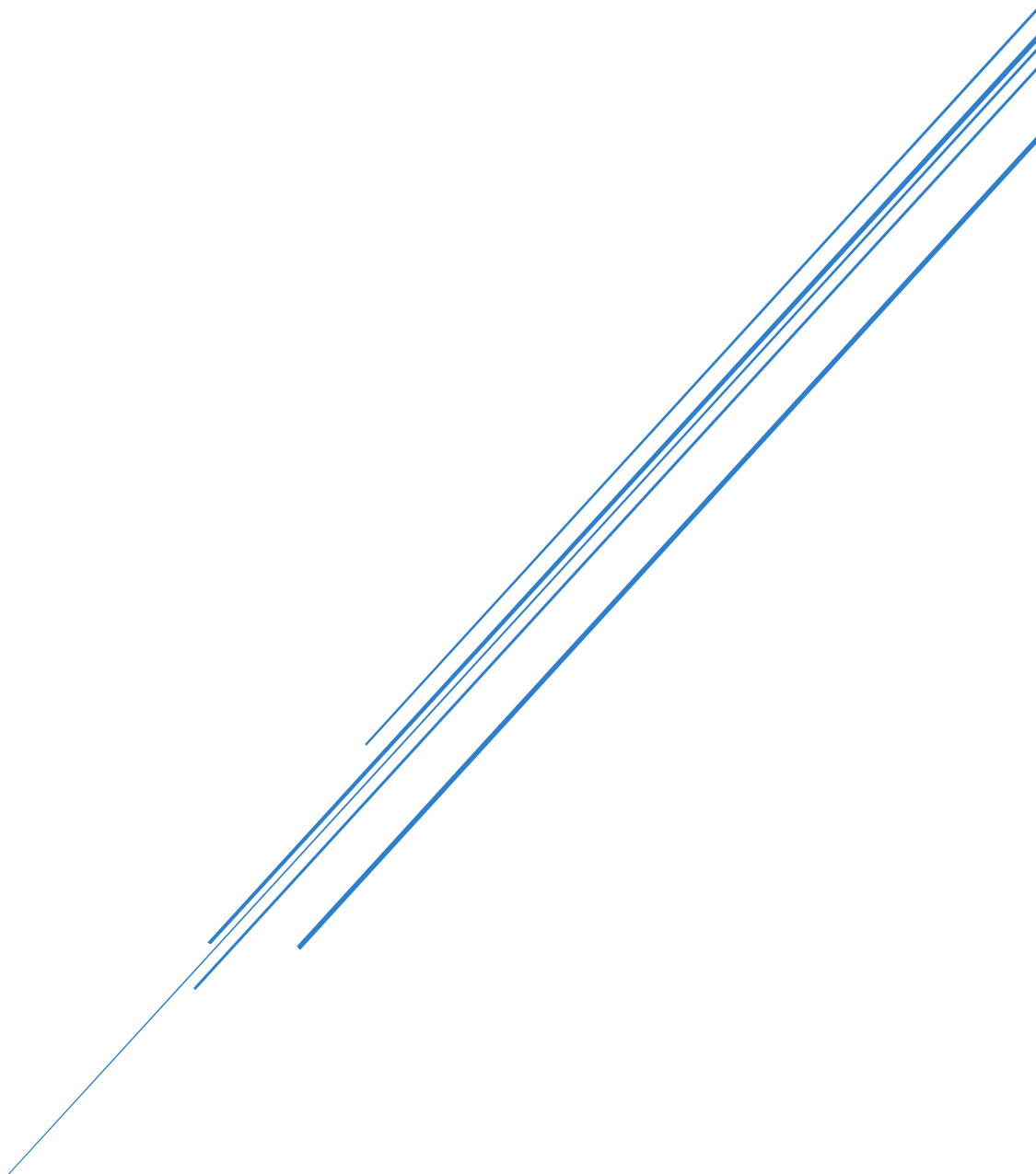


# CYBERSECURITY ARCHITECTURE REPORT

BLETCHLEY GRANGE HOTEL AND SPA

Author: Abhi Bhise | Security Architect



## Table of Contents

1. Executive Summary .....	2
2. Requirements .....	3
2.1 System Context Diagram .....	3
2.2 Data Classification .....	4
2.3 Information Asset Inventory .....	4
2.4 Functional Requirements .....	6
2.5 Non-Functional Requirements .....	7
2.6 Spa Employee Registration Process .....	8
3. Architecture .....	10
3.1 Component Architecture Diagram .....	10
3.2 Threat-Risk Register .....	12
3.3 Deployment Architecture Diagram .....	14
4. Operations .....	16
4.1 Threat Detection Use Cases .....	16
4.2 Incident Response Runbook .....	17
5. Governance .....	19
5.1 Viability Assessment (RAID Log) .....	19
5.2 Architecture Decision Record .....	23
6. Conclusion .....	25

## List of Figures

### Figure 1. Architecture Overview Diagram 2

Figure 2. System Context Diagram .....	3
Figure 3. Employee Registration Swimlane Diagram .....	8
Figure 4. Component Architecture with Security Overlay .....	11
Figure 5. Deployment Architecture with Data Flow .....	15

## List of Tables

Table 1: Data Classification Scheme .....	4
Table 2: Information Asset Register .....	5
Table 3: Process Steps and Controls .....	9
Table 4: Separation of Duties Matrix .....	9
Table 5: Comprehensive Threat-Risk Assessment .....	12
Table 6: Security Monitoring Use Cases .....	16
Table 7: Risks .....	19
Table 8: Assumptions .....	20
Table 9: Issues .....	21
Table 10: Dependencies .....	22
Table 11: Architecture Decision Record - Health Data Encryption Implementation .....	23

# 1. Executive Summary

Bletchley Grange represents a boutique hotel and spa venture requiring immediate cloud infrastructure deployment to support its operational launch within six weeks. The organisation currently operates without established security controls, creating significant exposure to cyber threats and regulatory non-compliance risks that could compromise customer data, damage its reputation, and result in substantial financial penalties.

The primary security challenge begins from a complex multi-vendor ecosystem spanning multiple jurisdictions. The Hotel Management System (HMS) operates as a European SaaS service managing customer bookings and financial transactions, whilst the Spa Management System (SMS) processes highly sensitive health data through custom applications with dependencies on Health4Life services located in India. This architectural complexity introduces multiple attack vectors, data handling concerns, and GDPR compliance challenges requiring immediate attention. The overall structure of this ecosystem is depicted in the high-level architecture overview below (Figure 1), which illustrates the interconnected nature of the business systems, external services, and security functions. This diagram provides a strategic view of the operational landscape, showing how customers, staff, and third parties interact with the core Bletchley Grange systems.

The recommended security solution implements defence-in-depth principles anchored by a Zero Trust architecture. This is achieved through the One.ID identity management service, comprehensive data protection controls, and continuous threat monitoring via the MaxwellDetect MSSP services. The approach prioritises the rapid deployment of essential controls and establishing scalable security foundations for future growth. Implementation focuses on protecting the most critical asset that is “customer health data” through application-level encryption, network segmentation, and enhanced access controls.

This security architecture enables Bletchley Grange to achieve operational readiness within the constrained timeline whilst maintaining regulatory compliance and protecting customer trust through robust cybersecurity controls.

