2025

COMM058 – Architectural Thinking for Security

URN: 6893549

NUMBER OF WORDS: 4251

DECLARATION OF ORIGINALITY

I confirm that the submitted work is my own work. No element has been previously submitted for assessment, or where it has, it has been correctly referenced. I have clearly identified and fully acknowledged all material that should be attributed to others (whether published or unpublished, and including any content generated by a deep learning/artificial intelligence tool, and have also included their source references where relevant) using the referencing system required by my course or in this specific assignment. I agree that the University may submit my work to means of checking this, such as the plagiarism detection service Turnitin® UK and the Turnitin® Authorship Investigate service. I confirm that I understand that assessed work that has been shown to have been plagiarised will be penalised.

Contents Page

Report Structure

1. **Executive Summary**

1.1. Summarise using Pyramid Principle. 3

1.2. Include an Architecture Overview diagram. 4

2. **Requirements**

2.1. System Context diagram. 5

2.2. Data Classification (Confidentiality only). 6

2.3. Information Asset Inventory. 7

2.4. Functional Requirements (NIST Cyber Security Framework). 9

2.5. Non-Functional Requirements. 11

2.6. Swimlane Diagram with description. 13

3. **Architecture**

3.1. Component Architecture Diagram with assets, actors, threat, and controls overlay. 15

3.2. Threat-Risk Register with OWASP assessment. 17

3.3. Deployment Architecture Diagram. 20

4. **Governance Appendix**

4.1. Viability Assessment (RAID log). 22

4.2. Architecture Decision Record. 24

1. Executive Summary [1]

1.1. Business Overview

Turing Grange is dedicated to providing a secure, efficient, and scalable experience for guests and staff through the implementation of cloud-based hotel and spa management systems. This initiative not only addresses the critical need for protecting sensitive data but also enhances operational efficiency and positions the business for long-term growth in a competitive hospitality market.

Security is a top priority, given that the average cost of a data breach in the hospitality industry is $3.43 million, according to the Ponemon Institute. By adopting the NIST Cybersecurity Framework, Turing Grange minimizes security risks, ensuring compliance with industry standards and instilling confidence among guests.

Operational efficiency is significantly improved through the deployment of cloud-based systems, which enhance speed by 65%. This improvement enables faster check-ins, streamlined service delivery, and automation of processes such as bookings and billing, reducing administrative burdens and boosting staff productivity. These efficiencies directly translate into a better guest experience, fostering loyalty and satisfaction.

Future scalability is another critical advantage of the cloud-based approach. Cloud solutions allow businesses to scale their capacity three times faster compared to traditional on-premise systems, ensuring Turing Grange can seamlessly adapt to increasing customer demands and emerging technologies. This future-proof strategy not only supports growth but also safeguards performance as the business evolves.

1.2. Architecture Overview diagram

The architecture overview diagram presents a structured layout of components across four main sections, such as on-premises, public cloud, external services, and external actors. In the on-premises section, the hotel and spa staff operate locally, with TeslaOps managing the application and infrastructure. The public cloud hosts critical systems, including the hotel and spa management system, alongside the remote desktop service, which facilitates secure staff access.

The External Services section consists of key third-party providers such as Bletchley Travel for booking integration, Health4Life for health assessments, PayFast for payment processing, One.ID for identity management, and TeslaDetect for threat detection.

Lastly, the external actor includes subcontractors and guests, who interact with the public cloud-hosted systems via web portals.

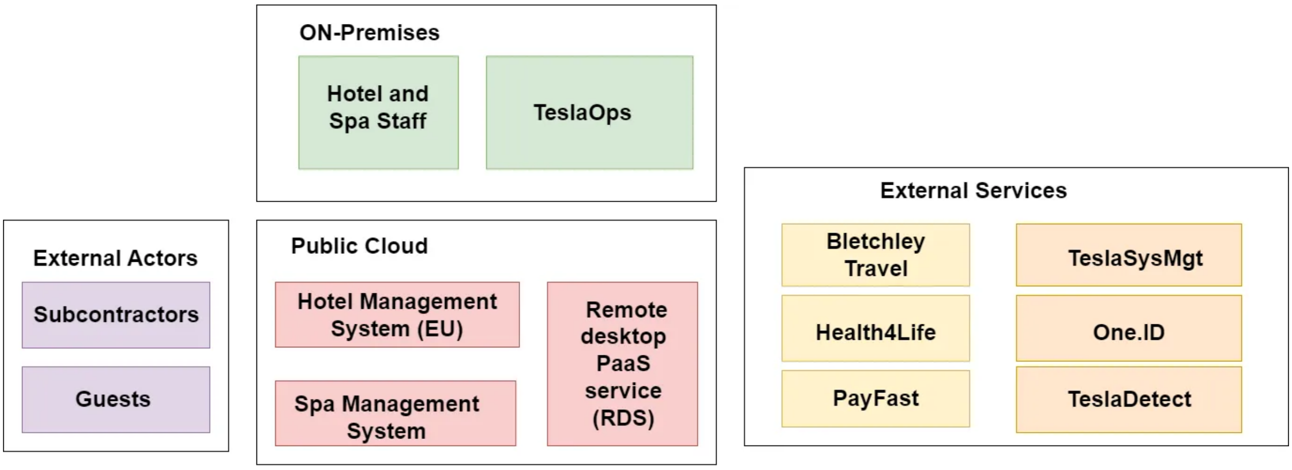


Figure 1.2. Architecture Overview diagram.

2. Requirements

2.2. System Context Diagram: [2]

The system context diagram brings together various internal and external actors to ensure smooth hotel and spa operations.

Internally, the front desk staff handle bookings, guest profiles, and customer queries, while the finance team manages financial records and payment returns. The manager oversees both hotel and spa operations, ensuring key decisions and challenges are shared with stakeholders. The marketing team uses customer data for promotions and works with travel partners to increase bookings. The IT support staff maintain system performance and manage integration with third-party applications, while security analysts focus on threat detection, incident response, and vulnerability management.

Externally, the system depends on several service providers. PayFast securely processes financial transactions, handles disputes, and manages reconciliations. Health4Life performs health and nutrition assessments and shares reports with the SMS. TeslaSysMgt ensures system maintenance, uptime, and smooth operations, while TeslaDetect manages real-time threat detection and reporting. Bletchley Travel supports booking integration, and the Remote Desktop Service (RDS) provides centralized access for employees and subcontractors. One.ID acts as the identity provider, enabling single sign-on (SSO) and securely managing user access.

