

Group - 5

Public Booking System (GovBook Services)

Group Members

Naman Vaidya (2540087)

Manthan Siddhpura (2524128)

Dharmik Dabgar (2536691)

Harsh Dhokiya (2545109)

Introduction

GovBook Services is a government agency that provides online appointment booking services for citizens. The system allows users to schedule appointments for:

- Passport applications
- Driving licence renewals
- Social service appointments
- Public health consultations

Since the system stores sensitive citizen information, strong security measures are required to protect confidentiality, integrity, and availability of data.

Data Classification Scheme

Data classification helps determine the level of protection required for different types of information.

Data Type	Classification	Reason
Public service information	Public	Available to everyone
Appointment schedules	Internal Use	Used by staff and citizens
Citizen names and contact details	Confidential	Personal information
Passport numbers	Highly Confidential	Government identity data
Health consultation records	Highly Confidential	Sensitive personal data
Employee credentials	Restricted	Critical system access information

Classification Levels

1. Public
2. Internal Use
3. Confidential
4. Highly Confidential
5. Restricted

Risk Assessment Methodology

Selected Methodology: NIST Risk Assessment Framework

The NIST framework is suitable because it:

- Is widely accepted internationally.
- Provides structured risk identification.
- Supports government organizations.
- Helps prioritize security controls.

Steps

1. Identify assets
2. Identify threats
3. Identify vulnerabilities
4. Determine likelihood
5. Determine impact
6. Calculate risk level
7. Recommend controls

Risk, Threat, and Vulnerability Assessment

Critical Assets

- Citizen database
- Booking application
- Web servers
- Authentication system
- Government network infrastructure

Threats

Threat	Description
Phishing	Stealing login credentials
Malware	Infecting systems
Ransomware	Encrypting data
DDoS Attack	Making services unavailable
Insider Threat	Unauthorized employee actions

Threat	Description
Data Breach	Exposure of citizen information

Vulnerabilities

Vulnerability	Impact
Weak passwords	Unauthorized access
Outdated software	Exploitable security flaws
Unencrypted database	Data theft
Poor access control	Privilege abuse
Lack of backups	Data loss

Risk Matrix

Risk	Likelihood	Impact	Risk Level
Data Breach	High	High	Critical
Malware Infection	Medium	High	High
DDoS Attack	Medium	High	High
Insider Threat	Medium	Medium	Medium
System Failure	Low	High	Medium

Highest Priority Risks

- Data Breach
- Malware Infection
- Ransomware Attack
- DDoS Attack

Gap Analysis Plan

Gap analysis identifies differences between current security and desired security.

Current State

- Basic authentication
- Limited security monitoring
- Manual patch management
- Limited encryption

Desired State

- Multi-factor authentication
- Continuous monitoring
- Automated patching
- Full data encryption
- Security awareness training

Gap Analysis Table

Area	Current State	Desired State	Gap
Authentication	Password only	MFA	High
Monitoring	Basic logs	SIEM monitoring	High
Encryption	Partial	Full encryption	Medium
Backup	Weekly	Daily automated	Medium
User Training	Limited	Quarterly training	High

Malware Attack and Exposure of Confidential Information

Possible Malware Attacks

Ransomware

Effects:

- Booking system unavailable
- Data encrypted
- Service disruption
- Financial losses

Spyware

Effects:

- Citizen information stolen
- Credential theft
- Privacy violations

Trojan Horse

Effects:

- Remote attacker access
- Data manipulation
- System compromise

Consequences of Data Exposure

- Identity theft
- Legal penalties
- Loss of public trust
- Financial losses
- Service disruption

Information Systems Security Countermeasures

Technical Controls

Multi-Factor Authentication (MFA)

Benefits:

- Stronger user authentication
- Reduced account compromise

Encryption

Benefits:

- Protects stored data
- Secures data transmission

Firewalls

Benefits:

- Blocks unauthorized traffic
- Reduces attack surface

Antivirus and Anti-Malware

Benefits:

- Detects malicious software
- Prevents infections

Intrusion Detection Systems (IDS)

Benefits:

- Monitors suspicious activity
- Provides alerts

Administrative Controls

- Security policies
- Employee training
- Incident response planning
- Access control procedures

Physical Controls

- CCTV monitoring
- Secure server rooms
- Access cards
- Visitor management

System Hardening

System hardening reduces vulnerabilities by minimizing attack opportunities.

Hardening Activities

Server Hardening

- Remove unused software
- Disable unnecessary services
- Apply security patches

Network Hardening

- Configure firewalls
- Segment networks
- Secure routers and switches

Application Hardening

- Secure coding practices
- Input validation
- Regular security testing

Database Hardening

- Encrypt sensitive data
- Restrict user privileges
- Monitor database activity

Benefits

- Reduced attack surface
- Better compliance
- Improved system stability
- Enhanced security posture

Security Activities and Business Success

Security contributes directly to organizational success.

Security Activity	Business Benefit
MFA	Reduced fraud
Encryption	Data protection
Backups	Business continuity
Monitoring	Faster incident detection
Security Training	Reduced human error
Patch Management	Fewer vulnerabilities

Overall Benefits

- Increased citizen trust
- Improved service availability
- Regulatory compliance
- Reduced financial losses
- Better operational efficiency

Recommendations

1. Implement Multi-Factor Authentication.
2. Encrypt all sensitive citizen data.
3. Conduct regular vulnerability assessments.
4. Deploy SIEM monitoring solutions.
5. Perform regular backups.
6. Train employees on cybersecurity awareness.
7. Develop an incident response plan.
8. Conduct annual penetration testing.

Conclusion

GovBook Services handles highly sensitive citizen information and therefore requires a comprehensive security strategy. By implementing a structured data classification scheme, conducting NIST-based risk assessments, addressing security gaps, hardening systems, and deploying appropriate security controls, the organization can significantly reduce risks and maintain secure, reliable public services while ensuring citizen trust and regulatory compliance.