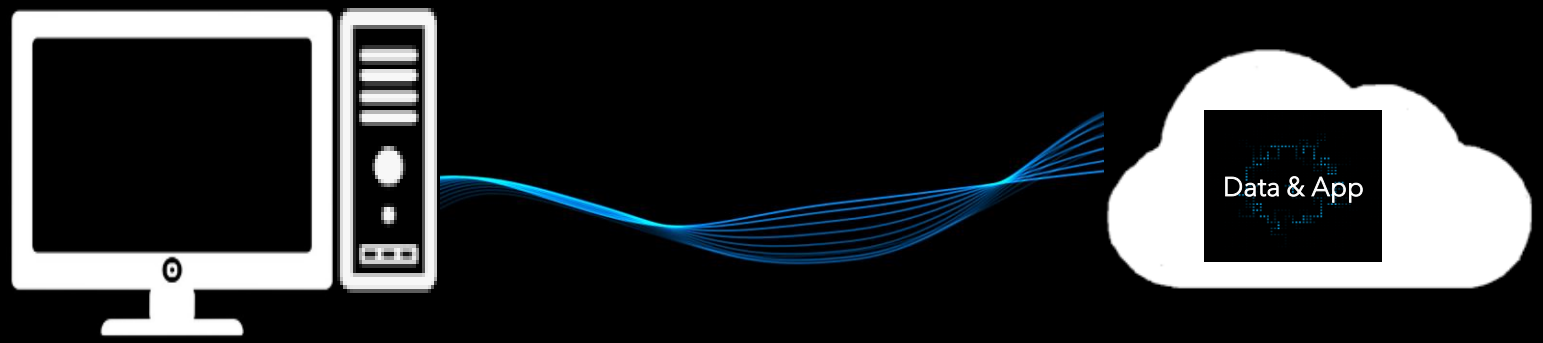
Cloud Audit

Understanding Cloud Computing

Understanding Cloud Computing

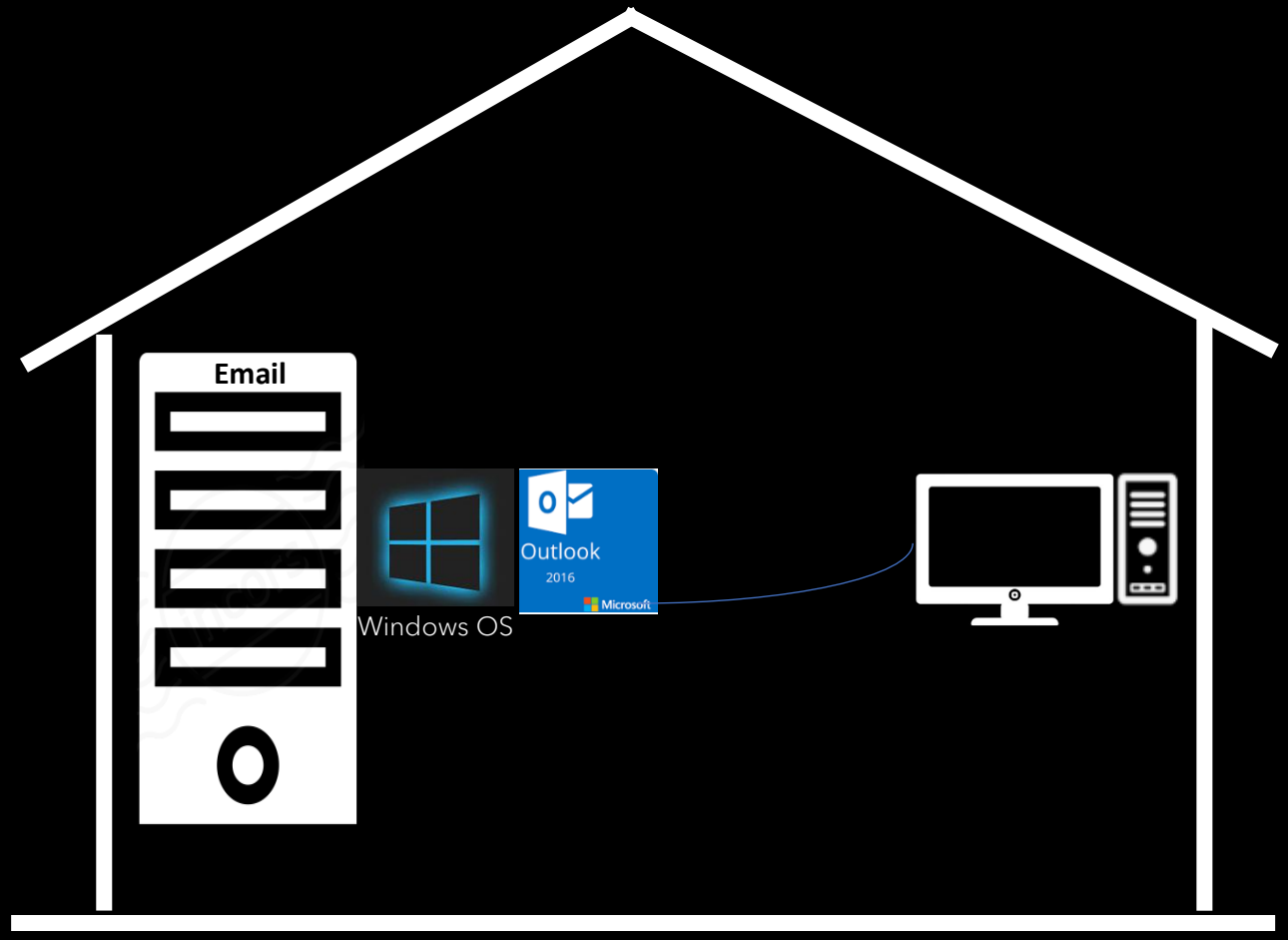
Data and applications stored and run on the cloud.



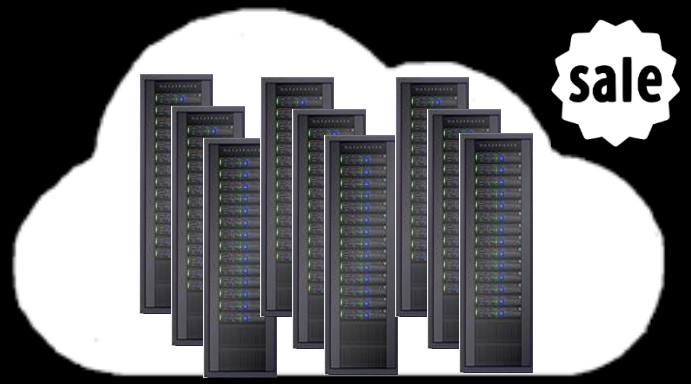
Cloud Computing is anything that involves delivering computer resources over the internet.

Cloud Computing History

Cloud Computing



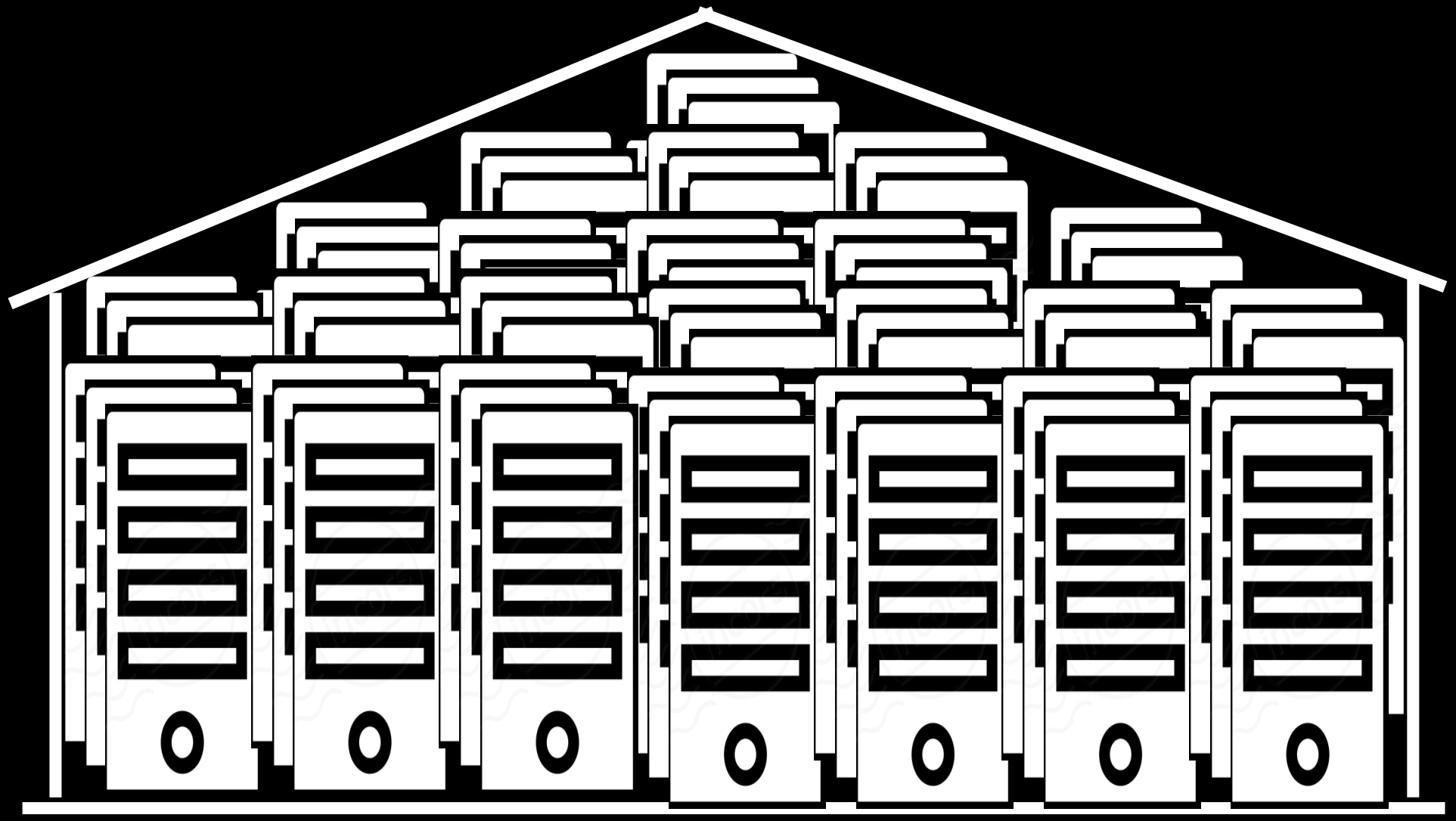
- ERP Software
- Web Servers
- Productivity Software
- Databases



