SCQ0089517, A.A. 2022/23 - SECURITY AND RISK: MANAGEMENT AND CERTIFICATIONS

Cybersecurity Assessment Report – Laboratory

A.Belli

Case #1 – 'Beta', a Civil engeneering counselling company

Beta company is in a civil engeneering counselling business and has around 150 people in 3 three different cities. All three offices are located in the same country.

It delivers counselling for both private construction companies and government entities through meetings held in presence and via webconference.

IT & Multimedia area of Beta Company purchased a public cloud based software for webconference meetings, as well for mail and storage services. These collaboration tools are protected by the same IAM system and go under the same contract with the same supplier.

Internal resources are available from the three offices through a private cloud service managed by a supplier that provides, by contract, a 24h/d 365d/y available service.

- Given the candidate is the CISO of the company, how would she/he perform the assessment against the Nist CSF? (who are the people to interview, how are the questions made?)
- What kind of NIST CSF controls would she/he consider relevant for the specific risks arised from the described activities, and why?
- Can the candidate describe the implementation of the controls considered the most relevant to reduce the risk?

The candidate can use the CSF to conduct the assessment and provide the answers.

Case #2 'Gamma', a private healthcare company

Gamma is a private healthcare organization that provides for many medical practice services.

The company operates in a single city, but has an administrative office dislocated from the site where it provides medical services.

The company has an internal IT department, with a private server for storing company data inside the administrative offices. The connection to the private server takes place via the normal national internet network. The company outsources the maintenance of the server and the connections to/from it to a small-sized external supplier.

The company uses a free cloud communication service for contact with patients (customers), including emails, calendars, and meetings when it is not possible for patients to travel to the clinic.

- Given the candidate is the Information Security and Privacy Manager of the company, how would she/he perform the assessment against the Nist CSF? (who are the people to interview, how are the questions made?)
- What kind of NIST CSF controls would she/he consider relevant for the specific risks arised from the described activities, and why?
- Can the candidate describe the implementation of the controls considered the most relevant to reduce the risk?

The candidate can use the CSF to conduct the assessment and provide the answers.