Security risk-oriented patterns
For the given process model (two diagrams below), apply the method of Security Requirements Elicitation from Business Processes (SREBP) and derive the security requirements for **Team** asset.

- **Team** asset is characterised by attributes
  - **Team info**
  - **Team representative**
  - **Participation decision**
  - **Region and league**
Your solution should illustrate the application of the security risk-oriented patterns (which are the part of the SREBP method). The solution should include:

- **SRP1:**
  - Security model (i.e., RBAC model) and
  - Derived list of security requirements

- **SRP2:**
  - Security model (i.e., collaboration model) and
  - Derived list of security requirements

- **SRP3:**
  - Derived list of security requirements (describing the input filtering)

- **SRP4:**
  - Security model (i.e., class diagram)
  - Derived list of security requirements (describing the requirements for the firewall architecture)

- **SRP5:**
  - Security model (i.e., RBAC model regarding the database)
  - Derived list of security requirements (including auditing and information hiding requirements)
Some illustration of the solutions
SRP1: Secure data from unauthorized access
SecReq.1: Only Football Federation Employee should *insert* Team (including all its attributes)
SecReq.2: Only Football Federation Employee should *update* Team information
SecReq.3: Only Football Federation Employee should *update* Team representative
SecReq.4: Only Football Federation Employee should *view* Team info
SecReq.5: Only Football Federation Employee should *update* Regions and leagues
SecReq.6: Football Federation Employee should *view* Regions and leagues
SecReq.7: Only Team Representative should *update* Participant decision
SecReq.8: Team Representative should *view* Regions and leagues
SRP2: Secure data transmitted between business entities
SecReq.9: ERIS should have unique identity in the form of key pairs (public key and private key) certified by a certification authority

SecReq.10: Football Federation Employee should encrypt and sign Team, Team info, Regions and Leagues (and other data communicated to ERIS) using keys before sending it to ERIS
SRP3: Secure business activity after data is submitted
SecReq.11: Register decision should filter the Participation decision.

SecReq.12: Register decision should sanitise the Participation decision to transform it to the required format.

SecReq.13: Register decision should canonicalise Participation decision to verify against its canonical representation.
SRP4: Secure business services against denial of service attacks
SecReq.14: Register decision should establish a rule base (i.e., a collection of constraints used by different firewalls) to communicate with the Team Representative.

SecReq.15: Packet Filter Firewall should filter the Team Representative’s address to determine if that is not a host used by the threat agent.

SecReq.16: Proxy Based Firewall should communicate to the proxy which represents Register decision to determine the validity of the request received from Team Representative.

SecReq.17: State Firewall should maintain the state table to check the Team Representative’s request for additional conditions on established communication.
SRP5: Secure data stored in/retrieved from the data store
SecReq.18: ERIS should audit the operations after the retrieval, storage or any other manipulation of data in the Team Database

SecReq.19: The ERIS should perform operations to hide/unhide data when they are stored/retrieved to/from the Team Database.
Thank you