To create a security case for Instant Messaging (IM) software, we will replace all placeholders in the provided security case pattern with specific information related to IM software. Here, I will illustrate how to apply the provided pattern by instantiating it specifically for an IM software product.

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

- \*\*G1: Instant Messaging Software is acceptably secure in Our System\*\*

- \*\*Contexts\*\*

- \*\*C1: Instant Messaging software allows real-time text transmission over the internet.\*\*

- \*\*C2: Our System includes servers and client applications on various devices.\*\*

- \*\*C3: Acceptably secure means meeting all specified security requirements including confidentiality, integrity, and availability.\*\*

- \*\*Strategy: S1 - Argument that IM software assets are under protection\*\*

- \*\*Justification: J1 - Protection of IM software assets supports that software is acceptably secure.\*\*

- \*\*Supported By\*\*

- \*\*G2: All identified IM software critical assets are protected\*\*

- \*\*Contexts\*\*

- \*\*C4: List of IM software critical assets includes user data, authentication information, and communication logs.\*\*

- \*\*Strategy: S2 - Respective arguments of IM software critical assets\*\*

- \*\*Justification: J2 - Relationship between IM software assets is clear and can be argued separately.\*\*

- \*\*Supported By\*\*

- \*\*G3: IM software critical asset "user data" is protected\*\*

- \*\*Strategy: S3 - Argument based on the type which the IM software critical asset belongs to\*\*

- \*\*Context\*\*

- \*\*C5: List of IM software critical asset types includes data types such as textual, multimedia, and metadata.\*\*

- \*\*Justification: J3 - Types of IM software assets are according to Personal Data Protection directives.\*\*

- \*\*Supported By\*\*

- \*\*G4: IM software critical asset "user data" which belongs to "textual" type is protected\*\* (Details on protection measures here)

- \*\*G4: IM software critical asset "user data" which belongs to "multimedia" type is protected\*\* (Details on protection measures here)

- \*\*G4: IM software critical asset "user data" which belongs to "metadata" type is protected\*\* (Details on protection measures here)

- \*\*...(Other G4 Goals for 4 total critical assets protected)\*\*

This hierarchical tree represents a specific instance of an assurance case for security of Instant Messaging software within a system, following the pattern provided and adapting it to include software-specific contexts and goals. The information is expanded at each level to provide detailed arguments supported by contexts and justifications, ensuring a comprehensive case for the security of the software. This is a simplified representation which can be extended with further details and evidence in practice.