Cloud Solution

for

KENTLOIS HOTEL AND SUITES

Olokeme Prosper Ombeh

Table of Contents

Page 4 - Cloud Principles and Design
- Business Description and Research
- Deployment Model
- Service Model
- Infrastructure Diagram

Page 7 - Cloud Networking & Storage
- Additional Business Research
- Procedures when ISP goes down
- Virtual Private Network
- Kinds of Files Stored
- How will Business Connect?
- Domain Name System
- Storage Providers
- Content Delivery Network

Page 10 - Assessing Cloud Needs
- Research
- Framework Diagram
- Baseline
- Feasibility
- Gap Analysis
- Gap Analysis Diagram

Page 14 - Engaging Cloud Vendors
- Capital and Operating Expenditures
- Potential Cloud Vendors
- Variable and Fixed Costs
- Licensing Model
- Evaluation of Cloud Vendors
- Service Level Agreement
- Migration Principles

Page 17 - Management and Technical Operations
- Aspects of Operating
- Development & Operations
- Financial Planning

Page 19 - Compliance and Security

Data Sovereignty
Regulatory Concerns
Industry-Based Requirements
International Standards
Certifications
Security Concerns, Measures, and Concepts

Page 22 - Governance and Risk

Risk Assessment
Risk Response
Documentation
Vendor Lock-In
Policies and Procedures

CLOUD PRINCIPLES AND DESIGN

Business Research

Business Name	Kentlois Hotel and Suites
Number of Employees	45 Employees
Location(s)	2 Locations
How long has the company been in business	Over 8 years
Purpose of the Business	Providing Hospitality services
Existing Technologies	• Wireless router connected to the internet • Security camera system connected to a flat screen • Laptop for basic internet access for administrative tasks
Other Notes	Technology Infrastructure is almost non-existent

Deployment Model

The best deployment model for this business is the Public Cloud because:

- The hotel does not have the IT infrastructure needed to run a private cloud
- This solution would require minimal maintenance, which is ideal for this business because it has no dedicated IT staff

Service Model

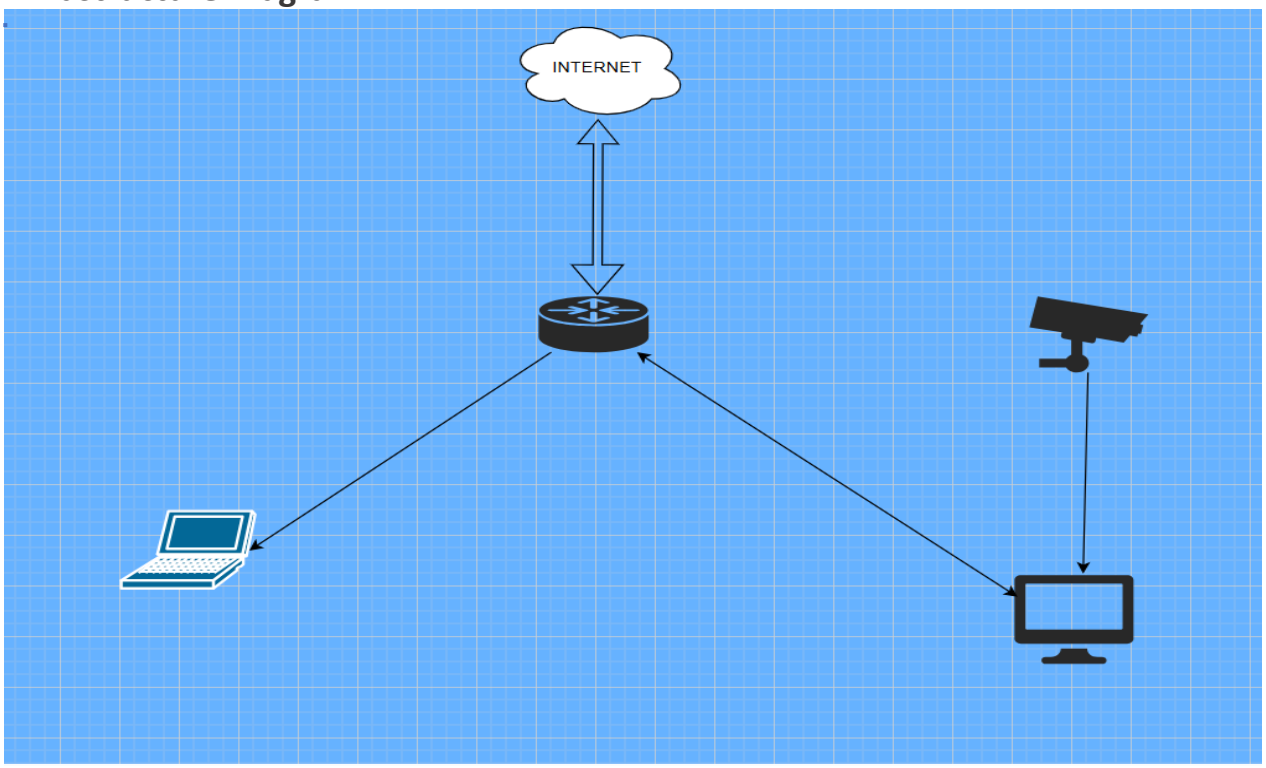
The best service model is Software as a Service (SaaS) because:

- The hotel can use cloud-based hotel management software to handle reservations, guest records, and billing
- SaaS solutions are easy to use, and they require no infrastructure management
- It allows guests to leave reviews and submit customer complaints online, helping the hotel improve customer satisfaction and service quality

Cloud Design for this Business

To ensure high availability and reliability, the hotel will implement a cloud-based reservation system, allowing guests to book rooms and leave reviews online. A cloud-based Point of Sale (POS) system for the bar and kitchen will also be integrated, improving efficiency and transaction tracking.
All guest records and business data will be backed up in a cloud storage location to prevent data loss. Secure access controls will be enforced, allowing only authorized staff to manage hotel operations.

