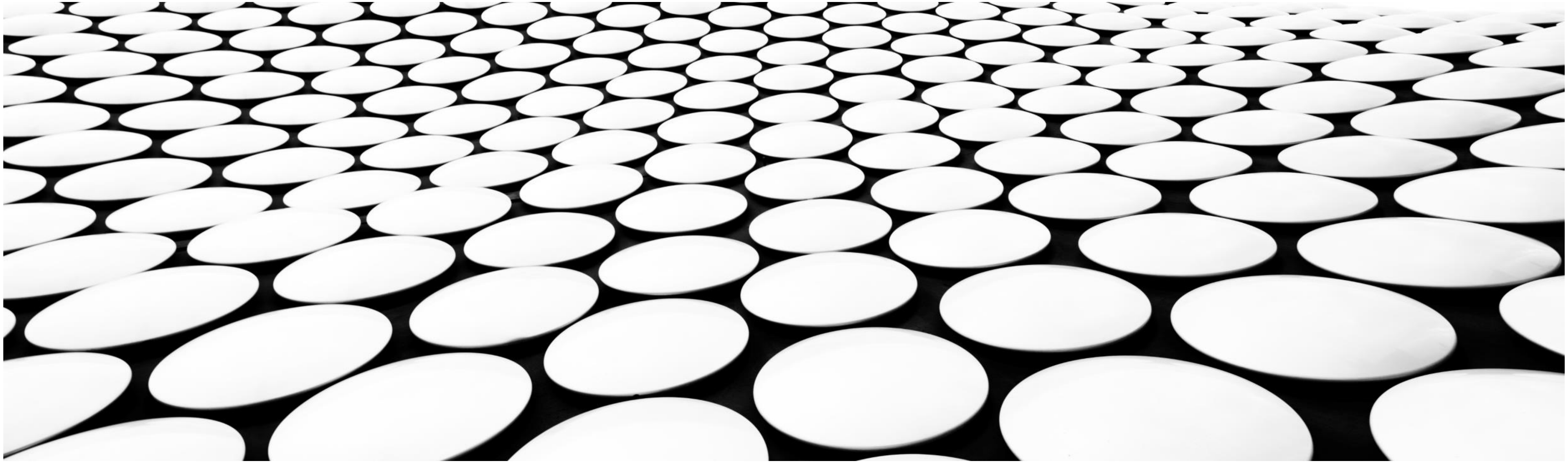
UNIT 2: UML MODELLING TO SUPPORT SECURE SYSTEM PLANNING

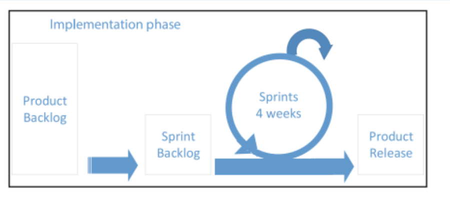
EXERCISES



QUESTION 1

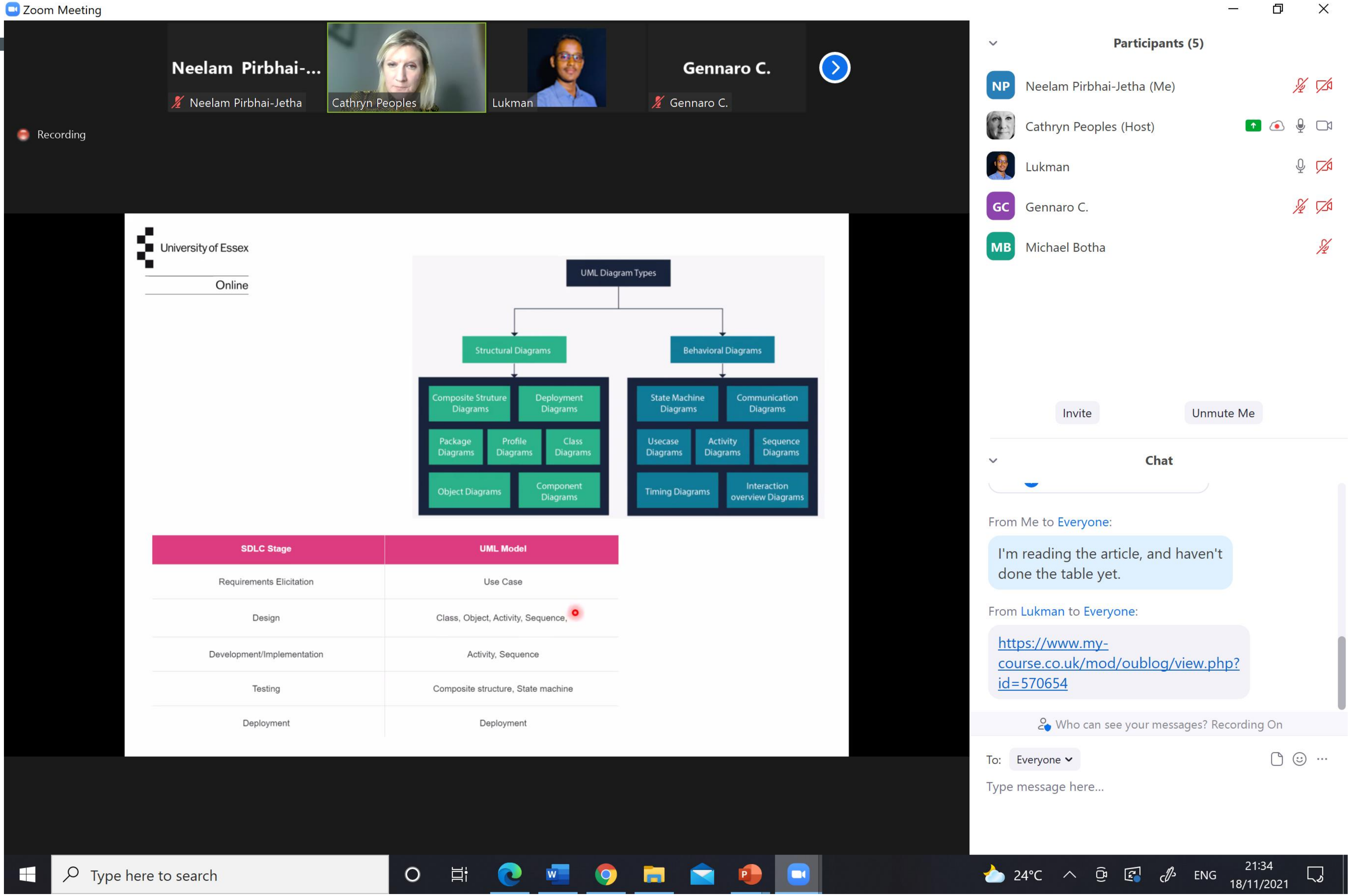
- **Create a 2-column multi-line table. In the left-hand column, include the software development stages of the Scrum agile life cycle approach to project management. In the right-hand column, describe the processes which you recommend are applied at each stage to ensure that secure software is produced 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*

- ***Personal Comments**: I had a few issues understanding the first question, but after the tutor's explanation, it was clearer that we had to put the phases in the first column, and the UML diagrams that can be used during the phases in the 2nd column*
- *I also came across an article:* Santos et al. (2016) "Using Scrum Together with UML Models: A Collaborative University-Industry R&D Software Project". Available from: *https://core.ac.uk/download/pdf/76176912.pdf* [Accessed 19 November 2021]

Software development stages of the Scrum agile life cycle approach to project management	Main steps/Explanation	Describe the processes which you recommend are applied at each stage to ensure that secure software is produced at the end of the development (UML DIAGRAM)
