Finally, the security transformation potentially could result in the transformed security code, which would help capturing security constraints of the software system. In the book the idea of the pattern-based transformation from security models (expressing the RBAC policy) to the security constraints will be illustrated.

1.7 Running Example

General description. In this book a Football Federation case is used as an example to show various principles of secure system modelling. This example was partially analysed in [107]; however in this book a hypothetical case is developed to illustrate different principles of secure system modelling and design. Fig. 1.4 provides some informal description of the system used in the Football Federation case. Like all organisation, Football Federation has a number of employees. For example, Football Federation Employee is carrying on the typical business workflows in organisation. To support his business activities he is using various systems. One of them is Electronic Registration Information System (ERIS), typically consisting of User Interface, Information Processing System, and Database, as illustrated in Fig. 1.4.

![Diagram](image)

Fig. 1.4 Informal Description of the Football Federation Case
ERIS is not a standalone application, but it is also connected to Other systems used within Football Federation organisation, and also Other systems existing in the environment. To maintain the Football Federation systems, a certain Infrastructure (including operating system(s), networks, connection channels, etc) should be established and constantly maintained. This is a responsibility of an Administrator, who is the employee of the Football Federation.

Additionally there might exist external users, such as Team Representative and Umpire, who potentially might access the ERIS for one or another service or needed information. Football Federation organisation is not isolated and potentially, as mentioned above, is connected to Other systems existing in this environment, which could potentially request for some services from ERIS or provide services by themselves.

Conceptual model. An extract of conceptual model of the ERIS system is presented in Fig. 1.5 as the UML class diagram. It includes five concepts: Game, Team, Player, Timetable and Umpire.

Game represents games organised and administered by the Football Federation. Games are described by their information (i.e., attribute gameInfo), assigned umpired (i.e., attribute umpire), game report (i.e., attribute gameReport), and confirmation of the game report (i.e., attribute confirmation).

Team describes the football teams which are members of the Football Federation. Each team is characterised by its information (i.e., attribute teamInfo, which might include name, city, sponsor, etc). Team has a team representative (i.e., attribute teamRep). Team makes decision about participating in the tournaments (i.e., attribute participationDecision). Finally, if participation decision is positive the information about teams region and league is added (i.e., attribute regionAndLeague).

Players are the members of the team. In this model, each player is described by his information (i.e., attribute playerInfo, which might include name, surname, position in the team, etc) and player’s performance in a certain game (i.e., attribute playerPerformance).

In Timetable a schedule of all games administered by the Football Federation are assembled. Timetable is described using time table information (i.e., attribute timeTableInfo, list of including league, playing teams, place, etc) and schedule of games (i.e., attribute schedule). In addition, each timetable should be confirmed by the league administrators (i.e., attribute timeTableConfirmation).

Finally, each game is assigned a certain number (typically 3-4) of Umpires. Each umpire is described by his umpire info (i.e., attribute umpireInfo including umpire’s name, surname, expertise, etc). Umpire also receives special access the ERIS (i.e., attribute umpireAccess), so that he could provide the information about his games (described using assignedGames attribute).

Business processes. BPMN value chain diagram describes how organisation’s business functions are related to each other in order achieve the business goals [190] [160] [54]. In Fig. 1.6 an extract of the ERIS value chain is provided. The selected subprocesses are

- Register team – registering teams to the ERIS system;
1.7 Running Example

- **Register player** – registering players and assigning them to the teams;
- **Register umpire** – registering umpires to the ERIS system;
- **Create leagues and divisions** – creating new league and preparing divisions;
- **Create timetable** – creating and preparing timetable;
- **Register game** – registering games and their results.

---

**Fig. 1.5 Class Diagram**

**Fig. 1.6 Business Process Value Chain**

The latter subprocess – **Register game report** – is expanded in Fig. 1.7. Here the Football Federation Employee decides to enter new game (see task **Enter new game**) and thus submits the game information (see task **Submit game info**) once the initial game information is received, the entry is created in the game storage (see task **Create game**). The Football Federation Employee also assigns the umpire (see task **Assign umpire**). After the game the Umpire submits game report (see task **Submit game report**). After the game report is updated (see task **Update game**
report) it needs to be confirmed by the Football Federation Employee (see task Confirm game report).

Fig. 1.7 Process to Register Game Report

1.8 Exercises

Exercise 1.1: Describe what is “system” in the football federation case. What are products/components of the system, its infrastructure applications, information technology staff, internal users and management, customers and other external users? To support your answer, fill in Table 1.1.

Exercise 1.2: Compare components and processes of different security risk management standardisation initiatives:

- ISO/IEC 2700x vs NIST;
- NIST vs BSI;
- BSI vs ISO/IEC 2700x.