Infrastructure Diagram



CLOUD NETWORKING AND STORAGE

Additional Business Research

Internet Service Provider Name	MTN
Data Connection Type	Satellite
Download and Upload speeds	39Mbps Download speed 46Mbps Upload speed
More than one ISP?	Airtel Networks Limited Satellite 30Mbps Download speed 37Mbps Upload speed

Procedures when ISP goes down

If the Hotel staff notices slow internet speeds or disconnection, they inform their supervisor. Then the supervisor logs into the router settings, changes the connection to the backup ISP, and restarts the network devices that need to be restarted.

Virtual Private Network

No VPN in place.

Kinds of Files Stored

The kinds of files that are currently stored on the Hotel's laptop are:

- Administrative and Financial records
- Security and Maintenance records
- Marketing materials like digital copies of Advertising banner.

How will the Business Connect?

Kentlois Hotel and Suites will use Cloud Networking Services to improve their operations and enhance customer service. The two primary ways the business will connect to cloud services are:

- Cloud-Based Hotel Management System Connection; The hotel will implement a cloud-based hotel management system like Little Hotelier to manage reservation, billing, and customer records. Hotel staff will connect to the system using laptops via a secure internet connection.
- Cloud Storage and Backup for Business Files; The hotel will use Microsoft OneDrive to store and back up critical business files including financial records and inventory logs. Employees will connect to the cloud storage service through the desktop application.

Domain Name System

Without DNS, hotel staff would have to remember numerical IP addresses instead of well-known domain names, this would make cloud communication difficult. DNS ensures that the hotel can efficiently connect to essential cloud networking services, improving operational efficiency.

Storage Providers

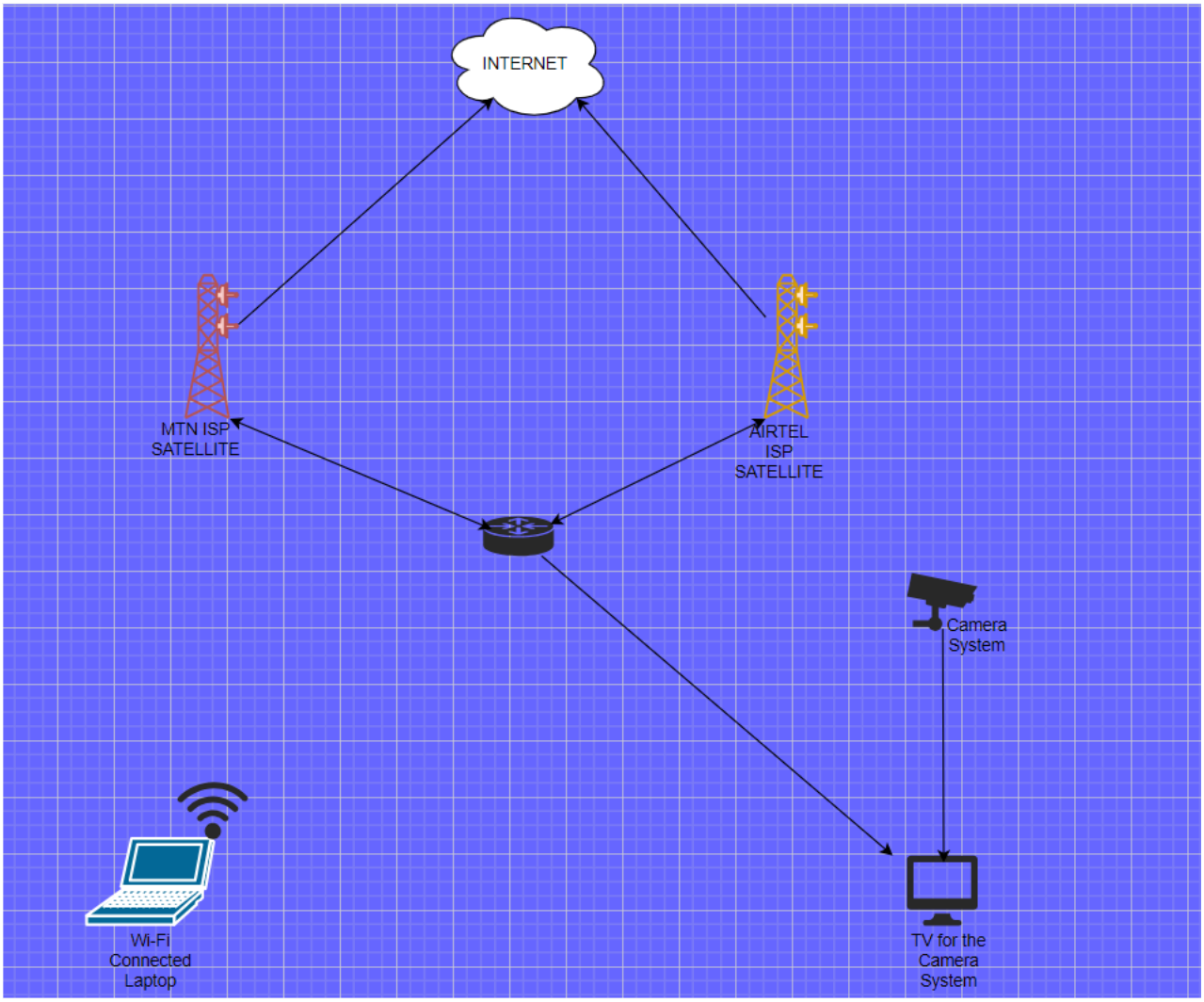
I would recommend Microsoft OneDrive. It works well with Microsoft Office Apps like Word and Excel, it provides file versioning and automatic backups to prevent data loss, and it is useful for storing invoices, hotel policies, and customer records securely.

