The USU Membership System is a secure, web-based application hosted on cloud servers, used for administrative purposes, that allows USU officers to approve/ reject their membership applications that are submitted by university-specific student unions. This makes it a multi-tenant SaaS architecture, as it is a single logical software used to serve multiple customers (the students). [i]  
The table below shows measurable quality requirements for this subsystem, that finds which quality characteristics should be taken into consideration when you are evaluating the properties of a software’s effectiveness[ii]

Each requirement below follows Rick Kazmans six part framework for quality analysis. Identifying source(USU officer), stimulus (event), artifact (USU Operating system), environment (Cloud platform), system response, and the measurable outcome.

Situation Under Study:

The USU OS allows authorized USU Officers to log in, review, and approve/reject membership applications from the authorized university student unions.

- Platform: Secure cloud-hosted web application.

- Users: USU Officers (authorized), Students

- Typical usage: Most usage at the start of each academic semester.

- Backend: Cloud database and REST API with role-based access control.

Stakeholders, Assets, and Risks:

Stakeholders – USU Officer (primary), System Administrator (supporting), Student Applicant (external)

Assets – Membership records, officer credentials, access logs, approval history

Risks – Unauthorised access, data breaches, downtime, and degraded performance under a heavy amount of traffic.

Security & Privacy

Scenario and description

Security is the protection against intentional subversion or forced failure. [viii]Only the authorised USU officers should be able to view the details, approve, or modify membership applications, ensuring all data remains confidential. As there could be sensitive information, such as names, student IDs, contacts, or IP addresses, login times and system actions which can reveal user behaviour patterns, this is considered personal data under GDPR.[iii] Therefore All transmitted and stored data (names, contacts, student IDs) Therefore data must be stored and encrypted using AES-256 for data at rest and TLS 1.3 for data in transmission following what the UK National Cyber Security centre recommends.

Metric and measure

Access control logs(An automated system that records who accessed what to help detect suspicious activity)

-encryption level(measures how strongly your data is encrypted and what key strength you use)

The number of unauthorised access attempts per year. Which are all metrics consistent with CyberSecurity KPIs for 2025 [v]

Target/ Goal

Aiming for 0 unauthorised access incidents per year.100% of data transmission logged and reviewed every month.(HTTPS/TLS). Must be encrypted using AES-256 for stored data TLS 1.3 standards as recommended by the National cybersecurity official website for secure protocols and protecting data in transit.[vi]

Verification

Perform penetration testing to detect vulnerabilities.

Confirm that the security updates are applied within 30 days of its release.

Conduct monthly access-control audits and possible log reviews too.

Performance

Scenario/Description

The performance is the degree to which a system/ component accomplishes its designated functions within given constraints; such as speed, accuracy or memory usage. [vii]The system should be able to process the users membership approvals quickly and efficiently, even under high usage and pressure, ensuring a minimum waiting time for USU officers. Linking to performance efficiency. [vi]

Metric/ Measure

Average server response time and maximum number of users before the system slows down, so should have low latency.

Target/Goal

Software quality must consider usability and responsiveness as user expectations rise. <=3 seconds average response time with up to 100 users meets the standard of the performance.

Verification

Conduct stress tests during peak periods to see if response times are <= 3 seconds. Perform load testing (100 people) to see how the system will run below 3 seconds and also find it’s breaking point to set limits on user activity.

Reliability

Scenario/Description

The approval service must be able to operate continuously with minimal downtime and service interruptions all year round. It is the isolation of failure to reduce societal risk.[vi] Ensures USU officers can always access the membership approval system when needed which reduces the risk to the reputation of the university.

Metric/Measure

Mean Time Between Failures (MTBF).

-Probability of failure on demand (e.g for one in every 1000 requests a service fails: FPD = 0.001

Target/Goal

≥ 99.9% system uptime; MTBF > 300 hours between service interruptions. [IIIX]

Verification

Record all the failure incidents and the recovery duration to calulate MTBF and MTTRand check that they are in the limit of the target/goal. Monitor the availability by doing 1-MTBF.

Scalability

Scenario/Description

Scalability is the ability to adjust the scale of the system depending on administrative, functional, geographic, load, generational and heterogenous factors. The USU Operation System should maintain performance as more university unions and student members are added and when the system expands to other users. (Administrative scalability). There is also functional scalability which is the ability to enhance the system by adding new functionality.

Metric/Measure

Maximum number of unions supported before response time degrades by >10%.

Target/Goals

System must support at least 500 active universities and 50,000 users without performance loss.

Verification

Perform stress and load tests with simulated traffic from 50,000 users.

Justification Paragraph

These quality requirements help to make sure that the USU OS runs securely, efficiently, and reliably across its cloud-based environment. By applying strong encryption and strict access controls, the system protects the user’s personal data and meets the security expectations set out by ISO/IEC 25010. Also, setting a performance target of around three seconds for each transaction keeps the system responsive for users

The reliability target of at least 99.9 percent uptime is similar to the standards used in commercial cloud SLAs. This makes sure users can access the system consistently throughout the year. Scalability is also important as the USU grows, as the platform needs to handle more student unions and members without slowing down or losing functionality. These metrics are shown through Engineering Council AHEP4 outcomes C3, C5 and C6 by focusing on system dependability, security, and long-term sustainability. My Quality targets also support the use case scenarios discussed in Lecture 3, by making sure the Approve Membership process remains secure and responsive under real life user conditions.

References

[i] Complete Guide to Multi-Tenant Architecture, Seetharamugn, Oct 1, 2024

[ii]ISO 25000 official site, ISO/IEC 25010, date:unknown

[iii] GDPR.EU official website,What is considered personal data under the EU GDPR?

[vi] National Cyber Security Center UK

[v] SecurityScorecard (2025) *20 Cybersecurity Metrics & KPIs to Track in 2025*

*[vi]* *Lecture 2 – Software Quality (Oxford Brookes University, 2025)*

*[vii] [ISO/IEC/IEEE 24765:2017]*

*[viii] [ISO/IEC/IEEE 15288:2015, Systems and software engineering – System life cycle processes, 4.1.41]*

*[iiiX] BMC Helix. (2024) Service Level Agreement (SLA) Examples and Template.*