What is Cloud

What is Cloud

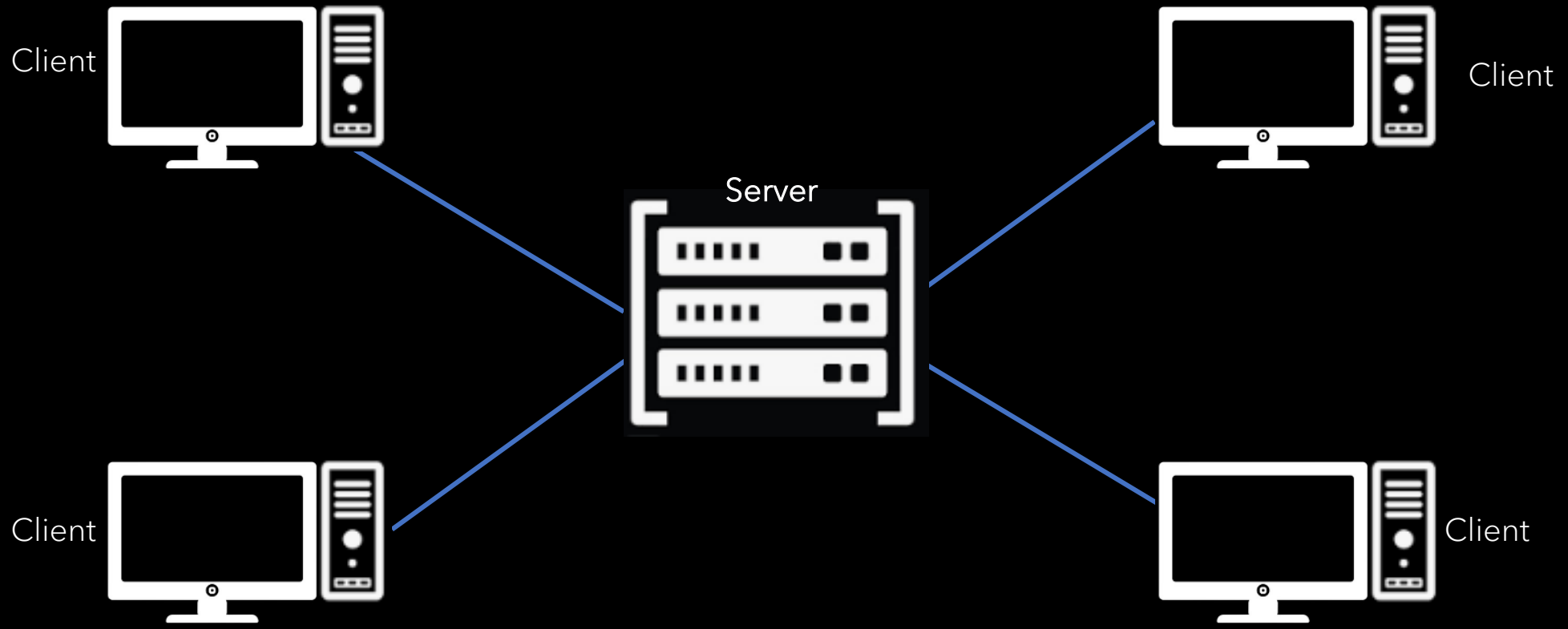
The cloud is just a big building filled with computers (servers).



Data Center

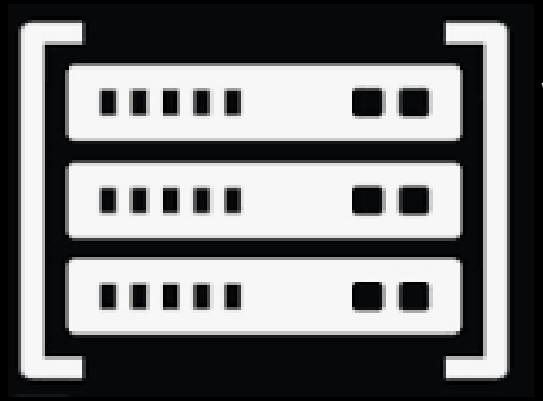
What is a Server

What is a Server



Connect using Internet or
Local Area Network (LAN)

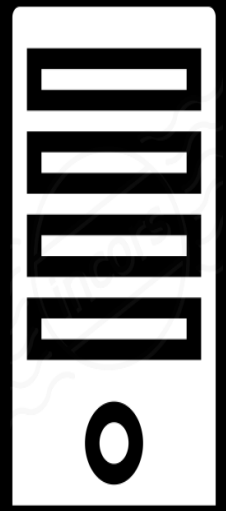
What is a Server



Website server

Database server

Email server

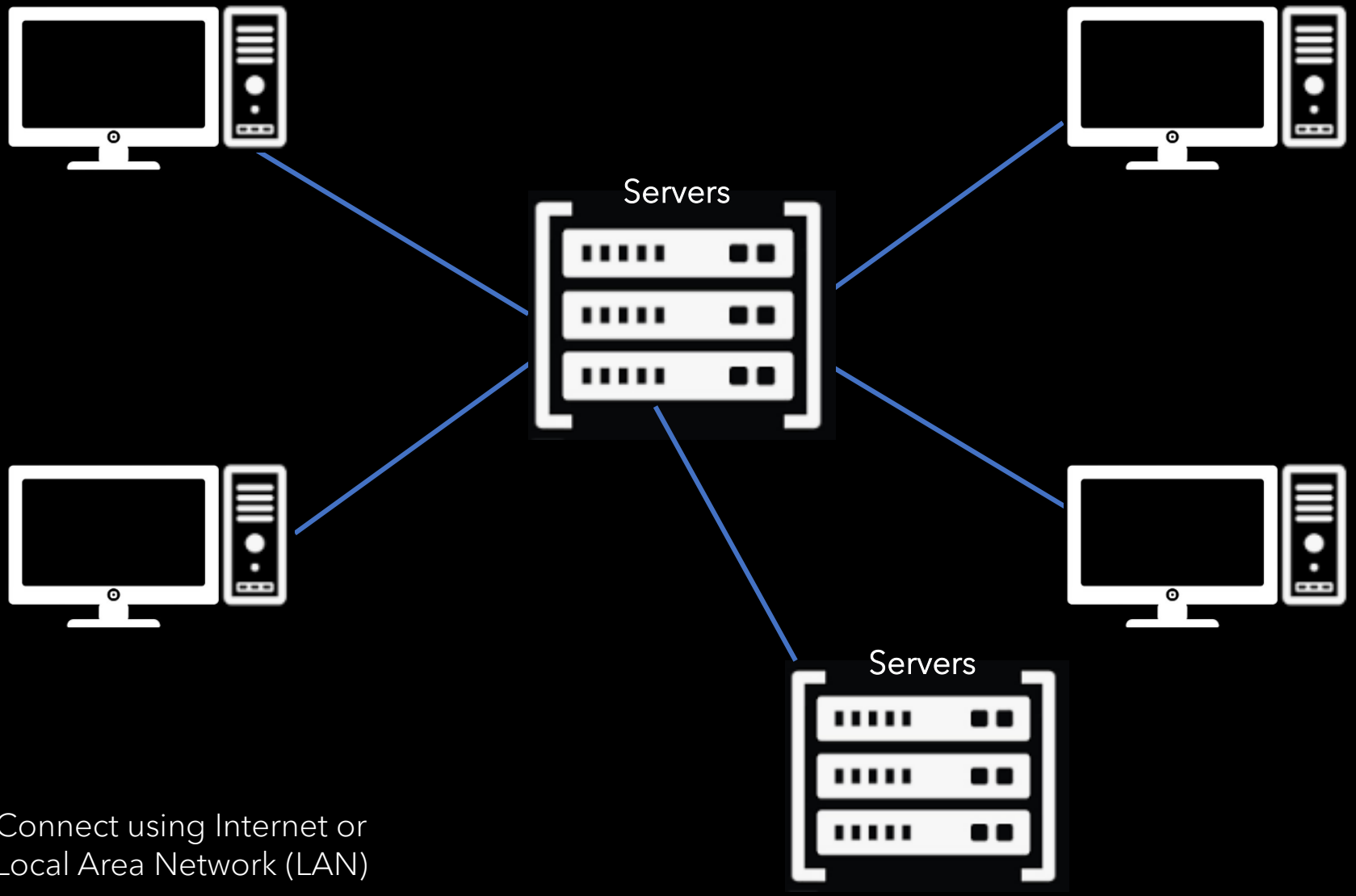


Website server

Database server

Email server

What is a Server

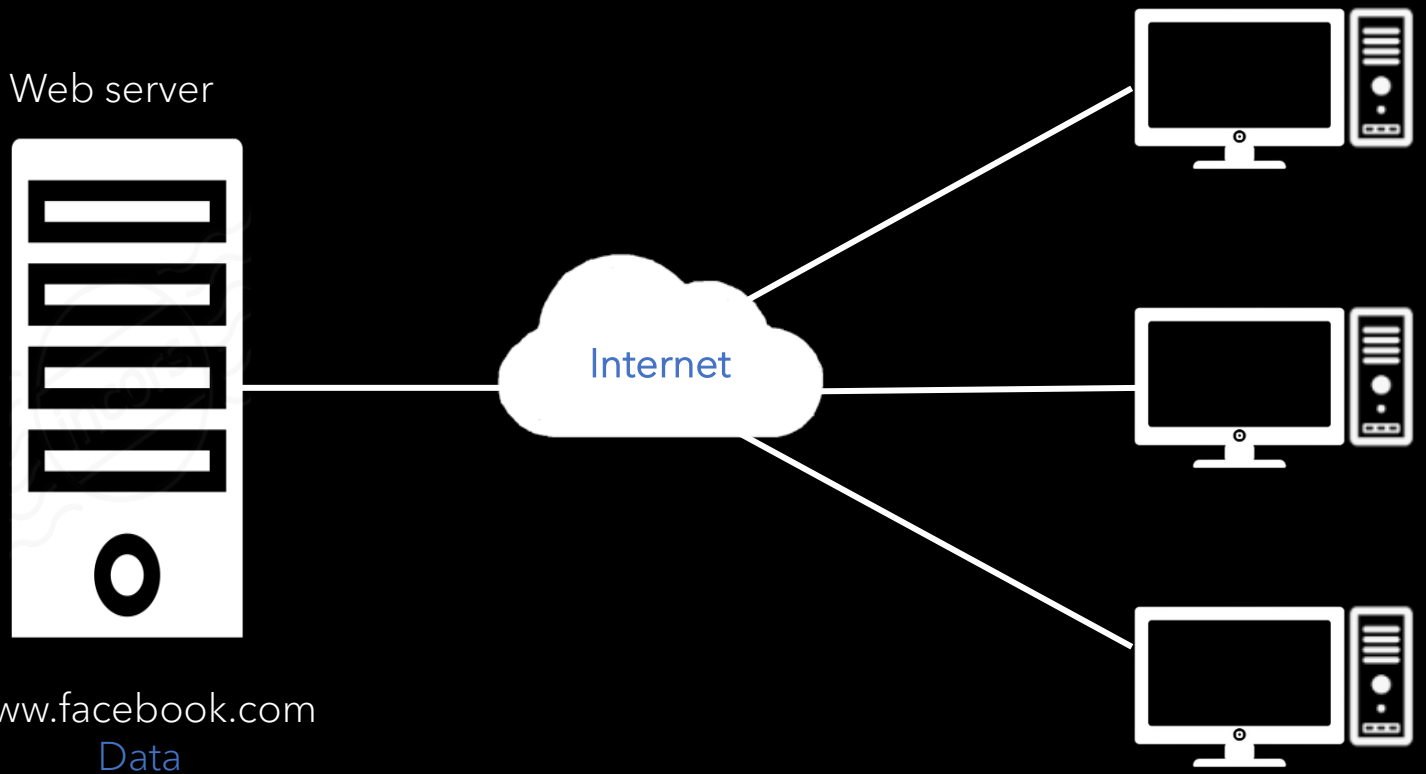


- Powerful (Large Workload)
- Fast
- High Storage
- Availability
- Data Backup
- Several Connections

Connect using Internet or
Local Area Network (LAN)

