Linnaeus University 2016-02-24
Department of Computer Science
OF

Information Security

Practical work #4, 1DV700, VT16

In this assignment, you will be working with fake company that your group is to investigate the information security of. The teaching assistants will play the role of the CTO of the company.

Your title will be Information Security Consultant and your task is to evaluate the company's interactions with information from all possible aspects and develop policies that will carry the company to ISO 27001 compliance. For that, you first have to study ISO 27002, which is the framework for achieving ISO 27001 compliance.

You will be organized into groups, each group having 5-6 students. Each group will create their own work on the company separately.

Your point of contact with the company will be with CTO. Interactions with him will be in forms of e-mail, booked interviews and documentation about the company.

First line of information security will start with us. From company's standpoint, we are outsourced personnel and have enough access to cause harm to their operational status. In a real world situation you would probably have to sign a NDA (Non-disclosure Agreement). In addition to that, you will already assess the relations of the company with other outsourced personnel, and develop necessary policies under Organizational Security - Outsourcing section.

Task 1

Within their busy business tempo, companies may rarely be able to spare time for you and your requests. Therefore interview time with the company is golden and you should make good use of this time. You should have a very good grasp of IEC-ISO 27002 in advance, and a huge list of questions that you should be asking.

Study the read the IEC-ISO 27001 standard document (and any supporting information you find useful on Internet). In the group have a discussion about all the areas of controls that the standard covers and what they cover. Then divide them between the group members (each member having two areas each, possibly with some overlap). Write an individual 2 pages summary of the security controls that you are responsible of. Try to come up with as many questions/requests as possible to be directed to company personnel, include only around 10 of them in your summary for us to assess that you are on the right track.

Task 2

It is time to make use of the knowledge you gained in Task 1. Appoint a team-leader in your group and set up a first meeting with the CTO.

Your title is Information Security Consultant and your task is to evaluate the company's interactions with information from all possible aspects and develop policies that will carry the company to ISO 27001 compliance. Once you decide on security controls that seem applicable, assign each control(s) to one/two team-member(s). Contact company via email, request any material you need and ask questions. Then each team-member prepares the policy document for the specific security control that he/she is responsible for.

In the end, all team-members combine their work and generate one complete INFOSEC policy document.

Team-leaders have to submit the final work on Moodle according to the deadline.