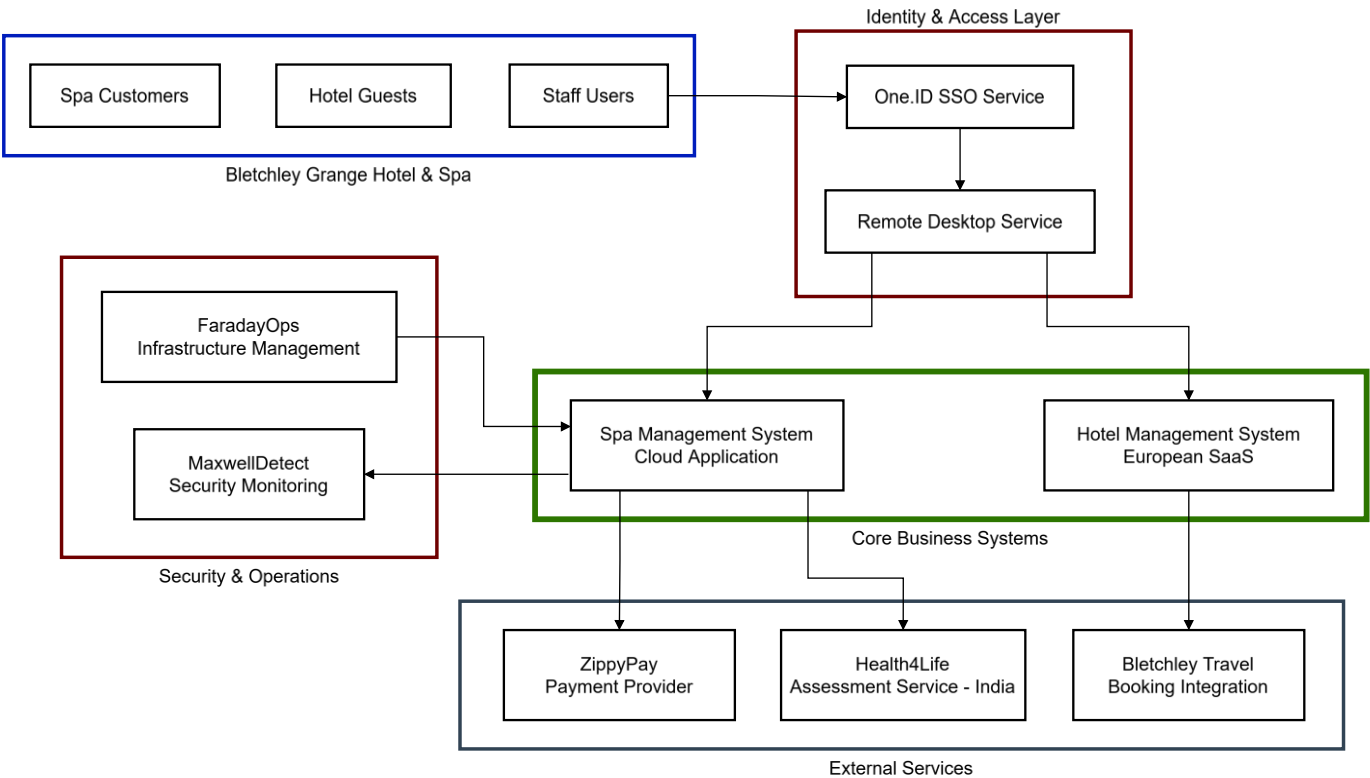


Figure 1. Architecture Overview Diagram

## 2. Requirements

### 2.1 System Context Diagram

To design an effective security architecture, we must first define what we are protecting. The system context diagram is a foundational document that establishes the scope of the Bletchley Grange system. It defines a clear boundary, separating the components we have direct control over from the external entities we interact with. This distinction is critical for understanding where our security responsibilities begin and end, and where we must rely on contractual agreements to enforce our security policies. For senior management, this diagram clarifies which parts of the business operation we own from a security perspective and which are managed by third-party partners.

Figure 2 illustrates this boundary. Components inside the line, such as the Spa Management System and its underlying database, are within our direct sphere of control. We are responsible for implementing and managing the security for these assets. Components outside the line, such as the HMS European SaaS, the ZippyPay payment provider, and the Health4Life assessment service, are external entities.

The diagram highlights several critical trust boundaries where sensitive data travels to external provider networks. The European location of the HMS provides inherent GDPR compliance advantages for booking data. However, the connection to the Health4Life service in India introduces complex data sovereignty challenges, as transferring UK citizens' health data outside the European Economic Area (EEA) requires stringent legal safeguards, such as Standard Contractual Clauses (SCCs), to be in place. Similarly, all financial data passed to ZippyPay must be protected according to the Payment Card Industry Data Security Standard (PCI DSS). Understanding these data flows and boundaries is the first step in defining our security requirements.

