Name, surname: Raimundas Matulevičius

1. Which identification requirement is not correct?

1.1. *ERIS* shall identify *Football Federation Employees* and *Team Representatives* – before allowing them to use its capabilities
1.2. *ERIS* shall not require a *Football Federation Employee* to identify himself/herself multiple times during a single session
1.3. *ERIS* shall identify other applications (both internal and external) before allowing them to use its capabilities
1.4. *ERIS* should identify *Football Federation employees* by scanning his/her employee card data

2. Which authentication requirement is not correct?

2.1. *ERIS* shall verify the identity of *Football Federation Employee* before allowing him/her to update his/her user information
2.2. *ERIS* shall verify the identity of *Team Representative* before allowing him/her to use *ERIS* capabilities
2.3. *ERIS* shall verify the identity of *Football Federation Employee* by checking the entered social security number before allowing him/her to change his/her password
2.4. *ERIS* shall verify the identity of *external other systems* before allowing them to use *ERIS* capabilities

3. Which authorization requirement is not correct?

3.1. *ERIS* shall allow other external systems to automatically email a *Team Representative’s password to that Team Representative’s email address*
3.2. *ERIS* shall not allow *Team Representatives* to successfully use a denial of service (DoS) attack to flood *ERIS* with legitimate requests of service
3.3. *ERIS* shall allow *Football Federation Employees* to obtain access to all of his/her own personal account information
3.4. *ERIS* shall not allow any *Football Federation Employee* to access any account information of any other *Football Federation Employee* or *Team Representative*

4. Which immunity requirement is not correct?

4.1. *ERIS* shall protect itself from infection by scanning all entered and downloaded data and software for known computer viruses, worms, Trojan horses, and other similar harmful programs
4.2. *ERIS* shall disinfect all files found to contain a harmful program if disinfection is possible
4.3. *ERIS* will use the Kaspar antivirus program to detect and disinfect all known viruses and Trojan horses
4.4. *ERIS* shall notify the Administrator if it detects a harmful program during a scan
Correct the following requirements:

5.1 The same subsystem shall also be able to generate visible or audible caution or warning signal for the attention of security or business analyst

5.1. The subsystem shall be able to generate visible signal for the attention of security analyst

5.2 The warning lamp shall light up when system intrusions is detected and the current workspace or input shall be saved

5.2.1. The warning lamp shall light up when system intrusions is detected.
5.2.2. The workspace shall be saved.

5.3 The user shall be able to view the current selected channel number, which shall be displayed in 14pt Swiss type on an LCD panel tested to standard 657-89 and mounted with shockproof rubber washers

5.3. The user shall be able to view the current selected channel number.

5.4 Users normally require early indication of intrusion into the system

5.4. Users require indication of intrusion into the system within 0.05s.

5.5 Security-related messages should be versatile and user-friendly

5.5 Security-related messages should be understood by 99 users out of 100. (user understandability of messages is tested by estimating the time which is taken by user when reacting to the security-related message).

5.6 The network shall handle all unexpected errors without crashing.

5.6 The network shall handle 99.99% of errors without crashing.