Content Delivery Network

A Content Delivery Network (CDN) reduces delays for the business in the following ways:

- CDN stores frequently accessed content on multiple servers worldwide. So, when a staff member tries to access the site, the CDN routes the request to the nearest server, reducing load times.
- If one CDN server goes down, another takes over, ensuring uninterrupted access to cloud networking services.

Updated Infrastructure Diagram

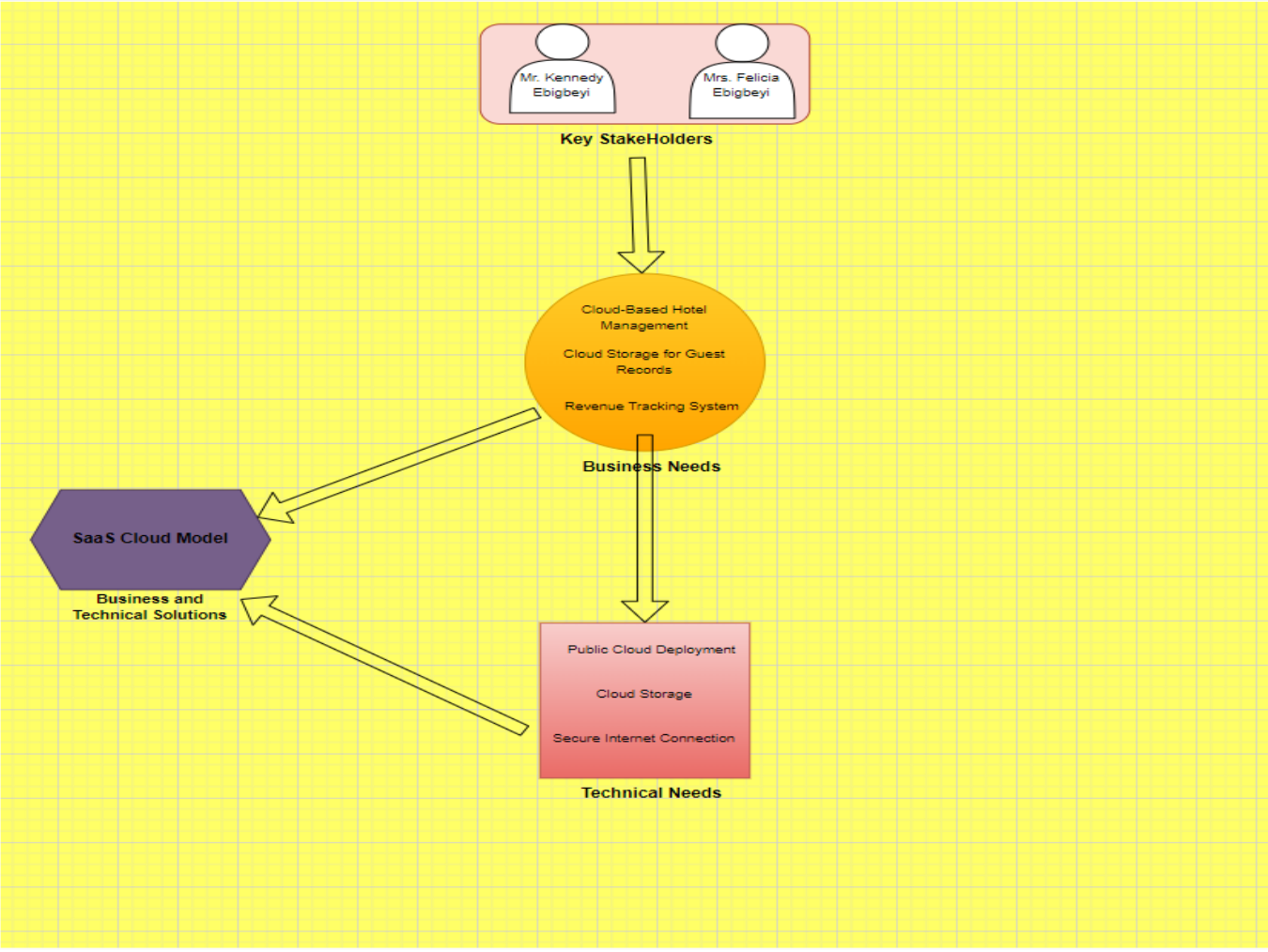

INTERNET
MTN ISP
SATELLITE
AIRTEL
ISP
SATELLITE
Camera
System
Wi-Fi
Connected
Laptop
TV for the
Camera
System

