Based on the provided security case pattern, here is a security case instantiated for an Instant Messaging (IM) software. Replacing placeholders and elaborating based on the domain information provided earlier:

```

G1: IM Software is acceptably secure in the operational environment

- C1: IM Software encompassing both internal structure and external manifestation

- C2: Operational Environment including servers and clients where IM software is deployed

- C3: Definition of "acceptably secure" entails complete protection of all critical assets against unauthorized access and data breaches

- S1: Argument that IM Software assets are under protection

- J1: Protection of software assets supports that IM software is acceptably secure

- G2: All identified IM software critical assets are protected

- C4: List of IM Software critical assets, which includes user account information, authentication information, login process, chat logs, registration information, and the registration process

- S2: Respective arguments of IM software critical assets

- J2: Relationship between assets is clear and can be argued separately

- G3: User account information is protected

- S3: Argument based on the type which the software critical asset belongs to

- C5: Types of assets according to PEDD classification: Process, Environment Entity, Data Exchange, Data Storage

- J3: Types of software assets are according to PEDD

- G4: Registration information, a type of Data Storage, is protected

- G4: Authentication information, a type of Data Exchange, is protected

- G4: Login process, a type of Process, is protected

- G4: Chat logs, a type of Data Storage, is protected

- G3: Registration process is protected

- G3: Authentication information is protected

- G3: Chat logs are protected

```

This representation constructs a hierarchical view following the GSN predefined structure using goals (G), strategies (S), contexts (C), and justifications (J) to construct an assurance case tailored to the security needs of IM software. Each sub-level goal (G3, G4) expands into discussions about specific critical assets and the protective measures in place, connected by strategies and supported by contexts and justifications that demonstrate compliance with the defined security objectives.