# **Special Topics** (CSE 490-R)

## Training minutes – Weeks 7-8

|  |  |
| --- | --- |
| **Date:**  **Instructor:**  **Student:** | June 12, 2022  Bro. Clements  Guillermo Oliva |

* **Prompts from assignment:**

1. Define Authentication, Authorization, Access.
   1. Authentication: It is the first step of the process. Its aim is simple – to make sure the identity is who they say they are. We run into it daily both in digital (username/password) and analog forms (ID/passport).
   2. Authorization: It defines the set of actions that the identity can perform after gaining access to a specific part of the infrastructure, protecting from threats that access controls alone are ineffective against.
   3. Access Control: Access control is the addition of extra authentication steps to further protect important segments. Once the identity proves they are who they say they are, access is granted. With access comes the authority to perform actions on whatever it is the identity has access to.

**Source**: <https://technologyconcepts.com/authentication-vs-access-controls-vs-authorization/>

1. Research on how to write a Risk statement.

i.e. Given the <Condition> there is a possibility that <EVENT> may occur, causing <CONSEQUENCES>.

Research information:

The Risk Statement is used to communicate the risk to the relevant stakeholders, if it is of sufficient importance. It should state clearly:

* + 1. What the risk is.
    2. What the trigger is for the risk. (What will cause it to happen)
    3. What the impact of the risk is if it happens
    4. In addition to this each risk should be:
       1. One single risk: Understandable to the audience intended. (it should be jargon free or non-technical if targeted at executives)

The key point is that if people understand what the risk is they can then help to mitigate it.

**Source:**

<https://theprojectmanagementguide.com/how-to-write-a-risk-statement/>

<https://www.pmi.org/learning/library/risk-identification-life-cycle-tools-7784>

Graphical user interface, application, Word

Description automatically generated

1. Write a security risk statement for each of the As
   1. Authentication
      1. If the backend is not integrated with authentication there is a possibility that any user can see restricted information (including data in the database)., causing the application to be completely exposed and vulnerable for a compromise.
   2. Authorization
      1. If the backend is not integrated with authorization there is a possibility that a threat actor could inject malicious payload into the system, causing the application to expose customer information or to serve as a middleware for credentials harvesting.
   3. Access Control
      1. If the backend is not integrated with access control there is a possibility that any user can perform UPDATE, DELETE operations on the database, or to allow access to admin level areas of the system, causing the system to either loose data or to be used to gain access to other registered account information.
2. Example 1 of a security implementation:

Diagram

Description automatically generated

Example 2:

