**Seminar 1: Scrum Security review**

Please carry out these activities before joining the seminar this week. Your answers will be discussed during the seminar.

**Question 1**

Create a 2-column multi-line table. In the left-hand column, include the software development stages of the Scrum agile life cycle approach to project management. In the right-hand column, describe the processes which you recommend are applied at each stage to ensure that secure software is produced at the end of the development. To support the preparation of your response, you can refer to the following literature:

Sharma, A. & Bawa, R. K. (2020) Identification and Integration of Security Activities for Secure Agile Development. *International Journal of Information Technology*.

**Blog Post: Question 2 (also e-portfolio activity)**

Some say that people are the biggest risk of cyber security.

Select five terms from ISO/IEC Standard 27000 Section 3 Terms and Definitions and write a 300-word blog post on how people can be managed to overcome cyber security attacks from the inside.

There will also be an opportunity to review your team’s progress during the seminar.

**Visible to participants on this course**

 ISO’s (2022) ISO (International Organization for Standardization) and IEC (International Electro Technical Commission) work together on standards and guides on conformity assessment within ISO/CASCO, the ISO policy development committee on conformity assessment The ISO 27000 group of norms is wide in scope and is relevant to associations of all sizes and in all areas. As innovation constantly advances, new principles are created to address the changing necessities of data security in various ventures and conditions.

**ISO 27001**

This is the focal norm in the ISO 27000 series, containing the execution prerequisites for an ISMS. This is essential to recall, as ISO IEC 27001: 2013 is the main norm in the series that associations can be reviewed and ensured against. That is on the grounds that it contains an outline of all that you should do to accomplish consistence, which is developed in every one of the accompanying principles.

**ISO 27002**

This is the focal norm in the ISO 27000 series, containing the execution prerequisites for an ISMS. This is essential to recall, as ISO IEC 27001: 2013 is the main norm in the series that associations can be reviewed and ensured against. That is on the grounds that it contains an outline of all that you should do to accomplish consistence, which is developed in every one of the accompanying principles.

## ISO 27017 and ISO 27018

These beneficial ISO norms were presented in 2015, making sense of how associations ought to safeguard delicate data in the Cloud. This has become particularly significant as of late as associations move quite a bit of their delicate data on to online servers. ISO 27017 is a code of training for data security, giving additional data about how to apply the Annex A controls to data put away in the Cloud. Under ISO 27001, you have the decision to treat these as a different arrangement of controls. In this way, you'd pick a bunch of controls from Annex A for your 'ordinary' information and a bunch of controls from ISO 27017 for information in the Cloud. ISO 27018 works in basically the same manner however with additional thought for individual information.

This is the most current norm in the ISO 27000 series, covering what associations should do while executing a PIMS (security data the board framework).

## ISO 27701

It was made because of the GDPR (General Data Protection Regulation), which educates associations to embrace "suitable specialized and hierarchical measures" to safeguard individual information yet doesn't state how they ought to do that. ISO 27701 fills that hole, basically blasting security handling controls onto ISO 27001.

Reference

Graham, A. (2019). What is the ISO 27000 series of standards? - IT Governance Blog. [online] IT Governance Blog. Available at: <https://www.itgovernance.co.uk/blog/what-is-the-iso-27000-series-of-standards>. [Accessed 21 June 2022].

A version of this blog was originally published on 10 October 2019

‌ ISO. (2022) ISO/IEC 27000:2018: Terms and Definitions. Available from: [**https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en**](https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en) [Accessed 21 June 2022].

<https://www.itgovernance.co.uk/blog/what-is-an-isms-and-9-reasons-why-you-should-implement-one> [Accessed 22 June 2022].