Initialisation & Planning Phase (Santos et al. 2016)	develop a product backlog To show specific users interactions to the system, for user stories	Use case
Implementation Phase (Santos et al. 2016)	 Implementation phase Product Backlog Sprint Backlog Sprints 4 weeks Product Release **Fig. 5.** The implementation phase Create the sprint backlog [sprint development; Sprint monitoring;	Class Diagram Activity Diagram
Review and Testing Phase	Sprint verification and validation; sprint closure and Planning;sprint rework]	State Diagram
Deployment Phase		

- Scrum is a management framework

TUTOR'S EXAMPLE



University of Essex

Online

UML Diagram Types

- Structural Diagrams
  - Composite Struture Diagrams
  - Deployment Diagrams
  - Package Diagrams
  - Profile Diagrams
  - Class Diagrams
  - Object Diagrams
  - Component Diagrams
- Behavioral Diagrams
  - State Machine Diagrams
  - Communication Diagrams
  - Usecase Diagrams
  - Activity Diagrams
  - Sequence Diagrams
  - Timing Diagrams
  - Interaction overview Diagrams

SDLC Stage	UML Model
Requirements Elicitation	Use Case
Design	Class, Object, Activity, Sequence,
Development/Implementation	Activity, Sequence
Testing	Composite structure, State machine
Deployment	Deployment

From Me to Everyone:

I'm reading the article, and haven't done the table yet.

From Lukman to Everyone:

https://www.my-course.co.uk/mod/oublog/view.php?id=570654

Who can see your messages? Recording On

To: Everyone

Type message here...

