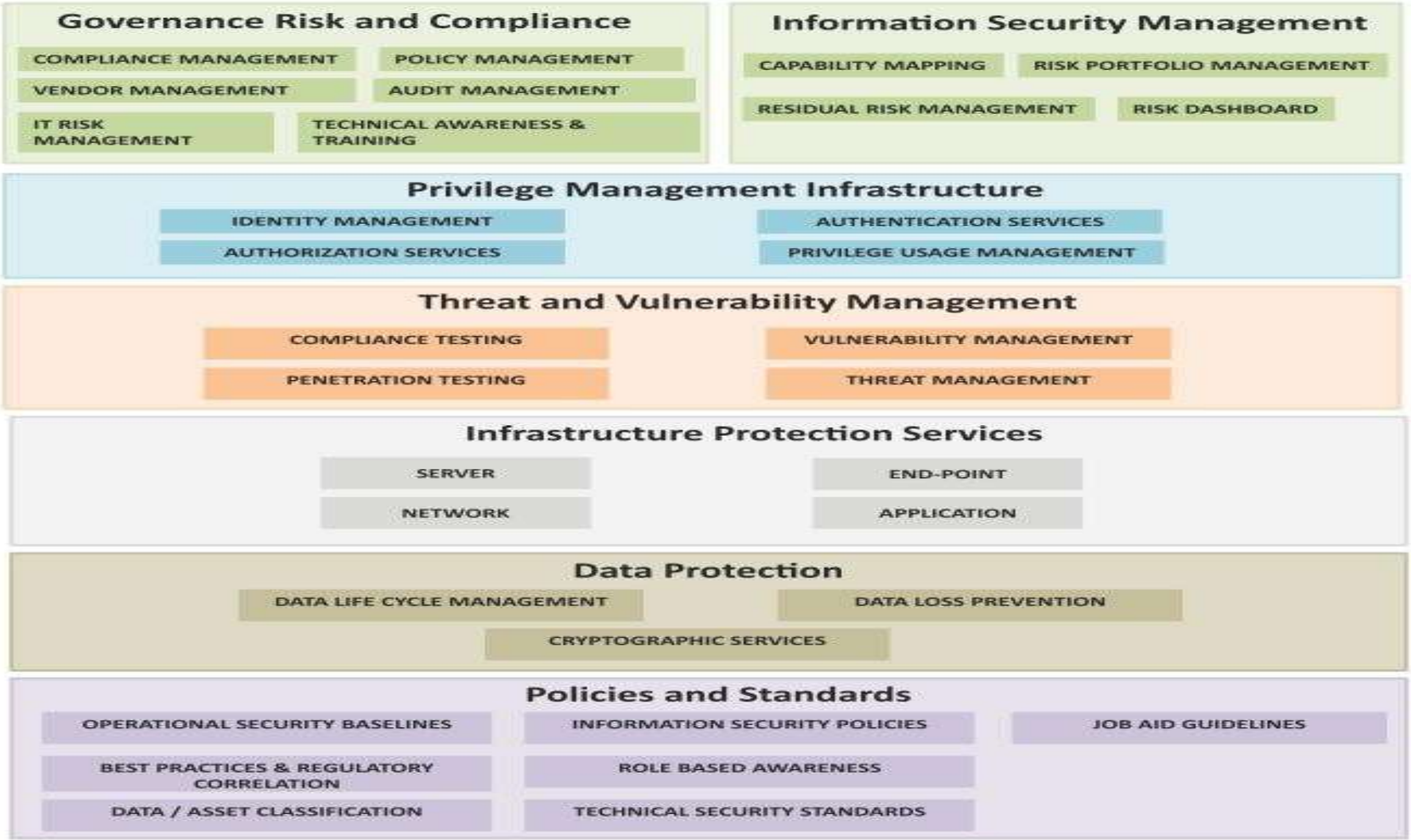
- Authentication
  - Authentication refers to digitally confirming the identity of the entity requesting access to some protected information.
  - In a traditional in-house IT environment authentication polices are under the control of the organization. However, in cloud computing environments, where applications and data are accessed over the internet, the complexity of digital authentication mechanisms increases rapidly.
- Authorization
  - Authorization refers to digitally specifying the access rights to the protected resources using access policies.
  - In a traditional in-house IT environment, the access policies are controlled by the organization and can be altered at their convenience.
  - Authorization in a cloud computing environment requires the use of the cloud service providers services for specifying the access policies.
- Security of data at rest
  - Due to the multi-tenant environments used in the cloud, the application and database servers of different applications belonging to different organizations can be provisioned side-by-side increasing the complexity of securing the data.
  - Appropriate separation mechanisms are required to ensure the isolation between applications and data from different organizations.

Cloud Security Challenges

- Security of data in motion
  - In traditional in-house IT environments all the data exchanged between the applications and users remains within the organization's control and geographical boundaries.
  - With the adoption of the cloud model, the applications and the data are moved out of the in-house IT infrastructure to the cloud provider.
  - Therefore, appropriate security mechanisms are required to ensure the security of data in, and while in, motion.
- Data Integrity
  - Data integrity ensures that the data is not altered in an unauthorized manner after it is created, transmitted or stored. Due to the outsourcing of data storage in cloud computing environments, ensuring integrity of data is important.
- Auditing
  - Auditing is very important for applications deployed in cloud computing environments.
  - In traditional in-house IT environments, organizations have complete visibility of their applications and accesses to the protected information.
  - For cloud applications appropriate auditing mechanisms are required to get visibility into the application, data accesses and actions performed by the application users, including mobile users and devices such as wireless laptops and smartphones.

CSA Cloud Security Architecture

- Cloud Security Alliance (CSA) provides a Trusted Cloud Initiative (TCI) Reference Architecture.
- TCI is a methodology and a set of tools that enable cloud application developers and security architects to assess where their internal IT and their cloud providers are in terms of security capabilities, and to plan a roadmap to meet the security needs of their business.
- Security and Risk Management (SRM) domain within the TCI Reference includes:
  - Governance, Risk Management, and Compliance
  - Information Security Management
  - Privilege Management Infrastructure
  - Threat and Vulnerability Management
  - Infrastructure Protection Services
  - Data Protection
  - Policies and Standards


Governance Risk and Compliance
COMPLIANCE MANAGEMENT
POLICY MANAGEMENT
VENDOR MANAGEMENT
AUDIT MANAGEMENT
IT RISK MANAGEMENT
TECHNICAL AWARENESS & TRAINING
Information Security Management
CAPABILITY MAPPING
RISK PORTFOLIO MANAGEMENT
RESIDUAL RISK MANAGEMENT
RISK DASHBOARD
Privilege Management Infrastructure
IDENTITY MANAGEMENT
AUTHENTICATION SERVICES
AUTHORIZATION SERVICES
PRIVILEGE USAGE MANAGEMENT
Threat and Vulnerability Management
COMPLIANCE TESTING
VULNERABILITY MANAGEMENT
PENETRATION TESTING
THREAT MANAGEMENT
Infrastructure Protection Services
SERVER
END-POINT
NETWORK
APPLICATION
Data Protection
DATA LIFE CYCLE MANAGEMENT
DATA LOSS PREVENTION
CRYPTOGRAPHIC SERVICES
Policies and Standards
OPERATIONAL SECURITY BASELINES
INFORMATION SECURITY POLICIES
JOB AID GUIDELINES
BEST PRACTICES & REGULATORY CORRELATION
ROLE BASED AWARENESS
DATA / ASSET CLASSIFICATION
TECHNICAL SECURITY STANDARDS

Authentication

- Authentication refers to confirming the digital identity of the entity requesting access to some protected information.
- The process of authentication involves, but is not limited to, validating the at least one factor of identification of the entity to be authenticated.
- A factor can be something the entity or the user knows (password or pin), something the user has (such as a smart card), or something that can uniquely identify the user (such as fingerprints).
- In multifactor authentication more than one of these factors are used for authentication.
- There are various mechanisms for authentication including:
  - SSO
  - SAML-Token
  - OTP