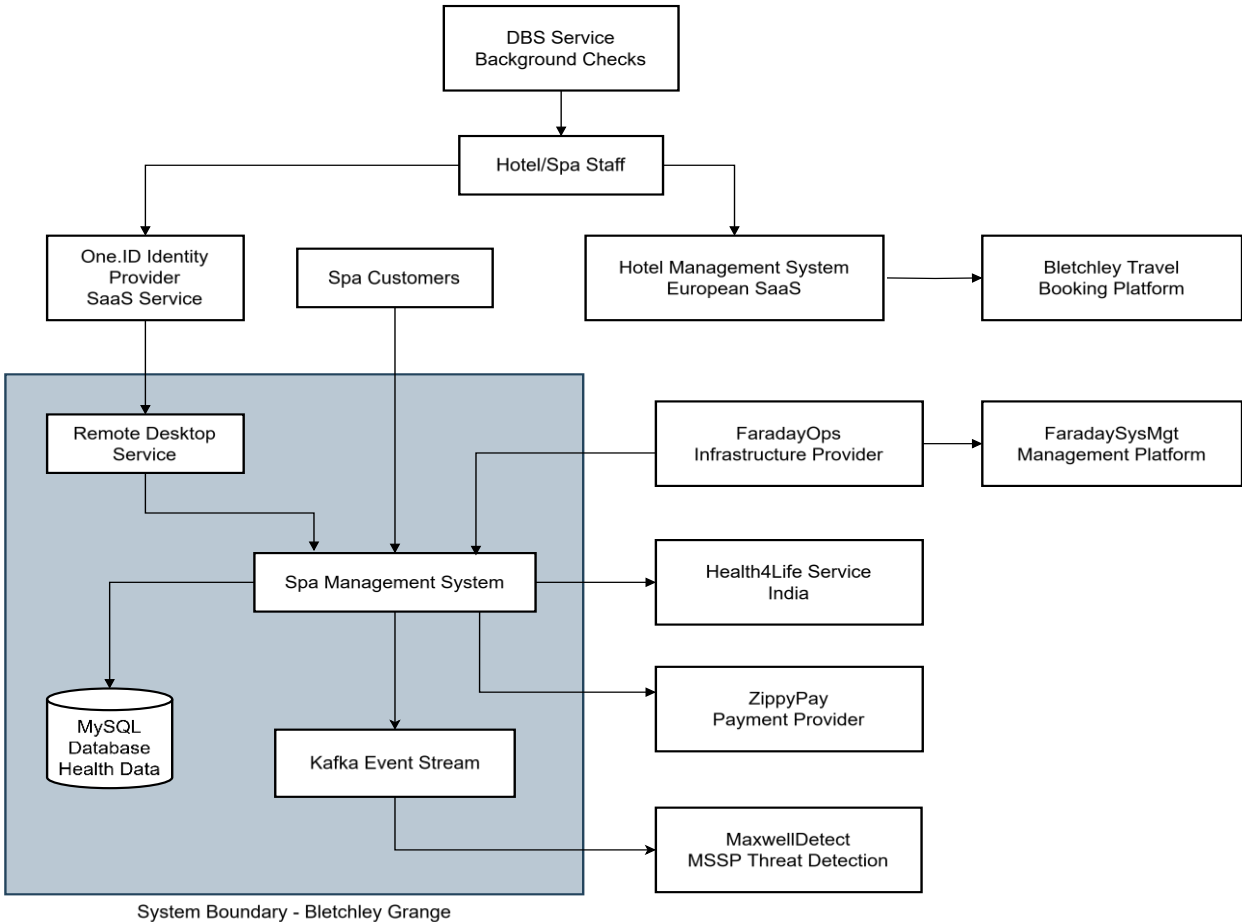


Figure 2. System Context Diagram

## 2.2 Data Classification

Data classification establishes protection requirements based on confidentiality impact and regulatory obligations. The classification scheme aligns with GDPR requirements and industry best practices for healthcare data protection. The purpose of this table is to create a common language across the business for understanding data sensitivity, ensuring that we apply the right level of protection to the right information, thereby optimising security spending and effort.

*Table 1: Data Classification Scheme*

Classification	Definition	Examples	Protection Requirements
<b>Highly Confidential</b>	Data requiring maximum legal protection under health/privacy laws	Health assessments, medical records, DBS check results	End-to-end encryption, restricted access, audit logging, data location controls
<b>Confidential</b>	Sensitive business data with high impact if compromised	Customer PII, booking details, payment data, staff records	Encryption in transit/rest, access controls, audit trails
<b>Internal</b>	Business operational data for internal use only	Staff schedules, system configurations, business procedures	Access controls, basic logging, network segmentation
<b>Public</b>	Information approved for public distribution	Marketing materials, facility information, published policies	Standard web security controls

Health data from Health4Life needs the highest protection under GDPR and health regulations. Payment data through ZippyPay must meet PCI DSS standards. Customer booking data requires GDPR-compliant handling.

## 2.3 Information Asset Inventory

The information asset inventory identifies the most critical data assets within Bletchley Grange, assigning ownership and estimating their value to the business. This register is essential for prioritising security investments. By understanding what our most valuable assets are and where they are located, we can focus our defensive efforts where they are most needed. The "Estimated Value" column is not a precise financial calculation but a risk-based estimate that considers potential regulatory fines, reputational damage, and operational disruption.

Table 2: Information Asset Register

Asset Name	Description	Data Classification	Storage Location	Primary Threats	Asset Owner	Estimated Value
<b>Customer Health Records</b>	Health assessments, treatment history, medical conditions	Highly Confidential	SMS MySQL Database (Cloud)	Data theft, unauthorised access, insider threats	Clinical Director	£500K+ (regulatory fines)
<b>Customer Booking Data</b>	Reservations, preferences, contact details, stay history	Confidential	HMS European SaaS	Data breach, system compromise, account takeover	Operations Manager	£100K+ (business impact)
<b>Payment Transaction Data</b>	Card details, billing information, payment history	Confidential	ZippyPay Integration	Financial fraud, data theft, PCI compliance breach	Finance Director	£250K+ (fraud/fines)
<b>Staff Authentication Data</b>	Login credentials, access permissions, MFA tokens	Confidential	One.ID Service	Account compromise, privilege escalation	IT Security Manager	£50K+ (system access)
<b>DBS Check Results</b>	Background verification records, criminal history checks	Highly Confidential	HR Systems (Internal)	Privacy breach, discrimination claims	HR Director	£200K+ (legal exposure)
<b>System Configuration Data</b>	Infrastructure settings, security configurations, API keys	Internal	FaradayOps Management Platform	System compromise, service disruption	Technical Director	£150K+ (operational impact)

The asset register clearly indicates that the customer health records stored in the SMS MySQL database are the organisation's crown jewels and, therefore, the highest value target for attackers. The distributed nature of the assets across multiple providers further complicates security management and underscores the need for a centralised approach to identity and monitoring.

## 2.4 Functional Requirements

The following security controls align with the NIST Cybersecurity Framework categories to address identified risks and compliance requirements for the Minimum Viable Product (MVP):

### IDENTIFY (ID) Controls:

- **REQ.2** Asset inventory management SHALL maintain current records of all hardware, software, data assets, and third-party services with quarterly validation cycles. [ID.AM-1]
- **REQ.3** A data governance framework SHALL classify all information assets according to sensitivity levels with mandatory labelling for Highly Confidential and Confidential data. [ID.GV-3]
- **REQ.4** Third-party risk assessments SHALL be conducted annually for all providers processing Confidential or Highly Confidential data, including on-site security reviews for critical suppliers. [ID.SC-2]
- **REQ.5** Cybersecurity roles and responsibilities SHALL be documented and assigned to specific personnel with annual review and update cycles. [ID.GV-1]

### PROTECT (PR) Controls:

- **REQ.6** Multi-factor authentication SHALL be mandatory for all accounts accessing Highly Confidential data, administrative functions, and remote access systems. [PR.AC-1]
- **REQ.7** Data encryption SHALL protect all Highly Confidential and Confidential data using AES-256 encryption both at rest and in transit, with separate key management for health data. [PR.DS-1]
- **REQ.8** Network segmentation SHALL isolate health data processing systems from general business networks using dedicated VPCs and firewall controls. [PR.AC-5]
- **REQ.9** Vulnerability management SHALL conduct weekly automated scans of internet-facing systems with critical vulnerability remediation within 72 hours. [PR.IP-12]
- **REQ.10** Access control policies SHALL implement least privilege principles with quarterly access reviews and immediate revocation upon role changes. [PR.AC-4]
- **REQ.11** Secure development practices SHALL include security code reviews, dependency scanning, and penetration testing for custom applications. [PR.IP-1]

### DETECT (DE) Controls:

- **REQ.12** Security event logging SHALL capture all authentication attempts, data access activities, and administrative actions with 12-month retention. [DE.AE-3]
- **REQ.13** Anomaly detection SHALL monitor for unusual data access patterns, privilege escalations, and bulk data extraction attempts with real-time alerting. [DE.AE-2]
- **REQ.14** Continuous monitoring SHALL provide 24/7 threat detection through MaxwellDetect MSSP with 15-minute alert response commitments. [DE.CM-1]
- **REQ.15** Security information correlation SHALL integrate logs from all system components to detect coordinated attack patterns. [DE.AE-1]

### RESPOND (RS) Controls:

- **REQ.16** Incident response procedures SHALL address health data breaches with notification capabilities meeting 72-hour GDPR requirements. [RS.RP-1]
- **REQ.17** Communication protocols SHALL enable rapid coordination between internal teams, third-party providers, and regulatory authorities during incidents. [RS.CO-2]
- **REQ.18** Incident containment capabilities SHALL enable immediate isolation of compromised systems whilst maintaining business continuity. [RS.MI-3]

### RECOVER (RC) Controls:

- **REQ.19** Backup and recovery procedures SHALL restore critical health data within 4-hour Recovery Time Objectives with daily backup validation. [RC.RP-1]
- **REQ.20** Business continuity planning SHALL maintain essential spa and hotel operations during

extended security incidents through alternative access methods. [RC.CO-3]

## 2.5 Non-Functional Requirements

### Performance Requirements:

- Authentication response times must not exceed 10 seconds for staff access during peak periods
- Health data encryption/decryption must not degrade application response times by more than 15%
- Security logging must consume less than 20% of total database storage capacity
- Threat detection processing must handle up to 15,000 security events per day without degradation

