FNSACC526

ASSESSOR GUIDE

Implement and maintain internal control procedures

Assessment 2 of 2

Case study project

Version 1 2020

Assessment Details

Task overview

For this assessment, you will need to complete a series of tasks demonstrating your ability to review corporate governance requirements and monitor internal control operating procedures through a case study assessment.

In this assessment, you must develop, implement and maintain at least three internal control procedures for the Bigger Than Big Corporation case study organisation.

You will use the five (5) basic components established in the Auditing Standard ASA 315 Identifying and Assessing the Risks of Material Misstatement through Understanding the Entity and Its Environment.

- The control environment
- Entity's risk assessment process
- Information system
- Control activities relevant to audit
- Monitoring of control

The third internal control procedure you develop, implement and maintain must relate to cyber security and the safe handling of payments and data.

You will examine the Control Policies and Policies and Procedures for the Bigger Than Big Corporation in the following areas.

a. Accounting Data Security and Integrity
b. BAS and IAS Reporting
c. Computer and Email Policy
d. Information and Records Management Policy
e. Internet Access and Computer Use Policy

Read the case study below and complete the following:

- Read each task carefully.
- Conduct any research needed to complete each task.
- Draw on your workplace skills and knowledge to assist with completing each task.
- Provide detailed responses to each task to demonstrate your skills and knowledge specific to each listed point.

Resources required for this assessment

- Access to corporate governance documentation from regulatory authorities, including but not limited to:
- ASIC
- ASX
- ATO
- Two (2) volunteers to participate in a role-playing activity
- A video recording device

The policies and procedures for Bigger Than Big Corporation, the simulated business used in this case study, is provided for you on the following pages. Refer to these policies and procedures when you complete the tasks included in this assessment.

Assessment Information

Submission

You are entitled to three (3) attempts to complete this assessment satisfactorily. Incomplete assessments will not be marked and will count as one of your three attempts.

All questions must be responded to correctly to be assessed as satisfactory for this assessment.

Answers must be typed into the space provided and submitted electronically via the LMS. Hand-written assessments will not be accepted unless previously arranged with your assessor.

Reasonable adjustment

Students may request a reasonable adjustment for assessment tasks.

Reasonable adjustment usually involves varying:

- the processes for conducting the assessment (e.g. allowing additional time)
- the evidence gathering techniques (e.g. oral rather than written questioning, use of a scribe, modifications to equipment)

However, the evidence collected must allow the student to demonstrate all requirements of the unit.

Refer to the Student Handbook or contact your Trainer for further information.

Please consider the environment before printing this assessment.

Case-study Scenario: Bigger Than Big Corporation

Case-study Scenario

Bigger Than Big Corporation (ACN 62 123 456 789) is a leading enterprise with operations in Cascade Peak and employs 60,000 people across 45 countries.

It was originally a small private company registered with the Australian Securities and Investment Commission (ASIC), but due to its global expansion, it's now listed as a public company on the Australian Stock Exchange (ASX).

As a listed company, Bigger Than Big Corporation has specific obligations to comply with ASIC and ASX listing rules. It also has continuous and periodic disclosure obligations with respect to regulatory authorities, including the ASX, the Australian Taxation Office (ATO), and the Office of State Revenue.

The company directors believe it is essential to meet all legal and corporate governance requirements per the ASX Corporate Governance Council.

Due to the ASX listing, existing internal controls must be reviewed, and new internal control procedures must be developed where necessary.

- One key area for review is the accounting systems and the accounting practices, as the company recently upgraded from a manual paper-based system to a cloud-based accounting system.
- The board has also noted that there may be additional compliance risks from the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) that came into effect on 2 April 2022. Accordingly, the board wishes to examine its exposure to cyber threats and the organisations' ability to monitor them.

You work as part of the accounting team at Bigger Than Big. The team is responsible for corporate governance and accounting operations in the company.

Access Bigger Than Big's intranet site from the link below and click on "Accounting Operations Division – Current Employees" to know each team member's role within the department.

Accounting Controls

https://compliantlearningresources.com.au/network/biggerthanbig/policies-procedures/accounting-controls/

- Username: uplearner
- Password: upeducation@123

Your supervisor Chris Kohler assigns you to review the company's ethical and corporate governance requirements, including the implementation and monitoring of the necessary internal control procedures to ensure legislative and organisational compliance.

This assessment requires you to complete a series of tasks following this project.

For this assessment, Bigger Than Big Corporation is based in your State/Territory.

Additional resources and supporting documents
To complete this assessment, you will need:

- Access Bigger Than Big's intranet site
- Username: uplearner
- Password: upeducation@123

Assessor Instructions for Assessment 2 Case study

Purpose of the Task

This assessment supports the industry requirement in a business organisation. In real life, professionals must review corporate governance requirements, implement, and monitor internal control operating procedures. This assessment will help the student demonstrate skill requirements in such situations, using a simulated workplace, the case study company the Bigger Than Big Corporation.

Guidance to Assessors About this Task

There is no due submission date for this task.

Review all evidence and mark using the assessment checklist and assessment marking criteria listed below.

Task Instructions: Case-study: Bigger Than Big Corporation

Task 1: Corporate Governance and Ethical Requirements

Steps

Access Bigger Than Big Corporation's Policies and Procedures from this link:

Bigger Than Big Corporation Staff Handbook

- Username: uplearner
- Password: upeducation@123

Review the following policies:

i. Computer and Email Policy

ii. Disclosure of Confidential Information Policy

iii. Information and Records Management Policy

iv. Internet Access and Computer Use Policy

1. Identify one (1) **ethical requirement** from each of the policies mentioned above. Then, analyse and explain how each ethical requirement can be applied to the organisation's internal operations.