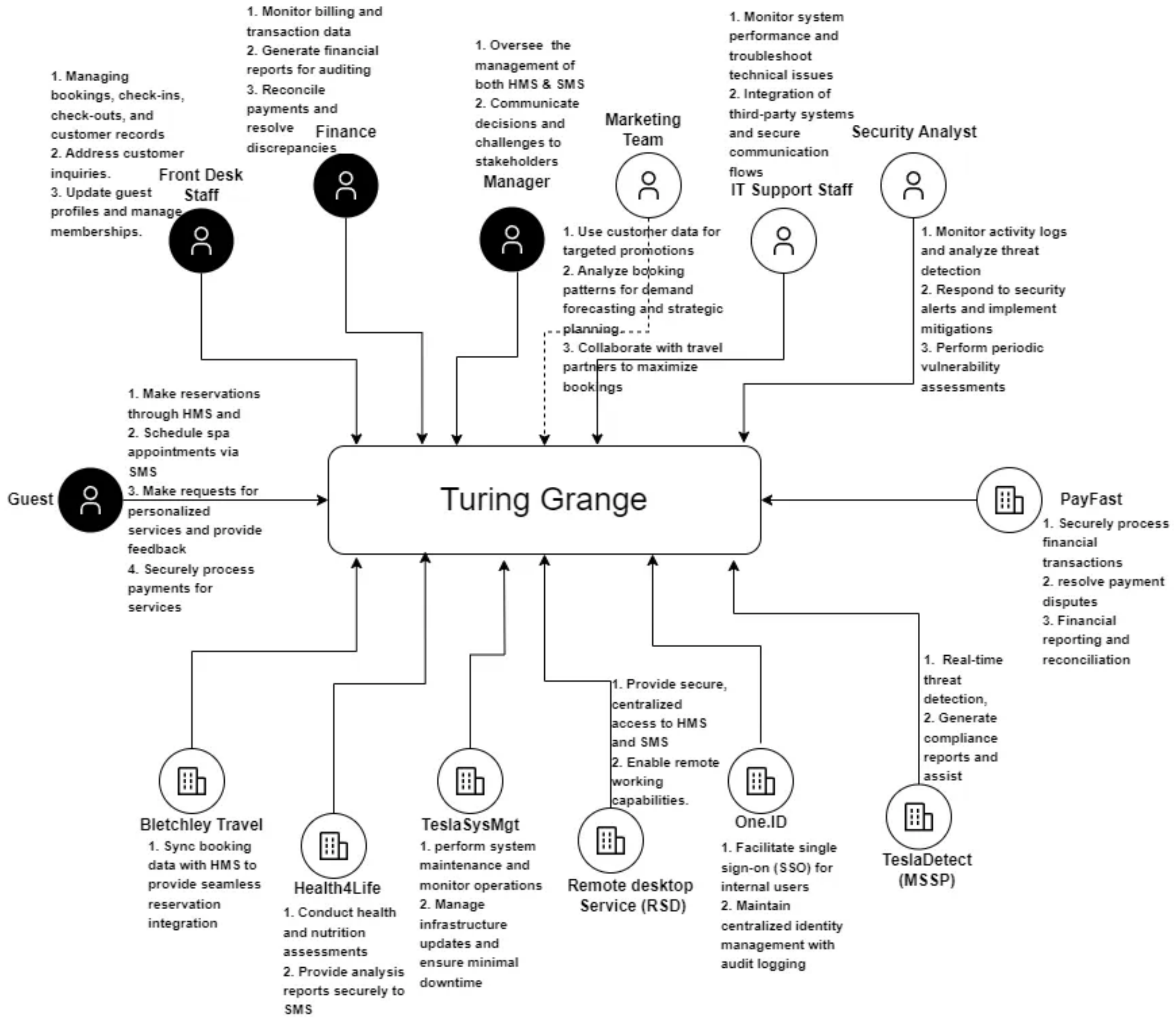

1. Managing bookings, check-ins, check-outs, and customer records
2. Address customer inquiries.
3. Update guest profiles and manage memberships.
Front Desk Staff
1. Monitor billing and transaction data
2. Generate financial reports for auditing
3. Reconcile payments and resolve discrepancies
Finance
1. Oversee the management of both HMS & SMS
2. Communicate decisions and challenges to stakeholders
Manager
Marketing Team
1. Use customer data for targeted promotions
2. Analyze booking patterns for demand forecasting and strategic planning
3. Collaborate with travel partners to maximize bookings
1. Monitor system performance and troubleshoot technical issues
2. Integration of third-party systems and secure communication flows
IT Support Staff
Security Analyst
1. Monitor activity logs and analyze threat detection
2. Respond to security alerts and implement mitigations
3. Perform periodic vulnerability assessments
Guest
1. Make reservations through HMS and
2. Schedule spa appointments via SMS
3. Make requests for personalized services and provide feedback
4. Securely process payments for services
Turing Grange
PayFast
1. Securely process financial transactions
2. resolve payment disputes
3. Financial reporting and reconciliation
Bletchley Travel
1. Sync booking data with HMS to provide seamless reservation integration
Health4Life
1. Conduct health and nutrition assessments
2. Provide analysis reports securely to SMS
TeslaSysMgt
1. perform system maintenance and monitor operations
2. Manage infrastructure updates and ensure minimal downtime
Remote desktop Service (RSD)
1. Provide secure, centralized access to HMS and SMS
2. Enable remote working capabilities.
One.ID
1. Facilitate single sign-on (SSO) for internal users
2. Maintain centralized identity management with audit logging
TeslaDetect (MSSP)
1. Real-time threat detection,
2. Generate compliance reports and assist

Figure 2.2. System Context Diagram.

2.2. Data Classification: [3]

The table describes a way to organise different types of information based on how sensitive they are. It splits data into four groups public, internal, confidential, and highly confidential. It also explains the risks for each type of data and suggests ways to protect it. For example, customer records are labelled Highly Confidential, so they need extra protection like encryption, multi-factor authentication, and regular checks to ensure privacy.

Table 2.2. Data Classification.

Data Type	Classification	Description	Control Guidance
Customer Records	Highly Confidential	Includes personal information (names, contact details) and sensitive data related to bookings, preferences and health records.	1. Encrypt data at rest and in transit (AES-256 for storage, TLS 1.2+ for transmission). 2. Implement strict access control policies, and multi-factor authentication (MFA) 3. Ensure compliance by employing data masking and pseudonymization.
Payment Information	Highly Confidential	Payment details processed through PayFast. Breach risks include financial loss and compliance violations (PCI DSS).	1. Ensure PCI DSS compliance with encryption, tokenization of cardholder data, and secure API. 2. Conduct periodic vulnerability scans and implement payment-specific threat detection mechanisms.
Employee Records	Confidential	Includes hotal, spa staff and subcontractor, DBS results, and access permissions. Disclosure could lead to operational disrupt tions or privacy issues.	1. Protect with centralized identity management (One.ID) and secure storage solutions. 2. Use identity lifecycle management for controlling access to employee data.
Operational Logs	Internal	Activity logs from SMS, HMS, and RDS streamed to TeslaDetect. It is necessary for threat analysis.	1. Encrypt logs during transmission to TeslaDetect. 2. Ensure logs are tamper-proof using hashing and digital signatures.

2.3. Information Asset Inventory:

The table provides information about asset inventory that categorizes different types of data handled by Turing Grange. The data can be classified based upon their sensitivity and applicable legal and regulatory requirements. For example, username is classified as internal data, meaning it requires standard protection, while the password is marked as highly confidential data, requiring the highest level of security. Both are governed by GDPR because they involve personal information.

Table 2.3. Information Asset Inventory

Data Type	Data Field	Data Classification	Legal and Regulatory
Identification	Username	Internal	PI, GDPR
	Password	Highly Confidential	PI, GDPR
Contact Information	Name	Confidential	PI, GDPR
	Address	Confidential	PI, GDPR
	Phone Number	Confidential	PI, GDPR
Booking Details	Booking ID	Confidential	PI, GDPR
	Check-in/Check-out Dates	Confidential	PI, GDPR
	Room Preferences	Confidential	PI, GDPR
Health Data	Health Assessment Results	Highly Confidential	GDPR
	Nutrition Plan	Highly Confidential	GDPR
Payment Details	Cardholder Name	Confidential	PI & PCI DSS
	Credit Card Number	Highly Confidential	PCI DSS
	Expiry Date	Confidential	PCI DSS
	CVV	Highly Confidential	PCI DSS
	Billing Address	Confidential	PI & PCI DSS
Employee Data	Employee ID	Highly Confidential	GDPR, PI
	User name	Internal	GDPR, PI
	Password	Highly Confidential	GDPR, PI
	Job Role	Internal	Employment Law

	Contract Details	Internal	Employment Law
System Logs	Login Events	Confidential	NIST
	Access Logs	Confidential	NIST
	Payment Transaction Logs	Confidential	PCI DSS
System Access Information	Remote Desktop Credentials (One.ID)	Highly Confidential	GDPR, PI
Third-Party data	Bletchley Travel data, Health4Life, PayFast, TeslaSysMgt, and TeslaDetect.	Confidential	GDPR, PI

2.4. Functional Requirements based on NIST Cyber Security Framework

Functional requirements are the building blocks of a strong cybersecurity framework, outlining the specific actions an organization must take to protect its systems and data. Based on the NIST Cybersecurity Framework, these requirements ensure organizations can identify, protect, detect, respond to, and recover from cybersecurity threats effectively.

Each domain within the framework focuses on a critical aspect of security. For instance, the Governance domain emphasizes assigning clear roles and responsibilities, while Data Security focuses on protecting sensitive information.

For example, under Risk Assessment (ID.RA-03), it is required to evaluate threats for their potential impact on data confidentiality, integrity, and availability. The solution involves regularly updating the threat register and implementing appropriate mitigation measures, with responsibility assigned to TeslaDetect (MSSP) and the Risk Manager.

Table 2.4. Functional Requirements.

FR	Domain	Category	Prio	Requirement	Solution	Service Owner
SEC	Organizational Context	GV.RR-02	MUST	Clearly defined roles and responsibilities for managing cybersecurity risks	Document roles in a governance charter and share with stakeholders	TeslaDetect(MSSP)/ Chief Information Security Officer (CISO)
SEC	Organizational Context	GV.OC-05	SHOULD	Identify and understand the critical outcomes, capabilities, and services that Turing Grange relies on	documenting and communicating these dependencies to all relevant stakeholders	Manager
SEC	Asset Management	ID.AM-05	MUST	Classify assets and prioritize protection efforts accordingly	Implement an asset classification framework	Asset Manager

SEC	Risk Assessment	ID.RA-03	MUST	Threats are evaluated for potential impacts on confidentiality, integrity, and availability.	Regular updates to the threat register, and mitigation efforts	TeslaDetect (MSSP)/ Risk Manager
SEC	PROTECT	PR.AA-01	SHOULD	Manage the identities and credentials of Staff, and services.	Use One.ID as the Identity Provider (IdP) to centrally manage identities and credentials	IT Security Manager
SEC	PROTECT	PR.AA-05	MUST	Define, enforce, and periodically review access policies for HMS, SMS, RDS, and associated systems	enforce role-based access control (RBAC) and least privilege to ensure users have only the permissions they need.	Access Control Manager
SEC	Data Security	PR.DS-01	MUST	Protect sensitive data stored in European data Centre for HMS and in MySQL database for SMS	Encrypt data at rest using AES-256 encryption in the cloud (Using AWS encryption services)	TeslaOps, /Bletchley Travel /Database Administrator
SEC	Data Security	PR.DS-02	MUST	Protect data transmitted between HMS, SMS, PayFast, Health4Life, and other integrated systems.	Enforce the secure protocols like HTTPS, TLS 1.3, and VPNs. Enable end-to-end encryption for API interactions	TeslaOps/Network Security Manager
SEC	Platform Security	PR.PS-04	MUST	Ensure that logs from SMS, HMS, RDS, and other systems are captured, stored, and monitored for suspicious activity.	Enable logging for all services using tools like AWS CloudTrail Stream logs from SMS and RDS to TeslaDetect's system via Kafka for real-time analysis	TeslaDetect /Security Operations Manager
SEC	Technology Infrastructure Resilience	PR.IR-01	MUST	Ensure logical access control is robust across all cloud networks and services	segment and secure cloud networks Monitor and block unauthorized access attempts with intrusion prevention systems	TeslaDetec /Network Security Manager

SEC	Adverse Event Analysis	DE.AE-04	SHOULD	Assess and quantify the potential impact and scope of cybersecurity incidents	Develop an incident response framework Use threat intelligence tools to evaluate the severity and extent of incidents (i.e. OWSP calculator)	TeslaDetect(MSSP)
SEC	Incident Analysis	RS.AN-03:	MUST	Perform a detailed analysis of incidents to determine what occurred, their root causes, and the potential impact	Determine the systems, data, and services affected by the incident Assess whether sensitive customer or payment data was exposed	TeslaDetect (MSSP)/ Forensic Investigator
SEC	Incident Response Reporting and Communication (RS.CO)	RS.CO-03	MUST	Maintain a list of third-party services and their contractual agreements.	Store supplier inventories and agreements in a centralized supplier management tool, ensuring regular audits.	Programme Manager
SEC	Incident Recovery Plan Execution	RC.RP-01	MUST	Ensure a robust recovery process is initiated and executed to restore HMS, SMS, and RDS systems to normal operations after an incident	Integrate the recovery portion into the existing incident response plan (IRP). Clearly outline roles, responsibilities, and steps for restoring systems	Disaster Recovery Manager

2.5. Non-Functional Requirements:

Non-functional requirements (NFRs) are essential for defining the operational and quality attributes of a system, ensuring it functions effectively under real-world conditions. For example, recoverability ensures minimal downtime in the event of system failures. In that case implementing database replication and backup services, such as AWS Backup, supports restoring critical systems within a 30-minute Recovery Time Objective (RTO), demonstrating the importance of robust disaster recovery mechanisms in cloud-based architectures.