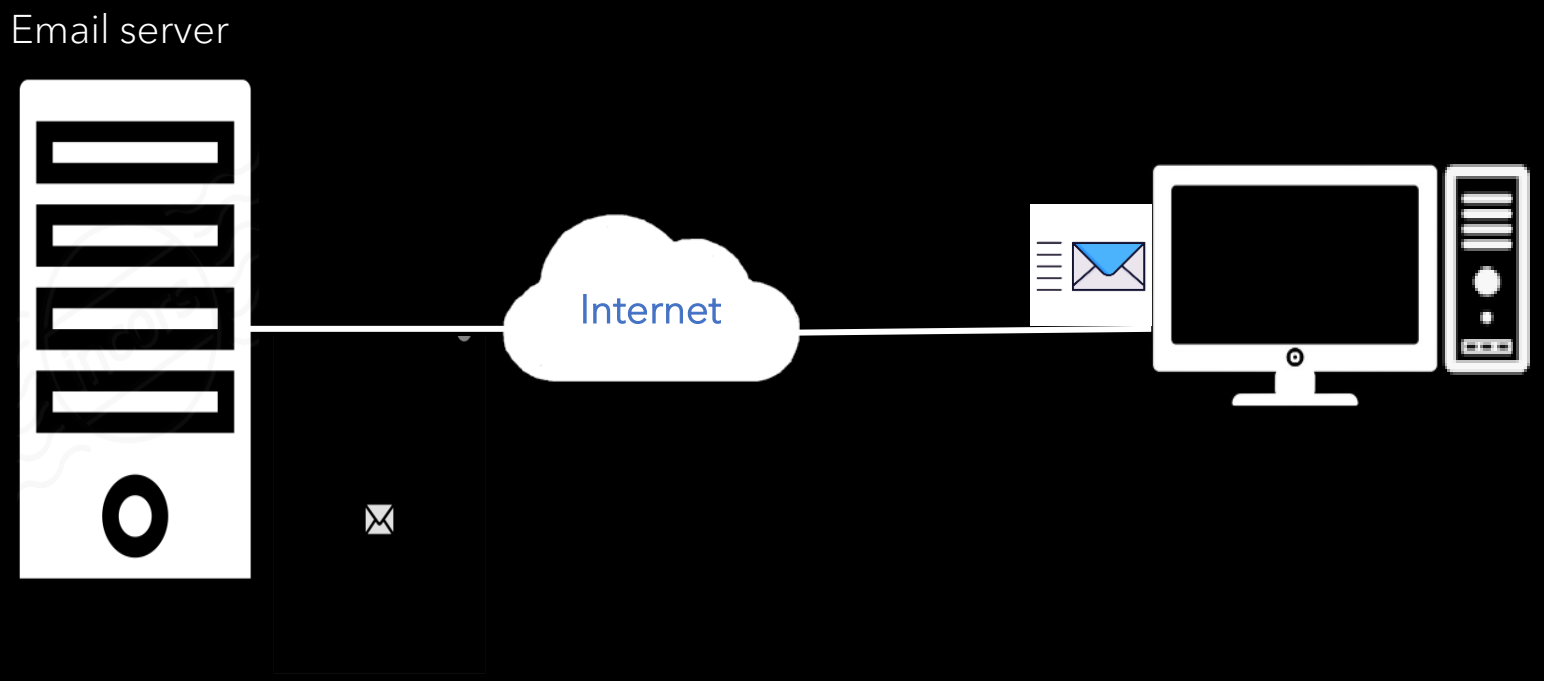
Services Provided by Servers

Services Provided by Servers



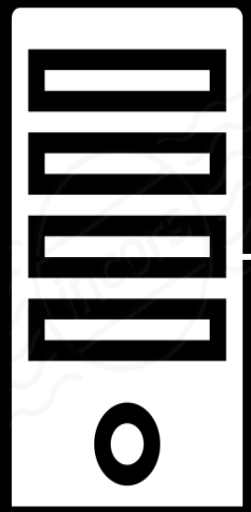
www.facebook.com
Data
HTML codes
Graphics
Software

Services Provided by Servers



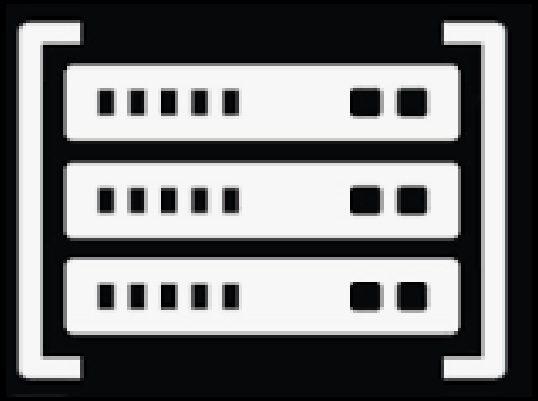
Services Provided by Servers

Database server



SQL

Microsoft
SQL Server
2022 Standard



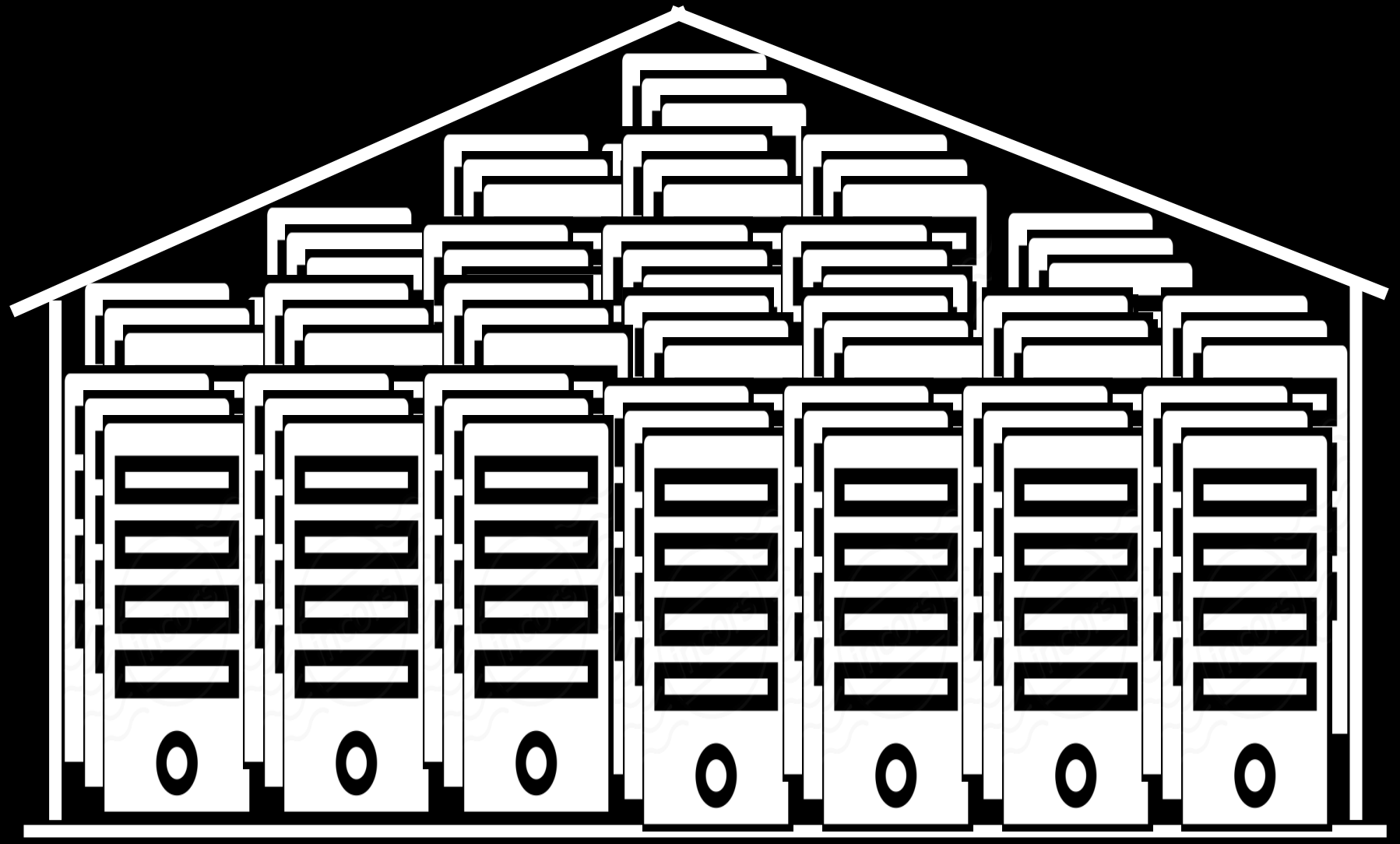
Website server

Database server

Email server

What is Cloud

Cloud is a big building filled with servers.



Data Center

- Running applications
- Storing data
- Processing data
- Web hosting
- Sharing files

A Local Area Network (LAN) is a network of interconnected computers and devices within a limited geographical area, such as an office building.

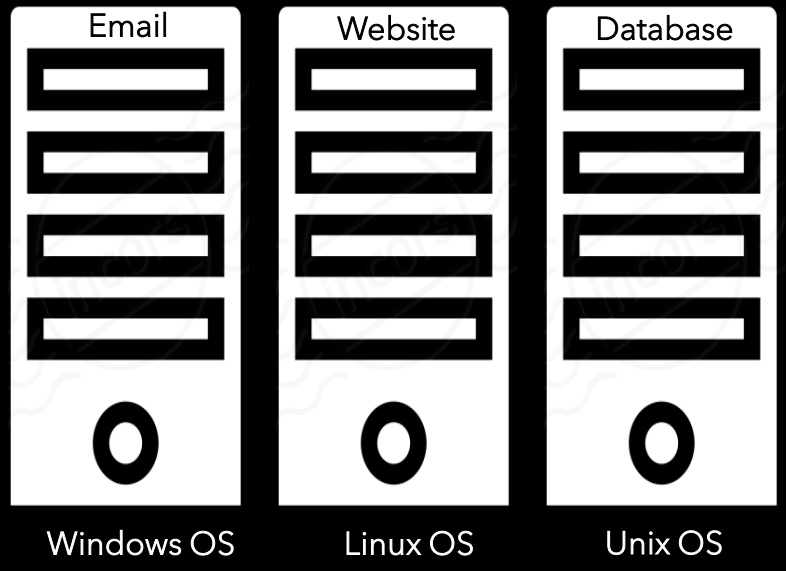
Virtual Machines (VMs)

Virtual Machines (VMs)

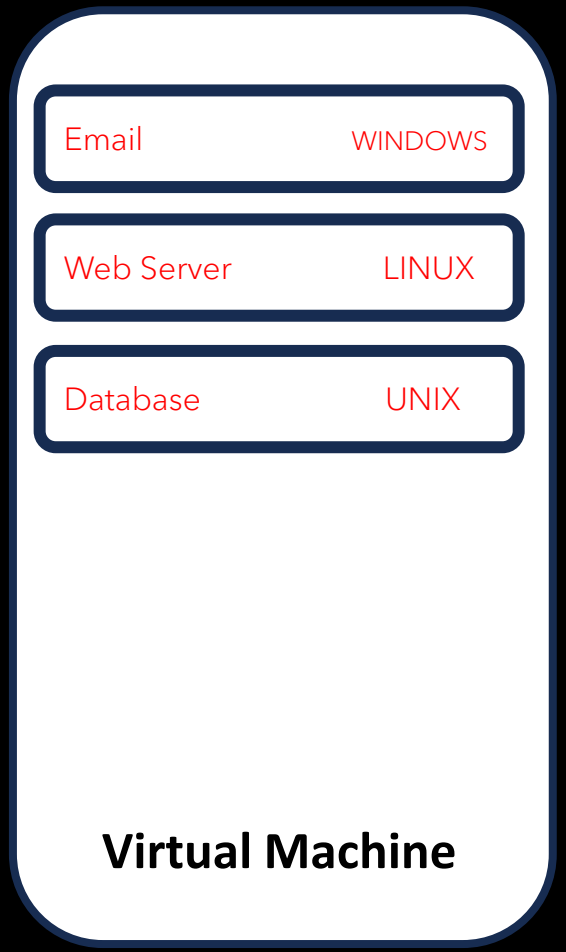
Virtual Machines (VMs) simulates computer hardware and software in a virtual (software) environment.