Marking guide
The student must identify one (1) ethical requirement from each of the policies outlined above. Then, they must analyse and explain how each ethical requirement can be applied to the organisation's internal operations. Responses and wording will vary; however, they must correspond to the policies mentioned above. Refer to the sample benchmark answers provided:

Submission instructions

Write your responses in the spaces provided below.

(Approximate word count 320-400 words)

Ethical Requirement	How It Applies to the Organisation's Internal Operations
i. Computer and Email Policy Employees must ensure that their work computers are not used for unlawful purposes (see Computer and Email Policy sec. 23.8)	Bigger Than Big must ensure that their computer systems will only allow access to programs or websites relevant to the work conducted by the employee. In addition, they must have a system in place to check if any fraudulent or suspicious activity is done on an employee's work computer.
ii. Disclosure of Confidential Information Policy Documents or software have controlled access as these are to be labelled accordingly on the level of confidentiality (see Disclosure of Confidential Information Policy sec. 25.1.b) Confidential information is to be only used for the benefit of the organisation and in line with their obligations as employees (see Disclosure of Confidential Information Policy sec. 25.1.c)	Authorised access to the organisation's documents and software must be set up to ensure that only relevant people can access confidential information.
iii. Information and Records Management Policy If an employee becomes aware of any illegal activity conducted by any person related to the organisation, they must be immediately reported to the supervisor (see Information and Records Management Policy sec. 26.1)	Processes for identifying and reporting illegal activities in the organisation must be in place to take immediate actions to prevent any future damage to the organisation.
iv. Internet Access and Computer Use Policy Social media use may interfere with normal duties or result in illegal activities such as bullying or sexual harassment. Internet Access and Computer Use Policy 1.4. Whilst the occasional use of computers for personal purposes will be tolerated (provided this is not otherwise a breach of this policy), you must not do so excessively or allow such conduct to interfere with your normal duties.	It may affect whether or how the organisation allows access to social media platforms using systems provided for work. It may also be reflected in the use of online monitoring systems and education and training programs

Ethical Requirement	How It Applies to the Organisation's Internal Operations
1.3.If you use any computer for an unlawful purpose, you may be reported to the police if a crime is involved. In addition, any other appropriate authority and your employment with us may be terminated for misconduct.	

2. Access the Australian Securities and Investments Commission's (ASIC) website through this link:

   ASIC Corporate Governance

   Review the guidance on corporate governance in line with Bigger Than Big Corporation's policies and procedures (Task 1.1). Identify the corporate governance requirement for each of the following aspects:

   - Disclosure of Directors
   - Handling Corporate Information
   - Information and Records Management Policy
   - Computer and Email Policy
   - Internet Access and Computer Use Policy

   Access Bigger Than Big Corporation's Policies and Procedures from this link:

   - Bigger Than Big Corporation Staff Handbook
     - Username: uplearner
     - Password: upeducation@123

   Analyse and explain how **each Corporate Governance Requirement** can be applied to the organisation's internal operations.

Marking guide
The student must identify the corporate governance requirements for each aspect specified above. Then, they must analyse and explain how each requirement can be applied to the organisation's internal operations. Responses and wording can vary; however, they should encapsulate the aspects of corporate governance mentioned above. Refer to the sample benchmark answers provided:

Submission instructions

Write your responses in the spaces provided below.

(Approximate word count 320-400 words)

Corporate Governance Requirement	How It Applies to the Organisation's Internal Operations
i. Disclosure of Directors: Directors are subject to heightened transparency requirements regarding their dealings in the company's securities. For example, directors of listed companies must disclose their interests in the shares of the company or its related corporate body. A director with a material personal interest in any matter that relates to the affairs of the company must generally notify the other directors of that interest.	Bigger Than Big Corporation must specify in their policies and procedures how, when and to whom the directors with a material personal interest in the organisation. It must also be clear how material, personal interest is defined in the organisation's context.
ii. Handling Corporate Information Listed companies must take responsibility for the management of their confidential information. Poor practices concerning the handling of confidential price-sensitive information can negatively affect market integrity and reputation, jeopardise the success of a transaction and may lead to ASIC action.	In line with the organisation's Disclosure of Confidential Information Policy, all corporate information must be handled responsibly by authorised people from the organisation to prevent inappropriate disclosure.
iii. Information and Records Management Policy The stability of financial markets can be threatened by cybercrimes. The Australian Securities and Investments Commission seeks to increase cyber resilience of beneficiaries across financial industries.	Boards should take ownership of cyber strategy and ensure Information and Records Management Policies are reviewed on a periodic basis to assess progress against success measures. Measures include time to breach detection, speed of response and recovery process.
iv. Computer and Email Policy It can take just one cyber vulnerability to threaten the stability of financial markets. ASIC's goal is to further improve the cyber resilience of entities in Australia 's financial market together.	Computer and Email Policies and procedures should be updated and reviewed periodically to assess progress against security measures. Measures can include frequent mandatory password changes, enforced password complexity, time to breach detection, speed of response and recovery processes.
v. Internet Access and Computer Use Policy Breaches in information security can threaten the reputation of an organisation and the stability of wider markets. The Australian Securities and Investments Commission seeks to increase the cyber resilience of beneficiaries across financial industries.	Internet Access and Computer Use Policy Policies and procedures should be updated and be reviewed regularly to assess progress against security measures. Measures include enforced password complexity, mandatory frequent password changes, time to breach detection, speed of response and recovery processes.

3. Access the latest version of the ASX Corporate Governance Principles and Recommendations through the quick links on this page:

   [Corporate Governance Principles and Recommendations]

   Refer to Principle 4: Safeguard the integrity of corporate reports: and select two (2) recommendations under it.

   Analyse and explain how each recommendation can be applied to Bigger Than Big's internal operations.

(Approximate word count 250-350 words)

Marking guide
The student must select two (2) recommendations under Principle 4 of the ASX Corporate Governance Principles and Recommendations. Then, they must analyse and explain how each recommendation can be applied to the organisation's internal operations Responses and wording will vary. However, the recommendations must correspond to those specified within the document. Refer to the sample benchmark answers provided:

Recommendation	How It Applies to the Organisation's Internal Operations
i. Recommendation 4.1 The board of a listed entity must have an audit committee composed of qualified and experienced members. The committee is responsible for disclosing information about the committee charter, qualifications and experiences of the members, and the frequency of meetings conducted by its members. If the listed entity does not have a committee, it must disclose this information to ASX, including the processes used by the entity to verify and safeguard the integrity of its corporate reporting.	Bigger Than Big must form an audit committee within the organisation as the ASX requires. Where there is no audit committee, they must report this information, including the independent processes conducted by the organisation for internal audit.
ii. Recommendation 4.2 The board of a listed entity must receive a declaration from the CEO or CFO that the organisation's financial records comply with accounting standards and that these reflect the accurate and fair view of the organisation's financial position before approving the financial statements for a reporting period.	The Bigger Than Big Corporation must ensure that the CEO has declared that the organisation's financial records are compliant with the standards and that these reflect the accurate and fair view of the company's financial position prior to approval and lodgement of these records.

Other responses may include Recommendation 4.3: A listed entity with an AGM should ensure that its external auditor attends its AGM and is available to answer questions from security holders relevant to the audit.	Bigger Than Big Corporation can ensure it maintains the organisation's integrity by allowing the external auditor to answer questions from security holders during AGM.

4. Access and read the article Australian Securities and Investments Commission article "Key questions for an organisation's board of directors" through the link on this page:

   Australian Securities and Investments Commission Article

   Analyse the Bigger Than Big's internal procedures through this lens and note down the answers to the questions posed.

Risk management framework

Question A: Are cyber risks an integral part of the organisation's risk management framework, and could this be improved? (Approximate word count 100 -200 words)
Student responses will vary but should address their impression of how the organisation • Addresses security and access in its Information and Records Management Policy • Addresses security and access in its Computer and Email Policy • Addresses security and access in its Internet Access and Computer Use Policy • If unknown, the student should include this. Responses can include the following The board could ensure that cyber risk is part of the broader risk framework and that exposure is recognised, and assessed for impacts based on clearly defined metrics such as response time, cost and legal or compliance implications. The board could consider whether more frequent periodic reviews could form part of the risk management framework. The board could ensure that third-party partners and service providers maintain similar mechanisms to ensure that cyber risks are an integral part of partner organisations' risk management frameworks or seek to do business only with those who do.

Question B: How often is the cyber resilience program reviewed at the board level, and could this be improved? (Approximate word count 100 -200 words)
Student responses will vary but should recognise the presence or absence of and frequency of the board-level review of: • its Information and Records Management Policy • its Computer and Email Policy • its Internet Access and Computer Use Policy If unknown, the student should include this.

The board could consider whether more frequent periodic reviews could form part of the risk management framework.

Identifying cyber risk

Question C: What risk is posed by cyber threats to the organisation's business, and what could be done to minimise risk?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

Different businesses are exposed to different cyber risks and different potential consequences, so threats may vary, but could include breaches to firewalls, attempts to access protected files and areas of data storage without sufficient clearance or passwords, denial of service attacks, unauthored password use and similar. The board could reflect on risks specific to the business of the organisation.

Without an understanding of the nature of the risk and its consequences, it is difficult for a board to set an appropriate risk tolerance for the risk and to ensure that the organisation's risk management framework effectively addresses cyber risks.

The board could ensure that third-party partners and service providers maintain similar mechanisms to Identify and minimise cyber risk or seek to do business only with those who do.

Question D: What further expertise would help the board understand and address the risk?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

Not all boards require general technology expertise; however, for many organisations, it is advisable to have one or more directors with specific knowledge of technology and its associated risks or a background in cybersecurity.

The board could consider using external cyber experts to review and challenge the information presented by senior management.

The board could ensure that third-party partners and service providers also maintain similar mechanisms for Identifying cyber risk or seeking to do business only with those who do.

Monitoring cyber risk

Question E: How can cyber risk be monitored, and what escalation triggers should be adopted?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

Different businesses are exposed to different cyber risks and different potential consequences, so threats may vary, but could include breaches to firewalls, attempts to access protected files and areas of data storage without sufficient clearance or passwords, denial of service attacks, unauthored password use and similar. The board could reflect on risks specific to the business of the organisation.

The board could set an appropriate risk tolerance for identified risks, ensuring that the risk management framework adequately addresses cyber risks.

The board could ensure that third-party partners and service providers maintain similar mechanisms to monitor cyber risk or seek to do business only with those who do.

Controls

Question F: What is the people strategy around cybersecurity, or what could b done to raise awareness and compliance?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

Malicious cyber activity can devastate an organisation's business operations; therefore, The board could consider providing more detailed information on the risk to senior management and staff.

Identifying a cyber risk can pose particular challenges; some best practice organisations use Artificial intelligence-driven solutions to deal with this challenge.

The board could ensure that third-party partners and service providers also maintain similar mechanisms to Monitor cyber risk or seek to do business only with those who do.

Question G: What evidence can you see of efforts to protect critical information assets, and how could this be improved?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

The board could ensure that the organisation's critical information assets are suitably secure. The board could ensure transparency around the location of all critical assets, how they are protected and how protection is assured.

Despite significant advances in cybersecurity technology, lack of staff awareness of safe cyber practices, social engineering or careless behaviours remains a major source of cyber issues.

A collective effort against cyber threats will best serve an organisation; Boards could ensure increased and sufficient investment in staff training, given it is a significant source of risk,

The board could ensure that third-party partners and service providers maintain similar Controls mechanisms or seek to do business only with those who do.

Response

Question H: What are the procedures in the event of a breach, and how could these be improved?

(Approximate word count 100 -200 words)

Student responses will vary but should include the following.

Boards could implement practices to communicate and report effectively, internally and externally, and manage breach situations.

Boards could ensure that scenario planning and testing have been done, to ensure that response plans are valid and up to date,

Boards could put security and customer trust as central considerations in their organisation's use of technology to deliver services.

Boards could ensure that third-party suppliers also have risk management and reporting plans in place around securing cyber assets

Task 2: Application of Corporate Governance Requirements

To ensure that the corporate governance requirements implemented at Bigger Than Big are accurate, you need to seek clarification from authoritative sources.

Based on your analysis in Task 1, lodge an online enquiry to the following to clarify the application of the corporate governance requirements into the organisation's internal operations:

- Australian Securities and Investments Commission (ASIC)
- Guidance: Clarify with them your responses to Task 1 Question 2.
- At least one (1) professional association (e.g., CPA Australia)

Guidance: Clarify with them your responses to Task 1 Question 3.

Ensure that your enquiries use clear and concise language suitable for the recipients and purpose.

Submission instructions

Write your enquiries in the templates provided below.

Guidance: There is no need to lodge an actual online enquiry. But you must provide your query/s in the templates provided below.

(Approximate word count 120-150 words)

Marking guide
Student must lodge an enquiry to an online enquiry to ASIC and at least one (1) professional association to clarify the application of the corporate governance requirements into the organisation's internal operations. There is no need for the student to lodge an actual online enquiry, but they must provide their responses in the templates provided below. Responses and wording may vary; however, they should correspond with their responses from Task 1 Questions 2 and 3.

To:	ASIC
Type of Enquiry	e.g. business
Subject:	e.g. Clarification on Corporate Governance

Description of Enquiry/Question:	Responses will vary but must align with their analysis of corporate governance requirements and their application to the organisation's internal operations policies and procedures (Task 1 Question 2). Specifically, this must cover the following: • Disclosure of Directors • Handling of Corporate Information The enquiry must ensure the use of clear and concise language suitable for the audience and purpose.

To:	At least one (1) professional association, e.g. CPA Australia
Type of Enquiry	e.g. business
Subject:	e.g. Clarification on Corporate Governance
Description of Enquiry/Question:	Responses will vary but must align with their analysis of corporate governance requirements and their application to the organisation's internal operations policies and procedures (Task 1 Question 3). Specifically, this must cover the following: • Two (2) selected recommendations from Principle 4 • Application of each recommendation The enquiry must ensure the use of clear and concise language suitable for the recipient and purpose.

Task 3: Internal Control Procedures

Case-study Scenario

You receive correspondence from ASIC and the professional association you've contacted regarding your enquiry on the corporate governance requirements for the business. In addition, they sent you further guidance on how these requirements can be applied to your organisation.

You inform your supervisor Chris Kohler of the responses you have received and the research you have done on Cybersecurity requirements.

Christ asks you to review, develop and amend the procedures for the following control mechanisms for the organisation to begin the update and implementation of the control procedures:

a. Accounting Data Security and Integrity
b. BAS and IAS Reporting

Your supervisor Chris Kohler reminds you that the board is concerned about potential compliance risks from the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) that came into effect on 2 April 2022.

Chris wants to know

- How the organisation handles its cyber-threat exposure through its policies and procedures?
- How the organisation monitors compliance with cybersecurity policies and procedures?
- What could be done to improve in this area?
- Submit draft changes or new draft policies and procedures.

Accordingly, Chris requests you to examine the following:

c. Computer and Email Policy
d. Information and Records Management Policy
e. Internet Access and Computer Use Policy

Refer to the following links to access information on these controls:

Bigger Than Big Accounting Controls

Bigger Than Big Policies and Procedures

- Username: uplearner
- Password: upeducation@123

1. Review the policies and procedures outlined above. Explain how the corporate governance requirements identified from Task 1 can be integrated into the procedures for these controls.

Specify the corporate governance referred to in your responses.

Marking guide

The student must review the following internal control procedures used by Bigger Than Big Corporation:

- Accounting Data Security and Integrity
- BAS and IAS Reporting
- Computer and Email Policy
- Information and Records Management Policy
- Internet Access and Computer Use Policy

The student's responses will vary but should explain how the corporate governance requirements identified from Task 1 can be integrated into the procedures for these controls. Responses will vary but must correspond with the specified corporate governance requirement.

Refer to the sample benchmark answers provided below.

Submission instructions

Write your responses in the spaces provided below.

(Approximate word count 450-550 words)

a. Accounting Data Security and Integrity

Student responses will vary but should include the following.

- In line with the requirement of handling corporate information, Bigger Than Big's policy must outline the persons authorised to access the organisation's accounting data.
- Seek to ensure that third-party partners and service providers maintain similar mechanisms to ensure Accounting Data Security and Integrity or seek to do business only with those who do.

b. BAS and IAS Reporting

Student responses will vary but should include the following.

- In line with the recommendation from ASX, the board must ensure that the CEO has declared that the BAS and IAS are true, accurate and compliant before these are submitted for reporting.
- Seek to ensure that third-party partners and service providers maintain similar BAS and IAS Reporting mechanisms or seek to do business only with those who do.

c. Computer and Email Policy

Student responses will vary but should include the following.