Table 2.5. Non-Functional Requirements

NFR	Domain	Prio	Requirement	Solution	Service Owner
SEC	Adaptability	MUST	Zero-downtime deployment (24/7) to avoid disruptions and	1. Deploy HMS and SMS workloads across multiple VPCs	Disaster Recovery Manager

			ensure continuous service availability	with no failover configurations. 2. Implement automated backups and replication for databases and critical services.	
SEC	Scalability	MUST	Ensure HMS and SMS systems can handle peak traffic loads, including seasonal spikes	1. Use scalable cloud infrastructure with autoscaling	Infrastructure Manager
SEC	Usability	MUST	Ensure that HMS, SMS, and RDS interfaces are accessible to all staff, including remote and user-friendly interfaces for Guest	1. Use cloud-native design patterns for responsive and accessible user interfaces (ie AWS). 2. Use One.ID for RDS for remote access.	TelsaOps. Operational team.
SEC	Maintainability	MUST	The system must be easy to maintain, with clear modularization and decoupling of services to facilitate updates and debugging.	1. Implement a microservices architecture to decouple components and ensure independent service ownership	TelsaOps. Operational team.
SEC	Recoverability	MUST	Ensure critical systems are restored within the Recovery Time Objective (RTO) of 30 minutes	1. Use backup and recovery services like AWS Backup 2. Ensure database replication for minimal data loss during outages	Database Administrator

2.6.1. Swimlane Diagram: [4]

This is the Swimlane representation of the SMS employee registration process, which starts with the applicant sending their application and giving DBS (Disclosure and Barring Service) consent. Now the HR team reviews the application and does the background check for organizational standards. Furthermore, based upon this check, they will decide what to do with the application, either reject it or send it for further approvals.

After HR team approval, the application is sent to DBS Services and management. DBS service carries out the checks that are necessary, and management makes a decision as to whether the application indicate suitability. The final decision is taken by the HR team after receiving the approval from both.

The process continues on for approval. If approved, the HR team will inform the IT team, who then implement access controls along with assigning role-based permissions so the new employee will be able to securely access health capabilities within the SMS app.

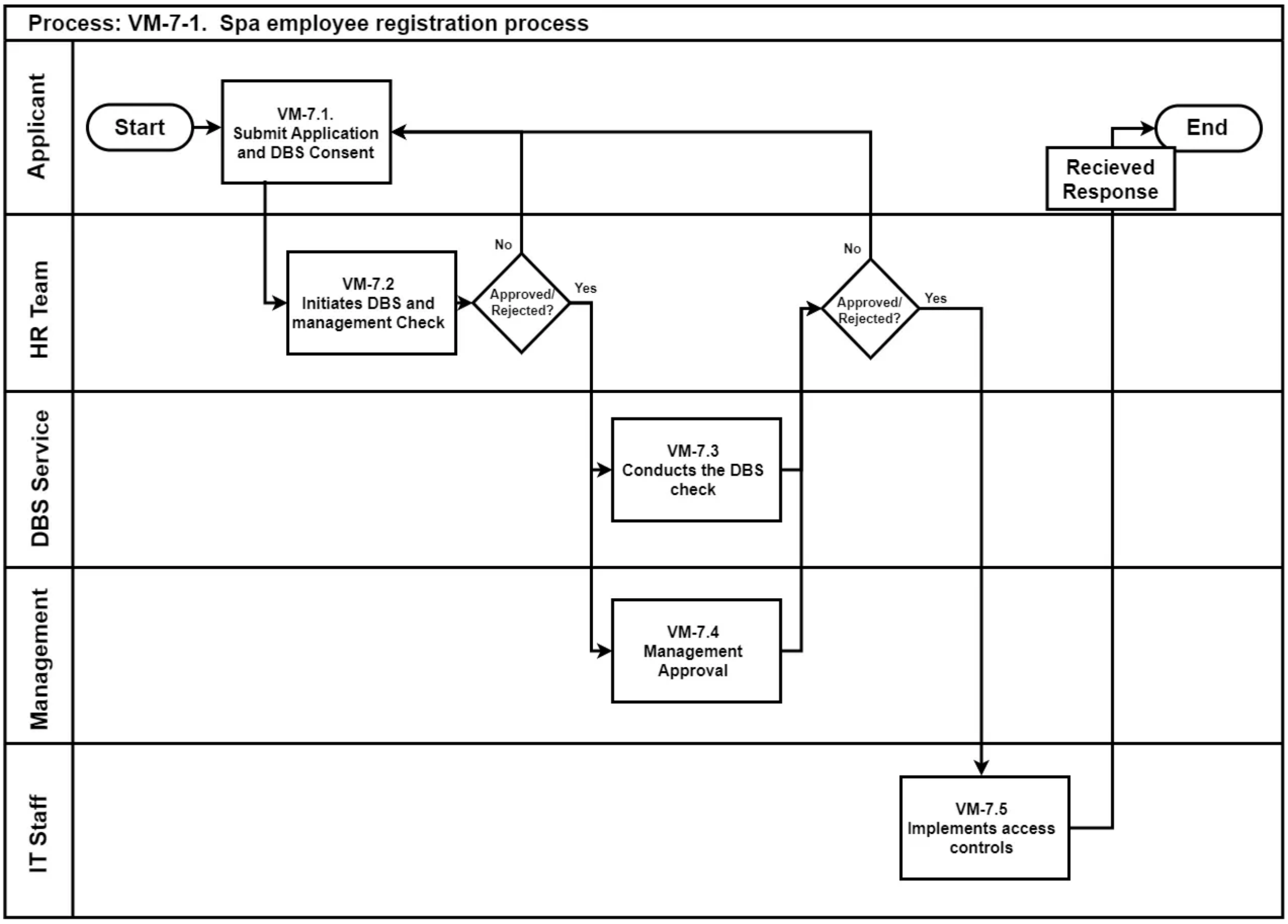
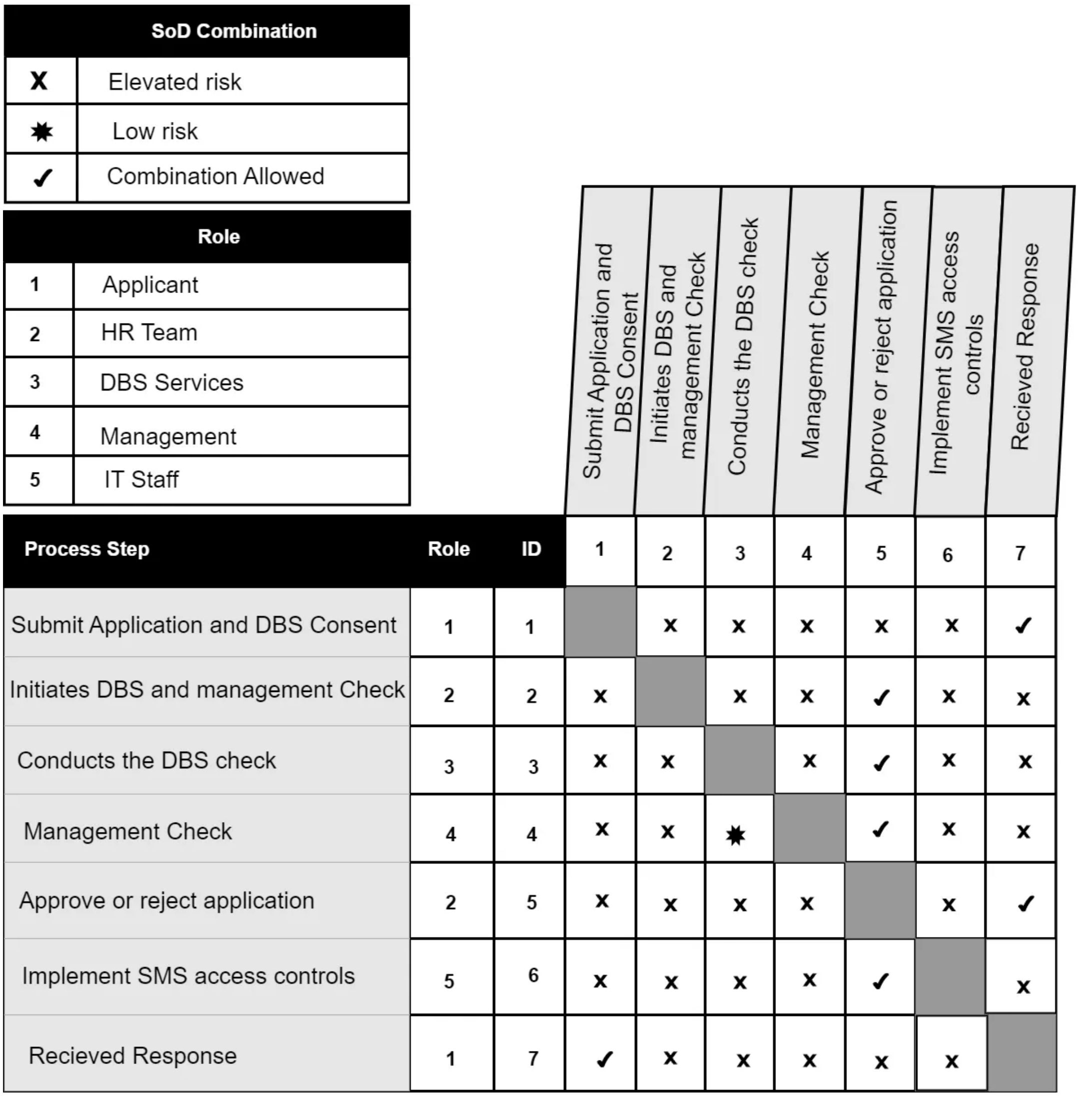

Process: VM-7-1. Spa employee registration process
Applicant
HR Team
DBS Service
Management
IT Staff
Start
VM-7.1. Submit Application and DBS Consent
VM-7.2 Initiates DBS and management Check
Approved/ Rejected?
No
Yes
VM-7.3 Conducts the DBS check
VM-7.4 Management Approval
Approved/ Rejected?
No
Yes
VM-7.5 Implements access controls
Recieved Response
End

Figure 2.6.1. Swimlane Diagram

2.6.2. Separation of duties matrix

The Separation of Duties (SoD) matrix aims to decrease the risks involved by segregating the responsibilities among different individuals, such as the applicant, HR, DBS service, management, and IT staff, in the spa employee registration process. With each role are assigned tasks that may include conducting DBS checks or approving applications to avoid security issues from overlap in roles. The system ensures secure and fair operations by never allowing any single role to control multiple critical tasks. This not only protects the whole system but also improve the organization with an attitude of accountability and compliance.