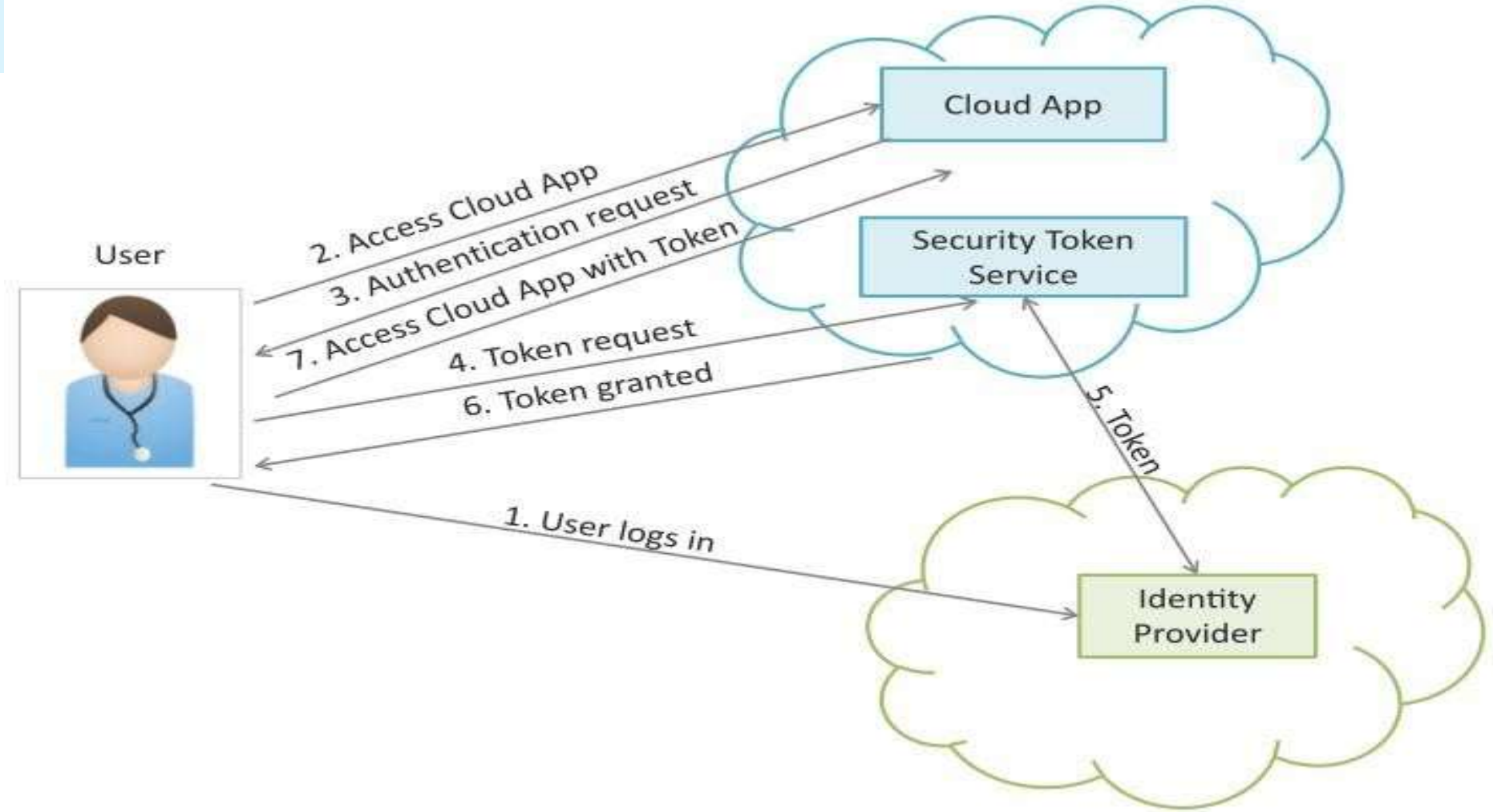
Single Sign-on (SSO)

- Single Sign-on (SSO) enables users to access multiple systems or applications after signing in only once, for the first time.
- When a user signs in, the user identity is recognized and there is no need to sign in again and again to access related systems or applications.
- Since different systems or applications may be internally using different authentication mechanisms, SSO upon receiving initial credential translates to different credentials for different systems or applications.
- The benefit of using SSO is that it reduces human error and saves time spent in authenticating with different systems or applications for the same identity.
- There are different implementation mechanisms:
  - SAML-Token
  - Kerberos

SAML-Token

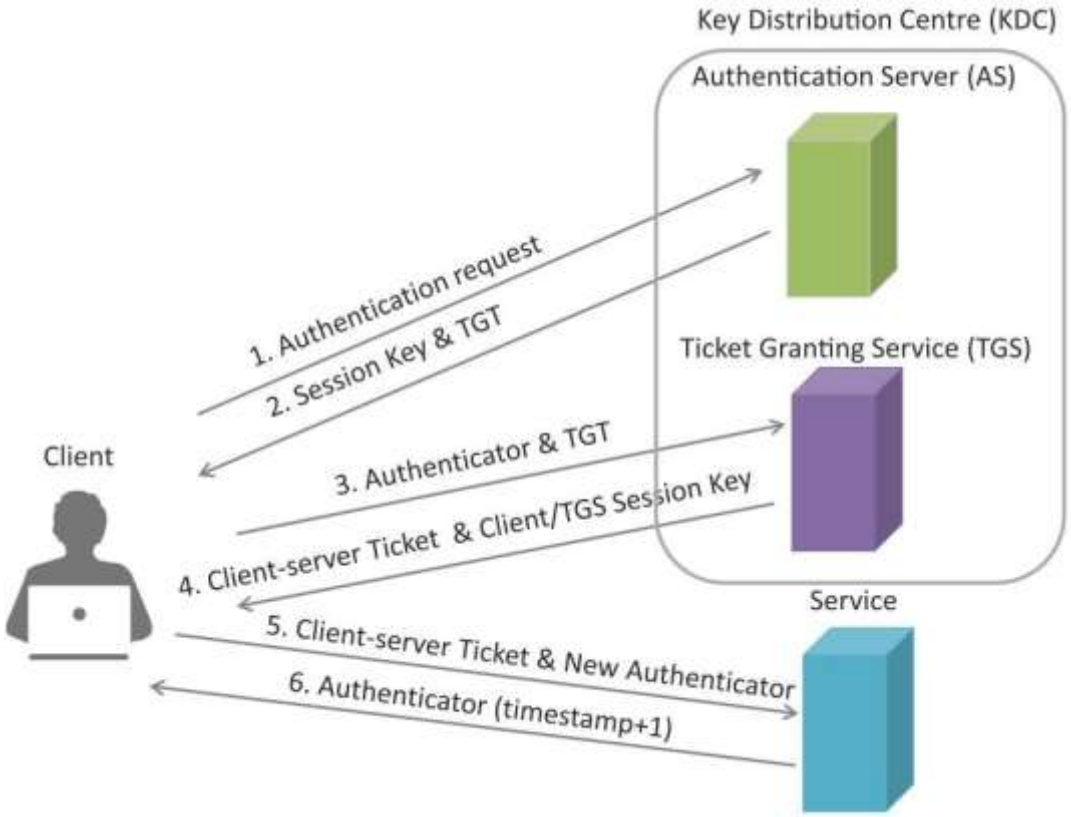
- Security Assertion Markup Language (SAML) is an XML-based open standard data format for exchanging security information (authentication and authorization data) between an identity provider and a service provider.

- SAML-token based SSO authentication
  - When a user tries to access the cloud application, a SAML request is generated and the user is redirected to the identity provider.
  - The identity provider parses the SAML request and authenticates the user. A SAML token is returned to the user, who then accesses the cloud application with the token.
  - SAML prevents man-in-the-middle and replay attacks by requiring the use of SSL encryption when transmitting assertions and messages.
  - SAML also provides a digital signature mechanism that enables the assertion to have a validity time range to prevent replay attacks.


Cloud App
Security Token Service
Identity Provider
User
2. Access Cloud App
3. Authentication request
7. Access Cloud App with Token
4. Token request
6. Token granted
5. Token
1. User logs in

Kerberos

- Kerberos is an open authentication protocol that was developed At MIT.
- Kerberos uses tickets for authenticating client to a service that communicate over an un-secure network.
- Kerberos provides mutual authentication, i.e. both the client and the server authenticate with each other.