### Availability Requirements:

- Critical security services (authentication, logging, monitoring) must achieve 99.9% uptime during business hours
- MaxwellDetect monitoring must provide continuous coverage with maximum 10-minute detection delays
- Identity services must support up to 300 concurrent staff sessions during peak seasonal periods

### Scalability Requirements:

- Security controls must accommodate 100% growth in staff and customer data over 2 years
- Access control systems must handle seasonal workforce variations of  $\pm 50\%$
- Monitoring infrastructure must scale to process 50,000+ daily security events during peak operations

## 2.6 Spa Employee Registration Process

A secure and robust employee registration process is fundamental to protecting sensitive information. For Bletchley Grange, where staff will handle highly confidential health data, this process is not merely an administrative task but a critical security control. It ensures that only properly vetted and authorised individuals are granted access, and that their access rights are strictly limited to what is necessary for their role (the principle of least privilege). The swimlane diagram in Figure 3 visually maps out this process, showing the clear handoffs and responsibilities between different departments. This visual representation is invaluable for auditing purposes and for ensuring all stakeholders understand their role in the security chain.

The process begins with the HR Department, which is responsible for the initial application and, crucially, for initiating the background check with the external DBS Service. The "decision" diamond shows a critical control gate: if the DBS check is not clear, the process terminates. This prevents an unvetted individual from proceeding further. Once HR approves employment, the process moves to the Line Manager, who is responsible for assessing the need for health data access and providing the necessary training. Finally, the SMS Administrator performs the technical account creation within the One.ID service. This multi-stage process, involving three distinct roles, is a practical implementation of the Separation of Duties principle.

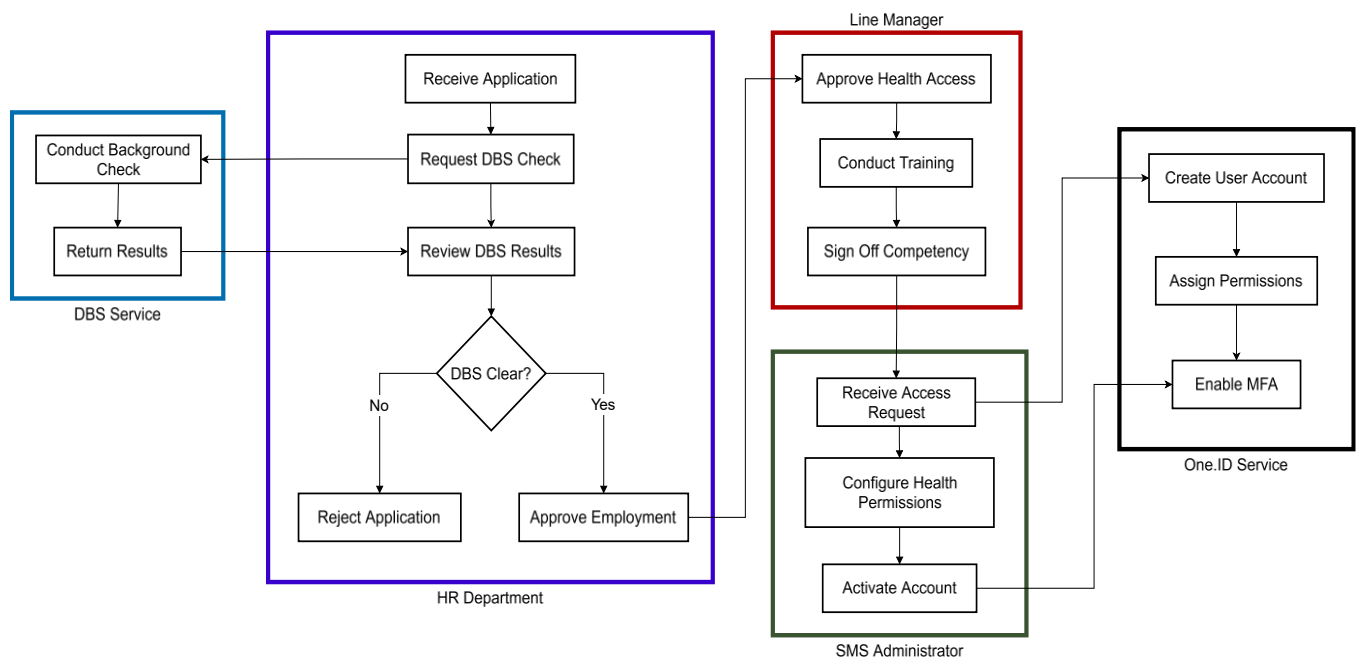


Figure 3. Employee Registration Swimlane Diagram

The tables below further detail the controls at each step and formalise the separation of duties, creating an auditable trail of accountability.

*Table 3: Process Steps and Controls*

Process Step	Responsible Party	Required Controls	Approval Authority
<b>Application Submission</b>	HR Department	Identity verification, reference validation, document authentication	HR Manager
<b>DBS Check Initiation</b>	HR Department	Secure transmission, tracking reference, confidential handling	HR Manager
<b>Background Verification</b>	DBS Service (External)	Secure processing, result confidentiality, audit trail	Automated System
<b>DBS Results Review</b>	HR Manager	Risk assessment, confidential storage, decision documentation	Senior Management
<b>Health Access Evaluation</b>	Line Manager	Role justification, competency assessment, training verification	Clinical Lead
<b>Technical Account Creation</b>	SMS Administrator	Least privilege assignment, audit logging, secure credential delivery	IT Security Manager

The Separation of Duties matrix in Table 4 explicitly prevents a single individual from controlling the entire access lifecycle. For example, the HR Department can approve employment, but only the Line Manager can approve access to health data, and only the SMS Administrator can technically provision that access. This ensures that multiple checks and balances are in place before an employee can touch the company's most sensitive asset.

*Table 4: Separation of Duties Matrix*

Function	HR Dept	Line Manager	SMS Admin	IT Security	Senior Mgmt	Clinical Lead
Employment Decision	✓				✓	
Health Access Approval		✓				✓
Technical Access Setup			✓	✓		
DBS Results Review	✓				✓	
Account Monitoring				✓		

## 3. Architecture

### 3.1 Component Architecture Diagram

The component architecture diagram translates our requirements into a logical solution design. It serves as the security blueprint for the Bletchley Grange system, moving beyond high-level business functions to show how specific application components and security controls work together. For a senior management audience, this diagram provides a clear visual answer to the question: "How are we actually protecting our assets?". It is layered to show the flow of user interaction down to the data storage, and importantly, it is overlaid with the key assets, actors, threats, and controls.

As shown in Figure 4, the architecture is divided into logical layers: User, Management, Application, and Data.

- **User Layer:** Contains the actors interacting with the system, including legitimate Staff Users and malicious actors like External Attackers.
- **Management Layer:** Houses the security operations functions provided by MaxwellDetect and the infrastructure management by FaradayOps.
- **Application Layer:** Contains the core business applications like the SMS and the Remote Desktop Service.
- **Data Layer:** The foundation where the most critical information assets, such as Health Records and Payment Data, are stored.