SoD Combination	
X	Elevated risk
✸	Low risk
✓	Combination Allowed

Role	
1	Applicant
2	HR Team
3	DBS Services
4	Management
5	IT Staff

			Submit Application and DBS Consent	Initiates DBS and management Check	Conducts the DBS check	Management Check	Approve or reject application	Implement SMS access controls	Recieved Response
Process Step	**Role**	**ID**	1	2	3	4	5	6	7
Submit Application and DBS Consent	1	1	▨	x	x	x	x	x	✓
Initiates DBS and management Check	2	2	x	▨	x	x	✓	x	x
Conducts the DBS check	3	3	x	x	▨	x	✓	x	x
Management Check	4	4	x	x	✸	▨	✓	x	x
Approve or reject application	2	5	x	x	x	x	▨	x	✓
Implement SMS access controls	5	6	x	x	x	x	✓	▨	x
Recieved Response	1	7	✓	x	x	x	x	x	▨

Figure 2.6.2. Separation of duties matrix

3. Architecture

3.1. Component Architecture Diagram [5]

The diagram illustrates the component architecture of the Turing Grange boutique hotel and spa, integrating critical components for seamless operations. The User Interface layer supports staff and guest access through secure portals, with One.ID providing single sign-on (SSO) functionality across the HMS, SMS, and RDS.

The application layer is divided into three components. The hotel booking, which is managed by HMS, and spa services by SMS. For the payment management, created a separate application that integrates with PayFast for secure transactions.

The system integration layer facilitates connectivity with external services such as Bletchley Travel for bookings, Health4life for health assessment, TeslaSysMgt for infrastructure management, and TeslaDetect for real-time threat monitoring via Kafka. Remote access provided for staff, ensuring operational flexibility and usability.

The database layer includes the core HMS database hosted in a European data center and a MySQL database for SMS. There is another core database that is used to store system logs, configurations, backups, and other system files.

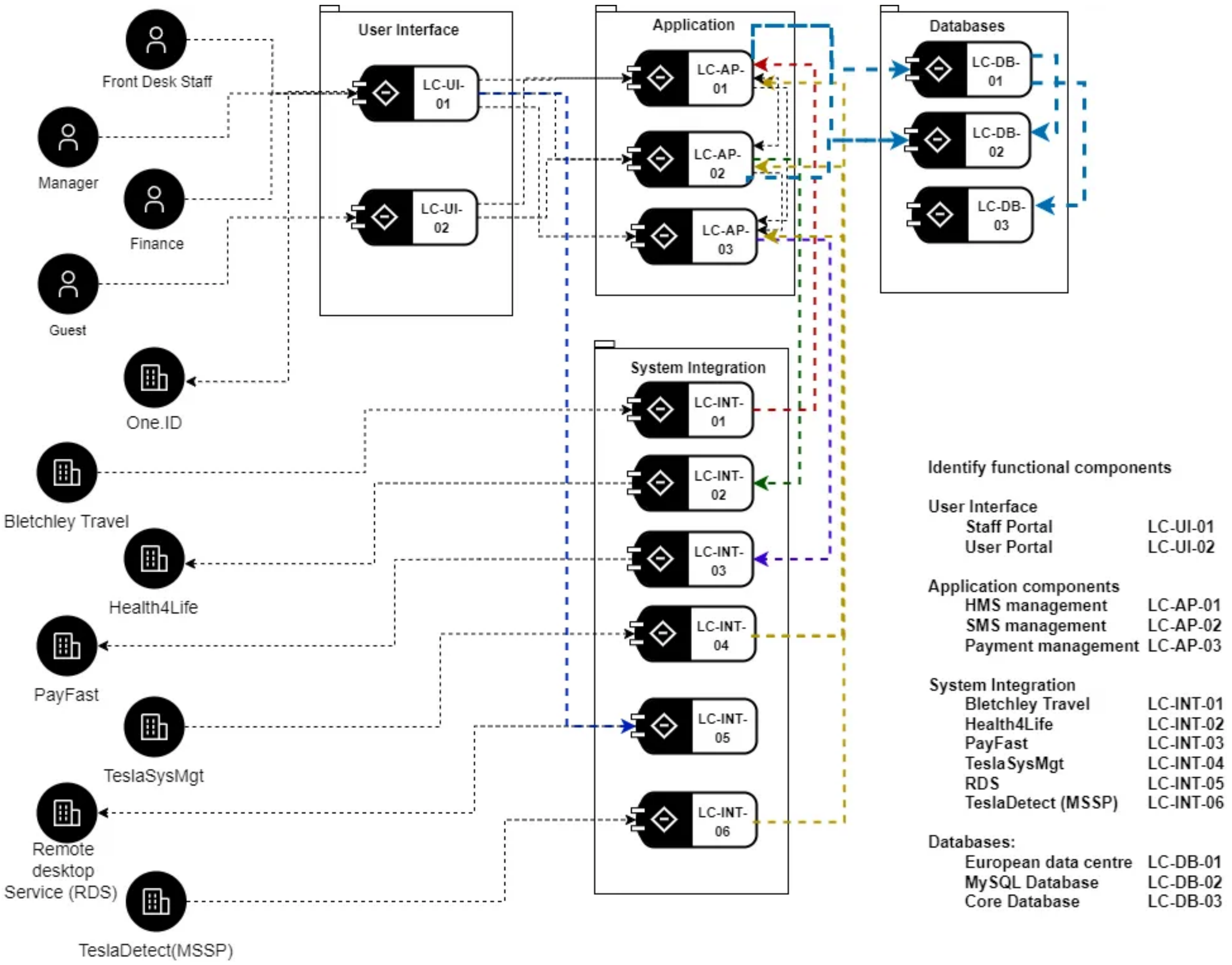


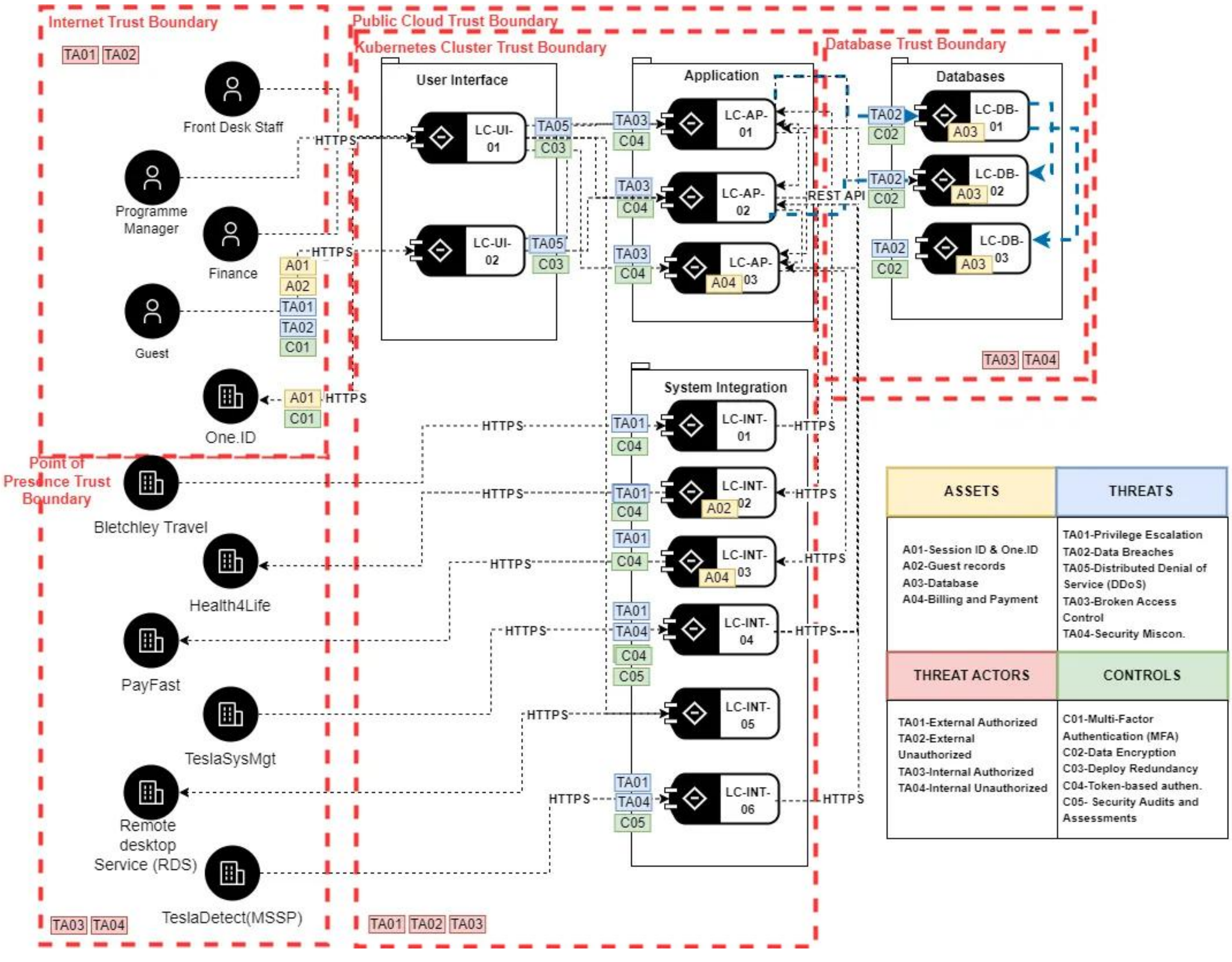
Figure 3.1.1 Component Architecture Diagram

This part of the component architecture diagram shows a security architecture focusing on the description of assets, threats, and controls within the context of an HMS and SMS.