ASSESSING CLOUD NEEDS

Research

Key Stakeholders	Mr. Kennedy Ebigbeyi, CEO/MD Mrs. Felicia Ebigbeyi, CFO Mr. Segun Edema, Chief Security Officer
Single Point of Contact for each department	Mr. Jackson Ojuyenum, Front desk Supervisor **Ms. Miracle Amurun, Bar Supervisor** **Mrs. Felicia Ebigbeyi, Kitchen Operations Manager** **Mr. Segun Edema, Chief Security Officer**
SPOC for the organization	Mr. Kennedy Ebigbeyi, CEO

Framework Diagram



Baseline

The current IT environment is underperforming due to minimal technological adoption and reliance on manual processes. Some of the current challenges are:

- Slow reservation process – Bookings are recorded manually in physical books, leading to inefficiencies and errors.
- Limited data security – Guest records and financial documents are stored on a single laptop, increasing the risk of data loss due to hardware failure.
- Limited staff efficiency – Employees spend additional time managing records manually rather than focusing on customer service.

Since the hotel does not have formal IT infrastructure or performance tracking, system performance is evaluated based on observations and hospitality industry standards.

Feasibility

Future business needs require cloud adoption to improve efficiency, security, and scalability. Kentlois Hotel and Suites have basic internet connectivity and can migrate to the cloud with minimal investment. The existing capabilities include:

- Internet Connection**:** Two ISPs (MTN and Airtel) provide adequate connectivity for cloud-based services.
- Basic IT Infrastructure**:** The hotel currently has a laptop for administrative tasks, which can be used to access cloud-based hotel management and storage solutions.
- No Complex Legacy Systems**:** Since the hotel does not have on-premises servers or traditional software, migration will be straightforward and cost-effective.

Several hotel operations can be offloaded into the cloud to improve efficiency. Some of these capabilities include:

- Hotel Management System – Currently done manually using paper records. But it can be offloaded to the cloud by using a cloud-based hotel management system like Little Hotelier.
- Billing and Payments – Currently done manually using paper receipts. It can be offloaded to the cloud by using a cloud-based POS and billing system.
- Data Storage and Backup – Currently stored on a local laptop. It can be offloaded to the cloud by using Microsoft OneDrive.
- Employee Coordination – Employees' schedule is currently created manually. It can be offloaded to the cloud by using cloud-based scheduling apps.
- Guest Reviews and Complaints – These are currently being handled manually in person, this can be messy, as some customers tend to get loud and angry when dropping a complaint. This can be avoided by using online review and complaint features on Little Hotelier software.

Gap Analysis

Currently, the business relies on manual processes for booking, guest management, and billing, which leads to inefficiencies and a higher risk of errors. The lack of a standardized IT governance framework means there are no clear policies for data security, access control, or compliance, leaving the business vulnerable to data breaches and operational disruptions. Additionally, employees are not adequately trained to use cloud-based systems, which could hinder adoption and efficiency. The hotel's storage

system consists of locally stored files on a single device, posing a significant risk of data loss and limiting accessibility. Security measures are also insufficient, as there are no centralized access controls, firewalls, or backup mechanisms to protect sensitive customer and financial information. Furthermore, the hotel's IT operations are reactive rather than proactive, with no real-time system monitoring or automated issue resolution in place.

The table below identifies key gaps between the current state of this business and the desired future state.

Category	Current State	Goal	Action Needed	Priority	Owner	Due Date
Business	**Manual booking and guest management using physical records**	**Implement a cloud-based Hotel Management System for automated bookings**	**Adopt SaaS-based hotel management software**	**High**	**IT Manager**	**Q2 2025**
People	**Staff rely on manual processes for reservations, billing, and reporting**	**Train employees to use cloud-based systems**	**Provide staff training on using cloud tools**	**High**	**HR Department**	**Q3 2025**
Governance	**No formal IT governance or policies in place**	**Establish IT governance framework for cloud adoption**	**Define cloud policies, security measures, and compliance standards**	**Medium**	**IT Manager**	**Q4 2025**
Platform	**No cloud storage, files stored locally on a laptop**	**Secure cloud storage with automatic backups**	**Adopt Microsoft OneDrive for file storage**	**High**	**IT Manager**	**Q3 2025**
Security	**No centralized security management; high risk of data loss**	**Implement cloud-based security with role-based access and automatic backups**	**Set up data encryption, access control, and backup policies**	**High**	**Chief Security Officer**	**Q3 2025**

Operations	**No automated IT system monitoring**	**Implement cloud-based monitoring & automated alerts**	**Deploy cloud-based monitoring tools**	**Medium**	**IT Manager**	**Q4 2025**

ENGAGING CLOUD VENDORS

Capital and Operating Expenditures

Some Capital Expenditures relating to Kentlois Hotel and Suites are:

- Hotel Management Software Implementation – Investing in a cloud-based hotel management system will streamline key business operations, including booking, guest management, and financial reporting. Since this requires a significant upfront investment and provides long-term benefits, it qualifies as capital expenditure.
- Network and IT Infrastructure Upgrade – The purchase of networking equipment such as routers, switches, and security systems will enhance the hotel's IT capabilities. These assets are necessary for ensuring a stable and secure digital environment.

