Assessment Instruction

SEC-202: Secure Startup

Spring 2026

General Information

Competency Code:	SEC-202
Competency Title:	Secure Startup
Semester:	Spring 2026
Instructor Information:	Charnon Pattiyanon, Ph.D. (charnon@cmkl.ac.th)

Assessment Overview

With the success of small businesses and start-ups worldwide, younger generations are increasingly motivated to pursue this path. Launching a new start-up requires comprehensive consideration of many aspects—human resources, legal matters, and system infrastructure. However, security threats to start-ups are becoming more prevalent, as these companies often have fewer security controls in place. This competency invites you to explore security controls and measures that ensure your start-up is established securely. You are expected to design and implement an appropriate organizational structure for your start-up, accompanied by suitable security measures.

To ensure that, as a student, you have the ability to establish an organizational design for a secure start-up company, this assessment is designed for you to apply the knowledge, techniques, and experience you have learned to a group project that creates a mock start-up. The assessment also promotes your analytical skills by requiring sufficient and valid justifications to support your design.

Assessing Skills

- [SEC-202:00010] – Understand the lifecycle of data and information withint startup operations.
- [SEC-202:00020] – Design an integrated landscape of security controls for the mock startup company.
- [SEC-202:00030] – Evaluate the existing use of data and information withint a startup company and critically assess its security measures.

Pre-Cautions

- **Express your answers form your own ideas and perspective.** Plagiarism is unacceptable. You must cite referenced sources properly to acknowledge their originality and must not copy partial or entire ideas from your peers. If content or ideas are found to be remarkably similar between two or more submissions, or if orginal material is copied from other works without proper citation, all students will receive a score deduction as a consequence of disciplinary action.

- **Demonstrate deep understanding through critical analysis and original insight**. Overreliance on AI-generated content without substantial original thought will negatively impact the assessment score.
- **Justifications** should explain a decision or finding in a "why" style, providing adequate technical and valid rationale. For example: "I believe that this security control is the best choice for ensuring endpoint seucirty because it is an enterprise-grade solution with relatively-low cost for installation." There will be no one-size-fit-all solution or criticism for writing a justification; your skill will be evaluated on the clarity of your justification.
- **Inquiries:** Students are encouraged to ask instructors any questions about the assessment or competency content via email or other agreed channels. However, students are not allowed to submit an assessment report and ask for feedback; such a submission will be treated as a report submission.
- **Optional questions** may be provided in this assessment with a clear indicator. Students may omit them from the report without affecting the final grade. However, optional questions may be considered in cases when a student receives a boderline score between two mastery levels or fails the competency. The optional question can contribute to the final score but will not exceed 10% of the overall score, at the instructor's discretion.

Sumission Policy

- You are allowed to submit your work only once per semester, unless specified otherwise. You may submit your work and then request feedback from the instructor. However, it is at the instructor's discretion whether to provide feedback.
- All submissions must be completed **through the Canvas system only**, as your scores need to be stored and transferred to the university's system. Submissions made via any other channel will not be recognized as official, and you will not receive a score for your work.
- At the end of each semester, **CMKL University** sets a deadline for students to submit their assessments for all enrolled competencies. If you fail to submit your work by the stated deadline, you will not receive any score. In such cases, you must retake the competency in future semesters. While you may submit a request for consideration of a late submission, approval is subject to the instructor's discretion and the university's operational constraints.

Assessment Instruction

The total score for this assessment is 300 points, with each skill contributing 100 points. Please carefully follow the instructions below:

1. Each student must team up with other students (teams of **up to four members**). If the enrollment cannot be divided evenly by four, one team may have five members.
2. Each team must select a mock startup company to establish. It can be a real startup you are creating or a fictitious startup you intend to develop.

3. You must identify the core product(s) and service(s) of the company. The description should be clear enough to define the company's operations and business processes.
4. Each team must write a full report on the organisational design for the secure startup company. The report template, provided separately with these instructions, outlines the minimum requirements that every team must meet, but teams are free to add additional details beyond this baseline. Any extra information that enhances clarity may positively influence the final score.
5. Each team must prepare a presentation deck summarising your organisational design from various security perspectives and submit it by **Sunday, 28 February 2026, 11:59 PM**. The presentation must align with the full report template.
6. Each team must present its organisational design to the class on **Monday, 1 March 2026**, during the scheduled class time.
7. Each team must submit the full report described in item 4 on **Friday, 1 May 2026, 11:59 PM** via Canvas. Late submissions will not be accepted, as the deadline is set by the university. It is advisable for teams to submit the report as soon as it is completed.

Important Dates for the Assessment

• **Submission Deadline for the Presentation Deck:**	February 28, 2026, 11:59PM
• **Presentation Date for the Assessment Project:**	March 1, 2026
• **Submission Deadline for Assessment Report:**	May 1, 2026, 11:59PM