Task 2 Quality Requirements(USU Operating System)

Introduction

This analysis was covered up for the USU Operating System, a platform used by USU Officers to regulate federation level activities.

Regarding software quality, information security, accessibility and cloud computing, the criteria are in line with accepted worldwide standards. By addressing the aspects of dependability, performance, usability, security, and compliance, they make sure that the USU-OS not only serves its intended function but also provides a long-term, user-centred, secure service.

Reliability and Availability

- The USU Operating System (USU-OS) shall maintain **annual uptime ≥ 99.95%**, ensuring continuity of nationwide student union operations.
- System failures are required to be recoverable within **two hours** for minor incidents and **six hours** for major failures, consistent with international software quality expectations.
- A **disaster recovery mechanism** shall be in place, including automated data replication across multiple regions, to ensure resilience against catastrophic failure (IBM, 2023).

Performance and Scalability

- The system is expected to support **at least 500 concurrent USU Officers** without performance degradation, aligning with performance efficiency standards.
- Routine tasks (e.g., event creation, membership approvals) shall complete in **≤ 3 seconds**, reflecting established usability thresholds (Nielsen Norman Group, 2023).
- The architecture shall be **scalable** to accommodate **200% growth in participating unions** within five years, in line with cloud application scalability guidance.

Usability and Accessibility

- The USU-OS interface has to conform to **WCAG 2.1 Level AA** accessibility standards, ensuring inclusivity for officers with disabilities (W3C, 2018).
- Training for new officers shall require **no more than two hours**, demonstrating system learnability and intuitive design.
- The interface shall provide **multi-language support**, with English as the default and Welsh plus EU languages available for inclusivity.

Security and Data Protection

- The system should implement **role-based access control (RBAC)**, restricting critical operations to authorised personnel only.
- All data transmissions must use **end-to-end encryption (AES-256 or equivalent)**, ensuring confidentiality and compliance with GDPR.
- Regular **penetration tests and vulnerability scans** shall be performed to safeguard system integrity and prevent exploitation.

Compliance and Auditability

- The system shall comply fully with **UK GDPR** and the **Data Protection Act 2018**, ensuring lawful processing of personal data.
- **Audit logs** should be maintained for at least **five years**, documenting officer activities (e.g., event approvals, membership changes).
- Logs must be **tamper-proof, exportable, and analysable**, ensuring transparency and accountability during internal or external audits.

References

- IBM (2023) *Disaster recovery and business continuity*. Available at: https://www.ibm.com/topics/disaster-recovery
- Nielsen Norman Group (2023) *Response time limits: Usability guidelines*. Available at: https://www.nngroup.com/articles/response-times-3-important-limits/
- W3C (2018) *Web Content Accessibility Guidelines (WCAG) 2.1*. Available at: https://www.w3.org/TR/WCAG21/