Operating Expenditures are:

- Cloud Service Subscription – The hotel will require ongoing cloud services for data storage, computing, and software applications. These recurring costs, such as monthly or annual cloud service fees, fall under operating expenditure.
- Internet and IT Maintenance Costs – Continuous internet access is essential for business operations, guest connectivity, and cloud-based services. Additionally, regular maintenance and software updates incur ongoing expenses, making them part of operational expenditures.

Potential Cloud Vendors

Some potential Cloud Vendors I would recommend are either **Amazon Web Services (AWS)** or **Microsoft Azure.**

Variable and Fixed Costs

Fixed Costs:

1. Cloud Service Subscription Fees – The hotel will incur a consistent annual fee for cloud-based storage, computing power, and hotel management software. Since this cost remains stable regardless of the number of guests or transactions, it is classified as a fixed cost.
2. Utilities – The cost of essential utilities such as electricity remains unchanged month to month, making it a fixed cost that must be covered regardless of occupancy levels.

Variable Costs:

1. Housekeeping and Laundry Supplies – The cost of cleaning products, linens, and guest amenities varies depending on the number of occupied rooms. Higher guest traffic increases these expenses, making them a variable cost.
2. Food and Beverage Inventory – The cost of purchasing ingredients, beverages, and other consumables for the hotel's bar and kitchen fluctuates based on guest demand. During peak seasons, more supplies are required, increasing expenses, while during low occupancy periods, costs decrease.

Licensing Model

To effectively manage cloud costs while ensuring scalability, the hotel should adopt a Pay-as-You-Go Licensing Model. Under this model:

- The hotel only pays for the cloud resources it consumes, avoiding unnecessary expenses.
- No upfront payments or long-term contracts are required, providing financial flexibility.
- Costs adjust dynamically based on usage, making it ideal for handling peak and off-peak seasons.

Evaluation of Cloud Vendors

To determine the best cloud vendor for Kentlois Hotel and Suites, a Proof of Concept (PoC) was conducted using official documentation, case studies, and feature comparisons from Amazon Web Services (AWS) and Microsoft Azure. The evaluation focused on key hotel business needs, including storage, security, system integration, and scalability.
A PoC was chosen as the evaluation method because it allows for a theoretical assessment of AWS and Azure without deploying resources. This approach involves analyzing vendor documentation, case studies, and customer success stories to determine how their cloud services perform in real-world hotel environments.

Evaluation Criteria	Amazon Web Services (AWS)	Microsoft Azure
Cloud Storage	AWS S3 offers secure, scalable storage with high availability	Azure Blob Storage provides integrated backup solutions for guest records
Hotel Management System (HMS) Integration	AWS supports SaaS-based HMS	Azure integrates seamlessly with Microsoft-based HMS platforms
Cost Efficiency	AWS pay-as-you-go pricing model allows flexibility	Azure's subscription-based model is predictable for budgeting
Performance & Scalability	AWS provides auto-scaling features for peak seasons	Azure offers hybrid cloud capabilities for gradual cloud migration

Based on the PoC evaluation, both AWS and Microsoft Azure offer great cloud solutions that align with the hotel’s operational needs.

- AWS is well suited for scalability and security, making it a strong choice for the hotel since it expects future growth.
- Azure integrates seamlessly with Microsoft-based applications, making it ideal for the hotel if it plans on using Microsoft Office and related software.

Service Level Agreement

AWS: AWS provides SLAs tailored to specific services. For instance, Amazon EC2 offers a Region-Level SLA with a Monthly Uptime Percentage commitment of at least 99.99% when instances are deployed across multiple Availability Zones. If they fail to meet the agreed upon uptime, customers can claim service credits. The amount of credit depends on the extent of the downtime.

Azure: Microsoft Azure also specifies SLAs for individual services. For example, Azure Storage guarantees a 99.9% uptime, ensuring data availability and redundancy. They offer service credits when uptime falls below the SLA's guaranteed level.

Migration Principles

To ensure a smooth transition from manual processes to cloud-based solutions, the hotel should follow these key migration principles:

1. Adopt a Phased Migration Approach
   - Start with non-critical workloads like cloud storage, before moving core systems like the Hotel Management System.
   - Gradually transition employees to cloud-based systems to minimize disruption.
2. Prioritize Security and Compliance
   - Implement Multi-Factor Authentication (MFA) and encryption for data protection.
   - Regularly audit cloud security policies and backup strategies.
3. Manage Costs and Optimize Cloud Resources
   - Monitor cloud usage and costs to avoid unnecessary expenses.
   - Regularly review cloud service plans and subscriptions to ensure they align with business needs.

By following these migration principles, Kentlois Hotel and Suites can transition smoothly to the cloud, improving efficiency, security, and scalability while minimizing risks and disruptions.

