Part 1: Security

**Authentication**

It is the process that determines who has access to certain parts of the company. Authentication occurs when the user shows some credentials to get access, those credentials are like IDs or tokens.

**Authorization**

Authorization is linked to the level of access that a user or group can have within a product.

**Access**

It is the permission for a user or group to enter a product.

**Risk Statement:**

A risk statement needs to include two or three elements:

* Event or Condition
  + A possible future event that could affect the program
* Consequences
  + The consequences of the event affect the program. Those are usually in terms of cost, schedule or performance.
* If known, the Cause of the Events
  + The root of the possible event that could affect the program

**Authentication Risk Statement:**

If the Authentication process is not running properly. Nobody would be able to log into the program, causing low traffic in our program.

**Authorization Risk Statement:**

If the Authorization levels are not well-defined, some users will have credentials they should not possess, causing unauthorized access to some program levels and creating possible problems in the app.

**Access Risk Statement:**

If the permissions for a public user are switched with a developer user. The public users could modify the program, creating problems in the app.