- Updating the policy and procedures to:
- Take into account the rise of social media and specify terms and conditions for its use.
- Link the policy to the requirements of the information and records management and Discrimination and Harassment Policies
- Include trigger points and the actions to take in the event of firewall breaches, attempts to access protected files and areas of data storage without sufficient clearance or passwords, denial of service attacks, or other irregular activity.
- Set an appropriate risk tolerance for the identified risks and ensure that the organisation's risk management framework effectively addresses cyber risks.
- Referencing the Corporate Compliance Policy in this policy and updating the Corporate Compliance Policy to include the importance of Cyber security measures
- Referencing Reporting and Notification policies in this policy and Updating the Reporting and Notification policy to include the importance of and processes for Cyber security reporting
- Ensure that third-party partners and service providers maintain similar mechanisms to monitor cyber risk or seek to do business only with those who do.

d. Information and Records Management Policy

Student responses will vary but should include the following.

Updating the policy and procedures to:

- Stress the importance of reporting breaches of privacy and confidential information
- include trigger points and the actions to take in the event of a data breach or breach of the policy
- include the reporting mechanisms for reporting breaches.
- Referencing the Corporate Compliance Policy in this policy and updating the Corporate Compliance Policy to include the importance of Cyber security measures
- Referencing Reporting and Notification policies in this policy and Updating the Reporting and Notification policy to include the importance of processes for Cyber security
- Ensure that third-party partners and service providers maintain similar Information and Records Management mechanisms or seek to do business only with those who do.

e. Internet Access and Computer Use Policy

Student responses will vary but should include the following.

- Updating the policy and procedures to include the actions to take in the event of a data breach or breach of the policy.
- Updating and expanding the policy and procedures to include specific requirements around breach trigger points for things such as unsuccessful password attempts, unauthorised file access,
- Establishing reporting processes.
- Referencing the Corporate Compliance Policy in this policy and updating the Corporate Compliance Policy to include the importance of Cyber security measures
- Referencing Reporting and Notification policies in this policy and Updating the Reporting and Notification policy to include the importance of processes for Cyber security reporting
- Ensure that third-party partners and service providers maintain similar Internet Access and Computer Use mechanisms or seek to do business only with those who do.

2. Using your findings, develop three (3) internal control procedures that reflect your review of the internal control procedures (Task 3 Question 1) and their integration with corporate governance requirements. You can use the Policies and procedures from the Bigger than Big Corporation as a base, updating or adding to them as required.

Use the Bigger Than Big Style Guide in designing the internal control procedures.

Bigger Than Big Style Guide

- Username: uplearner
- Password: upeducation@123

Ensure that your procedures use clear and concise language suitable for the audience and purpose.

Only one (1) submission is required. However, three (3) sets of internal control procedures must be included in the document.

Submission instructions

Submit your assessment via the LMS.

Save and submit the completed document as shown below.

- FNSACC526 Case Study Task 3 Internal Control Procedures.pdf

(Approximate word count 400-500 words)

Marking guide

The student must develop three (3) internal control procedures that reflect their review of the internal control procedures (Task 3 Question 1) and their integration with corporate governance requirements.

Assessor Guidance: Task three must be completed before the student submits task seven.

The assessor must offer feedback on task three for the student to maintain and further develop the procedures they have developed

Responses will vary depending on students' responses in Task 3 Question 1. And will reflect the following for example:

Accounting Data Security and Integrity

Responses here should reflect the Internal control procedures that affect accounting Data Security and Integrity

The procedures will need to include for each role in the organisation the level of access and authority for each role, e.g.

- Accounts clerk – nil authority to disclose information to others. Limited low level account access, including account creation, but not deletion.
- Account supervisor – authority to provide account information to financial institutions and government authorities. Medium level account access, including account creation, and deletion.
- Financial controller – full authority to disclose information in accordance with legislative, regulatory and organisational requirements. Full level account access, including account creation, deletion, and archiving

Student submission must be formatted following the Bigger Than Big Style Guide, including:

- The corporate logo
- Footers
- Font sizes
- Procedures must be written using clear and concise language suitable for the audience and purpose.
- Only one (1) submission is required. However, three (3) sets of internal control procedures must be included in the document

BAS and IAS Reporting

Responses here should reflect the Internal control procedures that provide measures to ensure proper approvals are obtained before lodgement dates. Procedures can also need to include timetables for BAS and IAS reporting to ensure compliance with legislation.

Student submission must be formatted following the Bigger Than Big Style Guide, including:

- The corporate logo
- Footers
- Font sizes
- Procedures must be written using clear and concise language suitable for the audience and purpose.

Only one (1) submission is required. However, three (3) sets of internal control procedures must be included in the document

Computer and Email, Information and Records Management and Internet Access and Computer use procedue

Responses here should reflect the Internal control procedures that affect cyber security, in the areas of:

- Computer and Email use
- Information and Records Management

- Internet Access

The procedure/s will need to provide the measures which must be taken, for example:

- Updating the policy and procedures to include the actions to take in the event of a data breach or breach of the policy.
- Updating and expanding the policy and procedures to include specific requirements around breach trigger points for things such as unsuccessful password attempts, unauthorised file access,
- Establishing reporting processes.
- Referencing the Corporate Compliance Policy in this policy and updating the Corporate Compliance Policy to include the importance of Cyber security measures
- Referencing Reporting and Notification policies in this policy and Updating the Reporting and Notification policy to include the importance of and processes for Cyber security reporting
- Ensure that third-party partners and service providers maintain similar Internet Access and Computer Use mechanisms or seek to do business only with those who do.

Student submission must be formatted following the Bigger Than Big Style Guide, including:

- The corporate logo
- Footers
- Font sizes
- Procedures must be written using clear and concise language suitable for the audience and purpose.

Only one (1) submission is required. However, three (3) sets of internal control procedures must be included in the document

Guidance: Task three must be completed before submitting task seven.

Your assessor will offer feedback on task three, which you will use to maintain and further develop the procedures you have developed

Task 4: Financial Delegations

1. Create a checklist to document the specific role and responsibilities of each employee involved in the company's accounting operations, ensuring you include payments.

