# Business Continuity Plan for MAISON

Rohan Shah

9/18/2024

## *1. Introduction*

The Business Continuity Plan (BCP) for MAISON is designed to ensure the continuation of critical business functions during any major disruptions, including cybersecurity incidents, natural disasters, or technical failures. This plan outlines the necessary procedures to maintain the availability of key systems such as the customer booking platform, IoT devices, and cloud infrastructure, while protecting sensitive guest information.

## *2. Background*

MAISON is a digital-first hotel startup with a heavy reliance on cloud infrastructure and IoT devices. As a fully remote operation, MAISON's ability to maintain seamless digital services is crucial to its brand and operational success. This BCP ensures that in the event of disruptions, critical operations can continue, and systems are restored efficiently. The focus is on key systems such as cloud servers, CRM, IoT-based hotel access controls, and third-party API integrations (e.g., car rentals).

## *3. Scope*

This Business Continuity Plan applies to:

- All cloud-hosted systems that store customer data and power the booking system.
- IoT devices deployed across MAISON’s hotels for room access, heating/cooling, and security.
- Third-party service integrations, particularly for payment processing and car rental services.
- Internal communication and remote work capabilities of MAISON’s corporate employees.

The BCP addresses scenarios where there is a loss of access to one or more critical systems, a data breach, natural disasters affecting data centers, or internal network failures.

## *4. Assumptions*

The following assumptions are made for the BCP:

- All key data is regularly backed up to secure cloud storage.
- Cloud infrastructure is hosted across multiple geographically dispersed data centers to ensure redundancy.
- The Incident Response Plan is in place to handle cybersecurity incidents.
- Third-party vendors are responsible for their portion of the shared responsibility model.
- Remote employees have access to VPNs and secure communication channels.

### *5. Concept of Operations*

The concept of operations for the Business Continuity Plan revolves around the following principles:

- **Preparedness**: Regular testing and validation of the BCP through simulations and recovery exercises.
- **Response**: Immediate actions taken by the Incident Response Team (IRT) to contain and mitigate disruptions.
- **Recovery**: Steps to restore all systems to normal operation following an incident.
- **Communication**: Timely and clear communication to stakeholders, customers, and third-party vendors during disruptions.

### *6. System Description*

MAISON's core business operations rely on a cloud-based system architecture that supports:

- **Cloud Hosting**: AWS and Azure services for storing customer and booking data, providing redundancy and scalability.
- **CRM**: A custom-built system that handles all guest communications and integrates with the AI concierge for customer service.
- **IoT Devices**: Smart locks and thermostats in hotel rooms, controlled remotely through the cloud.
- **Third-Party Integrations**: APIs that handle payment processing and rental car bookings, critical to the customer experience.

### *7. Overview of Three Phases*

1. **Preparation**: Regular training, system backup schedules, BCP simulations, and security audits to ensure readiness.

2. **Response**: Immediate containment of incidents (e.g., isolating compromised systems or initiating failover to backup systems).
3. **Recovery**: Full restoration of systems and services, including data validation and functional testing.

### *8. Roles and Responsibilities*

- **Business Continuity Manager**: Oversees the activation of the BCP, coordinates the recovery efforts, and communicates with stakeholders.
- **IT and Security Team**: Responsible for identifying the cause of the outage, implementing recovery procedures, and restoring systems.
- **Operations Team**: Ensures that critical customer-facing services, like booking and guest check-in, continue functioning.
- **Communication Lead**: Manages external communication with customers, vendors, and regulatory bodies.

| Task/Activity | Business Continuity Manager | IT and Security Team | Operations Team | Communication Lead | Senior Management | Third-Party Vendors |
|---|---|---|---|---|---|---|
| **Plan Activation** | A | R | C | I | I | I |
| **Notify Stakeholders** | A | R | C | R | I | I |
| **Outage Assessment** | R | R | C | I | A | I |
| **System Isolation/Containment** | I | A | I | I | C | I |
| **Cloud System Recovery** | C | A | I | I | C | R |
| **IoT Device Recovery** | C | A | I | I | C | R |
| **Communication to Customers** | I | I | I | A | C | I |
| **Third-Party Integration Recovery** | I | C | I | I | C | A |
| **Sequence of Recovery Activities** | A | R | I | I | C | I |
| **Recovery Testing** | R | A | R | I | I | I |
| **Recovery Declaration** | A | C | I | I | C | I |
| **Post-Incident Review** | A | C | C | I | R | I |

| | | | | | | |
|---|---|---|---|---|---|---|
| **Documentation** | A | R | I | I | C | I |
| **Backup Management** | C | A | I | I | I | R |
| **Cleanup** | C | R | I | I | C | I |

## Legend:

- **R (Responsible)**: The person(s) who perform the work.
- **A (Accountable)**: The person who ensures the task is completed and has ultimate decision-making authority.
- **C (Consulted)**: The person(s) consulted before a decision or action is taken.
- **I (Informed)**: The person(s) who are kept informed of progress or completion of tasks.

### *9. Activation and Notification*

The BCP is activated when the following criteria are met:

- A significant disruption to business operations lasting longer than one hour.
- A major security breach that compromises critical data or systems.
- Natural disasters that affect cloud hosting locations or IoT device functionality at hotel locations.

