Cybersecurity and the CIA triad

How to use this clinic

This clinic contains authentic QCAA external-assessment questions. For each question:

1. attempt the question on paper without looking ahead
2. compare your answer with the worked response and its explanation
3. use the complete QCAA sample response and marking criteria to check what earned the marks
4. add anything missing to your answer in a different-coloured pen.

> **Important:** The worked responses are examples, not scripts to memorise. A different answer can earn full marks when it identifies a relevant risk and supports it with accurate reasoning from the scenario.

Question 1: remote car-unlock app

Complete the question on paper before moving to the worked response.

QUESTION 12 (18 marks)

A mobile application (app) allows car owners to remotely unlock their cars if they lock the keys inside or their keys malfunction. Once users have created an account, they can request a remote unlock by entering their username and password.

The user data that is required to set up an account includes:

- full name
- date of birth
- home address
- driver licence number
- vehicle make, model and colour
- vehicle registration.

a) Analyse the information and evaluate risks to data confidentiality, integrity and availability for this app. Justify your response with three examples. *[6 marks]*

Do not write outside this box.

2021 QCAA external assessment, Question 12a. © State of Queensland (QCAA), CC BY 4.0.

Worked response: remote car-unlock app

Confidentiality: An attacker could intercept unencrypted data while it travels between the app and the service. This could reveal the owner's name, address, driver licence number and vehicle details to an unauthorised person. The risk affects confidentiality because private information has been disclosed to someone who is not permitted to see it.

Integrity: An attacker could alter the vehicle registration linked to an account or modify an unlock request while it is being transmitted. The service might then unlock the wrong car or treat a false request as genuine. The risk affects integrity because the stored or transmitted data is no longer accurate and trustworthy.

Availability: An attacker could flood the remote-unlock service with requests or otherwise interrupt its network connection. A legitimate owner who has locked their keys inside the car may then be unable to use the service when it is needed. The risk affects availability because an authorised user cannot access the system at the required time.

Why this response earns the marks

Part	What the response does
Confidentiality	Names specific private data, explains how an unauthorised person could obtain it, and connects disclosure to confidentiality.
Integrity	Names data that could be altered, explains the incorrect action that may follow, and connects untrustworthy data to integrity.
Availability	Names a believable interruption, explains its effect on the car owner, and connects loss of timely access to availability.

The question awards one mark for logically evaluating each risk and one mark for supporting each evaluation with a coherent example. That is why each paragraph contains both a conclusion and scenario-specific reasoning.

Official marking guide: remote car-unlock app

The complete extract below shows both QCAA's sample response and the criteria used to award the six marks.

Q	Sample response	The response:
12a)	A data confidentiality risk is the possibility that an unauthorised person could observe the user data in transit. For example, the app requires a password for the user to log in and the data would need to be encrypted so that it cannot be stolen. A data integrity risk is the possibility that the data could become corrupted, lost or be maliciously manipulated. For example, the wrong car might be unlocked or a hacker might use the data to cause distress. A data availability risk is the possibility that someone may interfere with transmission to prevent data packets from reaching the intended destination, allowing them to access the person's car so that they can steal it.	• logically evaluates risks to data – confidentiality **[1 mark]** – integrity **[1 mark]** – availability **[1 mark]** • justifies this evaluation by providing a coherent example of a risk to data – confidentiality **[1 mark]** – integrity **[1 mark]** – availability **[1 mark]**

QCAA Digital Solutions marking guide and response, 2021, Question 12a. © State of Queensland (QCAA), CC BY 4.0.

Question 2: hospital car-park system

The question concerns a hospital boom gate that records numberplates and requires staff to swipe an ID card. Read the context, then complete the six-mark CIA question on paper.

QUESTION 11 (9 marks)

Refer to Stimulus 1 in the stimulus book.