   The role of each employee in the Accounting Operations Division can be found here:

   Accounting Operations Division - Current Employees

   - Username: uplearner
   - Password: upeducation@123

Your responses can refer to the documentation or online sources that specify the job descriptions/responsibilities relevant to each employee's job role.

Your checklist must include the following:

- Each employee's job role
- Three (3) specific responsibilities for each job role
- One (1) internal control that needs to be implemented concerning the transactions processed by each employee

Guidance: See the Bigger Than Big's Accounting Controls intranet page, include any updates that may be affected by your suggestions in Task 3

There's no specific format to the checklist. However, you must use the Bigger Than Big Style Guide in designing the checklist.

(300 -400 words)

Bigger Than Big Style Guide

- Username: uplearner
- Password: upeducation@123

Save and submit the completed document as shown below.

- FNSACC526 Case Study Task 4 Financial Delegations.pdf

Marking guide
The student must create a checklist to document the specific roles and responsibilities of each employee involved in the company's accounting operations. The checklist must be designed using Bigger Than Big's Style Guide and must include the following: • Each employee's job role – is available from Bigger Than Big's intranet page. • Three (3) specific responsibilities for each job role. Responses will vary. However, the job descriptions/responsibilities must be relevant to each employee's role. • One (1) internal control that needs to be implemented concerning the transactions processed by each employee is available from Bigger Than Big's intranet page. Refer to the sample checklist provided below.

Employee Name	Area	Responsibilities	Internal Controls
Gloria	Cash Accounts	□ Cash transactions are appropriately authorised; □ credit card receipts are reconciled with invoices and receipts; □ cash transactions and bank accounts are properly recorded, classified and summarised in financial statements; □ cheques are pre-numbered and accounted for; □ adequate cash funds are available to meet operating expenses; and □ cash surpluses are invested appropriately.	□ Cash payments
Byron	Banking	□ Cash receipts and cheques are banked daily; □ deposits recorded; and □ bank reconciliations are prepared monthly	□ Cash receipts
Brigette	Petty Cash	□ Petty cash imprest system balanced daily; □ copies of receipts maintained; □ all payments authorised; and □ reimbursements are made as required.	□ Cash payments
Monica	Sales and Accounts Receivable	□ Customers have a satisfactory credit rating; □ invoice is prepared in accordance with authorised sales order; □ goods are not despatched without authorised sales order; □ receipts from credit sales and sales returns are properly recorded and authorised; □ accounts receivable subsidiary accounts are reconciled with accounts receivable control account; and □ overdue accounts are monitored	□ Accounts receivable
Gordon	Non-current assets	□ Asset registers are appropriately maintained and updated; □ acquisitions of non-current assets are approved and authorised; □ all non-current assets are accurately recorded in the accounting records; □ depreciation and other related expenses are calculated and charged appropriately; and □ appropriate authority is obtained concerning the disposal of non-current assets and recorded procedures.	□ Forward budgets

Kelly	Stock and inventory	□ No excessive holding of inventory, e.g. wastage; □ inventory movements are approved and recorded; and □ inventory items are periodically checked and reconciled with records.	□ Budget analysis
Marcus	Payroll	□ Accurate records are maintained for hours worked or employees working hours monitored; □ pay rates and payroll functions are authorised and accurate, e.g. calculation of gross pay, deductions, net pay, distributing payments to direct bank accounts; □ payroll figures are accurately recorded, and documentation is kept confidentially and stored in a secure environment, e.g. payroll information, including PAYG tax, payroll tax, and superannuation, is accurately recorded in appropriate ledger accounts; □ changes and records are authorised and updated in a timely manner, e.g. new employees and pay increases; and □ annual payment summaries are provided to employees in a timely manner.	□ Payroll □ Superannuation

2. Outline at least three (3) general steps which can be taken to ensure that the delegations and accountabilities of the Accounting Operations Division are maintained to ensure consistency and compliance as part of the internal control procedures. *(Approximate word count 50 -100 words)*

Marking guide
The student must outline at least three (3) general steps which can be taken to ensure that the delegations and accountabilities of the Accounting Operations Division are maintained to ensure consistency and compliance as part of the internal control procedures.
i. ii. iii. Responses will vary and may include: • Maintain accurate financial records. • Ensure true and fair financial statements are prepared and audited. • Ensure financial viability of the business to ensure payment of all debts. • Ensure all accounting standards are applied in the preparation of all financial information. • All reporting requirements to specific authorities, including ASIC, ASX, and the ATO, are met.

Task 5: Reporting Requirements - Role-play Activity

Pre-Roleplay Activity

This task will require you to role-play a meeting with your supervisor, Chris Kohler and bookkeeper Keira Hoystead. You will discuss the reporting requirements and timetables from specific regulatory authorities, which will be added to the policies and procedures of Bigger Than Big Corporation.

You will require access to:

- Information relating to the continuous and periodic disclosure obligations of the company to the given regulatory authorities:
    - ASX
    - ATO Taxation Requirements: IAS, BAS, PAYG (Withholding)
    - Office of State Revenue - Payroll Tax
    - Superannuation Fund
- Two (2) volunteers to assume the role of:
    - Your supervisor, Chris Kohler
    - The bookkeeper, Keira Hoystead
- Video camera or a mobile phone with video recording capabilities
- A safe environment to conduct the role-playing activity

Read the instructions carefully before proceeding.

Pre-Roleplay Task

Source information on the reporting requirements and the time frame the company follows with respect to the continuous and periodic disclosure obligations of the company to the following regulatory authorities:

- ASX (half-year and annual reports)
- ATO Taxation Requirements:
- IAS (refer to the current month)
- BAS (quarterly and monthly)
- PAYG (Withholding)
- Office of State Revenue - Payroll Tax (refer to your State/Territory)
- Superannuation Fund

Write your responses in the spaces provided below.