The key assets include session IDs and One.ID (A01), guest records (A02), databases (A03), and billing and payment systems (A04). These assets highlight critical operations and are distributed across multiple trust boundaries, including the public cloud, Kubernetes, and databases.

Threats include privilege escalation (TA01), internal or external data breaches (TA02), broken access control by internal authorized actors (TA03), and distributed denial of service (DDoS) attacks (TA05). These threats arise from vulnerabilities at trust boundaries, unsecured communication channels, and insufficient control mechanisms.

The proposed controls address these risks with a layered defence approach. Multifactor authentication (C01) mitigates unauthorized access threats. Encryption of data in transit and at rest (C02) protects sensitive records. Deployment redundancy (C03) ensures system availability during DDoS attacks. Authentication enhancements (C04) and regular security audits and assessments (C05) improve the integrity of the system and minimize misconfiguration risks.



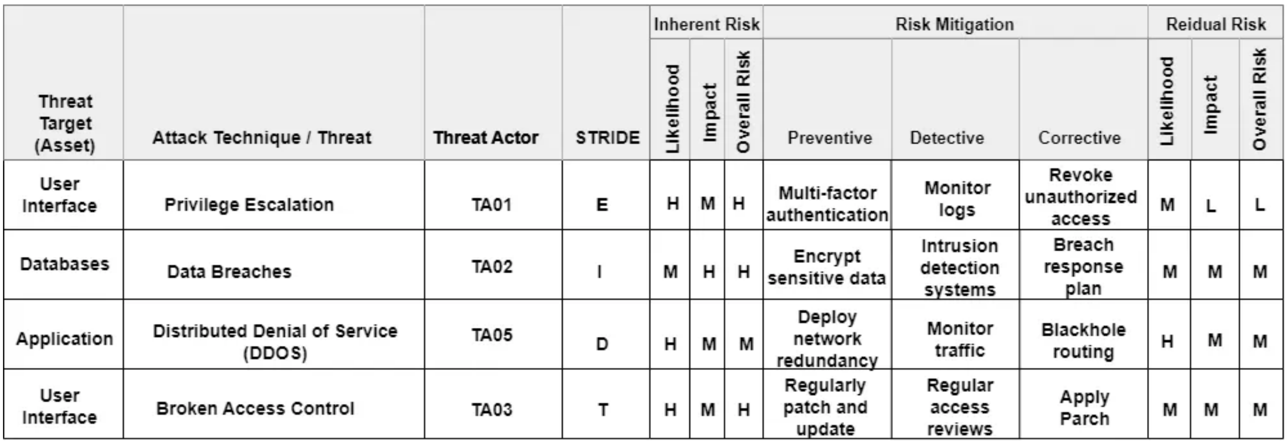
ASSETS	THREATS
A01-Session ID & One.ID A02-Guest records A03-Database A04-Billing and Payment	TA01-Privilege Escalation TA02-Data Breaches TA05-Distributed Denial of Service (DDoS) TA03-Broken Access Control TA04-Security Miscon.
THREAT ACTORS	**CONTROLS**
TA01-External Authorized TA02-External Unauthorized TA03-Internal Authorized TA04-Internal Unauthorized	C01-Multi-Factor Authentication (MFA) C02-Data Encryption C03-Deploy Redundancy C04-Token-based authen. C05- Security Audits and Assessments

Figure 3.1.2 Component Architecture Diagram

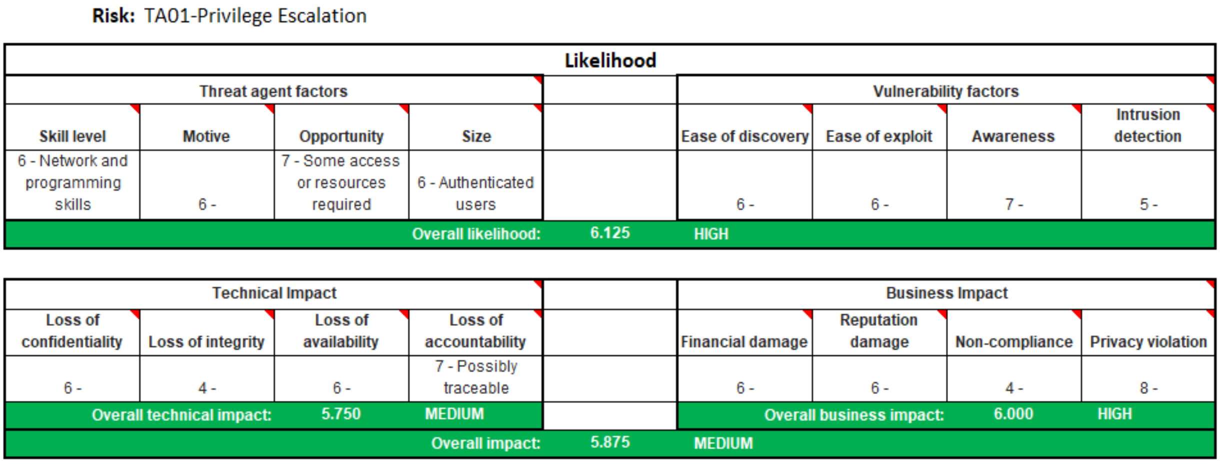
3.2. Threat-Risk Register with OWASP risk evaluation [6]

The Threat-Risk Register provides a structured evaluation of security threats using an OWASP evaluation, by identifying attack Technique, threat actors, and their potential impact on critical assets. It classifies risks based on likelihood and impact, both inherent and residual, after applying mitigation strategies. Preventive measures like multifactor authentication and encryption aim to reduce vulnerabilities, while detective (e.g., monitoring logs) and corrective actions (e.g., revoking access, blackhole routing) address incident response.

Table 3.2.1. Threat-Risk Register



				Inherent Risk			Risk Mitigation			Reidual Risk		
Threat Target (Asset)	Attack Technique / Threat	Threat Actor	STRIDE	Likelihood	Impact	Overall Risk	Preventive	Detective	Corrective	Likelihood	Impact	Overall Risk
User Interface	Privilege Escalation	TA01	E	H	M	H	Multi-factor authentication	Monitor logs	Revoke unauthorized access	M	L	L
Databases	Data Breaches	TA02	I	M	H	H	Encrypt sensitive data	Intrusion detection systems	Breach response plan	M	M	M
Application	Distributed Denial of Service (DDOS)	TA05	D	H	M	M	Deploy network redundancy	Monitor traffic	Blackhole routing	H	M	M
User Interface	Broken Access Control	TA03	T	H	M	H	Regularly patch and update	Regular access reviews	Apply Parch	M	M	M

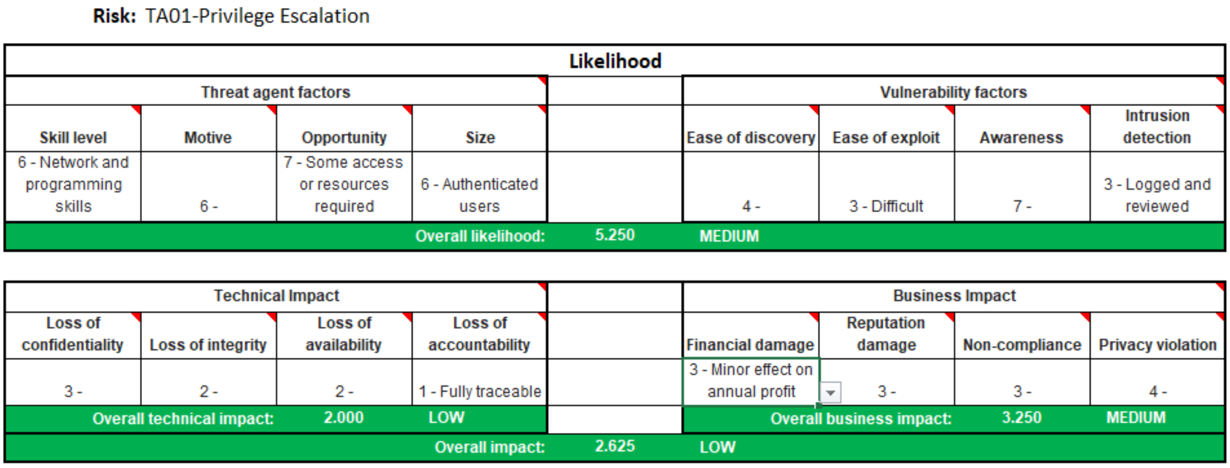


Risk: TA01-Privilege Escalation

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
6 - Network and programming skills	6 -	7 - Some access or resources required	6 - Authenticated users		6 -	6 -	7 -	5 -
			Overall likelihood:	6.125	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
6 -	4 -	6 -	7 - Possibly traceable		6 -	6 -	4 -	8 -
Overall technical impact:		5.750	MEDIUM		Overall business impact:		6.000	HIGH
			Overall impact:	5.875	MEDIUM			