### *10. Activation Criteria and Procedure*

**Activation Criteria**:

- Detection of a cyber incident affecting the cloud infrastructure (e.g., data breach or ransomware).
- Failure of critical IoT devices in hotels, impacting guest services.
- Extended downtime of third-party services affecting customer booking and check-ins.

**Procedure**:

4. Incident is reported through monitoring tools or staff alerts.
5. Business Continuity Manager assesses the situation and decides on BCP activation.
6. Notify the Incident Response Team (IRT) and relevant stakeholders.

### *11. Notification*

Once the BCP is activated, the following parties must be notified:

- Internal staff responsible for system operations and guest management.
- Third-party vendors involved in data storage, payment processing, and IoT device maintenance.
- Customers, if their bookings or data are directly impacted.

### *12. Outage Assessment*

**Outage Assessment** involves:

- Analyzing the scope of the disruption.
- Estimating the time required to restore services.
- Identifying critical systems that are offline and their impact on business functions.

The Incident Response Team will perform an initial analysis and determine the necessary recovery steps.

### *13. Recovery*

**Recovery Phases** are structured as follows:

7. **Immediate Response**: Isolate affected systems, notify key personnel, and begin containment.
8. **System Restoration**: Begin recovery of cloud-hosted services, CRM, and IoT infrastructure.
9. **Testing**: Validate that restored systems are functioning properly and securely.

### *14. Sequence of Recovery Activities*

Recovery will occur in the following order:

10. Restore access to the **cloud infrastructure** for booking services and guest data.
11. Re-establish connections with **IoT devices** to ensure hotel operations (e.g., room access).
12. Reactivate **third-party integrations** for payment processing and car rental services.
13. Conduct **testing and validation** of restored services before allowing guest access.

### *15. Recovery Procedures*

Specific recovery procedures include:

- **Cloud Infrastructure**: Utilize redundant cloud systems to restore booking data and guest information.
- **IoT Devices**: Reboot smart devices, apply firmware updates if needed, and validate connection to the central system.
- **Third-Party Integrations**: Ensure that APIs are restored and functioning, with real-time communication re-established.

### *16. Recovery Escalation Notices/Awareness*

If recovery efforts are delayed or more complex than expected, escalation notices will be sent to:

- **Senior Management**: To assess the business impact and decide on further resource allocation.
- **Third-Party Vendors**: To expedite resolution of external dependencies (e.g., API or cloud provider support).
- **Customers**: To keep them informed of extended downtime and expected recovery timelines.

### *17. Reconstitution*

Once the crisis has been managed and systems are stabilized, reconstitution involves:

- **Rebuilding the affected systems** (if necessary).
- **Reviewing the incident** to identify the root cause and prevent future occurrences.
- **Reporting** findings to senior management and regulatory bodies.

### *18. Concurrent Processing*

While recovery is underway, alternative systems or manual workarounds may be utilized to keep key services operational. This includes:

- **Manual Check-ins**: Allow guests to check in manually if the IoT system remains down.

- **Backup Systems**: Use backup servers or cloud environments to temporarily handle booking requests.

### *19. Validation Data Testing*

Once data is restored, it must be tested for integrity and consistency:

- **Cross-Verification**: Compare restored data against the last known good backup.
- **Sample Testing**: Validate a sample of restored customer data and booking records to ensure accuracy.

### *20. Validation Functionality Testing*

Before fully resuming operations, the following functionality must be tested:

- **Booking System**: Ensure that customers can book and check in without errors.
- **IoT Devices**: Test smart locks and other IoT devices to confirm they are functional.
- **Third-Party Integrations**: Verify that payment processing and car rental services are fully operational.

### *21. Recovery Declaration*

Once the systems have been fully restored and validated, the Business Continuity Manager will declare the recovery process complete, and normal business operations can resume.

### *22. Notification (Users)*

After recovery, users will be notified through:

- **Emails**: To inform customers that systems are back online.
- **App Notifications**: Updates sent to guests who may have experienced service interruptions.
- **Public Website**: Post updates regarding the system status and resolution.

### *23. Cleanup*

Cleanup involves:

- Removing any temporary workarounds or backup systems that were used.
- Ensuring all logs, forensic data, and incident details are securely stored for future analysis.
- Conducting a review of the incident to update the Business Continuity Plan based on lessons learned.

### *24. Offsite Data Storage*

Offsite data storage plays a critical role in recovery. MAISON ensures:

- **Cloud Backups**: Regular backups are stored in geographically diverse cloud locations to prevent data loss.
- **Access Control**: Only authorized personnel can access offsite backups during recovery operations.

### *25. Data Backup*

Data backup procedures include:

- **Daily Backups**: Automatic daily backups of all guest data, booking records, and critical system configurations.
- **Weekly Full Backups**: Full backups of the cloud infrastructure every week, stored securely in the cloud.

### *26. Event Documentation*

Every step of the recovery process must be documented, including:

- **Timeline of Events**: A chronological record of the incident, from detection to recovery.
- **Decisions Made**: Key decisions made during the recovery process and the rationale behind them.
- **Communications**: Copies of all notifications and communications sent to stakeholders.

### *27. Deactivation*

Once normal operations have resumed, the BCP will be deactivated:

- **Stand Down**: Notify all recovery teams that operations have been restored and the BCP is no longer active.
- **Post-Incident Review**: Schedule a review meeting to discuss the incident and assess the effectiveness of the recovery procedures.