### Assurance Case for Security of Instant Messaging (IM) Software

\*\*Goal 1: Ensure the instant messaging software provides confidentiality, integrity, and availability\*\*

- \*\*Strategy 1.1: Demonstrate that the IM software implements appropriate security controls\*\*

- \*\*Goal 1.1.1: Prove that all communications are encrypted\*\*

- \*\*Evidence 1.1.1.1:\*\* Certificates of encryption protocols used (e.g., TLS, SSL)

- \*\*Evidence 1.1.1.2:\*\* Security audit logs showing encryption in action

- \*\*Goal 1.1.2: Show that access controls are in place and effective\*\*

- \*\*Evidence 1.1.2.1:\*\* Documentation of access control policies

- \*\*Evidence 1.1.2.2:\*\* Audit report of access control implementations

- \*\*Goal 1.1.3: Ensure data integrity mechanisms are utilized\*\*

- \*\*Evidence 1.1.3.1:\*\* Use of MD5 or SHA hash functions

- \*\*Evidence 1.1.3.2:\*\* Hash check validation reports

- \*\*Strategy 1.2: Validate the implementation of security best practices and standards\*\*

- \*\*Goal 1.2.1: Ensures software compliance with standards such as ISO/IEC 27001\*\*

- \*\*Evidence 1.2.1.1:\*\* Certification of compliance with ISO/IEC 27001

- \*\*Evidence 1.2.1.2:\*\* Latest compliance audit results

- \*\*Goal 1.2.2: Conduct regular security audits and penetration testing\*\*

- \*\*Evidence 1.2.2.1:\*\* Schedule and records of past security audits

- \*\*Evidence 1.2.2.2:\*\* Penetration testing reports

- \*\*Strategy 1.3: Ensure robustness against common security threats\*\*

- \*\*Goal 1.3.1: Protect against data breaches\*\*

- \*\*Evidence 1.3.1.1:\*\* Incident response plans

- \*\*Evidence 1.3.1.2:\*\* Historical data on incident handling and outcomes

- \*\*Goal 1.3.2: Defend against Denial of Service (DoS) attacks\*\*

- \*\*Evidence 1.3.2.1:\*\* DDoS mitigation tools and techniques in use

- \*\*Evidence 1.3.2.2:\*\* Records of uptime and any related DoS incidents

- \*\*Strategy 1.4: Incorporate user training on security practices\*\*

- \*\*Goal 1.4.1: Ensure all users are aware of security policies and practices\*\*

- \*\*Evidence 1.4.1.1:\*\* Training logs and materials

- \*\*Evidence 1.4.1.2:\*\* Feedback and assessments of user understanding

\*\*Goal 2: Ensure compliance with relevant data protection laws and privacy standards\*\*

- \*\*Strategy 2.1: Adhere to international and national regulations such as GDPR\*\*

- \*\*Goal 2.1.1: Audit and certify data handling processes comply with GDPR\*\*

- \*\*Evidence 2.1.1.1:\*\* GDPR compliance certificate

- \*\*Evidence 2.1.1.2:\*\* Privacy Impact Assessment report

- \*\*Goal 2.1.2: Maintain transparency in data processing and user data rights\*\*

- \*\*Evidence 2.1.2.1:\*\* Publicly available privacy policy

- \*\*Evidence 2.1.2.2:\*\* Logs of user data access and corrections requests

- \*\*Strategy 2.2: Implement continuous monitoring and updates to privacy protection measures\*\*

- \*\*Goal 2.2.1: Regular updates to privacy policies and procedures\*\*

- \*\*Evidence 2.2.1.1:\*\* Change logs for privacy policies

- \*\*Evidence 2.2.1.2:\*\* Stakeholder communication records

- \*\*Goal 2.2.2: Conduct periodic reviews and updates of security policies regarding data protection\*\*

- \*\*Evidence 2.2.2.1:\*\* Review records

- \*\*Evidence 2.2.2.2:\*\* Update implementation records

This tree structure outlines major goals, strategies, and evidences to assure the security and compliance of IM software. Each leaf node (evidence) supports the corresponding goal directly above it, ensuring a comprehensible and traceable assurance case.