MANAGEMENT AND TECHNICAL OPERATIONS

Aspects of Operating

Data Management: Replication, Locality, and Backup	AWS provides Amazon S3 Cross-Region Replication (CRR) and Amazon RDS Multi-AZ deployments to ensure our business data is replicated across multiple locations for high availability. Locality options allow us to store sensitive customer and financial data in compliance with regional regulations. AWS Backup automates backups for critical hotel operations, ensuring seamless disaster recovery.
Availability: Zone & Geo-Redundancy	With AWS's Multi-AZ architecture, our hotel's reservation system and business applications can remain operational even if a data center goes down. Geo-redundancy with Amazon Route 53 and AWS Global Accelerator ensures fast access to services across multiple regions, reducing latency and downtime for our customers.
Disposable Resources	AWS's Elastic Compute Cloud (EC2) Spot Instances allow us to use temporary compute power for batch processing or analytics without long-term costs. We can scale down unused instances to optimize expenses without affecting performance.
Monitoring and Visibility: Alerts & Logging	With AWS CloudWatch, our business can monitor application performance, detect anomalies, and receive alerts for system failures. AWS CloudTrail ensures that all changes and activities within our infrastructure are logged for security and compliance purposes, allowing for proactive issue resolution.
Optimization: Auto-scaling & Right-Sizing	AWS Auto Scaling Groups help adjust the number of active servers based on demand, ensuring our hotel's online booking system remains responsive during peak seasons without overspending during low-traffic periods.

Development & Operations

Implementing DevOps practices in AWS will significantly enhance the efficiency, scalability, and reliability of our hotel business' digital services. By integrating software development (Dev) and IT operations (Ops) in the cloud, we can streamline service delivery, improve system reliability, and reduce downtime, ensuring a seamless experience for customers and employees.

1. Provisioning: Infrastructure as Code (IaC) and Templates

AWS provides tools like AWS CloudFormation and Terraform that enable our business to define and manage infrastructure using code. This allows us to:

- Ensure consistency by using pre-configured templates to set up identical environments across development, testing, and production stages.
- Reduce human errors by automating infrastructure provisioning, which minimizes misconfigurations that could cause system failures.

With Infrastructure as Code (IaC), we can quickly scale up our IT infrastructure during peak seasons and scale down when demand decreases, optimizing costs without affecting performance.

2. Quality Assurance (QA) Environments: Sandboxing, Load Testing, and Regression Testing

AWS provides sandbox environments and testing tools to ensure our applications run smoothly before deployment. These environments help us:

- Conduct load testing using AWS tools like AWS Load Testing Solution to simulate peak traffic conditions and ensure our online reservation system can handle increased user activity.
- Perform regression testing to ensure new updates do not break existing functionalities, preventing costly system failures.

By using AWS QA environments, our hotel's digital services can be thoroughly tested before launch, ensuring reliability and performance while minimizing risks of downtime or customer dissatisfaction.

Financial Planning

Moving our hotel business to AWS is exciting, but we also need to keep an eye on costs to make sure we're getting the best value. We don't want to overspend on resources we don't use, but we also need to ensure our systems run smoothly for guests making reservations, checking in, and enjoying their stay. Here's how we can plan financially for cloud resources while keeping things efficient and cost-effective.

1. Infrastructure: Compute, Storage, and Networking; AWS provides compute, storage, and networking services that are essential for running our hotel's booking system, customer database, and website.
   - Compute (EC2 instances): Our hotel's booking system and website need reliable servers to run 24/7. We'll budget for steady, always-on resources for critical operations and use flexible ones for less essential tasks.
   - Storage (S3): Guest records, reservation history, and security footage need a safe and scalable place to be stored. AWS S3 will store those files.
   - Networking (AWS VPC & CloudFront): We want guests to experience a fast, smooth online booking process, no matter where they are. Services like AWS VPC (for secure networking) and CloudFront (for speeding up website content) will help with that.

2. Instances: Reserved and Spot; AWS offers Reserved Instances and Spot Instances, which can help optimize costs for different workloads in our business.
   - Reserved Instances: Since our hotel booking system requires a consistent level of computing power, we can commit to 1-year or 3-year reserved EC2 instances at a lower price, reducing long-term costs.
   - Spot Instances: For things that don't need to run 24/7 like generating reports or testing new features, we can grab unused AWS resources at a discount using Spot Instances.

3. Licensing Type (Pay-as-You-Go) and Quantity; AWS follows a Pay-as-You-Go (PAYG) model, which aligns perfectly with our business needs. Instead of large upfront investments, we only pay for what we use.
   - Software Licensing: Some AWS tools, like databases and machine learning services, charge based on usage. Keeping track of these costs ensures we don't go over budget.

- Scaling Costs: Our business has peak seasons (holidays, conferences) when we need more computing power. Instead of paying for that capacity year-round, we can scale up only when needed, keeping our costs flexible.

With smart financial planning, we can get the best out of AWS without spending more than needed. By doing proper planning, we ensure that our hotel's tech is fast, reliable, and cost-efficient. This way, we focus on what matters most – delivering a great experience to our guests.

COMPLIANCE AND SECURITY

Data Sovereignty

Data sovereignty requires that our hotel's customer and booking data be stored and processed within our country's legal jurisdiction. Using AWS means ensuring compliance with local data protection laws, such as NDPR, to avoid legal risks.
We will select an AWS data center within our country or one that meets our legal requirements, implement encryption and security controls, and conduct regular compliance audits to maintain data integrity and customer trust.