The diagram tells a story of defence-in-depth. For example, a threat from an External Attacker (top left) targeting the Customer Health Records (bottom left) must first bypass the Identity & Access controls (One.ID SSO and Multi-Factor Authentication). If they manage to compromise an account and access the SMS, their actions are then constrained by security controls at the application layer, such as Threat Detection and Security Logging, which feed alerts to the MaxwellDetect MSSP. Furthermore, Network Segmentation prevents lateral movement, and the final layer of defence, AES-256 Encryption, ensures that even if the attacker reaches the database, the data itself remains unreadable. The threats identified on this diagram, such as Data Theft and Supply Chain Attack, directly inform the risk assessment that follows in the next section.

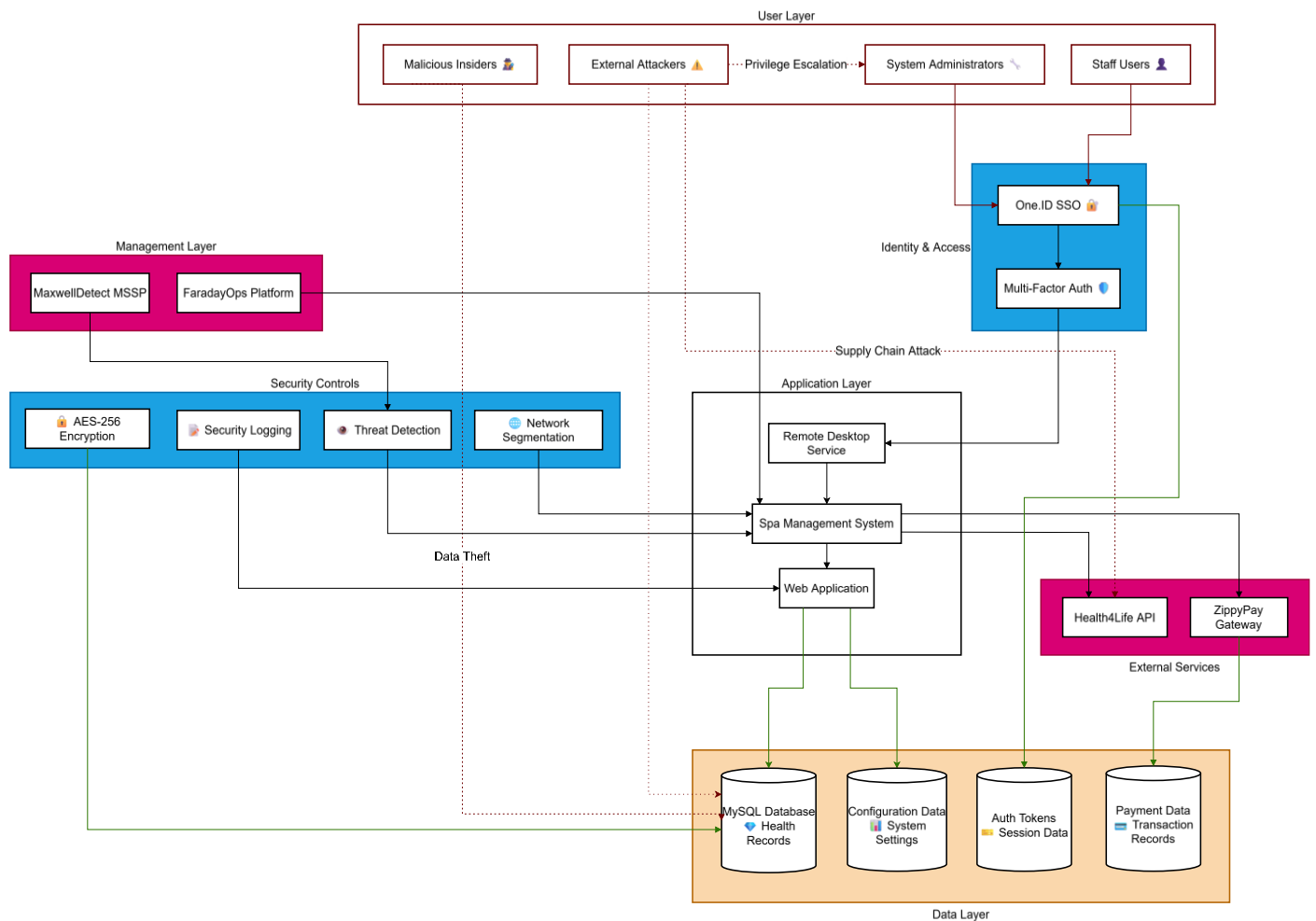


Figure 4. Component Architecture with Security Overlay

#### Security Overlay Elements:

- **Assets:** Customer Health Records (MySQL), Booking Data (HMS), Payment Data (ZippyPay), Authentication Tokens (One.ID)
- **Actors:** Staff Users, System Administrators, External Attackers, Malicious Insiders
- **Threats:** Data Exfiltration, Privilege Escalation, Supply Chain Attacks, Insider Data Theft
- **Controls:** Encryption, Access and Security Logging, Threat Detection, Network Segmentation, Multi-Factor Authentication

### 3.2 Threat-Risk Register

This register documents the most significant threats identified in the component architecture, evaluating their potential impact and likelihood to produce a risk score. This process, guided by the OWASP risk methodology, is crucial for prioritising our mitigation efforts. We focus on addressing the Critical and High-risk items first, ensuring that our resources are allocated effectively to counter the most potent dangers to the business.

Table 5: Comprehensive Threat-Risk Assessment

Threat ID	Threat Description	Threat Actor	Target Asset	Likelihood	Impact	Risk Score	OWASP Category	Mitigation Controls
<b>T001</b>	<b>Unauthorised Health Data Access -</b> External attacker exploits SMS application vulnerabilities to access customer health records through SQL injection or authentication bypass	External Cybercriminal	Customer Health Records	4 (Likely)	5 (Critical)	<b>20 (Critical)</b>	A03-Injection, A07-Auth Failures	REQ.7 (Encryption), REQ.8 (Segmentation), REQ.12 (Logging), REQ.9 (Vulnerability Mgmt)
<b>T002</b>	<b>Privileged Insider Data Theft -</b> FaradayOps administrator abuses legitimate access to extract customer data for financial gain or competitive intelligence	Malicious Insider	Customer Data, Health Records	3 (Possible)	4 (High)	<b>12 (High)</b>	A01-Access Control, A09-Logging Failures	REQ.6 (MFA), REQ.13 (Anomaly Detection), REQ.4 (Third-party Assessment), REQ.10 (Least Privilege)
<b>T003</b>	<b>Supply Chain Compromise -</b> Health4Life service compromised by nation-state actors seeking healthcare intelligence, leading to backdoor access to patient data	Nation-State APT	Health Records, Personal Data	2 (Unlikely)	5 (Critical)	<b>10 (Medium)</b>	A06-Vulnerable Components	REQ.4 (Supplier Assessment), REQ.8 (Network Segmentation), REQ.14 (Continuous Monitoring), REQ.11 (Secure Development)
<b>T004</b>	<b>Payment System Fraud -</b> Cybercriminals exploit ZippyPay integration weaknesses to conduct fraudulent transactions or steal payment card data	Financial Cybercriminal	Payment Transaction Data	4 (Likely)	3 (Moderate)	<b>12 (High)</b>	A04-Insecure Design, A02-Crypto Failures	REQ.7 (Encryption), REQ.13 (Anomaly Detection), Third-party PCI DSS compliance

*OWASP Risk Calculation Methodology:*

- **Likelihood Factors:** Attack frequency, skill level required, opportunity availability, threat actor motivation.
- **Impact Factors:** Financial loss, reputation damage, regulatory penalties, operational disruption.
- **Risk Matrix:** Critical (16-25), High (10-15), Medium (5-9), Low (1-4).