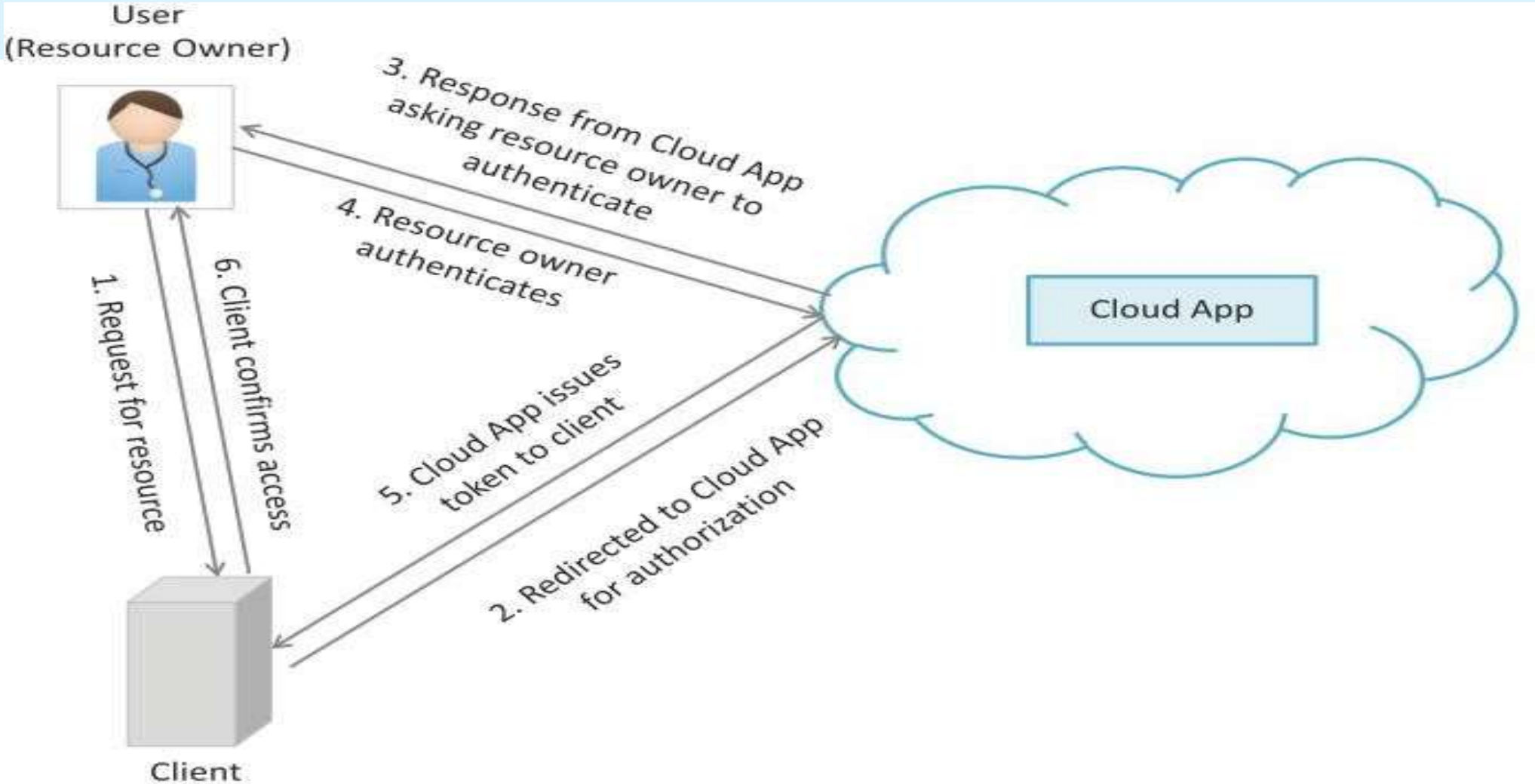


One Time Password (OTP)

- One time password is another authentication mechanism that uses passwords which are valid for single use only for a single transaction or session.
- Authentication mechanism based on OTP tokens are more secure because they are not vulnerable to replay attacks.
- Text messaging (SMS) is the most common delivery mode for OTP tokens.
- The most common approach for generating OTP tokens is time synchronization.
- Time-based OTP algorithm (TOTP) is a popular time synchronization based algorithm for generating OTPs.

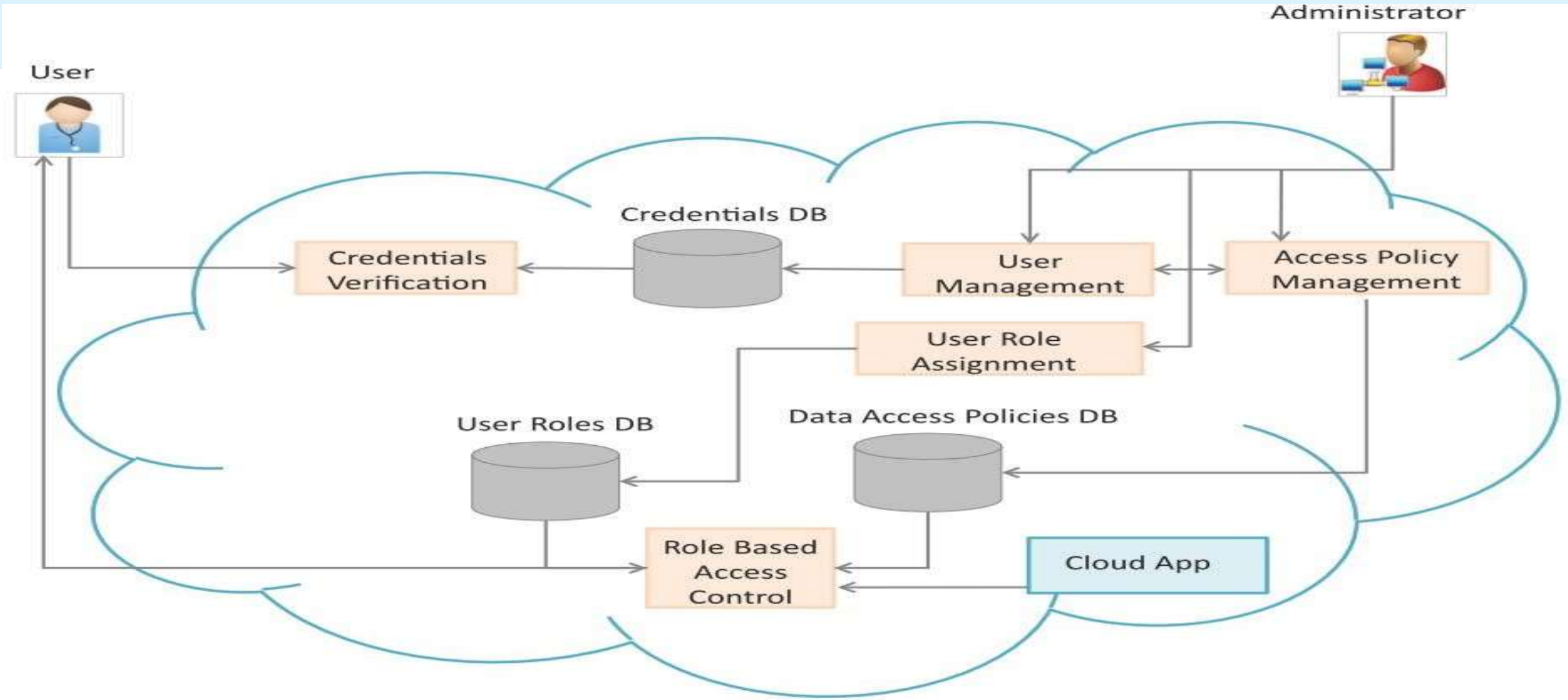
Authorization

- Authorization refers to specifying the access rights to the protected resources using access policies.
-
- OAuth
  - OAuth is an open standard for authorization that allows resource owners to share their private resources stored on one site with another site without handing out the credentials.
  - In the OAuth model, an application (which is not the resource owner) requests access to resources controlled by the resource owner (but hosted by the server).
  - The resource owner grants permission to access the resources in the form of a token and matching shared-secret.
  - Tokens make it unnecessary for the resource owner to share its credentials with the application.
  - Tokens can be issued with a restricted scope and limited lifetime, and revoked independently.


User
(Resource Owner)
3. Response from Cloud App asking resource owner to authenticate
4. Resource owner authenticates
1. Request for resource
6. Client confirms access
5. Cloud App issues token to client
2. Redirected to Cloud App for authorization
Cloud App
Client

Identity & Access Management

- Identity management provides consistent methods for digitally identifying persons and maintaining associated identity attributes for the users across multiple organizations.
- Access management deals with user privileges.
- Identity and access management deal with user identities, their authentication, authorization and access policies.
- Federated Identity Management
  - Federated identity management allows users of one domain to securely access data or systems of another domain seamlessly without the need for maintaining identity information separately for multiple domains.
  - Federation is enabled through the use single sign-on mechanisms such as SAML token and Kerberos.
- Role-based access control
  - Used for restricting access to confidential information to authorized users.
  - These access control policies allow defining different roles for different users.