Virtual Machines (VMs)

Physical Servers



An Operating System (OS) is a software that acts as an intermediary between a computer hardware and application software.



Services Provided by Servers

- Running 3 VMs (virtual machines)
- Running 3 different services
- Running 3 different operating systems

Cloud Computing
vs
Virtualization

Cloud Computing vs Virtualization

Cloud Computing is a broader concept that involves delivering various computing services over the internet.

Virtualization enables the creation of virtual instances of compute resources on a single machine.

Benefits of Cloud Computing

Benefits of Cloud Computing

- Cost Savings
- Reliability
- Scalability
- Flexibility
- Global Accessibility
- Security
- Maintenance
- Performance

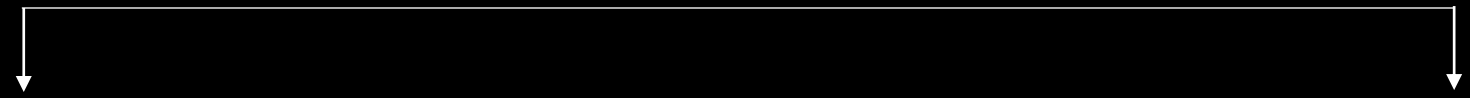
Cloud Service Providers (CSP)

Cloud Service Providers (CSP)

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)
- Alibaba
- IBM

Cloud Computing Models

Cloud Computing Models



Deployment Model

How services are made available to users or organizations.

Service Model

The different types of services provided over the cloud.

Deployment Models

Deployment Model

Public Cloud

aws

Google Cloud

Microsoft Azure

Private Cloud

Hybrid Cloud

UBER

TAXI

Public & Private Cloud

Characteristics of Deployment Model

Public Cloud

Cost-effective

Scalability

Shared infrastructure

Private Cloud

Enhanced security

Customization

Dedicated resources

Hybrid Cloud

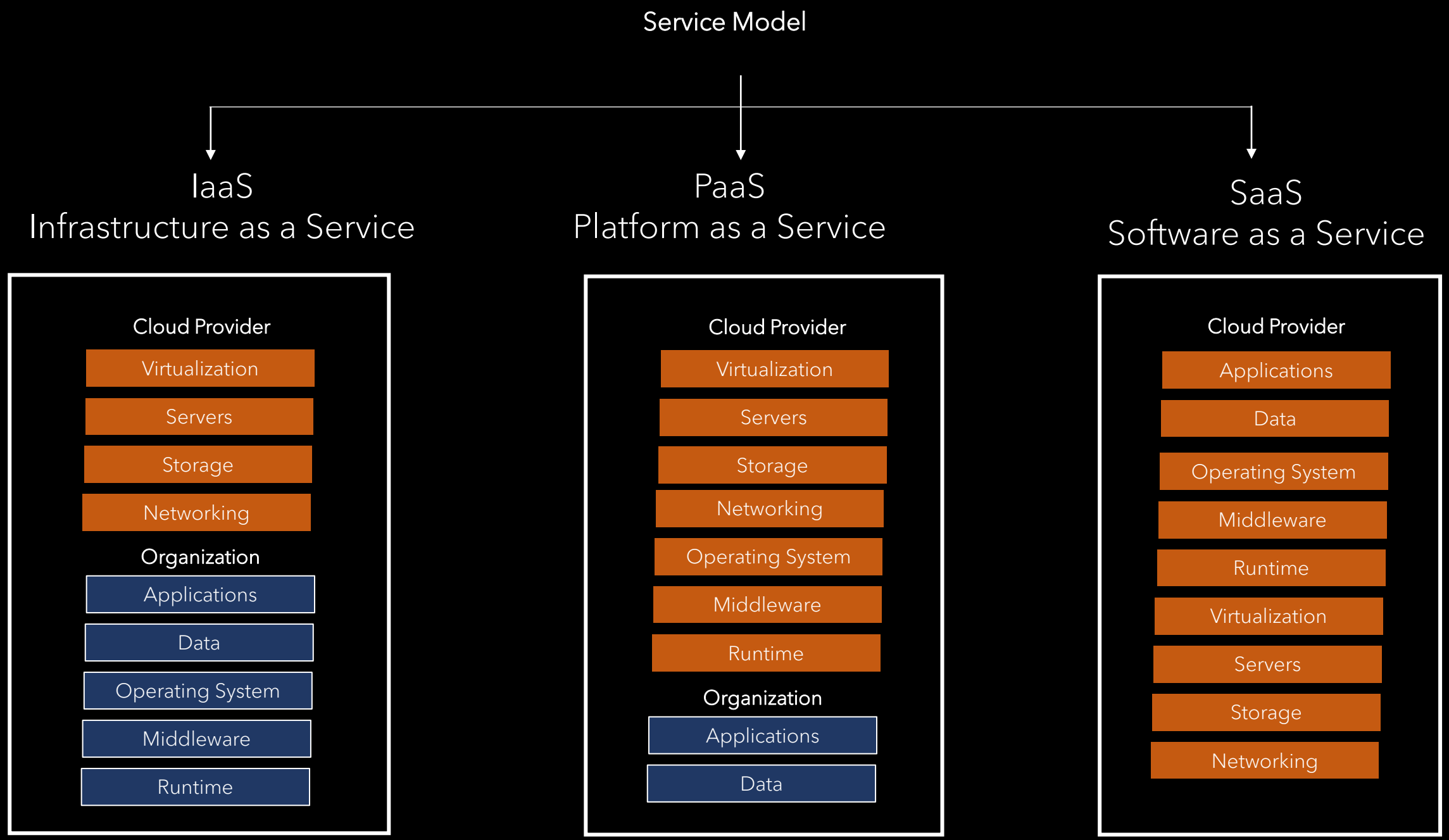
UBER TAXI

Data portability

Scalability

Flexibility

Service Models


Service Model
IaaS
Infrastructure as a Service
PaaS
Platform as a Service
SaaS
Software as a Service
Cloud Provider
Virtualization
Servers
Storage
Networking
Organization
Applications
Data
Operating System
Middleware
Runtime
Cloud Provider
Virtualization
Servers
Storage
Networking
Operating System
Middleware
Runtime
Organization
Applications
Data
Cloud Provider
Applications
Data
Operating System
Middleware
Runtime
Virtualization
Servers
Storage
Networking

Key Services & Solutions in Cloud Ecosystems

Key Services & Solutions in Cloud Ecosystems

- Compute Services
- Storage Services
- Databases
- Networking
- Analytics
- Identity & Access Management

Compute Services

Compute services refers to the cloud computing services that provide computing resources over the internet.

Processing power

Memory

Storage

Networking

Storage Services

Cloud storage provide a way for users and organizations to store, manage, and access their data over the internet.

Databases

Databases for storing, managing, and retrieving structured data in a scalable and flexible manner.

Relational databases

NoSQL databases

Specialized database

Networking

Networking services provide the infrastructure and tools necessary to establish and manage network in cloud environments.

Analytics

Cloud Analytics provide organizations with the tools and platforms needed to analyze and derive insights from large volumes of data stored in the cloud.

Identity & Access Management (IAM)

Cloud IAM provide organizations with the tools and capabilities to manage user identities, control access, and enforce security policies.

Key Solutions & Resources in Cloud Ecosystems

- Compute Services
- Storage Services
- Databases
- Networking
- Analytics
- Identity & Access Management

AWS Compute Services

AWS - Compute Services

Amazon Elastic Compute Cloud (EC2):

- Web service used to run virtual server “instances” in the cloud.
- EC2 instances can run Windows, Linux, or Mac OS operating systems.
- EC2 is used to run different applications and workloads.
- Web service interface allow users to obtain and configure capacity with minimal friction.
- Allow users to pay only for capacity used.

Other Services:

- Amazon Elastic Container Service (ECS)
- AWS Lambda
- AWS Elastic Beanstalk
- Amazon LightSail Instances

Microsoft Azure Compute Services

Microsoft Azure Virtual Machines

- AVM instances can run Windows, Linux, or Mac OS operating systems.
- AVM is used to run different applications and workloads.
- Auto-scaling options for users.
- Deployment options – web-based interface, command-line interface, Azure Resource Manager.
- Offers wide range of security features.

Other Services:

- Azure Functions
- Azure Container Instances
- Azure Kubernetes Service
- Azure Batch

Google Cloud Platform Compute Services

Google Cloud Platform - Compute Services

Google Compute Engine

- Web service used to create and run virtual machines “instances” in the cloud.
- GCE instances can run Windows, Linux, or Mac OS operating systems.
- GCE is used to run different applications and workloads.
- Compute Engine allows users to define & configure their environment.
- GCE includes live migration capabilities.
- Users can easily scale their infrastructure up or down based on demand.

Other Services:

- Google Cloud Run
- Google App Engine
- Google Kubernetes
- Google Cloud Dataflow

Cloud Governance

Cloud Governance

Set of policies, processes, and controls implemented by an organization to manage and optimize its use of cloud computing resources.

- Establishing guidelines for decision making
- Compliance with regulations & standards
- Managing the lifecycle of cloud services

Provide a framework to achieve business objectives while maintaining control, security and cost-effectiveness.

Cloudification

Cloudification

Cloudification refers to the process of migrating an organization’s infrastructure, applications, services, or data from on-premises to the cloud.

Transitioning to Cloud

Migration: Moving existing resources & assets to cloud environment.

Modernization: Adapting applications & processes to align with cloud capabilities.

Scalability & Flexibility: Utilizing scalability & flexibility offered by cloud.

Cost Optimization: Leveraging pay-as-you-go model and optimizing resource usage.

Enhanced Services: Taking advantage of managed services available in the cloud.

Accessibility & Collaboration: Enabling easier access to resources and fostering collaboration.