### 3.3 Deployment Architecture Diagram

The deployment architecture diagram shows how the logical components from the previous diagram are physically (or virtually) realised in the cloud environment. This diagram is essential for the technical teams responsible for building and maintaining the infrastructure, but it also provides assurance to senior management that the system is built on a secure and resilient foundation. It illustrates the practical implementation of key security principles like network segmentation.

Figure 5 shows the Bletchley Grange infrastructure segregated into multiple, isolated Virtual Private Clouds (VPCs). Think of a VPC as a private, sealed-off area within the public cloud. By separating services into different VPCs, we create strong boundaries that prevent a security breach in one area from easily spreading to another.

- **RDS Services VPC:** A dedicated zone for staff to access the systems, acting as a secure gateway.
- **SMS Production VPC:** The most secure zone, a digital vault containing the SMS application and the encrypted MySQL database with the customer health data.
- **HMS Production VPC:** A separate environment hosting the external European SaaS, ensuring hotel booking data is isolated from the SMS health data systems
- **Management VPC:** Used by our trusted partner, FaradayOps, for system administration. Access from this VPC to the SMS production environment is heavily restricted and monitored.
- **Security SIEM VPC:** Where all security logs are sent for analysis by MaxwellDetect. This is kept separate to ensure that even if the production systems are compromised, the security monitoring and alerting capabilities remain intact.

The diagram also highlights the **Architecturally Significant Data Flow** for a health assessment. This flow represents the highest-risk business process. The data originates from a staff member via the RDS VPC, is processed in the SMS Production VPC, and is then sent via a secure API to Health4Life in India. The results return along the same path and are stored in the encrypted database. Each step of this journey is protected by the segmented VPC architecture and other controls, demonstrating how our design directly mitigates the risks associated with this sensitive cross-border data transfer.

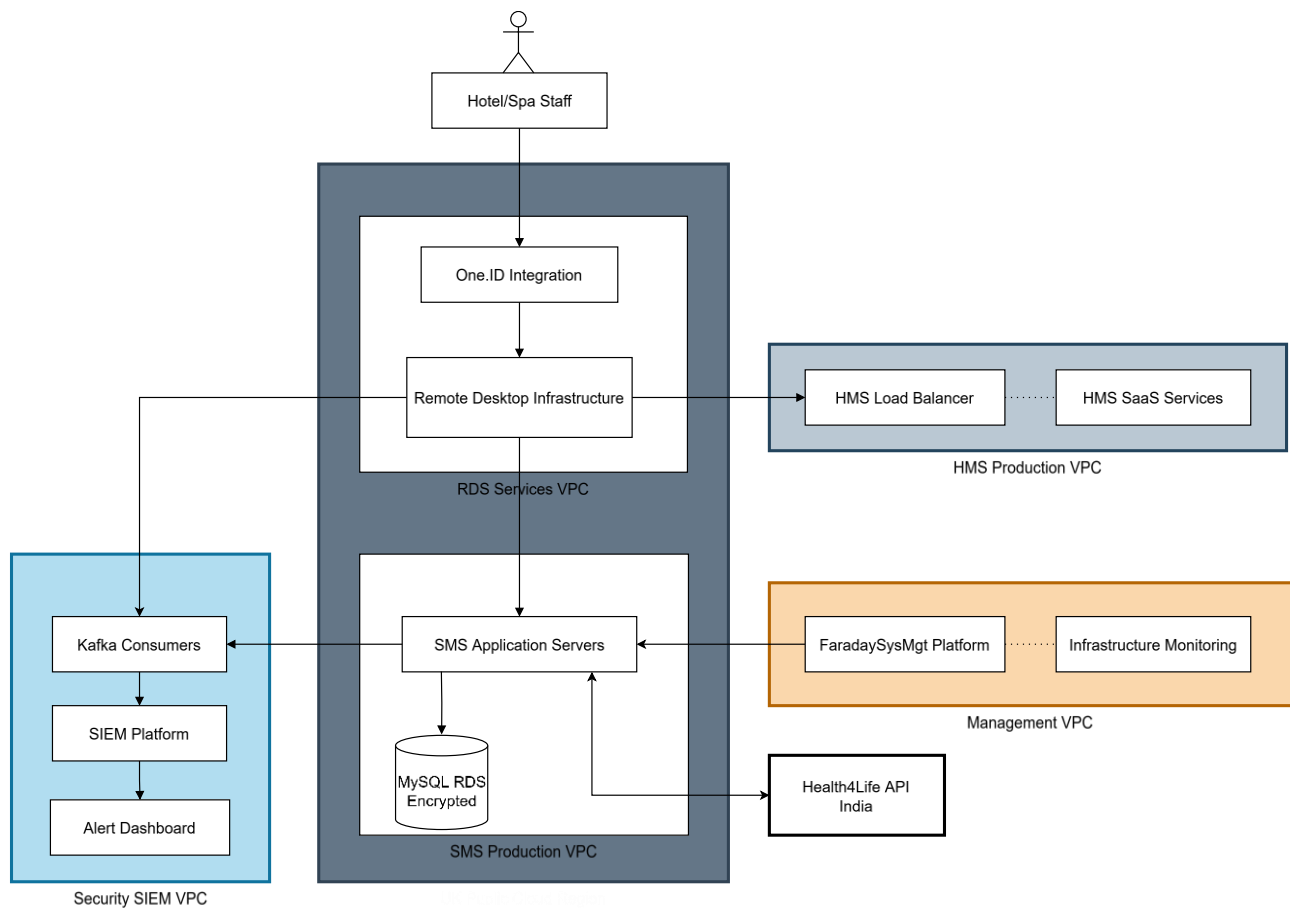


Figure 5. Deployment Architecture with Data Flow

#### Key Infrastructure Security Controls:

- VPC isolation between different service environments.
- Dedicated VPC for health data processing with restricted egress traffic.
- Network Access Control Lists (NACLs) limiting inter-VPC communication.
- Web Application Firewall (WAF) protecting internet-facing applications.
- VPN gateway for secure FaradayOps administrative access.

## 4. Operations

### 4.1 Threat Detection Use Cases

This table translates our security policies into specific, actionable detection rules for the MaxwellDetect monitoring team. Each use case defines what "bad" looks like for a particular threat scenario, allowing the security team to configure their tools to automatically flag suspicious activity. This moves us from a passive defence to a proactive monitoring posture.