Administrator
User
Credentials DB
Credentials Verification
User Management
Access Policy Management
User Role Assignment
User Roles DB
Data Access Policies DB
Role Based Access Control
Cloud App

Securing Data at Rest

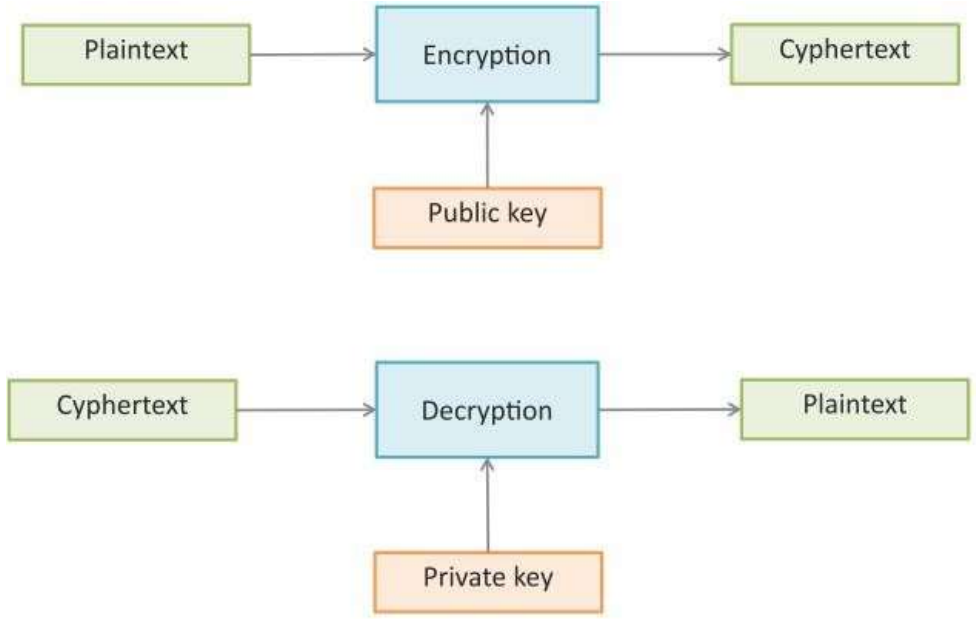
- Data at rest is the data that is stored in database in the form of tables/records, files on a file server or raw data on a distributed storage or storage area network (SAN).
- Data at rest is secured by encryption.
- Encryption is the process of converting data from its original form (i.e., plaintext) to a scrambled form (ciphertext) that is unintelligible. Decryption converts data from ciphertext to plaintext.
- Encryption can be of two types:
  - Symmetric Encryption (symmetric-key algorithms)
  - Asymmetric Encryption (public-key algorithms)

Symmetric Encryption

- Symmetric encryption uses the same secret key for both encryption and decryption.
- The secret key is shared between the sender and the receiver.
- Symmetric encryption is best suited for securing data at rest since the data is accessed by known entities from known locations.
- Popular symmetric encryption algorithms include:
  - Advanced Encryption Standard (AES)
  - Twofish
  - Blowfish
  - Triple Data Encryption Standard (3DES)
  - Serpent
  - RC6
  - MARS

Asymmetric Encryption

- Asymmetric encryption uses two keys, one for encryption (public key) and other for decryption (private key).
- The two keys are linked to each other such that one key encrypts plaintext to ciphertext and other decrypts ciphertext back to plaintext.
- Public key can be shared or published while the private key is known only to the user.
- Asymmetric encryption is best suited for securing data that is exchanged between two parties where symmetric encryption can be unsafe because the secret key has to be exchanged between the parties and anyone who manages to obtain the secret key can decrypt the data.
- In asymmetric encryption a separate key is used for decryption which is kept private.



Encryption Levels

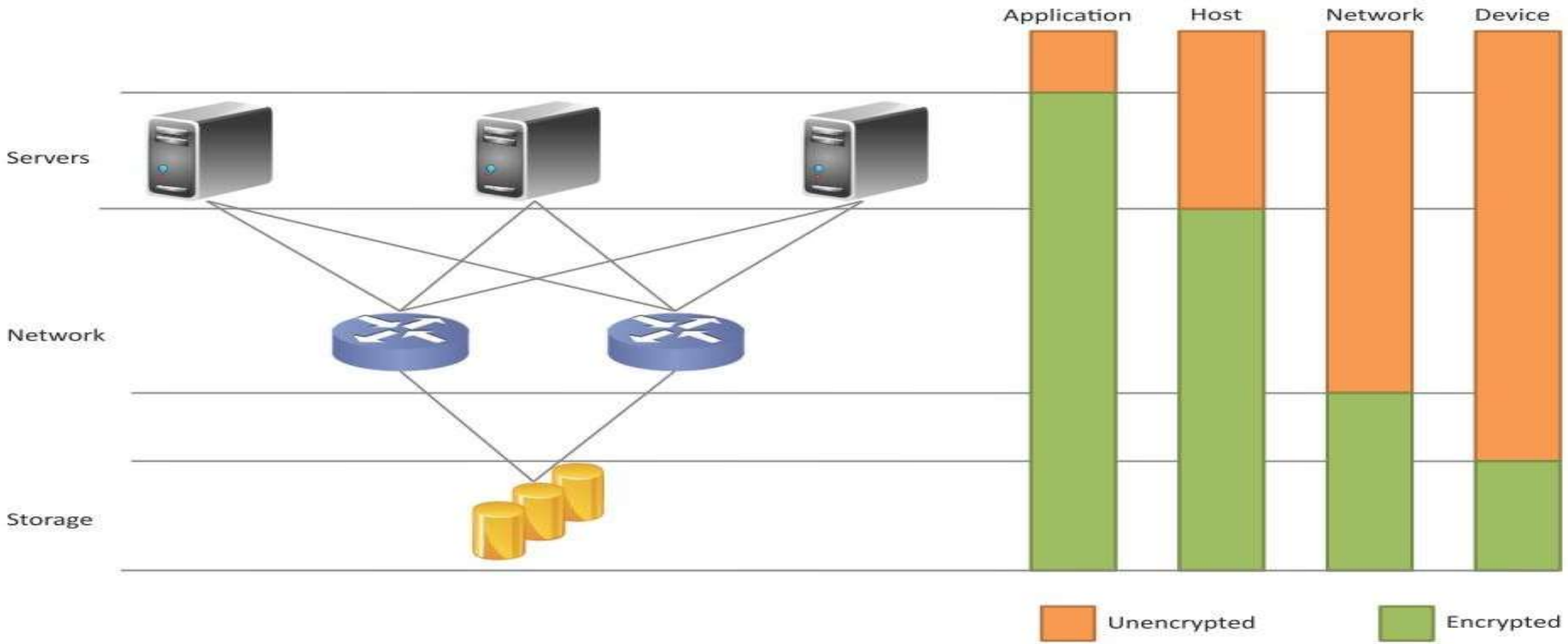
Encryption can be performed at various levels:

- Application
  - Application level encryption involves encrypting application data right at the point where it originates i.e. within the application.
  - Application level encryption provides security at the level of both the operating system and from other applications.
  - An application encrypts all data generated in the application before it flows to the lower levels and presents decrypted data to the user.
- Host
  - In host-level encryption, encryption is performed at the file-level for all applications running on the host.
  - Host level encryption can be done in software in which case additional computational resource is required for encryption or it can be performed with specialized hardware such as a cryptographic accelerator card.
- Network
  - Network-level encryption is best suited for cases where the threats to data are at the network or storage level and not at the application or host level.
  - Network-level encryption is performed when moving the data form a creation point to its destination using a specialized hardware that encrypts all incoming data in real-time.

