

Week 6: Planning for Contingencies

Naman Vaidya (2540087)

Prem Joshi (2537632)

Manthan Siddhpura (2524128)

Dev Gajera (2538542)

Yaskumar Bhingradiya (2528447)

GovBook Services – Week 6: Planning for Contingencies

Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

1. Introduction

GovBook Services is a government agency that operates an online public booking system, allowing citizens to schedule appointments for essential government services, including passport applications, driving licence renewals, social services, and public health consultations. As a public-facing system, it must remain available, secure, and reliable at all times. Any disruption to the system could delay critical public services, expose sensitive citizen information, reduce public confidence, and negatively affect government operations.

To minimise these risks, GovBook Services requires a comprehensive **Business Continuity Plan (BCP)** and **Disaster Recovery Plan (DRP)**. The Business Continuity Plan focuses on maintaining essential services during disruptions, while the Disaster Recovery Plan provides procedures for restoring IT systems and data after a disaster. Together, these plans ensure that critical public services continue with minimal interruption.

2. Scenario Analysis

GovBook Services faces a variety of natural and man-made threats that could interrupt business operations. Natural disasters include flooding, fires, severe storms, earthquakes, and pandemics. Floods or fires could damage office buildings, data centres, or network infrastructure, while severe weather may cause prolonged power outages or communication failures. A pandemic could reduce staff availability, making it difficult to provide support services.

Man-made threats are equally significant. Cybersecurity incidents such as ransomware attacks, Distributed Denial-of-Service (DDoS) attacks, malware infections, and unauthorised access could disrupt online services or expose confidential citizen information. Insider threats, including accidental deletion of data or deliberate sabotage by employees, could also affect system integrity. Hardware failures, software bugs, utility outages, and failures of third-party providers such as cloud hosting, SMS gateways, or identity verification services may prevent citizens from accessing online booking services.

To prepare for these situations, GovBook Services must identify its most important business functions and assets. The critical business functions include appointment booking, appointment confirmation and notifications, identity verification, staff access to booking schedules, customer support, reporting, and audit logging. These services depend on several key assets, including the booking application, web portal, application servers, database servers, internet connectivity, identity and access management systems, backup infrastructure, audit logs, staff workstations, cloud services, and operational documentation. Protecting these assets is essential to ensure business continuity and successful recovery.

3. Business Continuity Plan (BCP)

The Business Continuity Plan ensures that essential government services continue during an emergency. A dedicated Business Continuity Team should be established with clearly defined responsibilities.

The Executive Sponsor provides leadership, approves funding, and authorises major decisions during emergencies. The Business Continuity Manager oversees the development, implementation, testing, and maintenance of the continuity plan. The IT Operations Lead ensures the availability of IT infrastructure and coordinates failover procedures, while the Disaster Recovery Lead manages the restoration of systems following an incident. The Information Security Officer monitors cybersecurity risks and coordinates incident response activities. The Service Delivery Manager ensures that priority public services continue operating, the Communications Officer manages communications with staff, citizens, and the media, the Human Resources representative coordinates staffing and employee welfare, the Legal and Compliance Officer ensures compliance with government regulations, and the Vendor Liaison coordinates with external service providers.

Business continuity strategies should be selected according to the importance of the services provided. A **hot site** is the preferred recovery option because it provides fully operational infrastructure with real-time or near real-time replicated data, allowing services to resume almost immediately after a disruption. This is particularly important for government services where citizens rely on continuous system availability. A **warm site** offers partially configured infrastructure and can restore services within several hours, making it a lower-cost alternative. A **cold site**, although inexpensive, requires significant setup time and is therefore unsuitable for essential public services.

Shared-use strategies may also be adopted to improve resilience. GovBook Services could establish a timeshare agreement with another government department to share disaster recovery facilities or use a managed service bureau to provide technical support, cloud hosting, and backup services during emergencies. Mutual aid agreements with other government agencies may provide temporary office space or staffing support. In addition, specialised options such as cloud-based disaster recovery, mobile offices, portable workstations, and emergency telecommunications services can further strengthen business continuity.