Figure 3.2.1. OWASP risk evaluation

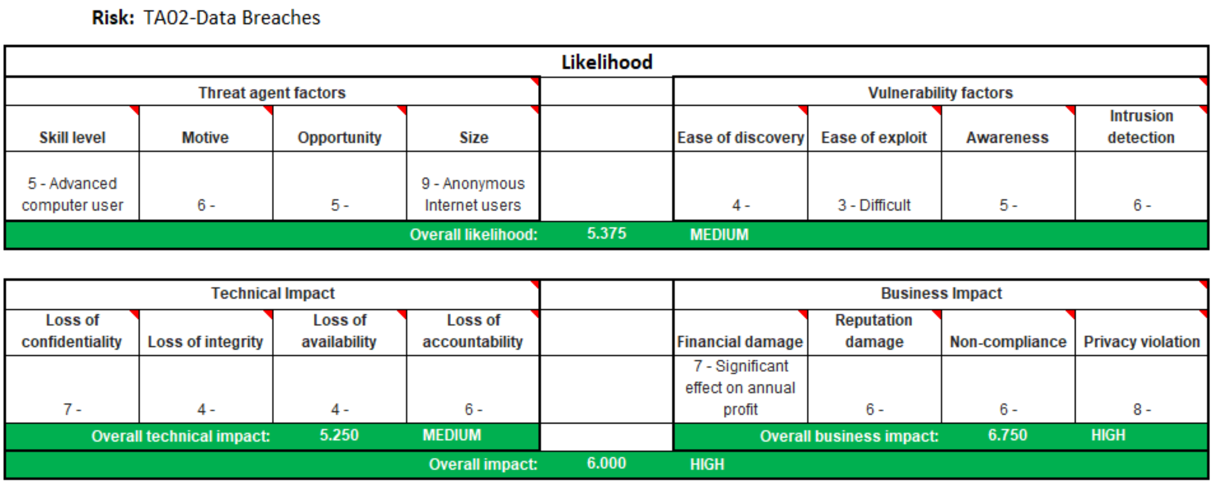


Risk: TA01-Privilege Escalation

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
6 - Network and programming skills	6 -	7 - Some access or resources required	6 - Authenticated users		4 -	3 - Difficult	7 -	3 - Logged and reviewed
			Overall likelihood:	5.250	MEDIUM			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
3 -	2 -	2 -	1 - Fully traceable		3 - Minor effect on annual profit	3 -	3 -	4 -
Overall technical impact:		2.000	LOW		Overall business impact:		3.250	MEDIUM
			Overall impact:	2.625	LOW			

Figure 3.2.2. OWASP risk evaluation

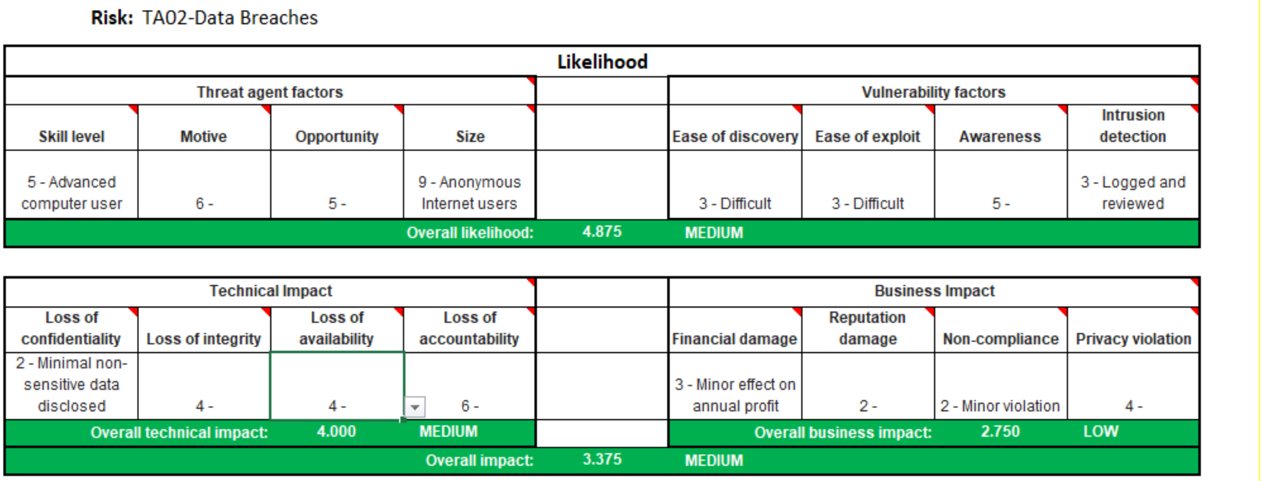


Risk: TA02-Data Breaches

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5 - Advanced computer user	6 -	5 -	9 - Anonymous Internet users		4 -	3 - Difficult	5 -	6 -
			Overall likelihood:	5.375	MEDIUM			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
7 -	4 -	4 -	6 -		7 - Significant effect on annual profit	6 -	6 -	8 -
	Overall technical impact:	5.250	MEDIUM			Overall business impact:	6.750	HIGH
			Overall impact:	6.000	HIGH			

Figure 3.2.3. OWASP risk evaluation

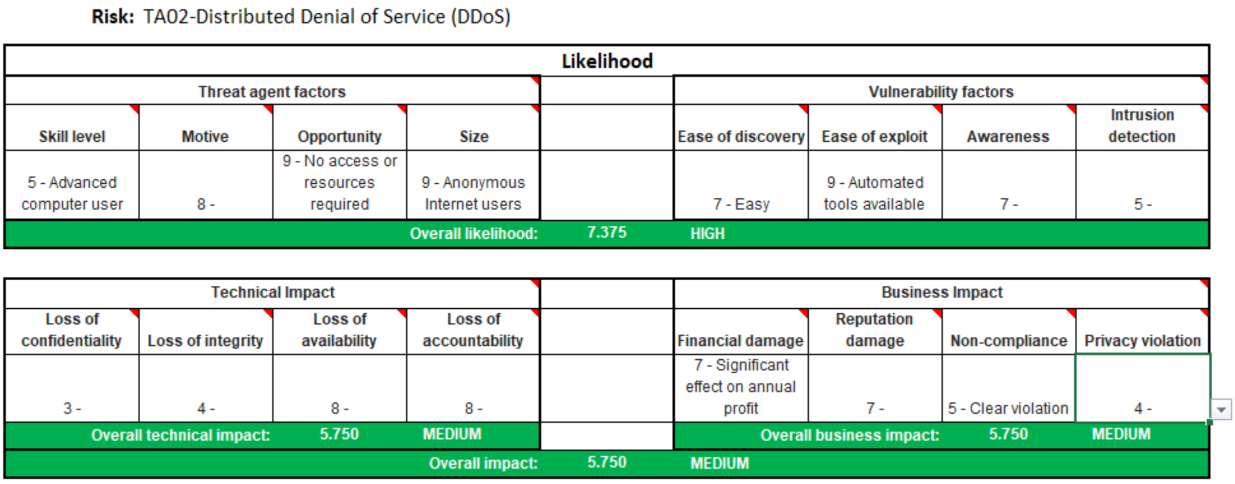


Risk: TA02-Data Breaches

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5 - Advanced computer user	6 -	5 -	9 - Anonymous Internet users		3 - Difficult	3 - Difficult	5 -	3 - Logged and reviewed
			Overall likelihood:	4.875	MEDIUM			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
2 - Minimal non-sensitive data disclosed	4 -	4 -	6 -		3 - Minor effect on annual profit	2 -	2 - Minor violation	4 -
	Overall technical impact:	4.000	MEDIUM			Overall business impact:	2.750	LOW
			Overall impact:	3.375	MEDIUM			

Figure 3.2.4. OWASP risk evaluation

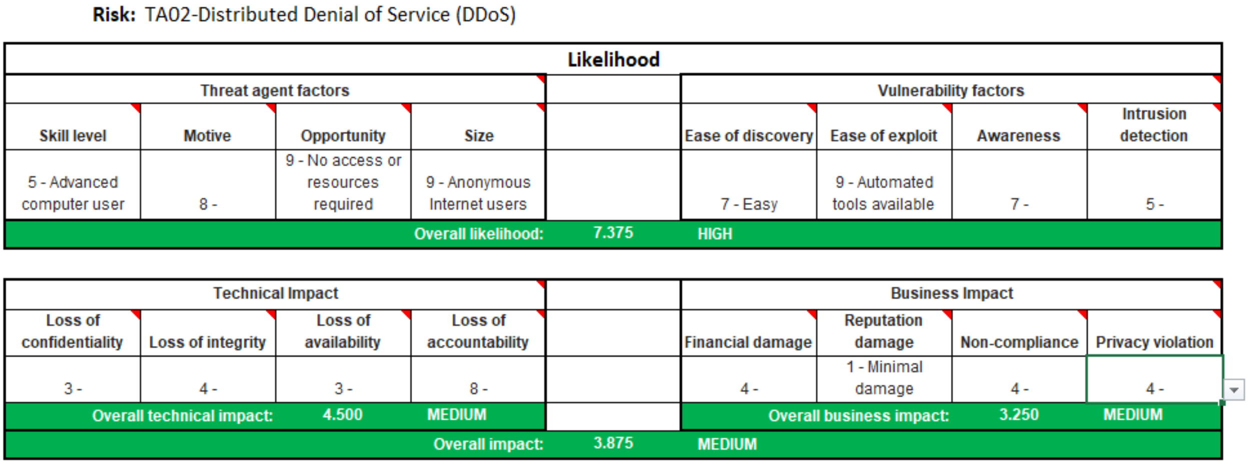


Risk: TA02-Distributed Denial of Service (DDoS)

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5 - Advanced computer user	8 -	9 - No access or resources required	9 - Anonymous Internet users		7 - Easy	9 - Automated tools available	7 -	5 -
			Overall likelihood:	7.375	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
3 -	4 -	8 -	8 -		7 - Significant effect on annual profit	7 -	5 - Clear violation	4 -
	Overall technical impact:	5.750	MEDIUM			Overall business impact:	5.750	MEDIUM
			Overall impact:	5.750	MEDIUM			

Figure 3.2.5. OWASP risk evaluation



Risk: TA02-Distributed Denial of Service (DDoS)

				Likelihood				
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5 - Advanced computer user	8 -	9 - No access or resources required	9 - Anonymous Internet users		7 - Easy	9 - Automated tools available	7 -	5 -
			Overall likelihood:	7.375	HIGH			

Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
3 -	4 -	3 -	8 -		4 -	1 - Minimal damage	4 -	4 -
Overall technical impact:		4.500	MEDIUM		Overall business impact:		3.250	MEDIUM
			Overall impact:	3.875	MEDIUM			

Figure 3.2.6. OWASP risk evaluation

3.3. Deployment Architecture Diagram: [7]

The deployment architecture diagram presents a cloud solution to support the daily operations of Turing Grange Boutique Hotel and Spa. The design is structured into different layers, with dedicated Virtual Private Clouds (VPCs). These VPCs are linked through a transit gateway, allowing secure and smooth communication across different environments while keeping them isolated for better security and operational efficiency.