Device

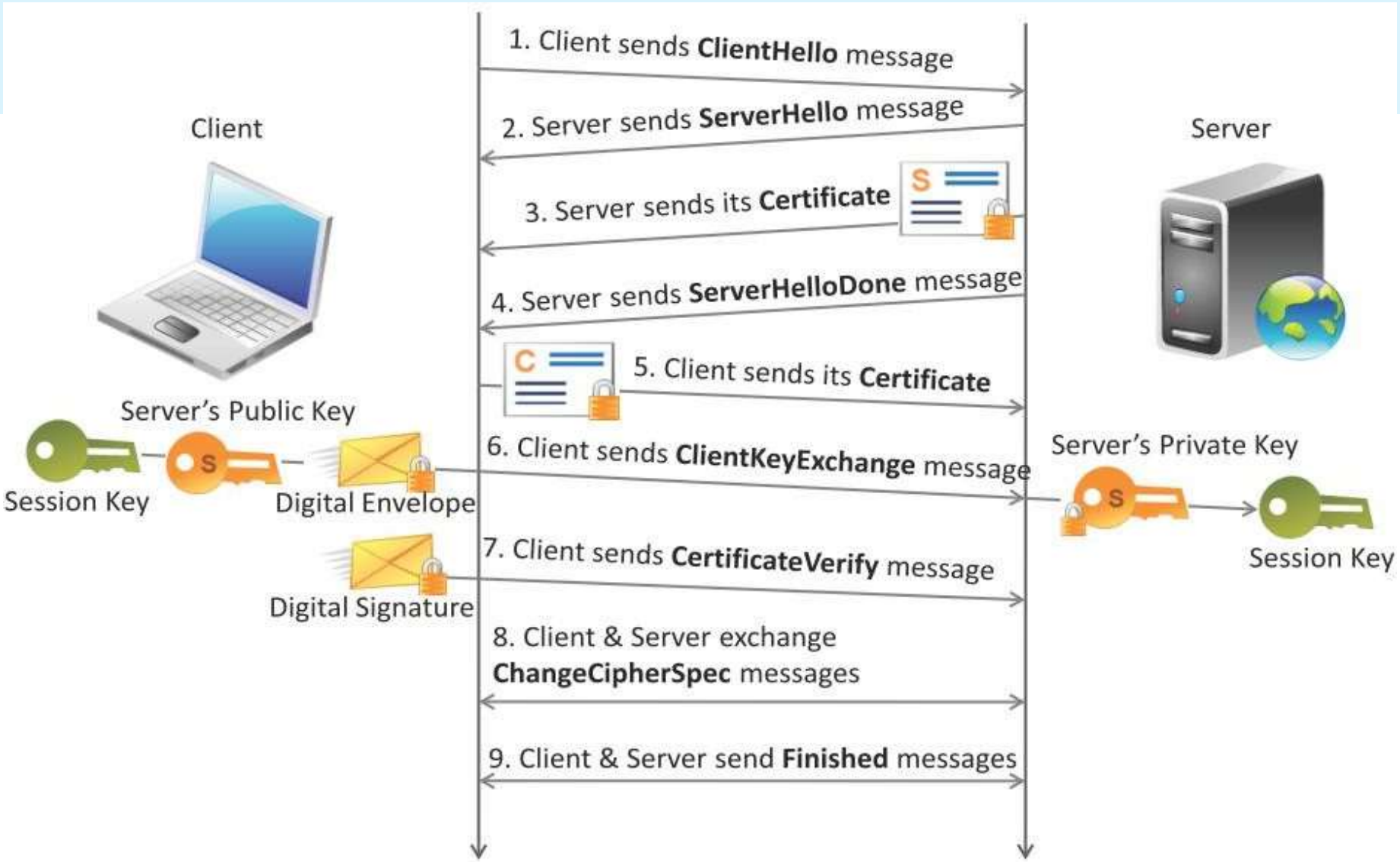
Device-level encryption is performed on a disk controller or a storage server.

Device level encryption is easy to implement and is best suited for cases where the primary concern about data security is to protect data residing on storage media.



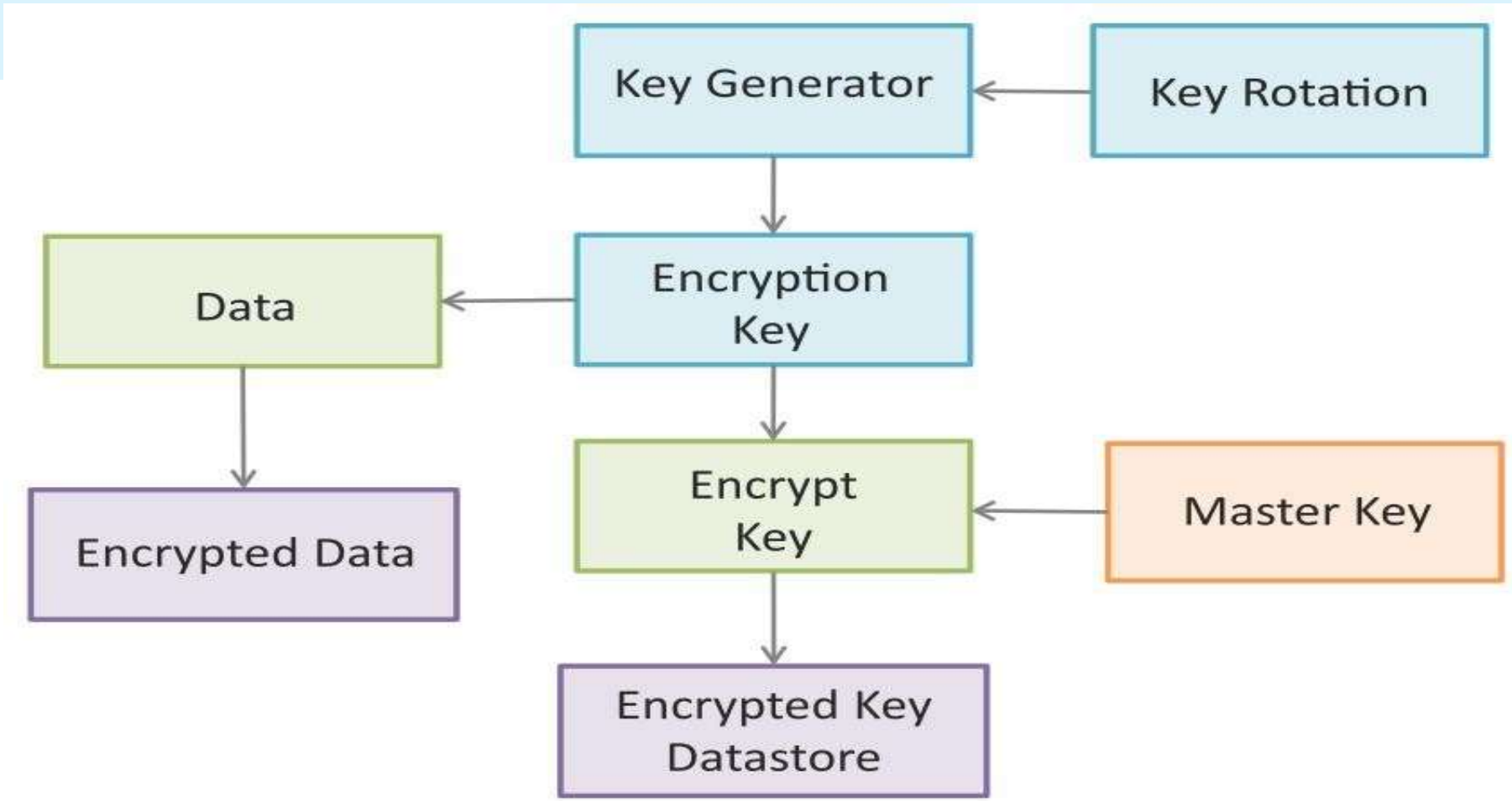
Securing Data in Motion

- Securing data in motion, i.e., when the data flows between a client and a server over a potentially insecure network, is important to ensure data confidentiality and integrity.
- Data confidentiality means limiting the access to data so that only authorized recipients can access it.
- Data integrity means that the data remains unchanged when moving from sender to receiver.
- Data integrity ensures that the data is not altered in an unauthorized manner after it is created, transmitted or stored.
- Transport Layer Security (TLS) and Secure Socket Layer (SSL) are the mechanisms used for securing data in motion.
- TLS and SSL are used to encrypt web traffic using Hypertext Transfer Protocol (HTTP).
- TLS and SSL use asymmetric cryptography for authentication of key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity.