(Approximate word count 400 -500 words)

Marking guide
The student must source and outline information on the reporting requirements and the time frame the company follows with respect to the company's continuous and periodic disclosure obligations to the following regulatory authorities. Note: Assessor must refer to information based on the current fiscal year to check if the reporting dates are correct. Refer to the benchmark answers below:

ASX

Reporting dates for 20XX: May vary with the year assessment is completed. The assessor must refer to information based on the current fiscal year to check if the reporting dates are correct.

- Half-year: 28 February and 31 August
- Annual: 30 April or 31 October

Reporting requirements:

- Annual shareholder letter
- Director's report
- Auditor's independence declaration
- Statement of comprehensive income
- Statement of financial position
- Statement of changes in equity
- Statement of cash flows
- Notes to financial statements
- Directors' declaration
- Independent auditor's report
- Corporate governance statement setting out whether or not the company has complied with the Corporate Governance Council's principles and recommendations
- Shareholder information

ATO Taxation Requirements: IAS

Specify the current month:

Reporting dates: Responses will vary depending on the month specified. Refer to this link for the reporting dates for specific months: https://www.ato.gov.au/Business/Reports-and-returns/Due-dates-for-lodging-and-paying/Due-dates-by-topic/Activity-statements/

Reporting requirements: Responses will also vary depending on the month specified. Typically, the company must lodge their monthly activity statements and payment on the reporting date.

ATO Taxation Requirements: BAS

Reporting dates:

Quarterly:

- 1st quarter – July, August, and September: 28 October
- 2nd quarter – October, November and December: 28 February
- 3rd quarter – January, February and March: 28 April
- 4th quarter – April, May and June: 28 July

Monthly: Usually on the 21st day of the month following the end of the taxable period.

Reporting requirements: Businesses must report any Goods and Services Tax (GST) received and paid to the ATO. A business can use an activity statement to report and pay GST a business has collected and claim GST credits.

ATO Taxation Requirements: PAYG (Withholding)

Reporting date: 14 August

Reporting requirements: If a business is operated as a company, the company must withhold amounts from payments made to employees and amounts made from payments to company directors for their services for taxation purposes. The company must report and pay report and pay withheld amounts to the ATO monthly, provide payment summaries to employees, and lodge an annual report after the end of each income year. The PAYG withholding payment summary annual report should be submitted to the ATO by 14 August each year.

Office of State Revenue - Payroll Tax

Specify your State/Territory:

Responses will vary depending on the requirements of the State/Territory. Refer to the following sample benchmark answer:

An organisation must register for payroll tax within seven (7) days after the end of the month where more than $21,153 a week in Australian taxable wages has been paid or where the organisation has become a member of a group that pays more than $21,153 a week in Australian taxable wages. Periodic returns are lodged monthly, and the return must be lodged seven (7) days after the end of the month. The annual return must be lodged by 21 July each year for the previous financial year.

Superannuation Fund

Under the superannuation guarantee law, a business must pay super contributions to eligible employees at a minimum rate of 9.25% of ordinary time earnings. Employees are then able to withdraw this money when they retire. The superannuation may be paid to the employee's nominated fund monthly or every two (2) months.

Additional tasks such as 'reviewing reports' or 'revising documents' must be added to the timeline as appropriate.

Refer to the following link for reporting and lodgement dates for the superannuation fund: https://www.ato.gov.au/Super/APRA-regulated-funds/Reporting-and-lodgment-dates/

Task 5: Reporting Requirements: Role-play Activity

Steps to take:

a. **Access the character brief from this link:**

[Reporting Requirements]

- ○ Username: uplearner
- ○ Password: upeducation@123

Copy the text into a Word document.

- Print these out and provide a copy to each of your participants.
- These will serve as your character brief during the role-play activity.
- This will guide you and your volunteers in completing the role-playing activity.

b. **In this role-playing activity, you must be able to:**

- Accurately discuss the reporting requirements and dates for the financial regulatory authorities relevant to the organisation.
- Demonstrate active listening and questioning skills to elicit, clarify, and convey information.

Guidelines and instructions can be found in the character brief.

Reminder: You must introduce yourself at the start of the video to confirm your identity as the student.

Guidelines:

a. The role-play must be recorded to demonstrate your completion of this activity. Save and submit the recorded video.

b. Ensure to demonstrate and discuss the requirements outlined in the character brief and the Roleplay Activity – Assessor's Checklist.

Option 1: Industry Peers OR Student participant/s

Role play instructions

The role-play/meeting must include at least two (2) participant/s, must not exceed 10 minutes, and must address all elements of the Observation Checklist below.

In this task, you will participate in a role/play meeting with others. These may be resourced using one of the following options:

1. Peer/s who you are already working with, in the industry your qualification relates to.
2. Fellow student/s who will play the role of a team member. Please contact your fellow student/s via the Discussion Forum and coordinate your role play with them directly.

If you cannot find a participant/s to play the role of the other team member/s, contact your assessor via the Discussion Forum, who will discuss options for pairing up with another student/s to complete this task.

Option 1: Peer/s participant

Should you complete this task with your Peer/s, you must fully brief all participant/s, providing them with the context of the role play/meeting, a role outline to play and a copy of the observation checklist so that they can prepare for the recording.

Peer/s will need to state their name and job title at the start of the recording to inform consent.

Option 2: Fellow student/s participant

Fellow student/s participating in the recording must be provided context to their role and responsibilities in the session and have reviewed the assessment activity and observation checklist to prepare for the recording.

Student/s will need to state their name and that they are a student (as their job title) at the start of the recording to inform consent.

Recording instructions

Your role play must be recorded with all participant/s captured in a virtual room using a system such as Zoom, Skype or Teams.

Consent to participate in the recording must be captured for all participant/s at the start of the meeting. This is achieved by the student reading the following statement at the start of the recording, with all participants replying their name and job title to inform consent.