Risks Associated with Cloud Computing

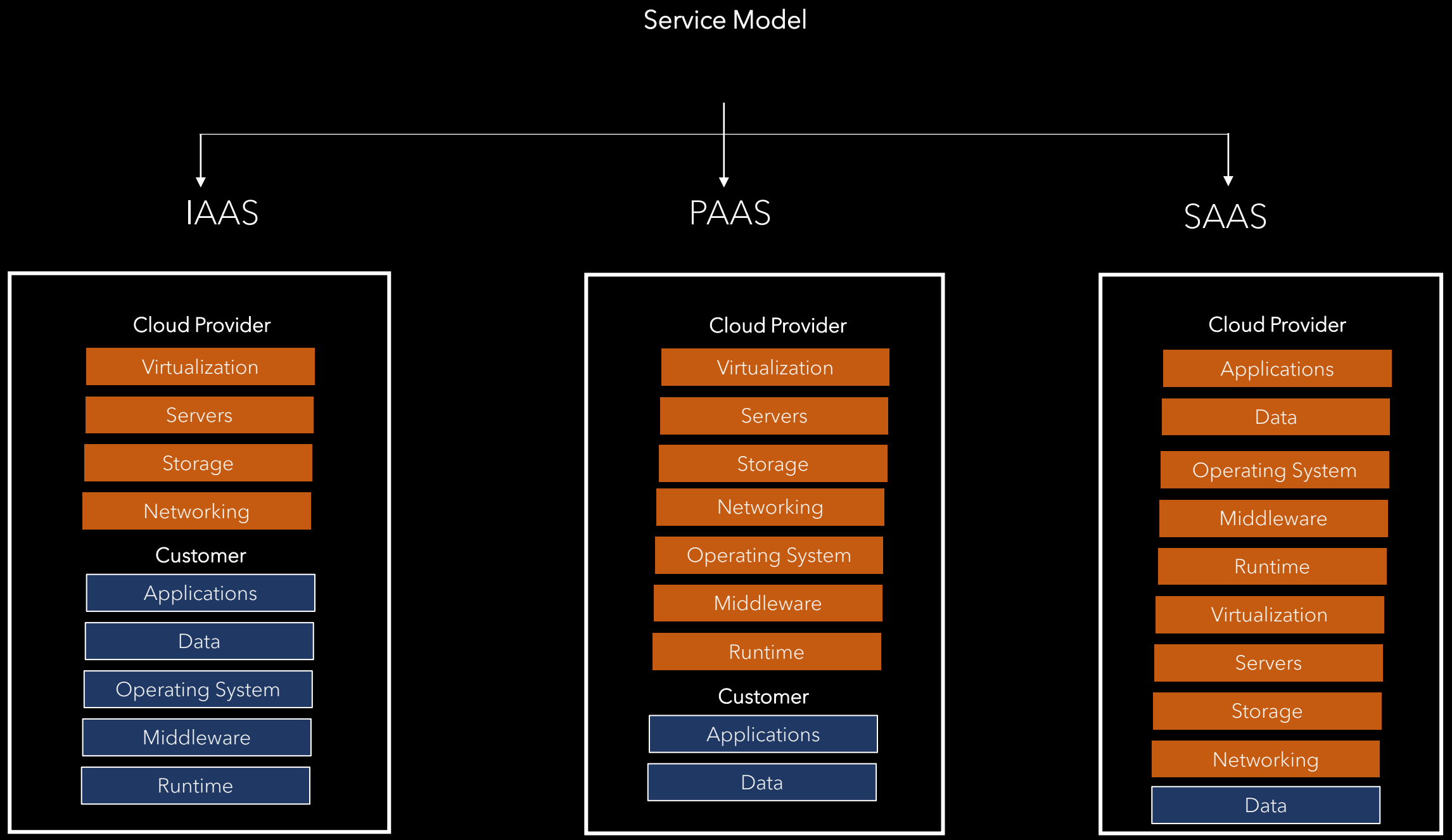
Risks Associated with Cloud Computing

- Data Security & Privacy
- Compliance & Regulatory Issues
- Reduced Visibility & Control
- Service Disruptions & Downtime
- Data Loss and Corruption
- Data Location Constraints
- Cost Management
- Incompatibility of Existing Architecture
- Skill Gaps & Training Needs

Shared Responsibility Model

Shared Responsibilityy Model

Distribution of security and management responsibilities between the cloud service provider (CSP) and the cloud customer.


Service Model
IAAS
PAAS
SAAS
Cloud Provider
Virtualization
Servers
Storage
Networking
Customer
Applications
Data
Operating System
Middleware
Runtime
Cloud Provider
Virtualization
Servers
Storage
Networking
Operating System
Middleware
Runtime
Customer
Applications
Data
Cloud Provider
Applications
Data
Operating System
Middleware
Runtime
Virtualization
Servers
Storage
Networking
Data

Audit

Audit is the examination and evaluation of financial & non-financial records, processes, operations, systems and applications

Types of Audit

Internal Audit Department

Internal Audit

- SOX Audit (IT)
- Cybersecurity Audit (IT)
- Information Systems Audit (IT)
- Cloud Audit (IT)
- Operational Audit
- Business Process Audit
- Compliance Audit
- Payroll Audit
- Human Resources Audit

CPA Consulting Firms

Financial Statement Audit

- Income Statement & Balance Sheet

CPA Consulting Firms

Attestation Engagements

- SOC Audit

- SOX Audit
- Cybersecurity Audit
- Information Systems Audit
- Cloud Audit
- Operational Audit
- Business Process Audit
- Compliance Audit
- Payroll Audit
- Human Resources Audit

IT Audit

Information Technology (IT)

Use of computer systems for creating, storing, retrieving, processing and transferring information.

Audit

Examination and evaluation of financial & non-financial records, processes, operations, systems etc..,

IT Audit is the examination and evaluation of an IT infrastructure – systems, networks, applications, data, policies and operations.

Types of IT Audit

Types of IT Audit | IT Audit Projects

- Cloud Audit
- Cybersecurity Audit
- Sarbanes-Oxley (SOX) Audit
- Service Organization Controls (SOC) Audit
- Information Systems Audit
- Operational Audit
- Compliance Audit

Types of IT Audit | IT Audit Projects

- Cloud Audit: Assessment of the security, compliance, and performance of cloud computing resources and services.

- Cybersecurity Audit: Assessment of the critical elements (devices, network, systems, data) of an organization's cyber infrastructure.

- SOX Audit: Assessment of Internal Controls over Financial Reporting (ICFR)in compliance with sections 302 & 404 of the SOX Act.

- Operational Audit: Evaluates process changes, procedures, pricing, resource allocation and associated internal control activities.

Internal Audit Projects

- Compliance Audit: Adherence to laws, regulations, internal & external policies, terms of contracts.

- Information Systems: Information & transaction processing systems and how people use those systems.

- Service Organization Control (SOC) Audit: Attest or confirm internal controls at service organizations are in place and are properly designed and operating effectively.

Who Performs A Cloud Audit

Who performs a Cloud Audit

Internal Auditors & External Auditors

- Internal Auditors are employees of the organization they audit.

- External Auditors are employees of a public accounting firm hired by an organization to conduct an audit.

Internal Auditor vs External Auditor

Internal Auditor	External Auditor
Company employees	Outside audit firm
Hired by the company	Appointed by shareholders' vote
Reports are used by management	Reports used by investors, lenders, creditors
Conduct audit throughout the year	Single annual audit

Who performs a Cloud Audit

Audit Report

Internal Audit Dept

IT Auditors

Auditors

ABC Company

External Auditors

IT Auditors

Auditors

CPA Firm

Deloitte.

pwc

KPMG

EY

Cloud Frameworks

Cloud security framework is a set of guidelines and best practices for protecting cloud resources.

Importance of Adopting A Cloud Framework

- Standardization
- Governance & Compliance
- Risk Management
- Cost Management
- Performance Optimization
- Architecture & Design
- Integration & Interoperability
- Change Management

Cloud Frameworks

- NIST (National Institute of Standards and Technology)
- Guidelines on Security and Privacy in Public Cloud Computing

- ISO 27017/27001 (International Organization for Standardization)

- CSA (Cloud Security Alliance)
- Cloud Controls Matrix (CCM) – Framework used to evaluate security controls.

Controls

Controls

A control is a procedure or policy that provides a reasonable assurance that an IT environment operates as intended, that data is reliable, and that the organization comply with applicable laws and regulations.

A control is any action, policy, procedure that helps an organization mitigate risk.

Controls

Safety Control

Access Control

Input Control

Safety Control

Identifying Control Weakness

Control Weakness

Control Test ⟷ Identify Weakness

Control weakness are failures in the design or effectiveness of the controls.

Control Weakness

Control Design

Are the controls designed appropriately?

Control Effectiveness

Are the controls operating effectively?

Control Gap

No control where we expect one to be

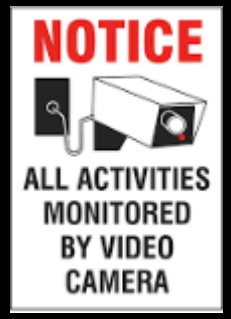
Control Design - Identifying Control Weakness

Control Design

Are the controls designed appropriately?

The control has been thoughtfully developed to address specific risks or objectives.

Store Break-In



Risk: Future Break-In

Control: Surveillance Camera

Identifying Internal Control Weakness

Control Design

Weak Password Policy

Risk: Unauthorized access

Control: Password

Control Effectiveness - Identifying Control Weakness

Control Effectiveness

Are the controls operating effectively?

The control is consistently and successfully accomplishing its intended purpose.

Store Break-In

Metal Door

Risk: Future Break-In

Control: Metal Door

Identifying Internal Control Weakness

Control Effectiveness

Are the controls operating effectively?

Access provisioning procedure

Risk: Unauthorized access

Control: Procedure

Control Gap - Identifying Control Weakness

Control Gap

A control does not exist where we expect a control to be present

Self Checkout

Risk: Shoppers not paying for items

Control: Employee stationed at Self-Checkout

Cloud Audit

Cloud Security Alliance (CSA)

Cloud Controls Matrix (CCM)

Cloud Security Alliance (CSA)

- Non-profit organization created to define and promote best practices for security cloud computing environment.
- Formed by Cloud Service Providers (CSP), vendors, and technology companies.
- Cloud Controls Matrix (CCM) is a security framework dedicated to managing risks in cloud computing.
- Cloud Controls Matrix (CCM) details security principles that organizations can implement to secure their cloud environment.

CSA Control Domains

Control Domains

- Governance, Risk and Compliance
- Application & Interface Security
- Identity & Access Management
- Data Security & Privacy Management
- Change Management
- Logging & Monitoring
- Endpoint Management
- Infrastructure & Virtualization Security
- Threat Vulnerability Management
- Cryptography, Encryption & Key Management
- Security Incident Management
- Human Resources
- Business Continuity Management
- Infrastructure & Virualization Security

Governance, Risk & Compliance

Ensuring adequate governance, risk management, and compliance capabilities to meet the needs of their customers.

Application & Interface Security

Ensuring the security of applications and APIs deployed in cloud.

Identity & Access Management (IAM)

Ensuring the security of user identities and access to cloud resources.

Data Security & Privacy (DSP) Management

Ensuring the security and privacy if data throughout its lifecycle.

Change Control & Configuration Management

Mitigating risks associated with changes & configuration of IT assets .

Logging & Monitoring

Ensuring that Cloud Service Providers (CSPs) have adequate logging and monitoring capabilities to detect and respond to security incidents .

Endpoint Management

Ensuring that endpoints are managed securely in cloud environments.

Threat Vulnerability Management

Assessing and mitigating vulnerabilities of an organization’s infrastructure.

Cryptography, Encryption & Key Management

Ensuring that cryptographic keys are managed securely in cloud environments.

Security Incident Management

Ensuring that Cloud Service Providers (CSP) have adequate incident management capabilities to detect, respond to, and recover from security incidents.

Human Resources

Managing the security of personnel involved in cloud operations.

Business Continuity Management

Ensuring adequate business continuity and disaster recovery capabilities.

Infrastructure & Virtualization Security

Ensuring adequate security controls in place to protect the underlying infrastructure and virtualization layers.

Cloud Audit Process

Types of Audit

Financial Statement Audit

- Income Statement & Balance Sheet Audit

Internal Audit

- Cloud Audit (IT)
- Cybersecurity Audit (IT)
- SOX Audit (IT)
- Operational Audit
- Compliance Audit
- Information Systems (IT)
- Audit Readiness

Attestation Engagement

- SOC Audit

IT Audit Process

Phase 1: Planning

Notification & request for Preliminary information.
Kick Off Meeting

Phase 2: Fieldwork

Walkthrough Meeting
Test of Design
Test of Operating Effectiveness
Status Meetings/Issue Validation

Phase 3: Reporting

Draft Report
Management Response
Closing Meeting
Report Distribution

Phase 4: Follow-Up

Follow-up & remediation

Planning Phase

Planning Phase

1. Determine the **Objective**, **Scope** and **Risk Considerations**

Planning Phase

1. Determine the **Objective - (The Why)**
    - Why are we conducting this test
        - Evaluate, determine, assess compliance
        - Determine certain goals are met
        - Assessing the reliability of data
        - Determine efficient use of resources
        - Evaluate safeguard of the organization's assets

Planning Phase

1. Determine the **Audit Scope – (Where - When - What)**
    - Remote / On-premise
    - Time period / duration of audit
    - Specific areas of review
    - Sample size
    - Sampling methodology

Planning Phase

1. Determine any **Risk Considerations**
    - New systems or applications onboarded
    - New changes to industry regulations
    - Specific issues identified in previous testing

Planning Phase

1. Determine the objective audit scope and risk considerations
2. Applications to be tested are selected from the Application list
3. Team members are assigned work and responsibilities
4. Review past audit workpaper
5. Send notification & request for preliminary information & documents – PBC List (Prepared by Client)
6. Conduct Audit Kick-off meeting: (External Auditors & Internal Auditors)
    - Audit period
    - Questions about the PBC List / requested documents
    - Concerns needed to be addressed

Note: We can obtain/pull some or most of the requested items ourselves during fieldwork.