Client
Server
1. Client sends **ClientHello** message
2. Server sends **ServerHello** message
3. Server sends its **Certificate**
4. Server sends **ServerHelloDone** message
5. Client sends its **Certificate**
Server's Public Key
Session Key
Digital Envelope
6. Client sends **ClientKeyExchange** message
Server's Private Key
Session Key
7. Client sends **CertificateVerify** message
Digital Signature
8. Client & Server exchange **ChangeCipherSpec** messages
9. Client & Server send **Finished** messages

Key Management

- Management of encryption keys is critical to ensure security of encrypted data.
- The key management lifecycle involves different phases including:
  - Creation
  - Backup
  - Deployment
  - Monitoring
  - Rotation
  - Expiration
  - Archival
  - Destruction
- Key Management Approach (example)
  - All keys for encryption must be stored in a data store which is separate and distinct from the actual data store.
  - Additional security features such as key rotation and key encrypting keys can be used.
  - Keys can be automatically or manually rotated.
  - In the automated key change approach, the key is changed after a certain number of transactions.
  - All keys can themselves be encrypted using a master key.


Key Generator
Key Rotation
Data
Encryption Key
Encrypted Data
Encrypt Key
Master Key
Encrypted Key Datastore

Auditing

- Auditing is mandated by most data security regulations.
- Auditing requires that all read and write accesses to data be logged.
- Logs can include the user involved, type of access, timestamp, actions performed and records accessed.
- The main purpose of auditing is to find security breaches, so that necessary changes can be made in the application and deployment to prevent a further security breach.
- The objectives of auditing include:
  - Verify efficiency and compliance of identity and access management controls as per established access policies.
  - Verifying that authorized users are granted access to data and services based on their roles.
  - Verify whether access policies are updated in a timely manner upon change in the roles of the users.
  - Verify whether the data protection policies are sufficient.
  - Assessment of support activities such as problem management.

Cloud Migration: A Seven-Step Process Model

A comprehensive guide to successfully transitioning your organisation to the cloud through a structured, proven approach.

Why Migrate to the Cloud? The Business Case

Cloud migration transforms how organisations operate, compete, and innovate. By moving to cloud infrastructure, businesses unlock agility, scalability, and cost-efficiency that traditional on-premises systems cannot match.

The cloud enables rapid deployment of new services, seamless scaling to meet demand, and pay-as-you-go pricing that aligns costs with actual usage.

Cost Efficiency

Reduce capital expenditure and shift to operational costs with scalable resources

Agility & speed

Deploy new applications and features faster than traditional infrastructure

scalability

Scale resources up or down instantly based on business needs and traffic

Reliability

Access enterprise-grade uptime and disaster recovery with cloud providers

Step 1: Assessment and Planning

Understanding Your Current Landscape

Every successful cloud migration begins with a thorough understanding of your existing environment. This foundational step involves cataloguing all applications, databases, and infrastructure components currently in use.

Teams assess dependencies, integration points, and performance requirements to create a comprehensive inventory that informs migration decisions.

01

Inventory Discovery

Document all systems, applications, and data sources

02

Dependency Mapping

Identify relationships and integration points

03

Requirements Gathering

Define business needs and technical specifications

04

stakeholder Alignment

Secure buy-in from all key teams and decision-makers

Step 2: Cloud

Evaluating Applications and Infrastructure

Readiness Assessment

This critical phase determines which applications are ready for cloud migration and which require modification or modernisation. Teams evaluate technical compatibility, security requirements, and cost implications for each workload.

Technical Compatibility

Review application architecture, dependencies, and technical requirements to identify migration feasibility and potential roadblocks.

security & Compliance

Assess security posture, data protection needs, and regulatory compliance requirements for cloud environments.

Cost Analysis

Calculate TCO comparison between on-premises and cloud, including migration costs and ongoing operational expenses.

Migration Priority

Rank workloads based on business value, technical readiness, and strategic importance to sequence migration effectively.

Step 3: Migration Strategy and Design

Choosing the Right Approach

Selecting the appropriate migration strategy for each workload is crucial for success. The six R's framework guides decision-making, from simple lift-and-shift approaches to complete application modernisation.

Rehost (Lift & Shift)

Move applications to cloud infrastructure without modification. Fast and cost-effective for legacy systems.

Replatform

Make minor optimisations during migration, such as upgrading databases or adjusting configurations for cloud.

Refactor (Re-architect)

Redesign applications to leverage cloud-native services and microservices architecture for maximum benefit.

Retire / Retain

Identify applications to decommission or keep on-premises based on business needs and migration costs.

Step 4: Migration Execution

Moving Your Workloads

With planning complete, teams execute the migration using phased approaches that minimise business disruption. Execution requires careful coordination across technical, security, and operations teams.

1. **Phase 1: Pilot**

   Migrate low-risk applications first to validate approach and build team expertise

2. **Phase 2: Incremental**

   Move workloads in batches based on priority and dependencies

3. **Phase 3: Completion**

   Finalise migration of remaining applications and validate end-to-end functionality

Execution Best Practices

- Use automated migration tools where possible
- Maintain parallel operations during transition
- Monitor performance continuously
- Document lessons learned for each phase

Common Challenges

- Data transfer bandwidth limitations
- Application compatibility issues
- Unexpected dependencies discovered
- Team resource constraints

Step 5: Validation and Testing

Ensuring Functionality and Performance

Post-migration validation ensures applications function correctly in the cloud environment. Testing covers functional requirements, performance benchmarks, security controls, and user experience.

Teams conduct comprehensive testing across multiple dimensions to verify that migration achieved intended outcomes without introducing new issues.

Functional Testing

Verify all features and workflows operate correctly in cloud environment

Performance Testing

Measure response times, throughput, and resource utilisation against benchmarks

security Validation

Confirm security controls, access permissions, and compliance requirements are met

User Acceptance

Gather feedback from end-users on experience and functionality

Step 6: Optimisation and

Managing Your Cloud Environment Post-Migration

Governance

Migration completion marks the beginning of ongoing cloud management. Optimisation focuses on cost control, performance tuning, and establishing governance frameworks that ensure efficient operations.

Cost optimisation

Right-size resources, implement auto-scaling, and use reserved instances to reduce expenses

Performance Tuning

Monitor metrics, identify bottlenecks, and optimise configurations for peak efficiency

Governance Framework

Establish policies for access control, resource provisioning, and compliance management

Key Optimisation Activities

- Implement tagging strategies for cost allocation
- Configure automated scaling policies
- Monitor and alert on cost anomalies
- Regular rightsizing of compute resources

Governance Requirements

- Identity and access management (IAM) policies
- Infrastructure as code (IaC) standards
- Security baseline configurations Audit and compliance reporting

Step 7: Operational Excellence and Continuous Improvement

Evolving in the Cloud

Cloud migration is not a destination but a continuous journey of improvement. Operational excellence involves refining processes, adopting new cloud capabilities, and fostering a culture of innovation that leverages the full potential of cloud computing.

Organisations should establish feedback loops that drive regular improvements based on performance data, user feedback, and emerging cloud technologies.

Monitor

Track metrics and gather performance data

Analyse

Identify trends and improvement opportunities

Learn

Gather feedback and refine approach

Implement

Deploy changes and new features

30%

Cost Reduction

Typical savings achieved through ongoing optimisation

50%

Faster Deployment

Reduced time to market for new features

99.9%

Uptime

Enterprise-grade availability with proper architecture

Key Takeaways and Next Steps for Your Cloud

Success Requires Structure

The seven-step model provides a proven framework that reduces risk and ensures comprehensive coverage of migration requirements.

Planning is Critical

Invest time in assessment and readiness evaluation before execution to avoid costly rework and migration failures.

Continuous Improvement Matters

Migration completion is just the beginning—ongoing optimisation and governance deliver sustained value from cloud investments.

Your Next Steps

01

Secure Executive Sponsorship

Align leadership on migration goals and secure necessary budget and resources

02

Build Your Migration Team

Assemble cross-functional team with technical, security, and operations expertise

03

Start Assessment Phase

Begin inventory discovery and cloud readiness evaluation for your environment

04

Partner with Experts

Consider engaging cloud migration specialists for complex transitions

> *"The cloud is not just about technology—it's about transforming how your organisation operates, innovates, and competes in the digital age."*

Organizational Readiness and change Management in the cloud Age

Introduction

- The studies for Organization for Economic Co-operation and Development (OECD) economics demonstrated that there is a strong correlation between changes in organization and workplace practices and investment in IT.
- In order to effectively enable and support enterprise business goals and strategies, IT must adapt new technologies and continually change.
- Organization should have a transition to a desirable level of CMM (Change Management Maturity) by having following key knowledge:
  - Domain 1: Managing the Environment, understanding the organization (people, process and culture)
  - Domain 2: Recognizing and Analyzing the Trends (Business and Technology), observer the key driver for changes.
  - Domain 3:Leading for Results, Assess organizational readiness and architect solution that delivers definite business values.

