**Executive Summary**

**Summary of Completed Tasks**

In the previous assessment, a thorough investigation was carried out into the security and backup-recovery procedures of the Online Shopping System (OSS). Our analysis involved a detailed examination of the system’s structure and operations to identify any security vulnerabilities that could compromise its integrity. We also evaluated the backup plans in place to ensure the system's resilience in the face of unexpected events or data loss. Additionally, we reviewed the system's compliance with GDPR security regulations to ensure the safeguarding of user data. (Al-Khayyal et al., 2020)

**Key Findings (Non-Technical Summary)**

**Security Vulnerabilities:**  
The system's password policies are insufficient, failing to meet the required standards for strong authentication. Outdated software components pose a significant risk, making the system vulnerable to exploitation. Furthermore, data transmission encryption is inadequate, exposing sensitive information to potential interception. Addressing these issues is critical to ensuring the security of the system and protecting the data it processes. (Hanif & Lallie, 2021)

A graph of strength distribution

Description automatically generated

**Password Strength Distribution** – A chart to show percentages of weak, medium, and strong passwords.

**Backup and Recovery Weaknesses:**  
The current backup system is unreliable, frequently encountering errors that put critical data at risk of loss or corruption. The absence of failover mechanisms and failure to meet modern security standards further weaken the system’s reliability. Additionally, the lack of regular testing hinders seamless recovery and could result in significant operational disruptions. Immediate action is necessary to improve backup processes and safeguard data integrity. (Chetioui et al., 2021)

A graph with a line

Description automatically generated

**Backup Testing Success Rate Over Time** – A time series chart with monthly data points to reflect backup testing outcomes.

**Assessment:**  
Open-source software (OSS) faces a wide array of security threats, both internal and external. These vulnerabilities could lead to severe business disruptions, including data breaches or losses. Proactively addressing these risks is essential to protecting the integrity of the organisation’s information assets.

A graph of different colored squares

Description automatically generated

**Component Version Comparison** – A chart to compare current (outdated) and latest versions for Web Server and Database components.

**Evaluation Against Security Standards**

The system’s current data protection measures, including encryption and consent mechanisms, fall short of GDPR compliance. Failure to address this promptly could result in serious repercussions. Immediate action is required to review and improve data protection methods to ensure user privacy and regulatory compliance.

**ISO/IEC 27001 Compliance:**  
The system does not meet the necessary standards for risk management and disaster recovery planning. Critical aspects such as data integrity and encryption are insufficient, falling short of ISO/IEC 27001 standards. To comply with these global information security standards, the organisation must prioritise risk management and disaster recovery strategies, ensuring robust data integrity and secure encryption mechanisms. (Hanif & Lallie, 2021)

**Backup and Recovery Plan**

A comprehensive and carefully implemented backup and recovery plan is essential to ensure the continuity of OSS. Key elements include data backups, redundancy, disaster recovery strategies, and proactive monitoring. Implementing a robust backup system will safeguard OSS resources, ensure minimal downtime, and enable rapid recovery from disruptions, enhancing business continuity and stakeholder trust. (Akour et al., 2022)

**Primary and Backup Servers:**  
To ensure continuous service during primary server outages, backup servers must be deployed to provide real-time failover. This will mitigate the risk of service interruptions caused by server failures.

**Backup Storage Technologies:**  
A combination of Hard Disk Drives (HDDs) for fast backup and Magnetic Optical Disks (MODs) for long-term, reliable storage is recommended. HDDs ensure quick data retrieval, while MODs maintain data integrity over extended periods, providing a robust backup solution. (Omolara et al., 2022)

Regular testing and monitoring of the backup system is vital to identify weaknesses, ensure recoverability, and detect potential threats. Mission-critical redundancy and monitoring logs are essential for maintaining backup integrity and preventing data loss.

A diagram of a security standards

Description automatically generated

**Compliance Scores** – A chart to visualize compliance scores for Encryption, Data Recovery, and Access Control.

**Conclusions**

Without significant improvements to the security and backup measures, OSS remains vulnerable to threats that could compromise sensitive information and system integrity. Failure to comply with GDPR and ISO/IEC 27001 standards not only exposes the system to legal risks but also threatens its operational stability.

Urgent action is required to establish a robust, well-monitored backup strategy to safeguard data integrity and ensure uninterrupted service. Proactively addressing these vulnerabilities will improve security, mitigate risks, and foster long-term system resilience. (Tran, 2020)

A diagram of a risk matrix

Description automatically generated

Risk Matrix: Severity vs Likelihood - Using numerical values to represent severity in the heatmap, with the risks annotated separately. Below is the updated risk matrix

**Recommendations (Ordered by Priority)**

1. **Strengthen Data Encryption:** Implement end-to-end encryption for all data to meet GDPR requirements. This is a critical priority.
2. **Implement Backup and Failover Systems:** Establish a failover mechanism with a secondary backup server to ensure continuity during primary server failures.
3. **Update Password and Access Controls:** Enforce stricter password policies and improve access controls to reduce security risks.
4. **Regular Backup Testing and Monitoring:** Continuously monitor and test backup systems to ensure their reliability and prevent data loss.
5. **GDPR Compliance:** Implement proper user consent mechanisms to comply with GDPR regulations.

These recommendations are prioritised based on their impact on business continuity, legal compliance, and customer trust.

**References**

Al-Khayyal, A., Alshurideh, M., Al Kurdi, B., & Aburayya, A., 2020. *The impact of electronic service quality dimensions on customers’ e-shopping and e-loyalty via the impact of e-satisfaction and e-trust: A qualitative approach*. International Journal of Innovation, Creativity and Change, 14(9), pp.257-281.

Hanif, Y., & Lallie, H. S., 2021. *Security factors on the intention to use mobile banking applications in the UK older generation (55+)*. Technology in Society.

Chetioui, Y., Lebdaoui, H., & Chetioui, H., 2021. *Factors influencing consumer attitudes toward online shopping: the mediating effect of trust*. EuroMed Journal of Business.

Akour, I., Alnazzawi, N., Alshurideh, M., Almaiah, M. A., Al Kurdi, B., Alfaisal, R. M., & Salloum, S., 2022. *A conceptual model for investigating the effect of privacy concerns on E-commerce adoption*. Electronics, 11(22), p.3648.

Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H., 2022. *The internet of things security: A survey encompassing unexplored areas and new insights*. Computers & Security, 112, p.102494.

Tran, V. D., 2020. *The relationship among product risk, perceived satisfaction and purchase intentions for online shopping*. The Journal of Asian Finance, Economics and Business, 7(6), pp.221-231.