Seminar 1 – Scrum Security Review
Question 1

References to security activities are derived from four most common security engineering processes, namely, Cigatel Security Touchpoints (“CT”), Common Criteria (“CC”), Microsoft SDL (“MS”) and CLASP (“CL”).

Engineering Process Definitions

- **Cigatel Security Touchpoints.** Lightweight integration of core activities n existing development processes to improve product security.

  Activities include *Security Requirements, Abuse Cases, Risk Analyses, Assumption Documentation, Static Code Analyses, Penetration Testing, Red Team Testing, Risk Based Testing, External Reviews.* (Baca & Carlsson, 2011)

- **Common Criteria.** An ISO-certified process and users can specify their security and functional requirements.

  Activities include Security Requirements, Security Definitions, Risk Analyses, Critical/Vulnerable Assets, UMLSec, Requirements Validation, Repository Improvement. (Baca & Carlsson, 2011)

- **Microsoft SDL.** Modified to suite agile environments and categorises activities based on *frequency of use.* (Sharma & Bawa, 2020).

  Activities include Security Requirements, Role Matrix, Design Requirements, Quality Gates, Cost analysis, Threat Modelling, Attack Surface Reduction, Security Tools, Coding Rules, Static Analysis, dynamic Analysis, Fuzzy Testing, Code Reviews, Incidence Response Planning, Final Security Review. (Baca & Carlsson, 2011)

- **CLASP (Comprehensive, Lightweight Application Security Process).** Provided by OWASP and provides best practices, activities and roles to integrate security.

Activities include Awareness, Threat Modelling, Resource and Trust Boundaries, Security Analysis of Requirements, Security Metrics, Specify Operational Environment, Global Security Policy, User Roles and Capabilities, Identify Attack Surface, Security Design Principles, Security Architecture, Code Signing, Security Tests, Source-level Security Review, Operational Planning and Readiness.

Proposed Mapping

Table 1 SCRUM mapping to security activities

SCRUM Lifecycle	Recommended Security Activity
Vision Majority Activity: **Security Requirements**	▪ Design requirements [MS] *Ensure design specifications fulfil security requirements.* ▪ **Security requirements** [CG, CC, MS] *Identification of security and privacy concerns handled by security experts.* ▪ Security definitions [CC] *Common language across the organisation of security-related terms and policies.* ▪ Education [CL] *All stakeholders are informed about importance of security engineering and highlights possible breaches.*
Product Backlog	▪ Role matrix [MS, CL]

SCRUM Lifecycle	Recommended Security Activity
Majority Activity: **Resource protection**	*Identification of roles and their access levels. Important for authentication and authorization.* ▪ Security architecture ▪ Acceptance criteria ▪ **Identify resources and trust boundaries [CL]; Critical/Vulnerable Assets [CC]; Attack Surface Reduction [MS];** *Structures network access and interaction points.*
Sprint Planning Majority Activity: **Risk Analysis**	▪ **Risk analyses** [CG, CC] *Validates areifacts and quality of work and mitigates existing architecture flaws.* ▪ Coding rules [MS] *Insecure functions are swapped out for safer alternatives.*
Sprints Majority Activity: **Static Code Analysis**	▪ **Static code analysis** [CG, MS] *Source code analysed for vulnerabilities.* ▪ Security testing [CL] ▪ Code reviews [MS, CL]
Sprint Review Majority Activity: **Testing**	▪ Dynamic analysis [MS] *Tools to aid in detecting memory corruption, privilege concerns and other security issues. Enables mitigation in following sprints.* ▪ **Vulnerability and penetration testing [CG]**

SCRUM Lifecycle	Recommended Security Activity
	Simulates real-world conditions and attacks.
Sprint Retrospective Majority Activity: **Incidence Response Planning**	▪ Final security review [MS] ▪ **Incident response planning** [MS] *Provides direction on actions required in a security emergency.*

Conclusion

In line with the findings from Sharma & Bawa (2020), the Microsoft SDL and CL indeed do play a vital role in incorporating security concerns into a SCRUM process (as shown in Table 1).

References

Baca, D. & Carlsson, B., (2011) Agile development with security engineering activities. *Proceedings of the 2011 International Conference on Software and Systems Process*:149-158.

Sharma, A. & Bawa, R.K. (2020) Identification and integration of security activities for secure agile development. *International Journal of Information Technology:* 1-14.

Bibliography

Moyón, F., Almeida, P., Riofrío, D., Mendez, D. & Kalinowski, M., (2020). Security Compliance in Agile Software Development: A Systematic Mapping Study. *46th Euromicro Conference on Software Engineering and Advanced Applications* (SEAA): 413-420.