VCE Applied Computing 2025–2028

Video 9

Background to Unit 4 Outcome 2
Data Analytics

VICTORIAN CURRICULUM AND ASSESSMENT AUTHORITY
VICTORIA State Government

Acknowledgement of Country

The VCAA respectfully acknowledges the Traditional Owners of Country throughout Victoria and pays respect to the ongoing living cultures of First Peoples.

VCE Applied Computing 2025–2028

Video 9

Background to Unit 4 Outcome 2
Data Analytics

VICTORIAN CURRICULUM AND ASSESSMENT AUTHORITY
VICTORIA State Government

Purpose of this presentation

- Overview of Unit 4 Outcome 2 Data Analytics
- Major changes to Unit 4 Outcome 2
- Outcome statement
- Key knowledge
- Key skills
- Assessment task

Unit 4 Outcome 2

VICTORIAN CURRICULUM AND ASSESSMENT AUTHORITY

VICTORIA State Government

Changes to Unit 4 Outcome 2

- Emerging trends
- Cryptography
- Updated assessment task (SAC)

Unit 4 Outcome 2

From the outcome statement

- Respond to a teacher-provided case study to analyse the impact of a data breach on an organisation, identify and evaluate threats, evaluate current security strategies and make recommendations to improve security strategies.

Unit 4 Outcome 2 – Key knowledge

- emerging trends in cyber security, including:
  - the use of artificial intelligence to protect data
  - authentication procedures
  - threat detection and response
  - analytics of user behaviour
  - privacy protection
- goals and objectives of medium and large organisations

Unit 4 Outcome 2 – Key knowledge

- the importance of data and information security to organisations, including:
  - safeguarding business operations
  - mitigating financial loss and reputational damage
  - compliance with legal obligations
- types of threats to the integrity and security of data and information used by organisations, including:
  - accidental
  - deliberate
  - events-based

Unit 4 Outcome 2 – Key knowledge

- characteristics of data integrity, including:
  - accuracy
  - authenticity
  - correctness
  - reasonableness
  - relevance
  - timeliness

Unit 4 Outcome 2 – Key knowledge

- consequences of diminished data integrity, including:
  - loss of reputation
  - poor decision-making
  - financial loss
  - legal issues
  - impacted operations
- criteria for evaluating the effectiveness of data and information security strategies, including:
  - confidentiality
  - integrity
  - availability

Unit 4 Outcome 2 – Key knowledge

- key legislation that affects how organisations control the collection, communication and security of their data and information, including:
  - *Health Records Act 2001* (HPP 1, 2, 4, 5)
  - *Privacy Act 1988* (Cwlth) (APP 1, 3, 4, 5, 6, 7, 11)
  - *Privacy and Data Protection Act 2014* (IPP 1, 2, 4, 5, 10)
- key legislation that instructs an organisation to notify impacted individuals and organisations in the event of an eligible data breach likely to result in serious harm, including:
  - *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Sections 26WE, 26WF, 26WH, 26WK, 26WL, 26WR)

Unit 4 Outcome 2 – Key knowledge

- ethical issues arising from the implementation of data and information security practices, including:
  - data collection and use
  - identity theft
  - lack of transparency in the event of a cyber security incident
- applications of cryptographic techniques to protect data at rest and in transit, including:
  - use of ciphers
  - symmetric and asymmetric keys
  - use of hashing functions

Unit 4 Outcome 2 – Key knowledge

- features of disaster recovery plans, including:
  - evacuation
  - backing up
  - restoration
  - communication
  - testing
- security controls for preventing and tracking unauthorised access to data and information and minimising data loss.

Unit 4 Outcome 2 – Key skills

- analyse a data breach and describe its impact on an organisation
- identify and evaluate the threats to the security of data and information
- examine and describe an organisation’s current data and information security strategies
- propose and apply criteria to evaluate the effectiveness of current data and information security strategies
- identify and discuss possible legal and ethical consequences of ineffective data and information security strategies
- evaluate the disaster recovery plan for an organisation
- recommend and justify improvements to current data and information security strategies.

Unit 4 Outcome 2

Contribution to final assessment

- School-assessed Coursework for Unit 4 will contribute 10 per cent to the study score.
- Total marks – 100

Unit 4 Outcome 2

Assessment task

The student's performance will be assessed using one of the following:

- structured questions
- a report in written format
- a report in multimedia format.

The case study scenario needs to enable:

- an analysis of the breach
- an evaluation of the threats
- recommendations to improve security strategies.

Task time allocated should be 100–120 minutes.

Contact

- Phil Feain – Digital Technologies Curriculum Manager (VCAA)
- Ph: (03) 9059 5146
- Philip.Feain@education.vic.gov.au

Authorised and published by the
Victorian Curriculum and Assessment Authority