To protect against common online threats, a Web Application Firewall (WAF) and Load Balancer are positioned at the network’s edge. This setup ensures that all incoming traffic is inspected before it reaches internal services. For third-party integrations, a Point of Presence (PoP) is used, providing dedicated connectivity that not only improves performance but also enhances security by avoiding public internet routes.

An API Gateway helps manage secure communication between external components and internal services, while a Next-Generation Firewall offers advanced threat protection by inspecting traffic and blocking potential risks. Additionally, access to the cloud infrastructure is tightly controlled with a Zero Trust Network Security (ZTNS) proxy, enforcing identity verification and continuous monitoring for all users, including hotel staff and subcontractors. Remote staff and subcontractors connect securely through a VPN, ensuring encrypted communication from external locations.

The Management VPC is specifically designed for administrative tasks. It includes a bastion host for controlled access, a Privileged Access Management (PAM) system to handle elevated permissions, and a vulnerability scanning proxy to regularly assess and mitigate potential risks.

The Production VPC hosts live applications (HMS and SMS), using Red Hat OpenShift to guarantee scalability and reliable performance. By keeping the production environment separate from development and testing, the architecture ensures that any changes or new features are thoroughly tested before they go live, minimizing the risk of issues in the production system.

At the base of the architecture, the cloud services layer includes essential components such as DNS services, monitoring tools, and a Security Information, Event Management (SIEM) system, AWS shield, and. These tools are key to keeping the system running smoothly, tracking performance, and identifying potential threats in real-time. The inclusion of Kafka for event streaming enables the collection of logs and telemetry data, which are then analysed by TeslaDetect.

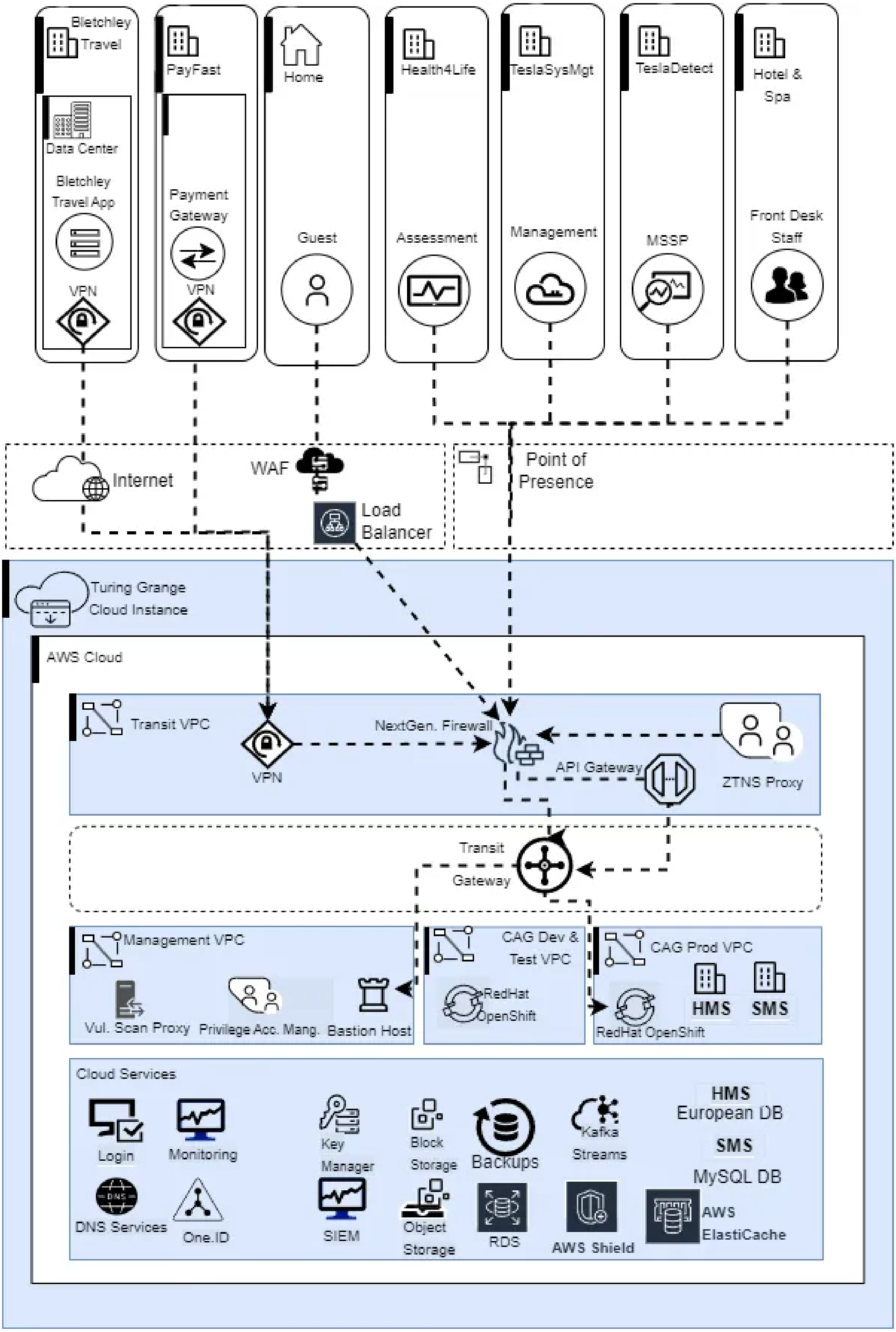

Bletchley Travel
Data Center
Bletchley Travel App
VPN
PayFast
Payment Gateway
VPN
Home
Guest
Health4Life
Assessment
TeslaSysMgt
Management
TeslaDetect
MSSP
Hotel & Spa
Front Desk Staff
Internet
WAF
Load Balancer
Point of Presence
Turing Grange Cloud Instance
AWS Cloud
Transit VPC
VPN
NextGen. Firewall
API Gateway
ZTNS Proxy
Transit Gateway
Management VPC
Vul. Scan Proxy
Privilege Acc. Mang.
Bastion Host
CAG Dev & Test VPC
RedHat OpenShift
CAG Prod VPC
HMS
SMS
RedHat OpenShift
Cloud Services
Login
Monitoring
Key Manager
Block Storage
Backups
Kafka Streams
HMS
European DB
SMS
MySQL DB
DNS Services
One.ID
SIEM
Object Storage
RDS
AWS Shield
AWS ElastiCache

Figure 3.3. Deployment Architecture Diagram

4. Governance Appendix:

4.1. Viability Assessment (RAID log): [8]

The RAID log highlights crucial areas of concern for the HMS and SMS deployment, including risks related to network segmentation, incomplete encryption, and undefined security controls. Assumptions regarding the stability of Kafka, secure configurations of cloud services, and isolated environments for development require validation to mitigate future vulnerabilities. Issues such as a lack of monitoring, incident response, and disaster recovery plans expose the system to operational risks. Dependencies on AWS, Health4Life, and PayFast emphasize the importance of external compliance and service reliability. Addressing these risks and dependencies is essential for maintaining system security, continuity, and performance.

Table4.1. Viability Assessment (RAID log)

RAID	Statement	Action	Owner & Date
R. 1	Lack of network segmentation increases the risk of a breach, exposing sensitive data like customer, payment, and health information.	1. Segment the network into distinct zones (e.g., public-facing services, internal HMS and SMS, database layers, and administrative zones) 2. Use Virtual Private Clouds (VPCs) and subnets provided by the AWS public cloud provider 3. Ensure that critical systems (e.g., payment systems, databases) are isolated from general user access.	TeslaOps Security Manager By: Week 1
R. 2	Security controls were not defined before installation of equipment, leading to weak access controls, poor network security, and misalignment with standards.	1. Perform an immediate security audit to assess the existing network security, access controls, and overall system architecture 2. Compare current configurations with industry standards (e.g., NIST) to identify divergences.	External Compliance Officer (CISO)/ TelsaDetect By: Week 2
R. 3	There is a risk that incomplete encryption for data in transit and at rest may expose sensitive customer information, leading to potential data breaches and regulatory violations.	1. Review all data flows across the system, including between the HMS, SMS, databases, and external services 2. Identify sensitive data (customer records, payment info, health data) and verify whether encryption is applied 3. Ensure all data transmitted over the network is encrypted using secure protocols such as TLS. 4. For APIs, ensure they use HTTPS or encrypted tunnels 5. Enable full-disk encryption (FDE) on servers and storage storing sensitive data (e.g., backups).	TeslaOps IT Security team By: Week 3
A. 1	It is assumed that AWS will provide DDoS protection via AWS Shield and ensure effective traffic	1. Verify AWS Shield protection and load balancer setup for traffic distribution. 2. Ensure auto-scaling is enabled to handle traffic surges.	AWS Cloud Administrator