A hospital has installed a state-of-the-art boom gate at the entrance to the staff car park. The boom gate scans and records numberplates and requires drivers to swipe their ID card for access.

a) Identify three Australian Privacy Principles that apply to the use of personally identifiable or sensitive data and explain how the hospital could implement each principle. *[3 marks]*

Australian Privacy Principle:

2024 QCAA external assessment, Question 11 context. © State of Queensland (QCAA), CC BY 4.0.

Question 2 continued

b) Analyse the scenario to determine a risk to data confidentiality, integrity and availability and make a recommendation for reducing each of these risks. *[6 marks]*

Confidentiality: _____

Integrity: _____

Do not write outside this box.

Question 2 continued

Availability:

Do not write outside this box.

2024 QCAA external assessment, Question 11b. © State of Queensland (QCAA), CC BY 4.0.

Worked response: hospital car-park system

Confidentiality risk and recommendation: Numberplates and staff identities could be viewed or linked by a person who does not need that information, exposing when particular employees enter the hospital. Restrict access to authorised staff using role-based permissions and record access in an audit log. This reduces the risk because only approved users can view the records and inappropriate access can be traced.

Integrity risk and recommendation: A staff member could lend an ID card to another driver, or a driver could register a false numberplate. The database would then connect the wrong person or vehicle with an entry event. Cross-check each scanned numberplate against the numberplate registered to the swiped staff ID before opening the gate. This reduces the risk because inconsistent data is rejected instead of being accepted as genuine.

Availability risk and recommendation: A network, server or storage failure could prevent the gate from checking authorised vehicles, leaving staff unable to enter the car park. Provide a secured offline copy of the authorised vehicle list and a tested manual override procedure. This reduces the risk because the gate can continue operating while the main system is unavailable.

Why this response earns the marks

There are six separate marking opportunities: one risk and one recommendation for each CIA element.

- The **risk** identifies the particular data or system function and explains what could go wrong.
- The **recommendation** names a specific control and explains how that control reduces the stated risk.
- Each recommendation matches its risk: permissions protect confidentiality, cross-checking protects integrity, and an offline fallback supports availability.

> **Notice:** Simply listing "encryption", "backups" or "authentication" would not explain how the recommendation helps this hospital system.

Official marking guide: hospital car-park system

The complete extract below shows QCAA's sample response beside the criteria for all six marks.

Q	Sample response	The response:
11b)	Confidentiality: The digital solution for capturing numberplate information and staff names poses risks for privacy, as personal data from various sources may be linked in unexpected ways. Only one trusted employee, like an IT manager, should have access to the database, and only after going through a review process approved by the hospital's recruitment and management staff. Information should only be shared between the IT manager and staff member in question, with no other parties privy to conversations or actions taken. Integrity: The data in the database must be error-free, but staff may attempt to abuse the system by providing access to family or friends by lending them their staff ID and obscuring their number plates to gain entry. To prevent staff from logging different numberplates, the system should crosscheck a list of permitted numberplates against IDs before granting access. Availability: The data may be vulnerable to hacking if allowed online, so a MicroSD card should be used for offline access by a trusted staff member. Physical security of the system and SD card should be maintained to prevent staff from damaging or destroying the digital solution. Data should be purged regularly, and the database should be detached and not accessible online. Numberplate data captured by the system should be encrypted and only accessible in extreme cases.	• analyses a risk to data – confidentiality **[1 mark]** – integrity **[1 mark]** – availability **[1 mark]** • makes a recommendation for reducing risks to data – confidentiality **[1 mark]** – integrity **[1 mark]** – availability **[1 mark]**

QCAA Digital Solutions marking guide and response, 2024, Question 11b. © State of Queensland (QCAA), CC BY 4.0.

Question 3: fundraising app

The scenario begins on the previous exam page. Read it first so that the risks in Question 12b can be linked to the app's actual constraints.

