Based on the given information and predicates for the assurance case pattern, here’s how you would instantiate a security case for Instant Messaging (IM) software, filling in the placeholders with specific information and developing the hierarchical tree structure as required:

```

Goal (G1, "IM software is acceptably secure in a corporate environment")

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

- Context (C2, "Definition and description of a corporate environment")

- Context (C3, "Definition of '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 of the type which the IM software critical asset belongs to")

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

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

- Goal (G4, "IM software critical asset which belongs to encryption type is protected")

- Goal (G4, "IM software critical asset which belongs to authentication type is protected")

- Goal (G4, "IM software critical asset which belongs to data storage type is protected")

- Goal (G4, "IM software critical asset which belongs to network communication type is protected")

```

Explanation:

1. \*\*Top-Level Goal (G1)\*\*: The primary objective, claiming that the IM software is acceptably secure in a specified environment (corporate environment), supported by specific contexts describing the software, environment, and the security criteria.

2. \*\*Strategy (S1)\*\*: Connects the top-level goal to its proofs, arguing that the assets of the IM software are well protected.

3. \*\*Subsequent Goals and Strategies\*\*:

- \*\*Goal (G2)\*\*: Focuses on the protection of all critical assets of the IM software. This goal is supported by strategies that break down the protection argument by asset type.

- \*\*Strategy (S2)\*\* and \*\*Goal (G3)\*\*: Further detail how each critical asset is protected.

- \*\*Strategy (S3)\*\*: Deals with categorizing assets by types, heavily contextualized by the organizational standards and industry definitions (PEDD).

4. \*\*Multiplicity\*\*:

- The strategy (S2) addresses each type of asset defined in context (C5) through multiple instances of goal (G4), each focusing on a different critical asset type such as encryption, authentication, data storage, and network communication.

This hierarchical representation encapsulates and visually represents the complexity and specificity needed in an assurance case and effectively shows how it supports the top-level claim.