	distribution through load balancers to maintain availability and performance.	3. Conduct periodic stress tests to assess performance under peak load.	
A. 2	It is assumed that the Kafka streaming setup between SMS, RDS, and TeslaDetect will remain stable under peak load.	1. Conduct regular load testing on Kafka to ensure it handles peak traffic. 2. Set up performance monitoring and alerts for Kafka brokers to detect anomalies early. 3. Optimize producer-consumer configurations for scalability.	TeslaDetect Operations Lead By: Week 2
A. 3	It is assumed that a separate environment exists for development, testing, and deployment of HMS and SMS to prevent untested components from being deployed directly into production, reducing risks of service disruptions and vulnerabilities.	1. Verify that a separate, isolated environment exists. 2. Ensure that it is configured with proper security controls and access restrictions 3. ensure that Red Hat OpenShift is used to manage Dev and Test, and Deployment environments, enabling scalability, and resource management.	AWS Cloud Administrator By: Week 3
I. 1	Monitoring and incident response details are unclear, causing a rise in delays to detection of threats and resolution. This could further escalate, causing harm before effective action is taken.	1. Develop a detailed incident response plan (IRP) that outlines procedure for identifying, assessing, and responding to various types of security incidents. 2. Define incident categories and ensure that response actions are proportionate to the severity of the incident. 3. Create templates for incident reports, allowing the response team to quickly document events.	TeslaDetect Incident Response Team By: Week 2
I. 2	There's no backup or disaster recovery plan for HMS and SMS data. Without it, a system failure or ransomware attack could result in data loss and major disruptions to operations.	1. Set up automatic, regular backups for HMS and SMS data, including system logs. 2. Store backups in multiple locations, such as both on-premises and in the cloud 3. The DR plan should include detailed steps for restoring data from backups, bringing services back online, and minimizing downtime	TeslaOps IT Admin and TeslaDetect Incident Response Team By: Week 3
D. 1	The project depends on the cloud provider (AWS Cloud) for hosting HMS and SMS. The provider must offer essential security controls, like	1. Verify that AWS provides the necessary encryption options for both data at rest and data in transit. 2. Verify AWS compliance with important security and privacy regulations 3. Ensure that AWS's shared responsibility model is clearly understood.	AWS Cloud Administrator By: Week 1

	encryption, IAM, and threat detection.		
D. 2	Health4Life and PayFast are vital for SMS functionality. Any security breach in these services could disrupt health assessments and payments, impacting the system's overall performance and data integrity	1. Request security certification and compliance document to confirm adherence to industry standards. 2. Ensure both services provide contractual guarantees for security and compliance. 3. Enforce end-to-end encryption for all communications between SMS, Health4Life, and PayFast. 4. Validate the use of secure API keys	Legal & Compliance Manager/Program manager By: Week 4

4.2. Architectural Decision Record:

An Architectural Decision Record (ADR) documents significant technical decisions made during a project, outlining context, options, and rationale. In this case, ADR01 focuses on adding AWS Shield and a load balancer to protect from DDoS attacks and improve availability and usability.

Table 4.2. Architectural Decision Record

Subject area		Application Security
Decision title		Integration of Load Balancer and AWS Shield for better security
Description		Deploy a cloud-based load balancer to manage traffic distribution across HMS, SMS, and RDS, ensuring system availability, reliability, and DDoS mitigation.
Problem statement		High traffic volumes and uneven load distribution may result in significant performance degradation, while Distributed Denial of Service (DDoS) attacks have the potential to overload the system, causing service outages and operational disruptions.
Assumptions		It is assumed that AWS Shield provides DDoS protection, automatic scaling, and HTTPS termination for secure and efficient traffic handling.
Motivation		Implementing a load balancer with AWS Shield improves performance, availability, and resilience against malicious traffic, ensuring continuous service.
Alternative #1	**Description**	**Implement AWS Shield (Standard) and Load Balancer as part of the initial deployment.**
	Advantages	• Cost-efficient since AWS includes basic DDoS protection. • Requires minimal configuration, native AWS support. • Offers built-in scalability and automatic traffic management.

	Disadvantages	• Basic protection may be insufficient against advanced Layer 7 attacks. • Limited effectiveness for large-scale or prolonged attacks. • No compensation for downtime caused by DDoS incidents.
	Expected effort/cost	Low initial cost with minimal setup effort.
Alternative #2	**Description**	**Third-party services like Cloudflare CDN and Cloudflare WAF for enhanced DDoS mitigation and web application protection**
	Advantages	• Provides continuous DDoS mitigation for Layers 3, 4, and 7. • Enhances user experience with a global CDN, reducing latency. • Offers advanced WAF configurations for targeted application protection. • Additional features such as bot management and rate limiting.
	Disadvantages	• Integration effort needed to align with existing AWS infrastructure. • Recurring subscription costs for premium Cloudflare services. • Lacks direct integration with TeslaDetect, necessitating a custom logging configuration.
	Expected effort/cost	Moderate to high, depending on the subscription cost.
Alternative #3	**Description**	**Deploy AWS WAF independently, without a load balancer**
	Advantages	• Low infrastructure requirements with minimal operational overhead. • Easy setup with minimal configuration effort. • Seamless integration with AWS services for efficient management.
	Disadvantages	• Limited DDoS protection against large-scale or complex attacks. • AWS WAF is designed for Layer 7 protection and may be less effective against Layer 3/4 DDoS attacks.
	Expected effort/cost	Provided by the AWS
Decision		**Adopt AWS Shield Standard along with load balancer for initial deployment**
Justification		Both offer a low-cost solution with built-in protection for initial deployment. As traffic increases or more advanced attacks emerge, Cloudflare's services can be added to improve security and performance.

Consequences	• Basic protection is ensured initially, with scaling needed for high traffic or complex attacks. • Integration of Cloudflare or AWS Shield Advanced may incur additional costs. • Regular monitoring and reviews are crucial for maintaining security. • Upgrading can enhance protection but may add complexity.
Derived requirements	• Enable TeslaDetect for real-time monitoring and threat detection. • future integration option for enhanced security and performance • Ensure redundancy and auto-scaling to maintain continuous service uptime
Related decisions	none

References

[1] E. Moyle and D. Kelley, "Practical Cybersecurity Architecture: A guide to creating and implementing robust designs for cybersecurity architects," Birmingham: Packt Publishing, 2020. [Online]. Available: https://cdn.ttgtmedia.com/rms/pdf/bookshelf_cybersecurity_architecture_excerpt.pdf

[2] E. Woods and N. Rozanski, "The System Context Architectural Viewpoint," presented at the 7th Working IEEE/IFIP Conference on Software Architecture (WICSA 2009), Cambridge, UK, Sep. 2009. [Online]. Available: https://www.eoinwoods.info/media/writing/WICSA2009-context-view-paper.pdf

[3] National Institute of Standards and Technology, *The NIST Cybersecurity Framework (CSF) 2.0*, NIST CSWP 29, Feb. 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[3] B. Khamayseh, N. Arman, and F. Khamayseh, "Security Requirements Classification into Functional and Non-functional," Proceedings of the 35th IBIMA Conference, Seville, Spain, Apr. 2020. [Online]. Available: https://scholar.ppu.edu/bitstream/handle/123456789/8872/Paper_IBIMA%20Conference.pdf?sequence=1

[3] A. Mellado, E. Fernández-Medina, and M. Piattini, "Examination and Classification of Security Requirements of Software Systems," *Proceedings of the International Conference on Computational Science and Its Applications (ICCSA 2006)*, Glasgow, UK, May 2006. [Online]. Available: https://ieeexplore.ieee.org/document/1684851

[4] J. Choi, J. Kim, and L. D. T. Khanh, "Software Analysis Models for SafeHome Project," KAIST, Daejeon, South Korea, Mar. 2009. [Online]. Available: https://swtv.kaist.ac.kr/courses/cs350-15/t4-analysis-model.pdf

[4] [Swimlane]E. Moyle and D. Kelley, Practical Cybersecurity Architecture. Packt Publishing, Oct. 2020. [Online]. Available: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=746a490f85d52c7c310a853a80629a35bbea926c

[5] IBM, "IBM Design Language," [Online]. Available: https://www.ibm.com/design/language/.

[5] A. Islam, S. Mazumder, and K. Andersson, "A systematic security assessment for smart manufacturing industry," *Journal of Cyber Security Technology*, vol. 4, no. 1, pp. 12–27, Dec. 2020. [Online]. Available: https://www.tandfonline.com/doi/full/10.1080/19393555.2020.1853855.

[6] OWASP Foundation, "OWASP Top Ten," [Online]. Available: https://owasp.org/www-project-top-ten/.

[6]J. Williams, "OWASP Risk Rating Methodology," OWASP Foundation. [Online]. Available: https://owasp.org/www-community/OWASP_Risk_Rating_Methodology.

[7] A. Al-Dhaheri, M. A. Serhani, and R. Dssouli, "Cloudifying Apps—A Study of Design and Architectural Considerations for Developing Cloud-enabled Applications with Case Study," *2014 IEEE/ACS 11th International Conference on Computer Systems and Applications (AICCSA)*, Doha, Qatar, Nov. 2014, pp. 270–277. [Online]. Available: https://ieeexplore.ieee.org/document/7015487

[7] S. Sharma, "Fortifying Network Integrity by Implementing Palo Alto's Zero Trust Model and Advanced Firewall Segmentation," ResearchGate, 2023. [Online]. Available: https://www.researchgate.net/publication/386424608_Fortifying_Network_Integrity_by_Implementing_Palo_Alto's_Zero_Trust_Model_and_Advanced_Firewall_Segmentation

Amazon Web Services, Inc., "AWS Well-Architected Framework," [Online]. Available: https://aws.amazon.com/architecture/well-architected/.

[8] J. Simonovic, "What Is a RAID Log? Benefits, Examples & Free Template," Plaky Learn, Oct. 2023. [Online]. Available: https://plaky.com/learn/project-management/raid-log/.

[8] J. Broome, "Architecture Decision Records," endjin blog, Jul. 2023. [Online]. Available: https://endjin.com/blog/2023/07/architecture-decision-records.

[8] M. Zimmermann, M. Wurster, and S. Wagner, "Using Architecture Decision Records in Open Source Projects—An MSR Study on GitHub," *IEEE Software*, vol. 41, no. 1, pp. 56–63, Jan.–Feb. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10155430.