Fieldwork Phase

Fieldwork

1. Schedule meetings with application or process owners to discuss the audit request
2. Conduct a **Walkthrough** to understand the application or process

Walkthrough - Fieldwork

- Walkthrough is a process performed to gain understanding of the system, application or process being tested.
- Walkthrough involves following a transaction or process from initiation to its completion
    - Examine if the internal controls are properly designed
    - Observe if there is a control gap
    - Ask probing questions
    - Gather initial evidence
    - Perform a test of 1 – Test a single transaction from initiation to completion

Fieldwork Stage

1. Schedule meetings with application or process owner to discuss the audit request
2. Conduct a Walkthrough to understand the application or process – Test control design
3. Test the operating effectiveness of the controls by selecting a sample (e.g., 20% up to max 40)
4. Request evidence to support samples selected
5. Conduct status meetings with application/process owners – discuss findings/progress/delays/needs
6. Conduct weekly internal status meeting within internal audit (IA) team – status/progress/deliverables

Reporting Phase

Reporting Stage

1. No Control Deficiency identified
    - Document test steps and results
2. Control Deficiency identified
    - Prepare a draft report - list of audit findings or control weaknesses found
    - Request response from management
    - Management provides remediation plan
    - Final audit report is created
    - Distribute final audit report – Exit memo or Exit meeting

Follow-Up Phase

Follow-Up

1. Follow-up to determine if control deficiency have been corrected
2. Obtain evidence / re-test control
3. Close the deficiency

Performing Cloud Audit

Test of Control Design

Test of Control Design

Control design is tested during a walkthrough.

Control Design: Is the control addressing the risk it was designed for?

Test of Control Effectiveness

Test of Control Effectiveness

Control effectiveness is tested after the walkthrough.

Control Effectiveness: Are the control activities consistently applied?

Controls Testing

Governance Risk & Compliance - Controls Testing

Governance Risk & Compliance – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Governance Program Policy & Procedures	GRC-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for an information governance program, which is sponsored by the leadership of the organization. Review and update the policies and procedures at least annually.	• Examine the policy and/or procedures related to information governance programs to determine whether the organization has developed a comprehensive strategy for information governance. • Examine policies and procedures for evidence of review at least annually.
Risk Management Program	GRC-02	Establish a formal, documented, and leadership-sponsored Enterprise Risk Management (ERM) program that includes policies and procedures for identification, evaluation, ownership, treatment, and acceptance of cloud security and privacy risks.	• Review ERM documentation, processes, and supporting evidence to confirm if the ERM program includes provisions for cloud security and privacy risk. • Obtain and examine supporting evidence to determine if the office or individual responsible reviews the information and, if issues were identified, if they were investigated and remediated appropriately.
Information Security Program	GRC-05	Develop and implement an Information Security Program, which includes programs for all the relevant domains of the CCM.	• Examine the policy and/or procedures related to the Information Security Program to determine whether the organization has developed and implemented a comprehensive strategy to manage Information Security. • Review the details of the information security program and establish if this meet security, availability, confidentiality, and privacy requirements, including information security function. • Confirm that identified gaps/issues are being tracked, monitored, and remediated with appropriate escalation where required.

Data Security & Privacy – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Data Flow Documentation	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	• Establish whether the organization has documented the roles and responsibilities for this process. • Select a sample of documents to check that they have been completed to the correct specifications and reviewed. • Review if data flow documentation includes assessment for accuracy, completeness, timeliness, and sustainability of data (flow).
Data Protection by Design	DSP-07	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	• Examine whether policy, standards, and procedures create a framework which fosters a culture and expectation of "security through design." • Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out.
Data Privacy by Design	DSP-08	Classify data according to its type and sensitivity level.	• Examine whether policy, standards, and procedures create a framework which fosters a culture and expectation of "security through design." • Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out.

Application & Interface Security - Controls Testing

Application & Interface Security – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Application & Interface Security Policy & Procedures	AIS-01	Establish policies and procedures for application security to provide guidance to the appropriate planning, delivery and support of the organization's application security capabilities.	• Verify that Application & Interface Security Policy is implemented to support organization's application security capabilities. • Examine policy and procedures for evidence of review at least annually.
Application Security Metrics	AIS-03	Define and implement technical and operational metrics in alignment with business objectives, security requirements, and compliance obligations.	• Examine policy and procedures for definition of operational metrics, security, and compliance requirements.
Secure Application Design & Development	AIS-04	Define and implement a SDLC process for application design, development, deployment, and operation in accordance with security requirements defined by the organization.	• Examine policy and procedures for definition of SDLC (Software Development Lifecycle), security, and compliance requirements. • Examine the state of implementation of the SDLC process. • Verify that the SDLC implementation is in accordance with requirements.
Automate Application Security Testing	AIS-05	Implement a testing strategy, including criteria for acceptance of new information systems, upgrades and new versions, which provides application security assurance and maintains compliance.	• Determine security assurance and acceptance criteria for the new information system(s). • Determine if the software release process is automated where applicable.
Automate Secure Application Deployment	AIS-06	Establish and implement strategies and capabilities for secure, standardized, and compliant application deployment. Automate where possible.	• Determine if segregation of duties (role and responsibilities) is clearly defined among security and application teams. • Determine if Identification and integration process is defined and verified for application deployment processes. • Evaluate the extent of automation deployed, and criteria used.

Identity & Access Management – Controls Testing

Identity & Access Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines

Identity & Access Management Policy & Procedures	IAM-01	Establish, document, approve, communicate, implement, apply, evaluate and maintain policies and procedures for identity and access management.
		Review and update the policies and procedures at least annually.
			• Examine policy and/or procedures related to IAM to determine if policy and/or procedure content:
			  • addresses the provisioning, modification and deprovisioning of logical access.
			  • establishes password complexity and management requirements.
			  • addresses authorization concept following separation of duties and least privilege.
			  • addresses privileged access management and access reviews.
			  • includes roles and responsibilities for provisioning, modifying and deprovisioning of logical access.
			• Examine if policy and procedures are reviewed and updated at least annually.

Strong Password Policy & Procedures	IAM-02	Establish, document, approve, communicate, implement, apply, evaluate and maintain strong password policies and procedures. Review and update the policies and procedures at least annually.	• Examine policy and/or procedures related to passwords to determine if minimum password complexity requirements are defined. • Determine if the organization enforces minimum password complexity requirements as defined in policy. • Examine policy and procedures for evidence of review at least annually.
Segregation of Duties	IAM-04	Employ the separation of duties principle when implementing information system access.	• Determine if divisions of responsibility and separation of duties are defined and documented. • Determine if information system access authorizations are established to support separation of duties.

Identity & Access Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Least privilege Principle	IAM-05	Employ the least privilege principle when implementing information system access.	• Examine the policy to determine the least privilege required for each role or user. • Evaluate the effectiveness of the implementation and review of policy.
User Access Provisioning	IAM-06	Define and implement a user access provisioning process which authorizes, records, and communicates access changes to data and assets.	• Determine if personnel required to approve system access requests are identified and documented. • Evaluate if access requests are documented and approved by required personnel prior to access provisioning.
User Access De-provisioning	IAM-07	De-provision or respectively modify access of movers / leavers or system identity changes in a timely manner to effectively adopt and communicate identity and access management policies.	• Determine if a process is established for removing logical access when users leave the organization or when access is no longer appropriate. • Determine if a timeframe for access removal and access modification is defined. • Verify that a process is established for removing existing system access and assigning appropriate access or for modifying existing access after internal transfer or change of job functions. • Determine if established processes for access removal and modification, within the defined time frame, are followed in practice.
User Access Review	IAM-08	Review and revalidate user access for least privilege and separation of duties with a frequency that is commensurate with organizational risk tolerance.	• Determine if the required frequency for review of accounts is established. • Determine if accounts are reviewed for compliance, including the level of access and conflicting access, following the principle of least privilege and consideration of separation of duties. • Determine if accounts are reviewed at the organization-defined frequency.

Identity & Access Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Management of Privileged Access Roles	IAM-10	Define and implement an access process to ensure privileged access roles and rights are granted for a time limited period and implement procedures to prevent the culmination of segregated privileged access.	• Determine if an access process, that includes requirements for limiting the time of privileged access roles and rights, is defined. • Determine if procedures address the prevention of culmination of segregated privileged access.
Strong Authentication	IAM-14	Define measures for authenticating access to systems, application and data assets, including multifactor authentication for at least privileged user and sensitive data access. Adopt digital certificates or alternatives which achieve an equivalent level of security for system identities.	• Determine if processes, procedures and technical measures for authenticating access to systems, applications and sensitive data are defined and maintained. • Determine if processes, procedures and technical measures for authenticating access to systems, applications and sensitive data are implemented and consistently followed in practice.
Password Management	IAM-15	Define, implement and evaluate processes, procedures and technical measures for the secure management of passwords.	• Determine if processes, procedures and technical measures for the secure management of passwords are defined. • Determine if processes, procedures and technical measures for the secure management of passwords are implemented and consistently followed in practice.

Data Security & Privacy - Controls Testing

Data Security & Privacy – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Security & Privacy Policy & Procedures	DSP-01	Establish policies and procedures for the classification, protection and handling of data throughout its lifecycle, and according to all applicable laws and regulations, standards, and risk level. Review and update the policies and procedures at least annually.	• Examine the organization's policy and procedures related to data privacy. • Determine whether policy and procedure content is sufficient to direct the compliant and lawful management of personal data and to address non-compliance. • Confirm whether policy addresses the requirement that the organization's data is used only for authorized purposes and in compliance with legislation and regulation. • Examine if the policy and procedures are reviewed on an appropriate basis.
Secure Disposal	DSP-02	Apply industry accepted methods for the secure disposal of data from storage media such that data is not recoverable by any forensic means	• Examine the organization's procedures and technical requirements related to the secure disposal of data from storage media. • Select a sample of disposal requests and assess whether they have followed the process through to completion. Confirm that all evidence was formally documented and recorded.
Data Classification	DSP-04	Classify data according to its type and sensitivity level.	• Establish if the organization's data classification matrix is aligned with the organization's data classification requirements. • Select a sample of data to confirm that each item has been classified appropriately.

Data Security & Privacy – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Data Flow Documentation	DSP-05	Create data flow documentation to identify what data is processed, stored or transmitted where. Review data flow documentation at defined intervals, at least annually, and after any change.	• Establish whether the organization has documented the roles and responsibilities for this process. • Select a sample of documents to check that they have been completed to the correct specifications and reviewed. • Review if data flow documentation includes assessment for accuracy, completeness, timeliness, and sustainability of data (flow).
Data Protection by Design	DSP-07	Develop systems, products, and business practices based upon a principle of privacy by design and industry best practices. Ensure that systems' privacy settings are configured by default, according to all applicable laws and regulations.	• Examine whether policy, standards, and procedures create a framework which fosters a culture and expectation of "security through design." • Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out.
Data Privacy by Design	DSP-08	Classify data according to its type and sensitivity level.	• Examine whether policy, standards, and procedures create a framework which fosters a culture and expectation of "security through design." • Review the organization's data breaches log, the security incidents log, and project change failure records for examples where this requirement was not followed correctly. Further, confirm that action plans were identified and carried out.

