To create the assurance case for Instant Messaging (IM) software using the provided security case pattern, follow the tree structure in Goal Structuring Notation after replacing the placeholders `{}` with specific information regarding the IM software.

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

1. \*\*Goal (G1, Instant Messaging (IM) software is acceptably secure in Operational Environment)\*\*

- Context (C1, Definition and description of Instant Messaging (IM) software)

- Context (C2, Definition and description of Operational Environment)

- Context (C3, Definition of what is meant by acceptably secure)

- \*\*Strategy (S1, Argument that IM software assets are under protection)\*\*

- Justification (J1, Protection of IM software assets supports that software is acceptably secure)

- \*\*Goal (G2, All identified IM software critical assets are protected)\*\*

- Context (C4, List of IM software critical assets)

- \*\*Strategy (S2, Respective arguments of IM software critical assets)\*\*

- Justification (J2, Relationship between assets is clear and can be argued separately)

- \*\*Goal (G3, IM software critical asset is protected)\*\*

- \*\*Strategy (S3, Argument by the type to which the IM software critical asset belongs)\*\*

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of software assets are according to PEDD)

- \*\*Goal (G4, IM software critical asset which belongs to the type Encryption Keys is protected)\*\*

- \*\*Goal (G4, IM software critical asset which belongs to the type User Data is protected)\*\*

- \*\*Goal (G4, IM software critical asset which belongs to the type Configuration Files is protected)\*\*

- \*\*Goal (G4, IM software critical asset which belongs to the type Authentication Data is protected)\*\*

### Hierarchical Tree Representation

```

- Goal (G1, Instant Messaging (IM) software is acceptably secure in Operational Environment)

- Context (C1, Definition and description of Instant Messaging (IM) software)

- Context (C2, Definition and description of Operational Environment)

- Context (C3, Definition of what is meant by acceptably secure)

- Strategy (S1, Argument that IM software assets are under protection)

- Justification (J1, Protection of IM software assets supports that software is acceptably secure)

- Goal (G2, All identified IM software critical assets are protected)

- Context (C4, List of IM software critical assets)

- Strategy (S2, Respective arguments of IM software critical assets)

- Justification (J2, Relationship between assets is clear and can be argued separately)

- Goal (G3, IM software critical asset is protected)

- Strategy (S3, Argument by the type to which the IM software critical asset belongs)

- Context (C5, List of IM software critical asset types in PEDD)

- Justification (J3, Types of software assets are according to PEDD)

- Goal (G4, IM software critical asset which belongs to the type Encryption Keys is protected)

- Goal (G4, IM software critical asset which belongs to the type User Data is protected)

- Goal (G4, IM software critical asset which belongs to the type Configuration Files is protected)

- Goal (G4, IM software critical asset which belongs to the type Authentication Data is protected)

```

This structure now effectively argues that the IM software is secure as per defined contexts and the protections applied to various critical assets.