# EV1. CONCEPTUAL MODEL Entity-Relationship Diagram

## Assessable Task 1

### Database Management (DBM)
### NSM/ASIR

Pau Miñana
2023-2024

# To Consider

Thiss activity is optional but evaluative: it may affect your evaluation grade.

> 🚫 If you look for solutions on the internet or ask the ChatGPT oracle, you will only be fooling yourself. Remember that ChatGPT is not infallible or omnipotent. It is a great tool for speeding up your work once you have mastered a subject, but using it as a shortcut when you are acquiring basic skills and knowledge is seriously detrimental to your learning.
>
> Try to solve the activities using the resources we have seen and the extended documentation you will find in the Virtual Classroom.

# INDEX

# 1. Instructions and rules

## 1.1. Description

You are required to produce a valid Entity-Relationship Diagram that conforms to the given specifications and is properly documented and annotated.

## 1.2. Deadline and grading rates

- EVALUATION ratio: 30% of the total grade is for the evaluable tasks.
- ACTIVITY ratio: 50% of the evaluable tasks grade (there are two per evaluation).
- DEADLINE: *23:59 on Monday 27th November 2023* (5 WEEKS).

## 1.3. Grading

Submission is not compulsory and there is no minimum mark. It will be graded from 0 to 10 according to the rubric provided in this document.

## 1.4. Resources

You should study and consult all the resources given on the virtual classroom, paying particular attention to the non-assessable tasks and all the extra material.

E-R is HIGHLY subjective so there is not only one right answer. Any decision that is not a consequence of a fact explicitly stated in the task must be properly explained.

## 1.5. Plagiarism

You should avoid other students copying your work and take care to prevent this situation.

This is an individual assignment. If authorship is suspected, an oral interview will be required.

## 1.6. Submission instructions

The assignment must be submitted as a single PDF containing the diagram generated by the technical editor and the annotations, with no cover page or special formatting.

*ONLY A TWO-PAGE PDF DOCUMENT*:

- 1 for the E-R diagram
- 1 to justify decisions

### 1.7. Solutions and grading results

You will receive the grade broken down by each criterion, and the overall score, along with any comments that provide suggestions on how you could improve.

## 2. Recommendations

1. Make a sketch with pen and paper before working with the PC.
2. Spend half of the total time on paper and the other half on the PC.
3. Try to avoid crossing lines. It is recommended to use upper case for entities and lower case for attributes. For relationships, capitalise at least the first letter.
4. Indicate all participations and cardinalities.
5. Choose appropriate names for entities, consistent with the use of singular/plural.
6. For specialisations (if any), always use the same notation (symbols or letters) throughout the diagram.
7. For the relationships, choose infinitives or the verb tense you think is most appropriate, being consistent in the rest of the relationships.
8. In the relations, use the notation you saw in class (not the coloured diamonds).
9. *Explain **briefly and in your own words** the decisions that are not clearly specified in this document statement and **justify any weaknesses**.*
10. *Only a 2 pages PDF document will be accepted: 1 page for the E-R diagram and 1 page to justify the decisions. A cover page, header or footer are not required*.

# 3. Rubric

| ASSESSABLE ITEMS | DETAILS | SCORE |
|---|---|---|
| Entities and Attributes. | Correct identification of the necessary entities.<br><br>.Proper identification of the necessary attributes (of any type).<br><br>Avoidance of unnecessary entities and attributes.<br><br>Correct setting of attribute constraints (if applicable). | 2,5 |
| Entity Relationships. | Correct identification of all relationships between entities.<br><br>Correctly sets the degree of relationships.<br><br>Correctly identifies the required attributes (if applicable). | 2 |
| Entity Participation.<br><br>Relationship Cardinality. | Correctly establishes the entities' participations.<br><br>Correctly establishes the cardinalities of relationships. | 2 |
| Existence Dependencies.<br><br>Identification Dependencies. | Correctly identifies existence dependencies.<br><br>Correctly identifies identification dependencies.<br><br>Appropriate nomenclature is in use. | 1 |

| ASSESSABLE ITEMS | DETAILS | SCORE |
|---|---|---|
| Specializations/Generalizations.<br><br>Aggregations. | Identifies and correctly expresses Sp/Gen (if applicable).<br><br>Identifies and correctly expresses aggregations (if applicable). | 1 |
| Quality of the ER diagram. | Clarity and accuracy of the diagram.<br><br>No line crossing.<br><br>No inconsistency. Inconsistency in an ER diagram is the use of upper and lower case, singular and plural letters without following any particular pattern... | 0,5 |
| Justifications. | No decision without its justification.<br><br>All dependencies properly justified. | 1 |

# 4. Statement

## Cyber Security Division

We need to create a database for the cyber security department of a company that provides various network services. It must store information about the attacks received and the measures available to combat them, with the following requirements:

The first requirement is to keep a record of the employees of this department. The DNI, full name (first name and surname), a unique alias, mobile phone and emails (there may be several) are stored.

In addition, a register of persons/profiles of interest will be maintained, consisting of hackers and crackers, identified by a code, whose available data will be stored, including DNI, alias, name and full address (postal address, postcode, city, province). The hacker's phone number and a contact email address may also be stored. For security reasons, only those who collaborate with the company are stored as hackers, all other profiles are considered crackers. These collaborations are always exclusive between the same employee and hackers, as the latter are very protective of their privacy. They will not even accept that the employee is in contact with other hackers. It is necessary to keep a record of these collaborators. If an employee who works with a hacker is dismissed, the hacker's data is cleared from the system.

As well, employees can also cooperate between them, this time freely, with any of their colleagues and as often as they want. For each day they work together, a record of their identities is held.

The system stores a list of attack types, classified by code, of which the name, description and the usual environment of attack are compulsorily stored. It is also necessary to know the list of measures to prevent or counter the different types of attacks. These measures, which are not exclusive to each attack, have a code, a name, a description and a success rate. The success rate depends on the type of attack and can be "High", "Medium" or "Low". As workers are very efficient, there is no kind of attack they are helpless against.

The attacks recorded are always of a specific type, and only one. They are identified by the attack type code and an index related to the number of times the attack has been detected. The date and time of the attack is also recorded. Each attack comes from one or more sources, if they can be detected. The same sources can be involved in different attacks. Of these sources, identified by code, it is interesting

to know the IP, the location and whether they are related to any of the crackers stored or not. Each source can correspond to no more than one cracker, although these may be the origin of many sources.

On the other hand, attacks can be directed at one or more targets. Of the possible targets, which are the services monitored by the system, we know the IP, the name and the type of service offered. For each target, attacks will always have some consequences of varying severity. Each consequence is exclusively registered with a code, a description and the percentage of severity. Each attack may also have several consequences on the same target.

Finally, it must be noted that for an attack to be recorded, it must first be detected by one of the employees. As they will quickly alert their colleagues, each attack is recorded as detected by a single worker, who must be known.