Data Security & Privacy – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Sensitive Data Transfer	DSP-10	Define, implement and evaluate processes, procedures and technical measures that ensure any transfer of personal or sensitive data is protected from unauthorized access and only processed within scope as permitted by the respective laws and regulations.	• Examine the organization's procedures and technical requirements for the secure and lawful transfer of personal data and sensitive data. • Select a range of personal data transfers and a range of sensitive data transfers to confirm that each transfer adhered to the organization's policy, procedures, and controls. Confirm that all relevant evidence was formally documented.
Data Retention & Deletion	DSP-16	Data retention, archiving and deletion is managed in accordance with business requirements, applicable laws and regulations.	• Establish that the organization maintains a source(s) of record of data types, owners, and retention periods. Select a range of entries to establish that the information recorded is correct. • Establish how the organization determines that its retention records are accurate and complete. • Confirm that the data retention process meets the organization's requirements as detailed in policy and procedures.
Data Location	DSP-19	Define and implement, processes, procedures and technical measures to specify and document the physical locations of data, including any locations in which data is processed or backed up.	• Confirm that the organization’s policy and procedures include details of guidelines for the storage and processing of data within the designated countries/regions/zones. • Establish that the organization maintains a source(s) of record of its physical data storage locations and can trace data lineage. • Select a range of entries to establish that the information is recorded appropriately. • Confirm that the data storage records are accurate and complete as detailed in policy and procedures.

Logging & Monitoring – Controls Testing

Logging & Monitoring – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Logging and Monitoring Policy and Procedures	LOG-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for logging and monitoring. Review and update the policies and procedures at least annually.	• Examine policy and procedures for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's logging and monitoring requirements. • Examine policy and procedures for evidence of review at least annually.
Audit Logs Protection	LOG-02	Define, implement and evaluate processes, procedures and technical measures to ensure the security and retention of audit logs.	• Examine the organization's log retention requirements. • Evaluate the policy and technical measures with respect to effectiveness.
Logging Scope	LOG-07	Establish, document and implement which information meta/data system events should be logged. Review and update the scope at least annually or whenever there is a change in the threat environment.	• Examine policy for the identification of loggable events, applications, or systems. • Examine the outputs of such identification, with respect to review and approval. • Examine scope for evidence of review at least annually.
Transaction / Activity Logging	LOG-11	Log and monitor key lifecycle management events to enable auditing and reporting on usage of cryptographic keys.	• Examine policy for logging and monitoring usage of cryptographic key usage lifecycle events. • Examine the process to identify such events. • Evaluate the review of these logs.
Access Control Logs	LOG-12	Monitor and log physical access using an auditable access control system.	• Examine policy for logging and monitoring physical access. • Examine the process to identify such events. • Evaluate the review of these logs.

Change Management - Controls Testing

Change Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Change Management Policy & Procedures	CCC-01	Establish policies and procedures for managing the risks associated with applying changes to organization assets, including application, systems, infrastructure, configuration. Review and update the policies and procedures at least annually.	• Examine policy and procedures to determine if they cover necessary parts of change management, including scope, documentation, testing, approval, and emergency changes. • Examine a sample record of changes to information assets, including systems, networks, and network services to determine if compliance is met with the organization's change management policy and procedures. • Examine if the policy and procedures are reviewed and updated at least annually.
Quality Testing	CCC-02	Follow a defined quality change control, approval and testing process with established baselines, testing, and release standards.	• Examine relevant documentation, observe relevant processes, and/or interview the control owner(s), relevant stakeholders, for change management and determine if the policy control requirements provided in the policy have been implemented. • Examine measures that evaluate(s) the organization's compliance with the change and configuration management policy and determine if these measures are implemented according to policy control requirements.
Unauthorized Change Protection	CCC-04	Restrict the unauthorized addition, removal, update, and management of organization assets.	• Examine the policy relating to the authorization of changes in assets. • Examine the implementation of such policy, technical controls, and their effectiveness.

Change Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Change Management Baseline	CCC-06	Establish change management baselines for all relevant authorized changes on organization assets.	• Examine policy and/or standards related to change management to determine if changes are formally controlled, documented and enforced to minimize the corruption of information systems. • Determine if the introduction of new systems and major changes to existing systems are formally documented, specified, tested, quality controlled, and the implementation managed.
Exception Management	CCC-08	Implement a procedure for the management of exceptions, including emergencies, in the change and configuration process.	• Verify that the organization establishes and documents mandatory configuration settings for information technology products. • Confirm that the process identifies, documents, and approves exceptions from the mandatory established configuration settings for individual components based on explicit operational requirements. • Determine that the organization monitors and controls changes to the configuration settings in accordance with organizational policy and procedures.
Change Restoration	CCC-09	Define and implement a process to proactively roll back changes to a previous known good state in case of errors or security concerns.	• Examine relevant documentation, observe relevant processes, and/or interview the control owner(s) and/or relevant stakeholders, as needed to ensure that roll back procedures are defined and implemented in accordance to the policy. • Select a sample of changes and examine the change management record to confirm that the change was assessed and included appropriate fallback procedures in the event of a failed change.

Security Incident Management – Controls Testing

Security Incident Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Security Incident Management Policy	SEF-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for Security Incident Management, E-Discovery, and Cloud Forensics. Review and update the policies and procedures at least annually	• Examine policy for adequacy, approval, communication, and effectiveness as applicable to planning, delivery and support of the organization's Security Incident Management, E-Discovery and Cloud Forensics. • Examine policy and procedures for evidence of review at least annually.
Incident Response Plans	SEF-03	Establish, document, approve, communicate, apply, evaluate and maintain a security incident response plan, which includes but is not limited to: relevant internal departments, impacted CSCs, and other business critical relationships (such as supply-chain) that may be impacted.	• Examine the processes to identify impacted stakeholders. • Determine if this plan meets stakeholder requirements.
Incident Response Testing	SEF-04	Define and implement, processes, procedures and technical measures for security breach notifications. Report security breaches and assumed security breaches including any relevant supply chain breaches, as per applicable SLAs, laws and regulations.	• Verify if there is a calendar of exercises available, if exercises are performed at planned intervals and when there are significant changes within the organization or the context in which it operates. • Verify if the organization has reviewed and acted upon the results of its exercising and testing to implement changes and improvements.
Security Breach Notification	SEF-08	Employ the separation of duties principle when implementing information system access.	• Verify if there is a formal program that documents the breach notification requirements for all regulatory or contractual domains that the organization asserts adherence to. • Verify if there is a periodic awareness program to ensure all those associated with information security incident response are aware of the procedures involved for their roles, responsibilities and authorities.

Threat & Vulnerability Management – Controls Testing

Threat & Vulnerability Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Threat and Vulnerability Management Policy and Procedures	TVM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to identify, report and prioritize the remediation of vulnerabilities, to protect systems against vulnerability exploitation. Review and update the policies and procedures at least annually.	• Examine policy for adequacy, currency, communication, and effectiveness. • Examine policy and procedures for evidence of review at least annually.
Malware Protection Policy & Procedures	TVM-02	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures to protect against malware on managed assets. Review and update the policies and procedures at least annually.	• Examine policy for adequacy, currency, communication, and effectiveness. • Examine policy and procedures for evidence of review at least annually.
Vulnerability Remediation Schedule	TVM-03	Define, implement and evaluate processes, procedures and technical measures to enable both scheduled and emergency responses to vulnerability identifications, based on the identified risk.	• Examine policy for adequacy, currency, and effectiveness. • Determine if technical measures are evaluated for effectiveness.
Penetration Testing	TVM-06	Define, implement and evaluate processes, procedures and technical measures for the periodic performance of penetration testing by independent third parties.	• Determine if the process for defining frequency of penetration testing is defined. • Determine if the process for selection of independent third parties is defined and evaluated.
Vulnerability Prioritization	TVM-08	Use a risk-based model for effective prioritization of vulnerability remediation using an industry recognized framework.	• Examine how the output of risk assessment of the vulnerabilities is used to inform prioritization of remediation. • Determine if the process is evaluated for effectiveness.
Vulnerability Management Reporting	TVM-09	Define and implement a process for tracking and reporting vulnerability identification and remediation activities that includes stakeholder notification.	• Examine policy and procedures related to tracking and reporting of vulnerabilities. • Examine the process to identify stakeholders. • Determine if the process is implemented.

Endpoint Management – Controls Testing

Endpoint Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Endpoint Devices Policy and Procedures	UEM-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for all endpoints. Review and update the policies and procedures at least annually.	• Examine policy for adequacy, currency, communication, and effectiveness. • Examine policy and procedures for evidence of review, at least annually.
Application & Service Approval	UEM-02	Define, document, apply and evaluate a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data.	• Determine if a list of approved services, applications and sources of applications (stores) acceptable for use by endpoints when accessing or storing organization-managed data have been identified and documented. • Determine if the identified and documented list of approved services, applications and sources of applications have been enforced. • Examine how endpoints are monitored for unauthorized services and the process to remove or terminate use of non-sanctioned resources.
Endpoint Inventory	UEM-04	Maintain an inventory of all endpoints used to store and access company data.	• Examine the asset register, with reference to endpoints. • Determine if endpoints that store and access company data are tagged and included in the asset inventory.
Operating Systems	UEM-07	Manage changes to endpoint operating systems, patch levels, and/or applications through the company's change management processes.	• Examine the organization's change management policy for controls related to changes on endpoints. • Determine if such controls are in place for making changes to production and infrastructure systems and if the controls are evaluated as effective.

Endpoint Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Anti-Malware Detection and Prevention	UEM-09	Configure managed endpoints with anti-malware detection and prevention technology and services.	• Examine the organization's anti-malware policy. • Determine if such controls are in place and evaluated as effective.
Software Firewall	UEM-10	Configure managed endpoints with properly configured software firewalls.	• Examine the organization's software firewall and other endpoint network protection policy. • Examine the policy on configuration of such controls. • Determine if such controls are in place and evaluated as effective.
Data Loss Prevention	UEM-11	Configure managed endpoints with Data Loss Prevention (DLP) technologies and rules in accordance with a risk assessment.	• Examine the asset register, with reference to endpoints. • Determine if endpoints that store and access company data are tagged and included in the asset inventory.

Infrastructure & Virtualization Security – Controls Testing

Infrastructure & Virtualization Security – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Infrastructure and Virtualization Security Policy and Procedures	IVS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for infrastructure and virtualization security. Review and update the policies and procedures at least annually.	• Interview the team to determine if policy and procedures have been documented. • Evaluate the documented policy to determine if it has been approved and communicated to the relevant internal and external teams. • Determine if the policy has been applied to the infrastructure and virtualization security operations and if relevant procedures have been drafted. • Determine if the procedures are periodically evaluated and if they are maintained, up to date, and relevant.
Network Security	IVS-03	Harden host and guest OS, hypervisor or infrastructure control plane according to their respective best practices, and supported by technical controls, as part of a security baseline.	• Examine the policy for communication between environments. • Determine if the inventory of allowed communication has been reviewed, at least annually. • Evaluate the effectiveness of the monitoring and encryption of such communication.
Operating System Hardening & Base Controls	IVS-04	Employ the separation of duties principle when implementing information system access.	• Determine if the host and the guest OS has been hardened as per best practices. • Determine if the hypervisor or infrastructure control planes are hardened as per best practices. • Determine if appropriate technical controls exist that ensure that the hardening is done. • Determine if a security baseline has been set up. • Determine if the security baseline contains information about the hardening done.