QUESTION 2: BLOG POST

- **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.
- **Remember to record your results, ideas and team discussions in your e-portfolio.**

BLOG POST

The ISO/IEC Standard 27000 document provides an overview of information security management systems (ISMS). Out of the 77 terms/definitions in Section 3, the following 5 terms were chosen to explain how people can be managed to overcome cyber security attacks from the inside: authentication (3.5), information security (3.28), information security incident management (3.32), risk communication and consultation (3.65) and outsource (3.51). *

Identity verification/**Authentication** is a must and is one of the most important items which can help reduce attacks from the inside. Each employee should be provided with an access code so that the system can determine whether the right person is getting access to the correct/authorised information.

This is closely linked to items mentioned in **'information security'** such as preservation of confidentiality (3.10), integrity (3.36), non-repudiation (3.48) and reliability (3.55). Access and diffusion of documents of the company by employees must be controlled and each transaction/access recorded. For example, digital signatures (together with other security measures) can ensure that it is a specific internal person who has approved a transaction.

Furthermore, to be up to date with IT breaches, an **information security incident management system** must be put in place. This is a set of "processes (3.54) for detecting, reporting, assessing, responding to, dealing with, and learning from information security incidents (3.31)".

Moreover, a company must continually conduct **risk communication and consultation processes** "to provide, share or obtain information, and to engage in dialogue with all stakeholders (3.37) concerning risk management, whether it is the existence, nature, evaluation, acceptability and treatment of risk". Continuous training on security and ethics, for instance, can reduce security errors.

Information leakage and confidentiality issues are often raised (Feng & al, 2020) when companies prefer to "**outsource"** to a third party or make an arrangement for an external organization (3.50) to perform certain activities. However, Scott Dodds (2021) posits that "outsourcing a business's security function to a managed service provider (MSP) could provide the ability to deliver greater compliance and greater efficiency of cyber security solutions". One way to control internal leakage can, therefore, be part outsourcing.

To sum up, the list of definitions and items in Section 3 of the ISO document is important to understand the information security management systems and the issues to be taken into consideration to manage security risks.

References:

Dodds, S. (2021) "When is the right time to outsource your security function?", *Network Security*, Issue 5. Available from: https://doi.org/10.1016/S1353-4858(21)00054-4 [Accessed 18 November 2021]

Feng et al. (2020) "To outsource or not: The impact of information leakage risk on information security strategy", *Information & Management*, Volume 57, Issue 5. Available from: https://doi.org/10.1016/j.im.2019.103215 [Accessed 18 November 2021]

ISO/IEC 27000:2018. Available from: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 18 November 2021]

COMMENTS OF TUTOR:

Excellent harnessing of the core terms here, Neelam, forming an integrated and coherent argument. I wonder, might there be an opportunity to argue that a dashboard of threat monitoring specific to the organisation might help with these challenges, with the task of creating the dashboard given to a restricted set of trusted staff. Might this help to improve the communication of risk and provide part of a security management system?

Ref 1. https://www.sciencedirect.com/topics/computer-science/security-dashboard

Ref2:https://www.healthcareitnews.com/news/cio-guide-building-dashboard-cybersecurity

Might a dashboard be something that you configure as part of your summative assessment deliverable?

Best wishes,

Cathryn

Food for thought:
add a security
dashboard (SD) in
our group project?
How?
Check SD in Python.

FURTHER RESEARCH ON SECURITY DASHBOARD FOLLOWING TUTOR'S COMMENTS:

- Find out about dashboard and security:
- build an intelligent security dashboard that displays security alerts and responds to the alerts by either suggesting corrective action or automatically taking corrective action (depending on the action) [Ref1]
- A good security dashboard needs to include the following for a specified/measured time period: An indication of current threat level to the organization; an indication of events and incidents that have occurred; a record of authentication errors; an indication of scans, probes and unauthorized access, and an indicator if those key measures are up, down or unchanged; brute force attacks against the system and non-compliant devices; policy violations; malware events; and phishing events, said Karl West, chief information security officer at Intermountain Healthcare in Salt Lake City, Utah. [Ref 2]

- **Security dashboard checklist (Ref2):**
- Following are what cybersecurity experts say should be on your security dashboard:
- Current threat level to the organization.
- Events and incidents that have occurred.
- Authentication errors.
- Scans, probes and unauthorized access.
- Brute force attacks against the system and non-compliant devices.
- Policy violations.
- Malware events.
- Phishing events.
- Detailed technical metrics specific to the controls that are employed to manage risks to existing and emergent threat vectors.
- Number of covered assets.
- Newly discovered assets.
- Decommissioned assets.
- Number of threats detected and their risk levels.
- Clear visibility into the risk landscape.
- Areas of training/awareness.
- Vulnerability management.
- Third-party risk management.
- Incident management.
- Overall risk management.
- Mean time to patch.
- Mean time to detect and respond to potential incidents.
- Average window of exposure.
- Number of exceptions/types of exceptions.
- Phish fail percentage.
- Impact of remedial training.