Basic Concept of organizational readiness

- People in the organization face the change as challenging. They have fear or uncertainties. This is called FUD syndrome: Fear, Uncertainty and Doubt.
- Employees are used to their roles and responsibility and are familiar with their environment and management's expectations.
- But when corporate changes are made, it is common that people tend to become uncomfortable and excited regardless the level and intensity of change.
- Surveys are made and studies say that project fails to meet the objectives, money are wasted, opportunities are lost due to lack of focus and interest in the change.

Drivers for changes: A framework to comprehend the competitive environment

- The five driving factors for change given by the framework are:
  - 1) *Economic (global and local, external and internal)*

Economic factors are usually dealing with the state of economy, both local and global in scale. Managers and groups are expected to deal with the unpleasant facts of shrinking market share, declining profit margins, unsatisfactory earnings, new and increasing competition. Managers are often asked to do more with less, and this is done during downturn.

  - 2) *Legal, political, and regulatory compliance*

This deals with issues of transparency, compliance and conformity. The objective is to be a good corporate citizen and industry leader and to avoid the potential cost of legal threats from external factors.

- *Environmental (industry structure and trends)*

Environmental factors usually deal with the quality of natural environments, human health, and safety.

- *Technology developments and innovation*

New technologies and innovations in every has played very important part and has changed the lives of so many fields.

- *Socio cultural (markets and customers)*

It sees the societal expectations and trends and how cloud computing change the world of markets and customers.

Creating a winning environment

- At the cultural level of an organization, change too often requires a lot of planning and resource. The management and executives communicate employees to make sure that every employee understands
  - 1) The new direction of the firm
  - 2) The urgency of the change needed
  - 3) What the risks are to – maintain status quote and making the change.
  - 4) What the new role of the employee will be
  - 5) What the potential rewards are.

Build the business savvy organization

Common change management models

- There are many different change management approaches and models.
- **1) Lewin's Change Management Model**

Kurt Lewin, a psychologist by training, observed that there are three stages of changes, which are ***Unfreeze, Transition and Refreeze***.

It is recognized that people tend to become comfortable in this freeze or unchanging environment and they wish to remain in this safe/comfort zone. Any disturbance to them will make them uncomfortable.

To encourage change, its necessary to unfreeze the environment by motivating people to accept the change. Motivation for change must be generated before change can occur. This is the unfreezing stage from which change begins.

The transition phase is when the change plan is executed and actual change is being implemented.

The last phase is Refreeze, this is the stage when the organization once becomes unchanging/fozen until the next time a change is initiated.

2) Deming Cycle(Plan, Do, Study,Act)

- The Deming cycle is also known as the PDCA cycle.
- It is a continuous improvement model with four sequential sub processes: Plan, Do, Check and Act.
- The PDCA cycle is usually implemented as an evergreen process, which means that the end of one complete cycle or pass flows into the beginning of the next pass and thus supports the concept of continuous quality improvement.
- **PLAN** :Recognize an opportunity and plan a change.
- **DO** : Execute the plan in a small scale to prove the concept.
- **CHECK** :Evaluate the performance of the change and report the results to sponsor.
- **ACT** : Decide on accepting the change and standardizing it as a part of the process.

Incorporate what has been learned from the previous steps to plan new improvements and begin a new cycle.

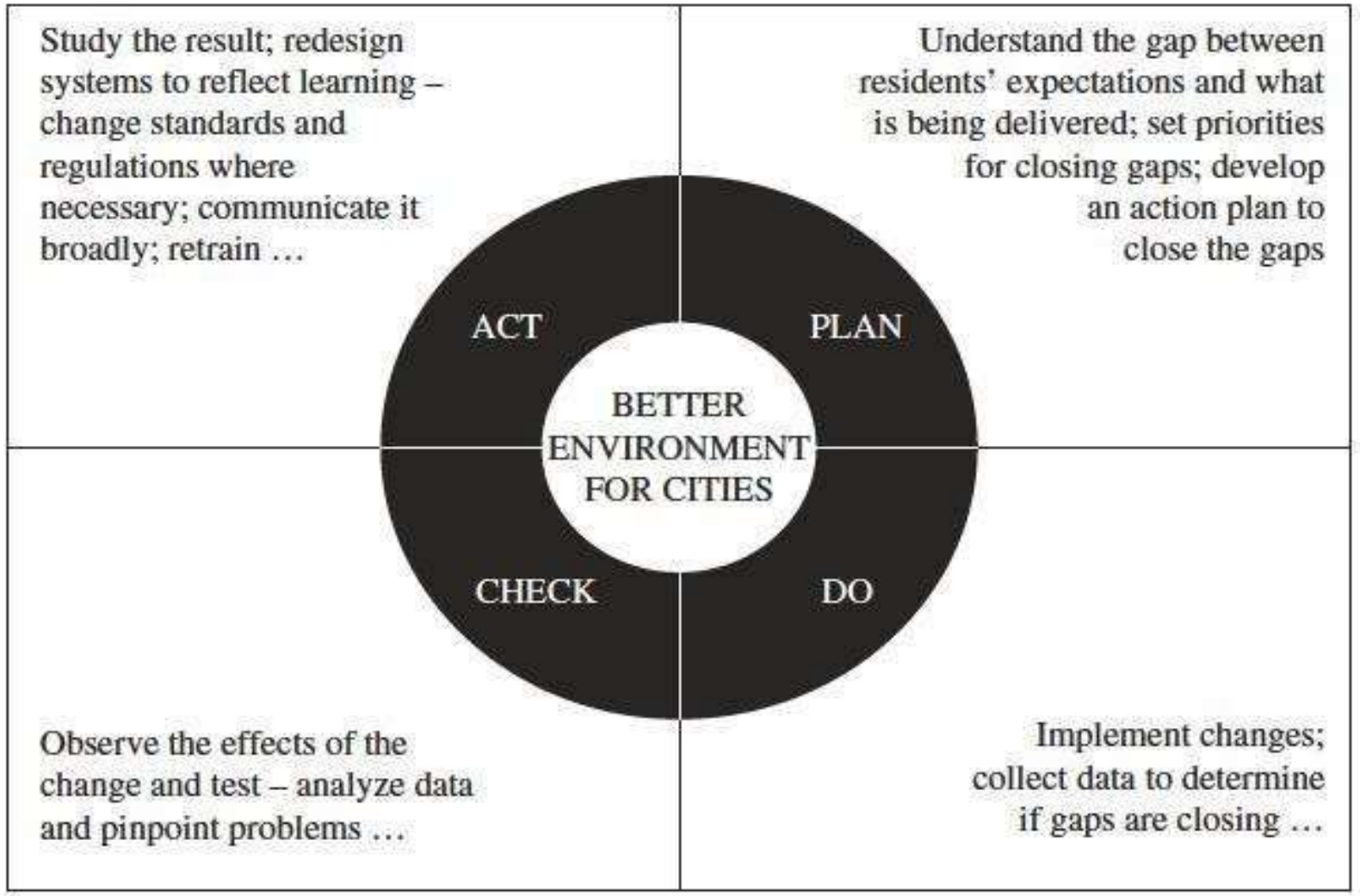


FIGURE 22.1. Deming's PDCA cycle.
Source: http://www.gdrc.org/uem/iso14001/pdca cycle.gif.

A Proposed Working Model : CROPS

- CROPS framework is a working model which stands for Culture, Rewards, Organization and Structures, Process, Skills and Competencies
- ***Culture :*** Corporate culture is a reflection of organizational (management and employees) values and belief.

  The culture of a group can be defined as, A pattern of shared basic assumptions that the group learned as it solved its problems of external adaption and internal integration, that has worked well enough to be considered valid and therefore, to be taught to new members as the correct way to perceive, think, and feel in relation to those problems.

Elements of organizational culture includes:

- Stated values and belief
- Expectations for member behavior
- Customs and rituals
- Stories and myths about the history of the organization
- Norms, the feelings evoked by the way members interact with each other
- Metaphors and symbols

- ***Rewards and Management System*** : This management system focuses on how employees are trained to ensure that they have the right skills and tools to do the right job. It identifies how to measure employee job performance and how company compensates them based on their performance. Reward is the most important that shapes employees values and beliefs.
- ***Organization and Structures*** : How the organization is structured is largely influenced by what the jobs are and how the jobs are performed. Business processes need to align with organizational vision, mission, and strategies in order to create customer and shareholder values.
- ***Process*** : Business process or business method as a collection of related, structured activities or tasks that produce a specific service or product for customers. A process is where the work gets done, and value creation occurs through transforming input into output.