The Business Continuity Policy should clearly define its purpose, scope, required resources, organisational roles, and staff training requirements. The purpose of the policy is to ensure uninterrupted delivery of public booking services while protecting sensitive information and maintaining public trust. The policy applies to all employees, contractors, IT systems, communication processes, and third-party service providers supporting GovBook Services. Resources required include redundant hosting environments, backup and replication technologies, emergency communication tools, remote access facilities, recovery documentation, vendor support contracts, and trained personnel. All employees with continuity responsibilities should receive regular training on incident reporting, communication procedures, recovery activities, and cybersecurity awareness.

The Business Continuity Plan should be regularly maintained through scheduled testing, annual reviews, simulation exercises, and updates following organisational or technological changes. Lessons learned from real incidents and exercises should be incorporated into future versions of the plan to ensure its effectiveness.

4. Disaster Recovery Plan (DRP)

The Disaster Recovery Plan focuses on restoring IT systems, applications, and data following a disaster. Disasters are classified according to their origin and speed of occurrence. Natural disasters include floods, fires, storms, and pandemics, while man-made disasters include ransomware attacks, DDoS attacks, data breaches, insider sabotage, hardware failures, software failures, and utility outages.

Rapid-onset disasters, such as fires, ransomware attacks, power failures, and server crashes, require immediate response and activation of the disaster recovery process. Slow-onset disasters, including hardware degradation, storage failures, staffing shortages, and software instability, develop gradually and allow more time for planning corrective actions.

Recovery priorities should be based on business impact. The highest priority is restoring the online booking portal because it provides essential services to citizens. The booking database should be restored next to ensure appointment information remains accurate and complete. Identity and access management systems, network connectivity, notification services, reporting systems, and internal administrative tools should then be restored according to their importance to business operations.

The recovery process begins with incident detection through monitoring systems, security alerts, or staff reports. Once a serious incident is confirmed, the Disaster Recovery Team is activated, and the event is formally declared. The next stage involves containing the incident by isolating affected systems, disabling compromised accounts, blocking malicious traffic, and preserving evidence for investigation.

Following containment, the team performs a damage assessment to identify affected systems, evaluate the integrity of backups, and estimate operational impact. Critical systems are then restored by activating the hot site or failover environment, restoring the booking application and database, and re-establishing secure network connectivity. Data recovery involves restoring clean backups, validating appointment records, checking audit logs, and reconciling any missing or duplicated transactions.

Throughout the recovery process, effective communication is essential. Senior management, employees, service providers, and government departments should receive regular updates. Citizens should also be informed about service disruptions, expected recovery times, and appointment rescheduling through official government communication channels. Once systems have been fully restored and verified, operations can gradually return to the primary production environment, followed by a review of lessons learned to improve future recovery efforts.

The Disaster Recovery Policy applies to all information technology systems supporting GovBook Services. Staff responsible for recovery activities should receive regular training on

backup restoration, failover activation, secure evidence handling, and emergency communications. Recovery capabilities should be tested periodically using realistic disaster scenarios involving both cyber incidents and physical disasters.

5. Testing, Maintenance and Continuous Improvement

Regular testing ensures that both the Business Continuity Plan and Disaster Recovery Plan remain effective. GovBook Services should use several testing methods, including desk checks, structured walkthroughs, simulation exercises, and technical recovery tests.

Desk checks involve reviewing the continuity and recovery plans to verify procedures, responsibilities, and contact information. Structured walkthroughs allow stakeholders to discuss their actions during a simulated incident and identify weaknesses in the plans. Simulation exercises replicate realistic disaster scenarios, such as ransomware attacks or data centre failures, enabling staff to practise their response without affecting live services. Technical recovery tests validate backup restoration procedures, failover capabilities, and system recovery in a controlled environment.

Following each exercise or real incident, the organisation should document findings, identify areas for improvement, update procedures, retrain staff where necessary, and review vendor agreements and emergency contact lists. Continuous improvement ensures that GovBook Services remains prepared for emerging threats and can continue delivering essential public services with minimal disruption.