Regulatory Concerns

Cloud Service Providers (CSPs) use **FedRAMP (Federal Risk and Authorization Management Program)** to ensure their cloud services meet strict security standards for U.S. government agencies. AWS follows **FedRAMP guidelines**, ensuring its cloud services meet high-security standards for government and private-sector use. This reassures us that our customer and business data will be handled with top-tier security.
FIPS require CSPs to use approved encryption methods to protect sensitive information, such as credit card transactions or personal customer data.

Industry-Based Requirements

As we transition our hotel's operations to AWS, understanding industry regulations helps us protect our business and customers.

- FERPA and HIPAA: Both laws protect sensitive information—FERPA safeguards student records, while HIPAA secures medical data. While our hotel may not directly deal with these, ensuring strong data privacy remains essential.
- FINRA: For financial institutions, FINRA enforces rules requiring businesses to retain financial transactions and communications. If our hotel expands to financial services, compliance with record retention becomes relevant.

- GLBA: The Gramm-Leach-Bliley Act (GLBA) ensures that businesses handling customer financial data protect it against unauthorized access. Since our hotel processes payments, AWS's encryption and access controls help us stay compliant.

By leveraging AWS's security features and compliance tools, we can ensure our cloud adoption meets industry standards while protecting our guests' and business data.

International Standards

International standards provide a framework for security, compliance, and efficiency in cloud computing. For Cloud Service Providers (CSPs) like AWS, adhering to standards such as ISO 27001 (information security management) and ISO 22301 (business continuity) ensures trust, reliability, and global acceptance of their services.
For our hotel, these standards mean that AWS provides secure, well-managed cloud environments that meet internationally recognized benchmarks. This helps us maintain data security, service availability, and compliance with global regulations, making it easier to expand operations or handle international guests' information securely.

Certifications

The CIA triad—Confidentiality, Integrity, and Availability—is the foundation of cloud security, ensuring our hotel's data is protected while remaining accessible when needed.

- Confidentiality ensures that only authorized personnel can access sensitive information, such as guest records and financial transactions. AWS provides encryption, access controls, and identity management to safeguard this data.
- Integrity guarantees that data remains accurate and unaltered, preventing unauthorized changes. AWS offers backup solutions and version control to maintain data integrity.
- Availability ensures that hotel services, such as online bookings and customer management systems, are always accessible. AWS achieves this through redundancy, failover mechanisms, and uptime guarantees.

By leveraging AWS, our hotel benefits from a secure and reliable cloud infrastructure that aligns with these principles.

Security Concerns, Measures, and Concepts

A threat is any potential danger that could compromise our hotel's data, operations, or security. For example, a phishing attack targeting our employees could lead to unauthorized access to customer reservations and financial records. We can identify such threats by monitoring unusual login attempts, educating staff on recognizing suspicious emails, and using AWS security services like AWS GuardDuty for real-time threat detection.
A vulnerability, on the other hand, is a weakness that could be exploited by a threat. For instance, if our hotel's booking system lacks multi-factor authentication (MFA), it becomes a vulnerability that

hackers could use to gain unauthorized access. The key difference is that threats are external dangers, while vulnerabilities are internal weaknesses that can be exploited. Addressing vulnerabilities, such as implementing strong authentication and regular security patches helps mitigate threats and protect our business.

To ensure our hotel's cloud infrastructure on AWS remains secure, we would use the following security assessment tools:

- AWS Security Hub – Provides a centralized view of our security status by aggregating alerts from multiple AWS services like GuardDuty, Inspector, and IAM Access Analyzer. This helps us continuously monitor compliance and detect vulnerabilities.
- Penetration Testing Tools (e.g., Metasploit, Burp Suite) – These allow us to simulate cyberattacks on our network to identify weaknesses before malicious actors exploit them.

By leveraging these tools, we can proactively protect customer data, ensure compliance with industry regulations, and maintain a secure and reliable cloud environment for our business.

Another interesting concept of cloud security is Access and Authorization. These two terms are usually used interchangeably, but they are different in meaning. Access refers to the ability to view or use a resource, such as logging into the hotel's reservation system. For example, employees may have access to guest check-in details. However, Authorization determines the level of access a user has. For instance, front desk staff may be authorized to view bookings, but only managers are authorized to modify room rates or issue refunds.

GOVERNANCE AND RISK

Risk Assessment

To protect our hotel's operations and customer data, it's important to identify our assets, evaluate the risks associated with them, and assign responsibility for managing those risks. Below are some basic assets of value to our business:

Asset	Type
Hotel Management System	Intangible
Guest Records	Intangible
Hotel Property	Tangible
Employee knowledge and skills	Intangible
Hotel Website and Online Booking portal	Intangible

Now we are going to identify some Qualitative risks that are associated with our business:

Risk	Risk Level	Risk Owner	Asset Owner
Damage to office devices	3 (Moderate)	Office Supervisor	Device User
HMS System downtime during peak seasons	4 (High)	Chief Operations Officer	HMS Provider
Website hacking	4 (High)	IT Admin	IT Admin

By identifying and categorizing assets, evaluating risks using a 1–5 scale, and assigning clear ownership, Kentlois Hotel and Suites can effectively manage threats and protect what matters most to the business.