Table 6: Security Monitoring Use Cases

Use Case ID	Detection Scenario	Data Sources	Detection Logic	Alert Conditions	Response Priority
UC001	<b>Health Data Unauthorised Access</b> - Detect abnormal access patterns to customer health records indicating potential data theft or insider threats	SMS application logs, MySQL query logs, One.ID authentication events, network flow data	Monitor health record queries for: volume anomalies (>baseline + 10%), temporal anomalies (access outside business hours), role violations (non-clinical staff accessing patient data), geographic anomalies (access from unusual locations)	<b>Critical Alert:</b> >50 health records accessed in 5 minutes, health data access 10pm-6am, admin accounts querying patient data, bulk extraction >200 records, access from non-approved countries	Immediate (0-15 min)
UC002	<b>Administrative Account Compromise</b> - Identify suspicious activities from privileged FaradayOps accounts indicating credential theft or insider threats	FaradaySysMgt platform logs, RDS session logs, system command histories, privilege escalation events	Analyse admin account activities for: authentication from new geographic locations, unusual command execution patterns, mass configuration changes, privilege escalation attempts, data export activities outside maintenance windows	<b>High Alert:</b> Admin login from new country, failed privilege escalation >5 attempts, configuration changes affecting >100 systems, data exports >1GB outside approved schedules	Urgent (15-30 min)
UC003	<b>Payment Transaction Anomalies</b> - Detect fraudulent payment processing patterns through ZippyPay integration indicating financial crime or system compromise	ZippyPay API transaction logs, SMS payment processing logs, customer booking correlation data, geographic transaction data	Examine payment patterns for: transaction amounts exceeding customer spending baselines, rapid successive transactions, blocked geographic regions, refund abuse patterns, velocity anomalies	<b>Medium Alert:</b> Single transaction >£1000 above customer average, >10 transactions in 10 minutes from same account, payments from high-risk countries, refund requests >£1500 within 48 hours	Standard (30-60 min)

## 4.2 Incident Response Runbook

When a security incident occurs, a calm, structured, and rapid response is essential to minimise the damage. This runbook provides a simple, non-technical checklist for the most critical incident scenario: a breach of customer health data. It ensures that everyone on the response team knows their role and the steps to take, from initial detection to regulatory notification, helping Bletchley Grange meet its 72-hour GDPR reporting deadline.

**Incident Type:** Unauthorised Health Data Access (UC001)

**Severity Classification:** Critical (involves protected health information)

**Regulatory Timeline:** 72 hours for GDPR breach notification

### Response Team Assembly:

- **Incident Commander:** IT Security Manager
- **Technical Lead:** SMS Application Owner
- **Legal Advisor:** Data Protection Officer
- **Communications Lead:** Marketing Director
- **External Support:** MaxwellDetect Senior Analyst

### Phase 1: Detection and Initial Response (0-15 minutes)

1. **Alert Reception:** MaxwellDetect monitoring system generates UC001 critical alert for suspicious health data access patterns
2. **Initial Triage:** On-call security analyst validates alert authenticity and escalates to IT Security Manager if confirmed as genuine security incident
3. **Team Activation:** IT Security Manager activates incident response team via automated notification system and establishes communication channel
4. **Evidence Preservation:** Immediately snapshot affected system logs and database states before any containment actions

### Phase 2: Investigation and Analysis (15-60 minutes)

1. **Scope Assessment:** IT Security Manager reviews affected health records, identifies potentially compromised accounts, and estimates data exposure volume
2. **Attack Vector Analysis:** Technical team examines system logs to determine attack methodology, entry points, and lateral movement indicators
3. **Impact Evaluation:** Legal advisor assesses regulatory notification requirements based on data sensitivity and exposure scope
4. **Timeline Construction:** Document precise chronology of suspicious activities and system access patterns

### Phase 3: Containment and Stabilisation (1-4 hours)

1. **Immediate Isolation:** Disable compromised user accounts in One.ID system and block suspicious IP addresses at perimeter firewalls
2. **System Quarantine:** If widespread compromise suspected, isolate affected SMS servers from network whilst maintaining emergency access procedures
3. **Credential Reset:** Force password resets for all potentially affected accounts and revoke existing authentication tokens

4. **Enhanced Monitoring:** Deploy additional logging and monitoring capabilities on affected systems to detect continued threat activity

**Phase 4: Eradication and Hardening (4-24 hours)**

1. **Vulnerability Remediation:** Apply security patches to affected applications and infrastructure components with FaradayOps coordination
2. **Access Control Strengthening:** Review and tighten access permissions for health data with mandatory re-authentication requirements
3. **Security Control Enhancement:** Update threat detection rules based on observed attack indicators and deploy additional protective measures
4. **System Integrity Verification:** Conduct comprehensive security assessment to ensure complete threat removal

**Phase 5: Recovery and Restoration (24-72 hours)**

1. **Gradual Service Restoration:** Incrementally restore SMS system access with enhanced monitoring and user behaviour analytics
2. **Security Testing:** Perform penetration testing and vulnerability assessments to validate security posture improvements
3. **Operational Validation:** Ensure all business functions operate normally with new security controls in place
4. **Continuous Monitoring:** Maintain elevated security alerting for 30 days post-incident to detect any residual threat activity

**Phase 6: Communication and Compliance (Ongoing)**

1. **Regulatory Notification:** Submit breach notification to Information Commissioner's Office within 72-hour legal requirement including detailed impact assessment
2. **Customer Communication:** Notify affected customers within regulatory timeframes with clear explanation of incident nature and protective actions taken
3. **Stakeholder Updates:** Provide regular updates to senior management, board members, and key business partners throughout response process
4. **Media Management:** Coordinate with communications team for potential media inquiries and public statement preparation

**Documentation and Evidence Management:**

- Maintain detailed incident timeline with timestamps for all response actions
- Preserve forensic evidence following chain of custody procedures for potential legal proceedings
- Document all business impact assessments and financial cost calculations
- Record lessons learned and security control improvements for future incident prevention

**Post-Incident Activities:**

- Conduct formal incident review within 7 days with all response team members
- Update incident response procedures based on lessons learned
- Enhance security awareness training focusing on identified vulnerability areas
- Review and update cyber insurance coverage based on incident costs and impacts

## 5. Governance

### 5.1 Viability Assessment (RAID Log)

The RAID log is a project management tool used to track Risks, Assumptions, Issues, and Dependencies. It provides a transparent overview of the key challenges facing the project, ensuring they are owned and actively managed.

**Risks:**

Table 7: Risks

ID	Risk Description	Impact Level	Probability	Mitigation Strategy	Risk Owner	Target Resolution	Status
R001	<b>GDPR Compliance Failure</b> - Health4Life data processing in India may violate GDPR data transfer requirements, potentially resulting in regulatory fines up to 4% of annual turnover (estimated £2M+ exposure)	High	Medium	Implement Standard Contractual Clauses (SCCs) with Health4Life; deploy additional encryption controls; establish data processing audit rights; consider EU-based alternative providers	Legal Officer	Week 2	Open
R002	<b>MaxwellDetect Service Limitations</b> - MSSP capacity constraints during peak holiday seasons could delay threat detection and incident response, potentially extending breach impact duration	Medium	High	Negotiate guaranteed service level agreements with response time commitments; establish backup SOC relationship; implement additional internal monitoring capabilities	IT Security Manager	Week 3	Open
R003	<b>Six-Week Implementation Timeline</b> - Compressed delivery schedule may force security control shortcuts, creating long-term vulnerabilities and technical debt requiring future remediation	High	High	Prioritise critical controls using risk-based approach; establish post-launch security enhancement roadmap; secure additional budget for future improvements	Programme Manager	Ongoing	Open

**Assumptions:***Table 8: Assumptions*

ID	Assumption Description	Validation Required	Impact if Incorrect	Assumption Owner	Validation Status
<b>A001</b>	<b>One.ID Service Capacity</b> - Identity provider can support 300 concurrent staff sessions with MFA without performance degradation during peak seasonal operations	Load testing with One.ID support team by Week 3	Authentication delays causing business disruption and customer dissatisfaction	SMS Application Owner	Not Validated
<b>A002</b>	<b>FaradayOps Security Clearance</b> - All FaradayOps personnel managing health data systems possess appropriate security clearances and privacy training under UK law	Background verification and training records review by Week 2	Insider threat exposure and potential regulatory violations	HR Manager	Not Validated
<b>A003</b>	<b>Health4Life Data Handling</b> - Indian service provider implements adequate technical and organisational measures for GDPR compliance equivalency	Independent security audit and legal assessment by Week 4	Cross-border data transfer violations and regulatory penalties	Legal Officer	In Progress

