Sure, here’s an example of a security assurance case for Instant Messaging (IM) software using Goal Structuring Notation (GSN) in a hierarchical tree format:

1. \*\*G1: Ensure Security of Instant Messaging (IM) Software\*\*

- 1.1 \*\*C1: IM software is widely used in sensitive communication\*\*

- 1.2 \*\*S1: Security best practices for IM software\*\*

- 1.3 \*\*S2: Security threats to IM software\*\*

2. \*\*G2: Protect Communication Data\*\*

- 2.1 \*\*S3: Importance of data security for users\*\*

- 2.2 \*\*S4: Data protection regulations\*\*

- 2.3 \*\*G2.1: Ensure End-to-End Encryption (E2EE)\*\*

- 2.3.1 \*\*S5: Benefits of E2EE\*\*

- 2.3.2 \*\*Sn2: Limitations of E2EE\*\*

- 2.3.3 \*\*Sn3: E2EE Industry standards\*\*

- 2.4 \*\*G2.2: Secure Storage of Messages\*\*

- 2.4.1 \*\*S6: Risks of data breaches\*\*

- 2.4.2 \*\*Cnt1: Use of secure storage technologies\*\*

- 2.5 \*\*G2.3: Protect Metadata\*\*

- 2.5.1 \*\*S7: Importance of metadata protection\*\*

- 2.5.2 \*\*Sol1: Anonymization of metadata\*\*

3. \*\*G3: Ensure Secure Authentication\*\*

- 3.1 \*\*C2: Need for user authentication\*\*

- 3.2 \*\*G3.1: Strong User Authentication Mechanism\*\*

- 3.2.1 \*\*S8: Two-Factor Authentication (2FA)\*\*

- 3.2.2 \*\*S9: Biometric authentication\*\*

- 3.3 \*\*G3.2: Mitigate Authentication Vulnerabilities\*\*

- 3.3.1 \*\*S10: Common vulnerabilities in authentication systems\*\*

- 3.3.2 \*\*S11: Countermeasures for vulnerabilities\*\*

4. \*\*G4: Maintain Software Integrity\*\*

- 4.1 \*\*S12: Risks of software tampering\*\*

- 4.2 \*\*G4.1: Secure Software Updates\*\*

- 4.2.1 \*\*S13: Importance of updating software\*\*

- 4.2.2 \*\*Sol2: Use of signed updates\*\*

- 4.3 \*\*G4.2: Protect Against Malware\*\*

- 4.3.1 \*\*S14: Common malware types targeting IM software\*\*

- 4.3.2 \*\*Cnt2: Use of anti-malware technologies\*\*

5. \*\*G5: Provide User Awareness and Training\*\*

- 5.1 \*\*C3: Users as a critical line of defense\*\*

- 5.2 \*\*G5.1: Inform Users About Security Best Practices\*\*

- 5.2.1 \*\*S15: Importance of user awareness\*\*

- 5.2.2 \*\*Sol3: User guides and tutorials\*\*

- 5.3 \*\*G5.2: Conduct Regular Security Training\*\*

- 5.3.1 \*\*S16: Benefits of regular training\*\*

- 5.3.2 \*\*Sol4: Training Programs and Workshops\*\*

6. \*\*G6: Monitor and Respond to Security Incidents\*\*

- 6.1 \*\*S17: Need for incident response\*\*

- 6.2 \*\*G6.1: Implement Continuous Monitoring\*\*

- 6.2.1 \*\*S18: Importance of continuous monitoring\*\*

- 6.2.2 \*\*Sol5: Use of monitoring tools\*\*

- 6.3 \*\*G6.2: Develop Incident Response Plans\*\*

- 6.3.1 \*\*S19: Benefits of having response plans\*\*

- 6.3.2 \*\*Cnt3: Steps involved in incident response\*\*

Each of these goals, contexts, solutions, and strategies represent a part of the overall security assurance case to ensure that the IM software is secure.