



VICTORIA UNIVERSITY OF
WELLINGTON
TE HERENGA WAKA

TEST – 2025
TRIMESTER 2

CYBR 271
CODE SECURITY

Time Allowed: THIRTY MINUTES

CLOSED BOOK

Permitted materials: Paper English language translation dictionaries are permitted.

Instructions: The test is worth **30 marks** in total. There are two sections: Multiple-choice Questions and Case Study.

Multiple-choice Questions

Circle the BEST answer. Each multiple-choice question is worth *one* mark. This section is worth **6 marks**.

Case Study

Write your answers in the boxes closest to each subpart of the question in this test script. If you use other spaces, clearly indicate where your answer is. You may use blank reverse sides of pages or the end page for extra space, working, or answers. Mark values are shown next to each subpart. This section is worth **24 marks**.

Return this test script at the end of the test.

SECTION A Multiple-choice Questions

Circle the best answer.

1. How does psychological acceptability **IMPACT** security controls?
 - A. If security is inconvenient, users find ways to bypass controls, weakening the system
 - B. Making security visible increases effectiveness
 - C. Requiring random complex passwords always improves things
 - D. Using more pop-ups strengthens compliance
2. Which scenario is an **EXAMPLE** of a "tampering" threat in STRIDE:
 - A. An attacker injects malicious code into a third-party JavaScript library loaded by the victim's browser
 - B. An attacker logs in using stolen credentials to view the victim's online records
 - C. An attacker tricks a staff member into revealing an admin password via phishing
 - D. An attacker floods a video streaming server with requests
3. Which of the following is **NOT** a common misunderstanding about attack trees?
 - A. Attack trees are simply diagrams with no analytical value.
 - B. Attack trees can only be used to represent attack paths, not plan defensive measures.
 - C. Attack trees remain accurate without regular updates as threats evolve.
 - D. Attack trees can be applied beyond cybersecurity, including in physical and social engineering contexts.
4. Why is it difficult to **CALCULATE** quantitative software risk compared to hardware risk?
 - A. Software is subject to unpredictable human factors and complex dependencies, making frequency and impact very hard to model reliably
 - B. Hardware always breaks at predictable intervals
 - C. Software bugs are always more severe than hardware bugs
 - D. There are more tools for hardware risk

5. Why might a static analysis tool **MISS** certain security flaws?
- A. It analyses code without executing it, so vulnerabilities dependent on runtime behavior or environment conditions may not be detected
 - B. It only scans external libraries and dependencies, ignoring application code
 - C. It randomly samples code lines to find weaknesses
 - D. It relies on penetration tests to trigger vulnerabilities
6. Which pair of tools are **CORRECTLY** matched to their primary role?
- A. OSV Scanner – finds public open source vulnerabilities; Static code analysis – find code issues
 - B. CVE – calculates severity; CVSS – generates unique vulnerability IDs
 - C. OWASP – issues bug bars; CAPEC – lists configuration standards
 - D. SBOM – tracks exploits; OVAL – checks licenses

SECTION B Case Study

7. You are the security consultant for **CloudLearn**, an online education platform delivering content to university students on a subscription basis.

(a) **(8 marks)** Consider this data flow in the **CloudLearn** system.


Authentication data flow (How students log in):

- Students (*interactors*) log in using username and password through either:
 - CloudLearn's login system (*process*), OR
 - Google/Microsoft login services (*interactors*)

Describe **ONE threat** that is applicable to either the data flow, process or interactors described above. Include the following details: (i) STRIDE category, (ii) Description of the threat, (iii) an example of how it could be carried out, and (iv) its business impact.

(b) **(6 marks)** Consider the threat you identified in 7(a) and construct a small realistic attack tree showing:

1. The root goal (your chosen threat)
2. Use AND/OR logic
3. Both a technical and non-technical attack vector

A large empty rectangular box with a black border, intended for the student to draw their attack tree. The box is currently blank.

- (c) **(10 marks)** Imagine that as part of threat modelling you've identified these potential security controls, but can only choose **TWO controls**. The table below includes each control's cost, a qualitative estimate of threat likelihood and impact, and the main attack vectors covered.

Opt.	Control	Cost	Likelihood	Impact	Vectors Covered
A	MFA for all accounts	\$50k	High	High	Credential theft, phishing, account takeover
B	Network firewall rules	\$30k	Medium	High	External intrusion, scanning exploits
C	Anti-malware + updates	\$40k	Medium	Medium	Malware, ransomware
D	Encrypt all student data	\$60k	Low	Very High	Data breach of stored records
E	Staff awareness training	\$25k	Very High	High	Phishing, social engineering, human error

Your task:

1. Identify the *most cost-effective* combination using their corresponding letters, for example A and C.
2. Briefly justify your choice considering:
 - Likelihood \times impact
 - Cost
 - Coverage of multiple attack vectors
3. Name **one piece of additional data** you would need for a **FAIR** quantitative risk analysis.

Answer continues...

Student ID:

SPARE PAGE FOR EXTRA ANSWERS

Cross out rough working that you do not want marked.

Specify the question number for work that you do want marked.

Student ID:
