

Oblig III: Security Risk Assessment

In this compulsory exercise (Oblig III) you will be trained in security risk assessment targeting the coaching service that you know from Oblig I

You are free to make assumptions as long as they are **stated explicitly** by you in your oblig-solution.

Your solution should be in the form of a single pdf-document.

THE SOLUTION SHOULD BE EASILY READABLE WHEN PRINTED IN A4 FORMAT. THIS INCLUDES TEXT IN THE CORAS DIAGRAMS.

You may work in groups of maximum three students or you may work alone. Hence, one solution may have up to three names. There should be no collaboration or copying between different groups. Hence, each group should solve the exercise independently.

You should use the CORAS tool <https://www.coras.tools/#/>

With respect to likelihood reasoning, you should use the rules for frequencies presented in the lectures on Security Risk Assessment. (In the CORAS book there are also rules for probability reasoning. They **should not** be used.)

It is a very good idea to start by carefully reading Chapter 3 of the CORAS book unless you have already done so (but note that this chapter does not use frequencies and the rules for frequencies that you should use).

Task

Assume you are under contract to conduct a security risk assessment of the remote coaching service you know from Oblig-I. The assessment should be conducted on behalf of the coaching service.

The risk assessment should be of size 250 man-hours (for the assessors).

Your task is to address some of these tasks as an assessor.

Question I

There should be at least one indirect asset. One of the indirect assets should be **reputation**.

Identify at least five direct assets of **relevance for the party** with respect to **the indirect assets**. Two of these five direct assets should be **compliance with privacy regulations** and **user safety**.

Make a CORAS asset diagram that correctly relates them.

For detailed advice, see Section 7.2.2 in the CORAS book.

Question II

Make a good **quantitative scale** for measuring harm (consequence) to the asset **compliance with privacy regulations**. It should have at least 5 values.

Question III

Make a good **qualitative scale** for measuring harm (consequence) to the asset **user safety**. It should have at least 5 values.

Question IV

Make a good **quantitative interval scale** for measuring likelihood using frequencies.

Question V

Make relevant threat diagrams with respect to the two direct assets **compliance with privacy regulations** and **user safety**. The diagrams should all together capture at least seven risks. The diagrams should be annotated with consequences and likelihoods in such a way that **they are consistent**. Every initiate relation, unwanted incident and threat scenario should be assigned a **frequency using the scale defined above**. Every leads-to relation should be assigned a **conditional probability different from 1**. Moreover, all **initiate, and leads-to relations should have at least one vulnerability associated with them** (i.e. represented in the diagram).

Question VI

Present the identified risks in a risk-matrix.

Question VII

Make a treatment diagram by annotating the threat diagrams from Question V with relevant treatments.

Question VIII

Assume that treatments are required for at least the three most important risks. Use the CORAS before-after style to illustrate the effect of these treatments on the already identified risks. The threat diagrams you have already drawn (Question V) correspond to the before situation. You are to "translate" these threat diagrams into threat diagrams expressed in the so-called before-after style reflecting the situation both before and after the implementation of the treatments.

For detailed advice, see Section 6 of

<https://breibakk.no/kst/Articles/2011.FOSAD.pdf>

Question IX

Any risk treatment will introduce some new risks (possibly with respect to some new assets). Update the threat diagrams from Question VIII to capture at least two new risks.

Question X

Present the risk matrix as it looks after the risk treatment (also considering the results from Question IX).