Risk Response

Risk response refers to how our business identifies, addresses, and manages risks that could impact operations, data security, and guest satisfaction. It's about choosing the right strategy to protect our

people, systems, and reputation. There are four Risk Responses: Mitigation, Acceptance, Avoidance, and Transference.

Mitigation Strategies

Risk mitigation involves reducing the likelihood or impact of threats. In our hotel's case, we use several strategies to lower risks:

- Implementing multi-factor authentication (MFA) to reduce the risk of unauthorized access.
- Using AWS CloudWatch and GuardDuty to detect suspicious activities.
- Regular backups of customer data to ensure business continuity in the event of a system failure or ransomware attack.

There is another risk response called Risk Acceptance. Risk acceptance means recognizing a risk but choosing not to take immediate action because the potential impact is low, or the cost of mitigation is too high. For example, we may accept a slight delay in nightly batch reports, knowing it doesn't significantly affect guest services or business operations.

There is also another option called Risk Avoidance. Risk avoidance is the preferred strategy when the impact of a risk is too high. In our case, this means not hosting our own physical servers on premises. Instead of exposing ourselves to risks like power outages, equipment theft, or maintenance issues, we avoid those risks entirely by using cloud-based solutions like AWS, which offer secure, scalable infrastructure with built-in redundancy. This is the preferred response because the probability of a threat occurring is eliminated.

As for Risk Transference, using AWS cloud services is a prime example of risk transference. By outsourcing infrastructure, data storage, and system security to a trusted CSP, we shift the responsibility for physical security, server maintenance, and system uptime to AWS. While we still manage our data and configurations, AWS takes on the heavy lifting of ensuring the environment is safe, secure, and reliable, reducing the burden on our internal IT resources.

Documentation

Documentation is critical for maintaining structure, clarity, and consistency in cloud-based operations. It serves as a record of decisions, configurations, processes, and incidents, ensuring that everyone on the team can understand and manage our systems effectively.

Proper documentation allows us to uncover and track important findings, such as:

- Unsecured Admin Access – During a routine system audit, we might find that an admin account for our Hotel Management System has no multi-factor authentication (MFA) enabled. This is a critical security gap. By documenting this finding, we can record the issue, track how and when it was resolved, and use it as a learning point for future system setups.
- Inconsistent Backup Configuration – A scheduled check might reveal that automated backups for the customer database are not configured properly. For example, backups may be missing for a specific department. Documenting this finding allows us to take immediate corrective action and update our backup procedures to prevent future oversights.

In summary, documentation is not just a formality, it is a guide that keeps our IT environment secure, efficient, and well-managed, supporting our business and our guests with confidence.

Vendor Lock-In

Vendor lock-in occurs when a business becomes overly dependent on a single cloud provider, making it difficult or costly to switch to another provider later. For Kentlois Hotel and Suites, this becomes a risk if we heavily invest in AWS-specific tools, configurations, or services that don't easily transfer to another platform like Azure or Google Cloud.
If AWS were to significantly raise prices, change service terms, or experience long-term issues, moving to another provider could involve downtime, retraining staff, data migration challenges, or even redesigning parts of our system, all of which can be costly and disruptive to hotel operations.

It is advised that we practice Data Portability. Data Portability means we can export and move our data easily between different systems or cloud providers. This is important for flexibility and reduces reliance on one vendor. While Vendor lock-in happens when our systems are so tied to one provider's technology that moving our data or applications becomes difficult or expensive.

Policies and Procedures

Data privacy is the practice of protecting personal and sensitive information from unauthorized access, use, or disclosure. In our hotel, this means ensuring that guest names, contact details, payment information, and booking history are securely stored and only accessible to authorized staff. Failing to protect guest data can damage our reputation, lead to legal penalties, and erode customer trust.

Some examples of important policies and procedures that we must adhere to are:

- Data Access Policy – This policy outlines who in the hotel can access customer data and under what conditions. It ensures that sensitive information is only available to authorized personnel like managers or reception staff, reducing the risk of data leaks or misuse.
- Password and Authentication Policy – This policy enforces the use of strong passwords and MFA for accessing our hotel systems, especially the hotel management system. It helps protect against unauthorized access due to weak or stolen passwords.

Change and Resource Management
Change management ensures that any updates to hotel systems like booking software upgrades or new cloud services are planned, tested, and rolled out with minimal disruption. We must have someone with the role of Change Manager that will analyze every change that we are about to implement, and make sure that the value added will be greater than the potential risk.
Resource management helps us allocate cloud services efficiently, like computing power, storage, and bandwidth so we don't overspend or underutilize the services that keep our hotel running smoothly.

In the case of the occurrence of a security event, these are the steps that should be followed for an incident response:

- Detection and Identification – Detect and confirm the security incident.
- Response and Reporting – The appropriate response should be immediately carried out to eradicate that security incident, then evidence should be gathered as to why the incident occurred. Lastly, the evidence should be analyzed, and the appropriate data should be reported to management.
- Recovery and Remediation – This involves bringing the system to its normal operating state and documenting what happened, what worked, and what can be improved to prevent future incidents.

The three basic rights of an Access Control List (ACL) that advanced ACLs are built on are:

- Read – Permission to view files or data
- Write – Permission to edit files or data
- Execute – Permission to run or execute a file or program