Secure Software Development Seminar 1: Scrum Security review

Question 1

The software development stages of the Scrum agile life cycle approach to project management	The processes recommended applying at each stage to ensure that secure software is produced at the end of the development.
Product backlog	Input to the product owner from executives, teams, stakeholders, end users, and customers to produce a prioritised list of features, etc. Initial education of the team has a good cost-benefit ratio and assigning security experts to security requirement activities. Risk analysis can reduce costs later on. Coding rules can be less costly than static code analysis and security tools. Testing (dynamic analysis, Pentest and security) have benefit but can be costly.
Sprint planning meeting	The team decides how much can be delivered by the end of the sprint. Design: Secure design principles, inspection requirements, risk analysis Implementation: Coding rules, security tools, static code analysis
Sprint backlog	Tasks are prioritised and broken out.
Sprint	This set duration can be 1-4 weeks and does not change during the cycle. This is further broken down into mesocycles by having 24-hour sprints and daily 15-minute or stand-up sprint meetings. These meetings can reflect on the previous day's work, suggest current planning, and highlight any problems they face. This can be coordinated by a scrum master with the development team and product owner. The scrum master can facilitate, coach and support in removing obstacles. The team should be self-organised, collaborative, high velocity and focused on delivery. The product owner will represent client interests, make informed decisions and have accountability. Testing occurs and release. The "Sprint Burndown" tracks estimated hours work outstanding against the "timeboxed" Sprint hours available.

Review	The review can be a lengthy meeting when the demonstration of the features is performed, feedback is given, and reprioritising product backlog items.
Increment	The product is usually ready for shipping and finished.
Retrospective	Similar style meeting to the review, however, identifying pitfalls or improvement areas are given or brainstorming new ideas for improvement.

Question 2

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.

Terms:

3.1 access control

3.3 Audit

3.63 Risk analysis

3.46 Monitoring

3.17 Corrective action

The management of people can support overcoming inside security attacks through various approaches.

Technical measures such as access control can support inside security attacks; however, there is a limitation in only this approach. Alternative non-technical approaches must be considered if the organisation is to maintain its security.

Holistically, a risk-driven approach that incorporates potential insider threats and can focus on workplace behaviour can be an adopted policy (Colwill, 2009). Education is key to staff that helps security training and awareness. This fundamentally supports behavioural change that can empower staff to be prepared for security risks such as phishing attempts and adapt to workplace culture. If education training is comprehensive, behaviours and responses of individuals can support a culture of security within the workplace whereby users know the reasons behind policy and encourage others to act accordingly (Loukaka and Rahman, 2017).

Other approaches can be more intrusive and may be deemed negative however can be necessary for organisations. Establishing baseline policies and procedures must all adhere to that extend tradition methods (ISO, 2018). Examples include test exercises or even incentive reward exercises that aim to encourage staff members to realise security concerns. Other approaches can be monitoring and personnel checks with focused risk assessments (Netwrix, N.D.). Staff can find this intrusive; however, with much support, humans are the most significant risk; then companies see this as a necessity in the benefit-cost relationship. Staff need to be fully aware of the consequences of such actions and what the corrective actions may be.

Colwill, C. 2009. Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report,* 14**,** 186-196.

Iso. 2018. *ISO/IEC 27000* [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en [Accessed 11 May 2022].

Loukaka, A. & Rahman, S. 2017. Discovering New Cyber Protection Approaches from a Security Professional Prospective. *International journal of Computer Networks & Communications,* 9**,** 13-25.

Netwrix. N.D. *Insider Threat Prevention Best Practices* [Online]. Available: https://www.netwrix.com/Insider_Threat_Prevention_Best_Practices.html [Accessed 11 May 2022].