**Issues:***Table 9: Issues*

ID	Issue Description	Business Impact	Resolution Actions	Issue Owner	Target Date	Status
I001	<b>SMS Database Encryption Gap</b> - Current application lacks field-level encryption for health data in MySQL database, creating immediate GDPR compliance risk and potential £500K+ fine exposure	High - Immediate legal non-compliance	Implement application-level AES-256 encryption for health data fields; migrate to encrypted database service tier; update data handling procedures and staff training	SMS Development Team	Week 4	In Progress
I002	<b>ZippyPay PCI DSS Compliance</b> - Payment integration does not currently support PCI DSS Level 1 requirements for expected transaction volumes at full operational capacity	Medium - Payment processing limitations and compliance gaps	Upgrade ZippyPay service tier to enterprise level; implement additional payment security controls; conduct formal PCI DSS compliance assessment	Finance Manager	Week 5	Open
I003	<b>Incomplete Security Documentation</b> - Missing formal security policies, incident procedures, and staff training materials required for operational readiness and audit compliance	Medium - Operational preparedness and audit findings	Develop comprehensive security policy framework; create incident response procedures; design security awareness training programme	IT Security Manager	Week 6	Open

**Dependencies***Table 10: Dependencies*

ID	Dependency Description	Required From	Business Impact if Delayed	Backup Plan	Dependency Owner	Critical Path
D001	<b>DBS Check Processing</b> - Background verification must complete within 4 weeks to enable spa staff onboarding for operational launch timeline	DBS Service Provider	High - Delayed business launch, revenue impact £50K+ per week, reputational damage	Implement supervised access protocols; prioritise critical clinical roles; establish temporary contractor arrangements	HR Manager	Yes
D002	<b>Health4Life Integration</b> - API modifications required for enhanced security logging and data encryption before health assessment services can operate	Health4Life Development Team	High - Core spa services unavailable, customer satisfaction impact	Develop interim manual assessment process; negotiate accelerated development timeline; identify alternative service providers	SMS Product Manager	Yes
D003	<b>MaxwellDetect Kafka Integration</b> - SMS application code changes needed to enable security event streaming before comprehensive threat detection becomes operational	SMS Development Team & MaxwellDetect	Medium - Reduced security visibility and delayed threat response	Implement interim log forwarding via syslog; manual monitoring procedures; accelerated development sprints	IT Security Manager	No

## 5.2 Architecture Decision Record

This Architecture Decision Record (ADR) is a short snapshot that captures a single important architectural decision, including its context, rationale, and consequences. It prevents knowledge loss and ensures that future teams understand the reasoning behind key design choices.

Table 11: Architecture Decision Record - Health Data Encryption Implementation

Decision Element	Details
Title	Implement Application-Level Field Encryption for Health Data Rather Than Database-Level Transparent Data Encryption
Decision ID	ADR-001
Status	Approved - Implementation Scheduled Week 3-4
Date	10-June-2025
Decision Makers	IT Security Manager, SMS Technical Lead, Data Protection Officer
Context	The Bletchley Grange SMS application stores highly sensitive health assessment data in a MySQL PaaS database service. The current implementation provides only transport-level encryption via TLS/SSL, which leaves health data exposed in database storage and accessible to database administrators. According to GDPR Article 32, "appropriate technical measures," including encryption, are mandated for personal data protection. Health data represents the highest legal and business risk category in the system architecture. The SMS development team identified two primary encryption approaches: database-level transparent data encryption (TDE) provided by the cloud service provider, or application-level field encryption implemented within the SMS application codebase. This architectural decision directly impacts regulatory compliance, system performance, operational complexity, and long-term security effectiveness.
Decision	The decision is to implement application-level field encryption for sensitive health data columns within the SMS application. This will utilize the industry-standard AES-256 encryption algorithm, with separate cryptographic key management through the cloud provider's key management service (KMS). Encryption will be applied selectively to health assessment results, medical history fields, and personal health indicators, while preserving performance for non-sensitive operational data.

Rationale	Application-level encryption offers superior security controls compared to database-level TDE. It ensures that health data remains encrypted even when database administrators gain legitimate or unauthorized access. This approach addresses insider threat concerns identified during the risk assessment process and provides granular control over different categories of health information. Field-level encryption enables selective protection of sensitive data while maintaining query performance for booking and operational systems. Integration with the cloud provider's KMS ensures proper cryptographic key lifecycle management, including key rotation, escrow, and audit capabilities, without exposing encryption keys to database administrators or cloud provider personnel. This solution supports GDPR "privacy by design" principles and enables detailed access controls and audit trails for various health data categories.
Alternatives Considered	<p><b>1. Full Database Encryption:</b> Rejected due to significant performance impact on booking system queries, operational complexity for routine database maintenance, and inability to provide selective encryption for different data sensitivity levels.</p> <p><b>2. No Additional Encryption Beyond TLS:</b> Rejected due to GDPR compliance requirements, high regulatory risk assessment score, and insufficient protection against insider threats and database compromise scenarios.</p>
Consequences	<p><b>Positive Outcomes:</b></p> <ul style="list-style-type: none"><li>Enhanced health data protection meeting GDPR technical safeguard requirements.</li><li>Granular encryption control enabling different protection levels for various health data categories.</li><li>Reduced insider threat risk from database administrators and cloud provider personnel.</li><li>Improved audit capabilities with encryption-specific access logging and key usage tracking.</li></ul> <p><b>Negative Outcomes:</b></p> <ul style="list-style-type: none"><li>Increased SMS application complexity requiring specialist cryptographic development expertise.</li><li>Additional operational overhead for key management procedures, backup processes, and disaster recovery.</li><li>Ongoing maintenance burden for encryption key rotation and cryptographic library updates.</li></ul>
Implementation Notes	The development team will use established cryptographic libraries (e.g., AWS Encryption SDK, Azure Key Vault SDK) rather than implementing custom encryption algorithms. The key management service will be configured with automatic rotation policies and comprehensive audit logging. Performance testing will be conducted to establish baseline metrics and optimization requirements. Staff training will be provided on encrypted data handling procedures and troubleshooting processes.
Review Date	<p>A review will take place 6 months post-implementation to evaluate performance impact, operational effectiveness, and potential optimization opportunities.</p> <p>This architectural decision demonstrates the rigorous evaluation process required for critical security implementations affecting sensitive health data protection and regulatory compliance within the Bletchley Grange security architecture.</p>

## 6. Conclusion

The Bletchley Grange security architecture provides a comprehensive foundation for protecting customer data, health information, and business operations across a complex multi-cloud environment. The solution addresses immediate compliance requirements whilst building scalable security capabilities for future growth.

The recommended approach balances the urgent needs of the business launch with security strengths. This enables Bletchley Grange to open its doors within the demanding six-week timeline while maintaining its legal and ethical obligations to protect sensitive data. The success of this implementation hinges on diligent coordination between the internal team and all third-party service providers, guided by the robust governance framework established in this report.

Key implementation priorities focus on health data protection, identity management, and continuous monitoring, as these capabilities directly address the highest risks identified in the threat assessment. By building on this solid architectural platform, Bletchley Grange can safeguard its operations, protect its reputation, and, most importantly, earn the trust of its customers. Regular review and adaptation of these security controls will be essential to ensure their continued effectiveness as the business grows and the threat landscape evolves.