Infrastructure & Virtualization Security – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Production and Non-Production Environments	IVS-05	Separate production and non-production environments.	• Verify if production and non-production environments are appropriately segregated. • Verify if the segregation is reviewed and managed during change management. • Verify the classification of data contained in each environment.
Network Architecture Documentation	IVS-08	Identify and document high-risk environments.	• Examine the criteria for identifying high-risk environments. • Examine the inventory of high-risk environments, and periodicity of review.

Business Continuity Management - Controls Testing

Business Continuity & Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Business Continuity Management Policy & Procedures	BCR-01	Establish business continuity management and operational resilience policies and procedures. Review and update the policies and procedures at least annually.	• Examine policy and procedures for adequacy and effectiveness as applicable to business continuity and resilience. • Examine policy and procedures for evidence of review at least annually.
Risk Assessment & Impact Analysis	BCR-02	Determine the impact of business disruptions and risks to establish criteria for developing business continuity and operational resilience strategies and capabilities.	• Examine the policy to determine business impact and the criteria for developing business continuity. • Evaluate the process to review and approve the policy.
Business Continuity Strategy	BCR-03	Establish strategies to reduce the impact of, withstand, and recover from business disruptions within risk appetite.	• Determine if the organization has established a risk appetite. • Determine if the organization has established strategies to reduce impact of business disruptions, within the organization's risk appetite.
Business Continuity Planning	BCR-04	Establish, document, approve, communicate, apply, evaluate and maintain a business continuity plan based on the results of the operational resilience strategies and capabilities.	• Evaluate if the organization's operational resilience strategies and capabilities are used as an input for the policy and implementation. • Examine policy and procedures for evidence of review.
Business Continuity Exercises	BCR-06	Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.	• Examine the plans for business continuity and operational resilience tests, with reference to their intended outputs. • Examine the schedules of such tests and their periodicity. • Evaluate if the plans are tested upon significant changes, or at least annually.

Business Continuity & Management – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Communication	BCR-07	Establish communication with stakeholders and participants during business continuity and resilience procedures.	• Determine if the organization has identified stakeholders and participants. • Examine the procedures for communication with identified stakeholders and participants.
Backup	BCR-08	Periodically backup data stored in the cloud. Ensure the confidentiality, integrity and availability of the backup, and verify data restoration from backup for resiliency.	• Examine the requirements for the security of such backups. • Evaluate the effectiveness of the backup and restore.
Disaster Response Plan	BCR-09	Establish, document, approve, communicate, apply, evaluate and maintain a disaster response plan to recover from natural and man-made disasters. Update the plan at least annually or upon significant changes.	• Examine the policy and procedures for adequacy, approval, communication, and effectiveness as applicable to a disaster response plan. • Examine the policy and procedures for evidence of review, upon significant changes, or at least annually.
Response Plan Exercise	BCR-10	Exercise the disaster response plan annually or upon significant changes, including if possible local emergency authorities.	• Examine the policy for planning and scheduling disaster response exercises, and involving local emergency authorities, if possible. • Evaluate if plans are tested upon significant changes, or at least annually.

Human Resources – Controls Testing

Human Resources – Controls Testing

Control Title	Control ID	Control Description	Audit Guidelines
Background Screening Policy & Procedure	HRS-01	Establish, document, approve, communicate, apply, evaluate and maintain policies and procedures for background verification of all new employees (including but not limited to remote employees, contractors, and third parties). Review and update the policies and procedures at least annually.	• Verify that the background verification required is mapped to the risks and data classification. • Examine the policy and procedures for evidence of review at least annually. • Examine Human Resources tickets upon hire which trigger background review and final confirmation from third party conducting background reviews showing it has been completed and how exceptions or failed checks have been addressed.
Acceptable Use of Technology Policy & Procedures	HRS-02	Establish policies and procedures for defining allowances and conditions for the acceptable use of organizationally-owned or managed assets. Review and update the policies and procedures at least annually.	• Verify that a definition of organizationally-owned or managed assets exists and is implemented. • Verify, via Interviews or otherwise, that the policy is communicated to users. • Examine policy and procedures for evidence of review at least annually.
Security Awareness Training	HRS-12	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	• Verify that a definition of sensitive organizational and personal data exists and is implemented. • Verify, by Interviews or otherwise, that the training program has been implemented. • Verify that the scope of the training program extends to all employees with access to such data.
Personal & Sensitive Data Awareness training	HRS-13	Provide all employees with access to sensitive organizational and personal data with appropriate security awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	• Verify that a definition of sensitive organizational and personal data exists and is implemented. • Verify, by Interviews or otherwise, that the training program has been implemented. • Verify that the scope of the training program extends to all employees with access to such data.

Cloud Service Providers Environment

Assessing CSP Environment

- Send Internal Audit team to test CSP environment.
- Request for CSP internal audit report

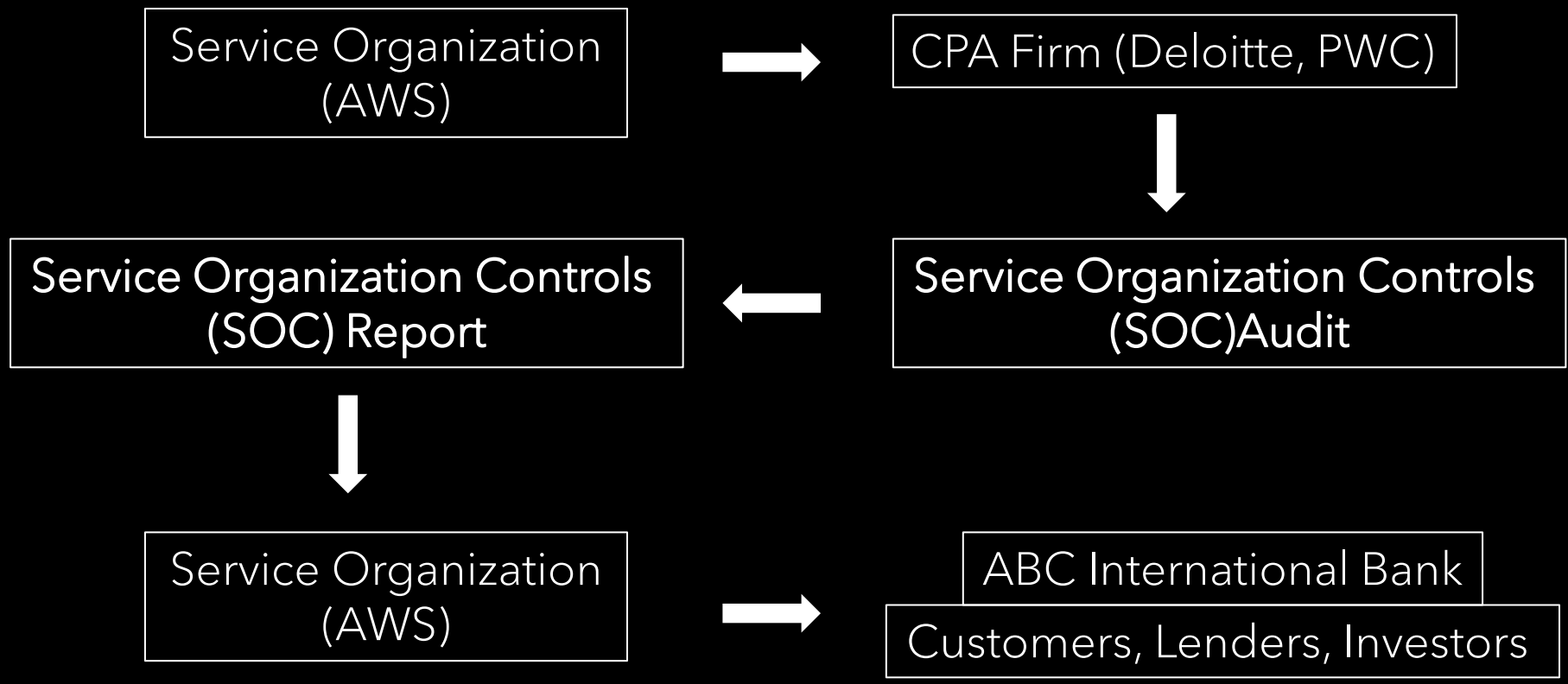
What reasonable assurance do we have to rely on the service providers ?

Request for a SOC Report (Service Organization Controls)

Service Organization Controls (SOC)

Service Organization Controls (SOC) Audit

Service Organization Controls (SOC) Audit



Categories of SOC Audit

- Test internal controls over financial reporting (ICFR)

Test internal controls relevant to:

- Security
- Availability
- Privacy
- Confidentiality
- Processing integrity

Contains sensitive information and not shared widely or shared under “Non-Disclosure Agreements” (NDA’s)

Test internal controls relevant to:

- Security
- Availability
- Privacy
- Confidentiality
- Processing integrity

Shared publicly

SOC Audit Types

Type I: Describes the controls the service providers have in place and report the auditor's opinion on the suitability of the controls. Testing is not done on the controls.

The auditor does not give an opinion on whether the controls are working effectively.

Type II: Test the design and operating effectiveness of controls over a period – Typically 12 consecutive calendar months. More rigorous and intensive than Type I as it covers a greater span of time and requires a more thorough investigation of system designs and processes.

Categories of SOC Audit

Category	Scope
SOC 1	Financial statement controls
SOC 2	Security, Availability, Privacy, Confidentiality, Integrity (**Private report**)
SOC 3	Security, Availability, Privacy, Confidentiality, Integrity (**Public report**)
Report Type	Tests
Type 1	Suitability of controls
Type 2	Suitability & effectiveness of controls

SOC Report

Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed

Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

Section 4: Testing

- Tests of Controls
- Test Results
- Control Environment & Objectives
- Complementary Controls

SOC Report

Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed

Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

Section 4: Testing

- Tests of Controls
- Test Results
- Control Environment & Objectives
- Complementary Controls

SOC Report

Complementary Controls

- End user controls
- 3rd party company (sub-service) controls

- Complementary User Entity Controls (CUEC) : End User Controls
- Complementary Controls at Subservice Organizations: 3rd party company

SOC Report

Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed

Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

Section 3: Description of Systems

- Detailed information on Systems & Infrastructures
- Risk Assessment
- Control Environment & Objectives
- Complementary Controls

Section 4: Testing

- Tests of Controls
- Test Results

SOC Report Testing

Section 1: Independent Auditor's Report

- Audit Scope
    - Period
- Auditors Opinion
    - Controls are presented fairly
    - Controls are designed appropriately
    - Controls are operating effectively

- Auditors Opinion / Passed or Failed
    - Unqualified Opinion: Achieves all requirement (Passed)
    - Qualified Opinion: Achieves most requirements (Passed)
    - Adverse Opinion: Material weakness (Failed)

SOC Report Testing

Section 1: Independent Auditor's Report

- Audit Scope
  - Period
- Passed or Failed / Auditors Opinion
  - Unqualified Opinion
  - Qualified Opinion
  - Adverse Opinion

Section 2: Management Assertion

- Facts & Assertions by Management
- Product & Services Offered
- IT Systems & Controls

Section 3: Description of Systems

- Complementary User Entity Controls (CUEC)

Section 4: Testing

- Test Results
  - Deficiencies identified

SOC Report Testing

Section 3: Description of Systems

- Complementary User Entity Controls (CUEC)
    - IT auditor identifies all Complementary User Entity Controls
    - Meets with system/application owner to test the CUECs

Section 4: Testing

- Test Results
    - Identify deficiencies in the SOC report
    - Assess impact of deficiencies
- Auditors Report
    - CUEC test results
    - Assessment of deficiencies
    - SOC Report auditor's opinion