- ***Skills and Competencies***: Specialized skills that become part of the organizational core competency enable innovation and create a competitive edge. Organizations that invest in research and development which emphasize investing in people's training and well-being will shape a winning strategy.

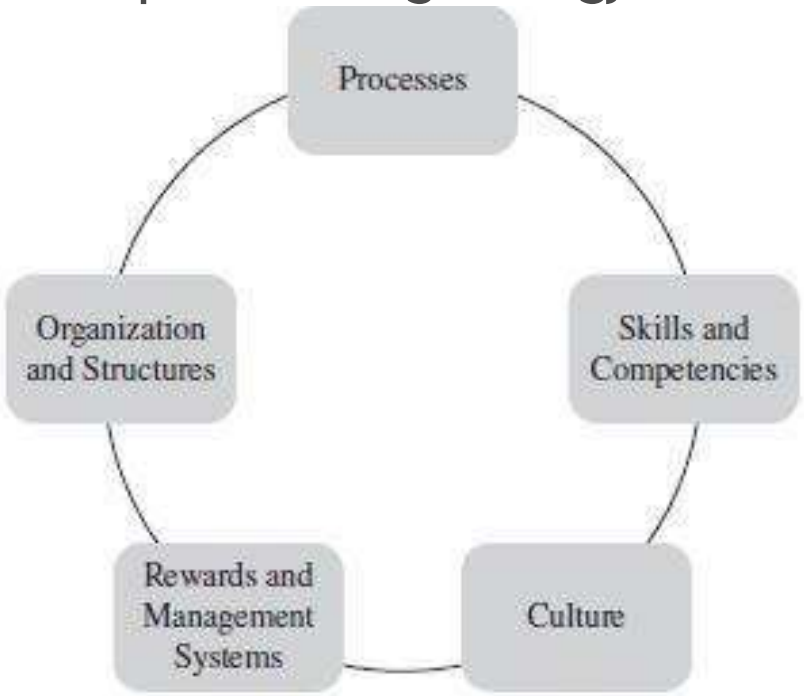


FIGURE 22.2. CROPS framework.

Change Management Maturity model (CMMM)

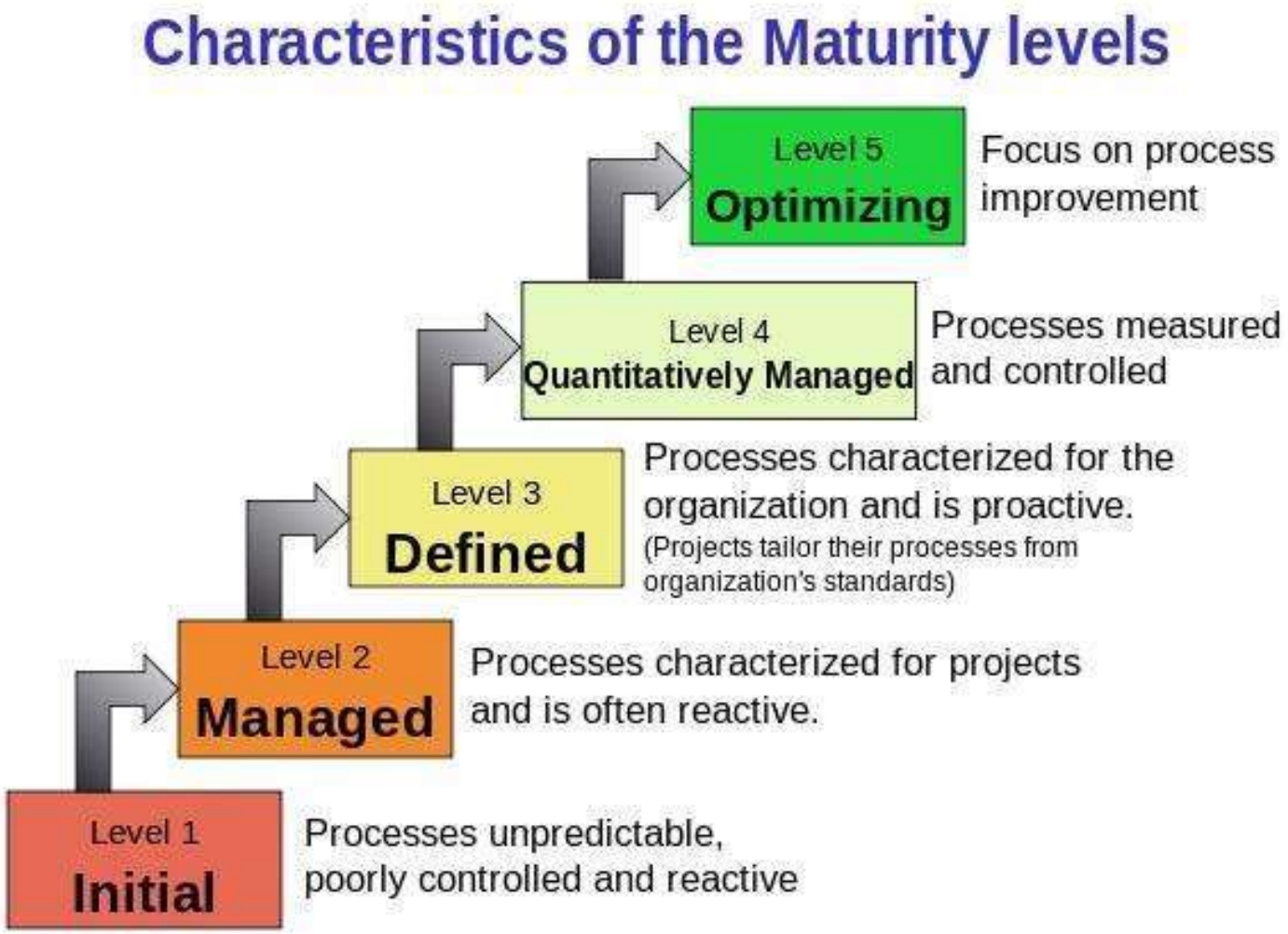
- A Change Management Maturity Model (CMMM) helps organization to analyze, understand, and visualize the strength and weakness of the firm's change management process and identify opportunities for improvement and building competitiveness.
- The model should be simple enough to use and flexible to adapt to different situations
- The business value of CMMM can be expressed in terms of improvements in business efficiency and effectiveness. All organizational investments are business investments, including IT investments. The resulting benefits should be measured in terms of business returns.
- Therefore CMMM value can be articulated as the ratio of business performance to CMMM investment;

$$\text{ROIT (CMMM)} = \frac{\text{Estimated Total business performance improvement}}{\text{Total CMM investment (TCO)}}$$

Where,

- ROIT : Obeserved business value or total return on investment from IT initiative (CMMM)
- Business performance improvement – Reduce error rate
- Increase cutomer/user satisfaction – customer and employee retension
- Increase market share and revenue
- Increase sales from existing customer
- Improve productivity
- CMMM investment – initial capital investment and total cost of ownership over the life of investment

CMM levels


Characteristics of the Maturity levels
Level 5
Optimizing
Focus on process improvement
Level 4
Quantitatively Managed
Processes measured and controlled
Level 3
Defined
Processes characterized for the organization and is proactive.
(Projects tailor their processes from organization's standards)
Level 2
Managed
Processes characterized for projects and is often reactive.
Level 1
Initial
Processes unpredictable, poorly controlled and reactive

Organizational Readiness self-assessment: (Who, When, Where and How)

- An organizational assessment is a process intending to seek a better understanding of *as-is (current)* state of the organization.
- It also defines the roadmap required to fill the gap and to get the organization moving toward where it wants to go.
- The process implies that the organization needs to complete the strategy analysis process first and to formulate the future goals.
- The assessment can be conducted by either an internal or external professional. During the effective organization readiness assessment, it is desirable to achieve following:
  - Articulate and reinforce the reason for change.
  - Determine the as-is state
  - Identify gap between future and current state
  - Assess barriers to change
  - Establish action plan to remove barriers.

- It is also important to select the right people for the assessment across the organization.
- Asking right questions is also essential. The assessment should provide insight into your challenges and help determine some of the key questions that need to be asked.