The coding club was unable to develop all the app's intended features in four weeks. The following processes were done manually during the first fundraising event:

- updating inventory
- authenticating users
- updating account balances.

b) Analyse the scenario to determine a risk to data confidentiality, integrity and availability. Justify each risk in your response. *[6 marks]*

Risk to data confidentiality: _____

Risk to data integrity: _____

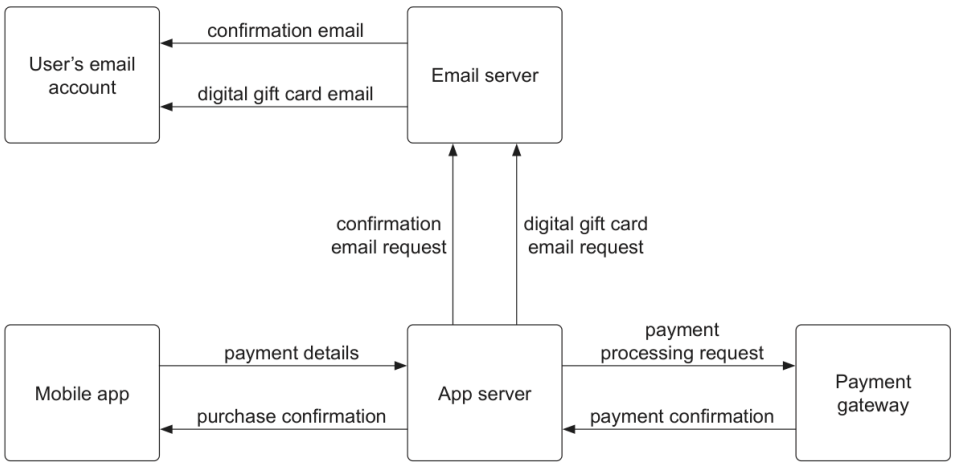
Do not write outside this box.

Question 3 continued

Risk to data availability: _____

QUESTION 13 (4 marks)

The diagram shows the data exchange involved in purchasing digital gift cards on a mobile app. After making a purchase, the user receives a confirmation email, and then a second email containing the digital gift card.



Do not write outside this box.

2025 QCAA external assessment, Question 12b. © State of Queensland (QCAA), CC BY 4.0.

Worked response: fundraising app

Risk to confidentiality: User authentication is being completed manually. A volunteer could mistake one person for another or allow somebody to access an account without properly verifying their identity. That person could then view private student, staff or financial information belonging to another user. This is a confidentiality risk because sensitive information may be disclosed to an unauthorised person.

Risk to integrity: Inventory is being updated manually during a busy fundraising event. A sale could be missed, entered twice or recorded against the wrong item, making the stored quantity different from the real quantity. This is an integrity risk because the inventory data is no longer accurate and the app may allow an item to be oversold.

Risk to availability: Account balances are also being updated manually. If volunteers are busy or calculations are delayed, the current balance may not be available when a customer attempts another purchase. This is an availability risk because authorised users cannot obtain the up-to-date account information when it is required.

Why this response earns the marks

Each two-mark paragraph performs two jobs:

1. **Determines a relevant risk:** it selects a plausible problem caused by one of the manual processes named in the scenario.
2. **Justifies the risk:** it explains the cause, the specific data or function affected, the consequence, and why that consequence belongs to the named CIA element.

For example, saying only "manual inventory updates are an integrity risk" states a conclusion. Explaining that an update may be missed, that the stored quantity becomes inaccurate and that an item may be oversold provides the justification.

Official marking guide: fundraising app

The complete extract below shows QCAA's sample response and the criteria for Question 12b.

QCAA sample response

12b)	Risk to data confidentiality: There is no user authentication process implemented; therefore, updating account balances and accessing user details risks the confidentiality of private information of all users, staff and students, including financial information. Risk to data integrity: Updating inventory manually during a fundraising event would be a time-consuming process. There is a real risk to data integrity that could lead to overselling if the inventory data is not accurate at the point of sale. Risk to data availability: Manually updating account balances risks the availability of user account information due to the delay caused by manually processing calculations while managing other distractions during a fundraising event.

QCAA marking criteria

- determines and justifies
  - a risk to data confidentiality **[2 marks]**
  - a risk to data integrity **[2 marks]**
  - a risk to data availability **[2 marks]**

QCAA Digital Solutions marking guide and response, 2025, Question 12b. © State of Queensland (QCAA), CC BY 4.0.