"This session/presentation is being recorded for assessment purposes for my course with Swinburne Open Education. This session will be recorded and submitted through my course online learning platform to my assessor for grading. All participant/s in this session indicate their consent to be included in this recording by stating their name and job title."

The time taken to capture consent at the start of the recording does not count towards the recording time limit.

Include this recording as part of your assessment submission.

Marking Guide
The student must submit a video recording, no more than ten (10) minutes long, of their discussion with Chris Kohler and Keira Hoystead. Refer to the assessor's checklist provided. The assessor must mark all items as 'YES' if the student has satisfactorily completed each requirement. Comments must also be provided for each item.

Assessment marking criteria: Task 5: Observation checklist

During the demonstration of skills, the student has satisfactorily (S) or unsatisfactorily (U):

		S	U
1	Stated their name and the date when the video was recorded. Look for: The student stated their name and the date when the video was recorded	□	□
2	Accurately discussed the reporting requirements and reporting dates for the relevant financial regulatory authorities. Look for: Reporting requirements and dates for each of the following regulatory authorities were discussed: • ASX (half-year and annual reports) • ATO Taxation Requirements: ○ IAS (refer to the current month) ○ BAS (quarterly and monthly)	□	□

	○ PAYG (Withholding) • Office of State Revenue - Payroll Tax (relevant to their State/Territory) • Superannuation Fund Refer the student's discussion to their responses in the Pre-Roleplay Activity.		
3	Demonstrated active listening and questioning skills to: ▪ Elicit, ▪ clarify, and ▪ convey information Look for: • If the student demonstrated active listening and questioning skills through the following: • Maintaining eye contact • Not interrupting the speaker • using open and closed questions • Clarifies information through verbal nods and paraphrasing	□	□

Task 6: Timetables for Implementing Corporate Governance Requirements

Use the information discussed in the role-playing activity in Task 5 to complete the following:

a. Complete the timetables for lodging reports on the following:

- ASX
- ATO Taxation Requirements:
  - IAS
  - BAS
  - PAYG (Withholding)
- Payroll Tax
- Superannuation Fund

Use the template provided.

b. In the Event column, specify the activity and the reporting requirement, e.g. lodge-half year report with ASX.

c. In the Date column, specify the reporting date discussed with Chris Kohler and Keira Hoystead.

d. Save and submit the completed document. Use the filename: FNSACC526 Case Study Task 6 Timetables.pdf

Marking guide
The student must submit the completed timetables for lodging reports based on their role-play activity in Task 5. Responses will vary depending on the month specified/month discussed. However, the reporting dates must accurately correspond to the requirement of the regulatory authorities as outlined in Task 5 Pre-Roleplay Activity. Refer to the benchmarked template for sample responses.

Write your responses in the spaces provided in the template below.

BIGGERTHANBIG
CORPORATION

Timetable for the Month of October

ASX

Event	Date
Lodge half-year report 1 with ASX	28 February 20xx
Lodge half-year report 2 with ASX	31 August 20xx

Payroll Tax

Event	Date
Lodge periodic return	Must be seven (7) days after the end of the periodic month, i.e. 7 November 20xx

Superannuation Fund

Event	Date
Pay super guarantee contributions for quarter 1 (1 July – 30 September)	28 October 20xx
Lodge income tax return for super funds	31 October 20xx

Add more rows for each requirement, where necessary.

Timetable for the Month of: October

Instalment Activity Statement (IAS)

Event	Date
Quarter 1 (July–September) activity statements lodged electronically – final date for lodgement and payment	11 Nov 20xx
October monthly activity statements – final date for lodgement and payment	21 Nov 20xx

Business Activity Statement (BAS)

Event	Date
Lodge GST paid, and GST received	28 February 20xx+1

PAYG (Withholding)

Event	Date
Lodge PAYG withholding payment summary annual report	14 August 20xx+1

Add more rows for each requirement, where necessary.

Task 7: Produce, Review and Distribute Required Reports

In this task, you will implement the internal control procedures required to meet corporate governance reporting requirements; you have been asked to generate specific reports.

For this task, you will need to generate the following reports:

a) **Payroll Summary for the current month:**

You may use any software or template to generate a payroll summary. However, the report you generate must correspond with the timesheets you complete.

- Complete the following timesheets to assist you in generating the payroll summary:

Bigger Than Big Time Sheets

  - Username: uplearner
  - Password: upeducation@123

- Prepare the payroll summary for the three (3) employees.

Guidance: There is no specific template for the payroll summary; however, this document must reflect the details provided in the submitted timesheets.

- Save and submit the completed documents using the following filenames:
  - FNSACC526 Case Study Task 7 Time Sheets.pdf
  - FNSACC526 Case Study Task 7 Payroll Summary.pdf

b) **Balance Sheet for the current month:**

- Enter the following details into the excel balance sheet template provided in this link:

Bigger Than Big Balance Sheet Details

Balance Sheet Template

- Username: uplearner
- Password: upeducation@123

- Save and submit the completed document as a PDF spreadsheet using the following filename:
  - FNSACC526 Case Study Task 7 Balance Sheet.pdf

Marking guide
The student must submit the following documents based on the details provided: a. Completed Timesheets: this is supplementary evidence to assist the student in generating their payroll summary. Details in the timesheets will vary depending on the month entered by the student. However, the following details must be found in the timesheet: ▪ The month and year on all timesheets. ▪ All Mondays in the timesheet should record 8 hours for all employees. ▪ Keira Hoystead must have one (1) recorded sick leave on a Thursday for her second timesheet.

- There are no absences recorded on the student's timesheets.
- There is no overtime work recorded in all employees' timesheets.
- Where the student entered a month with a public holiday, they must specify 'P.H.' on the timesheet.

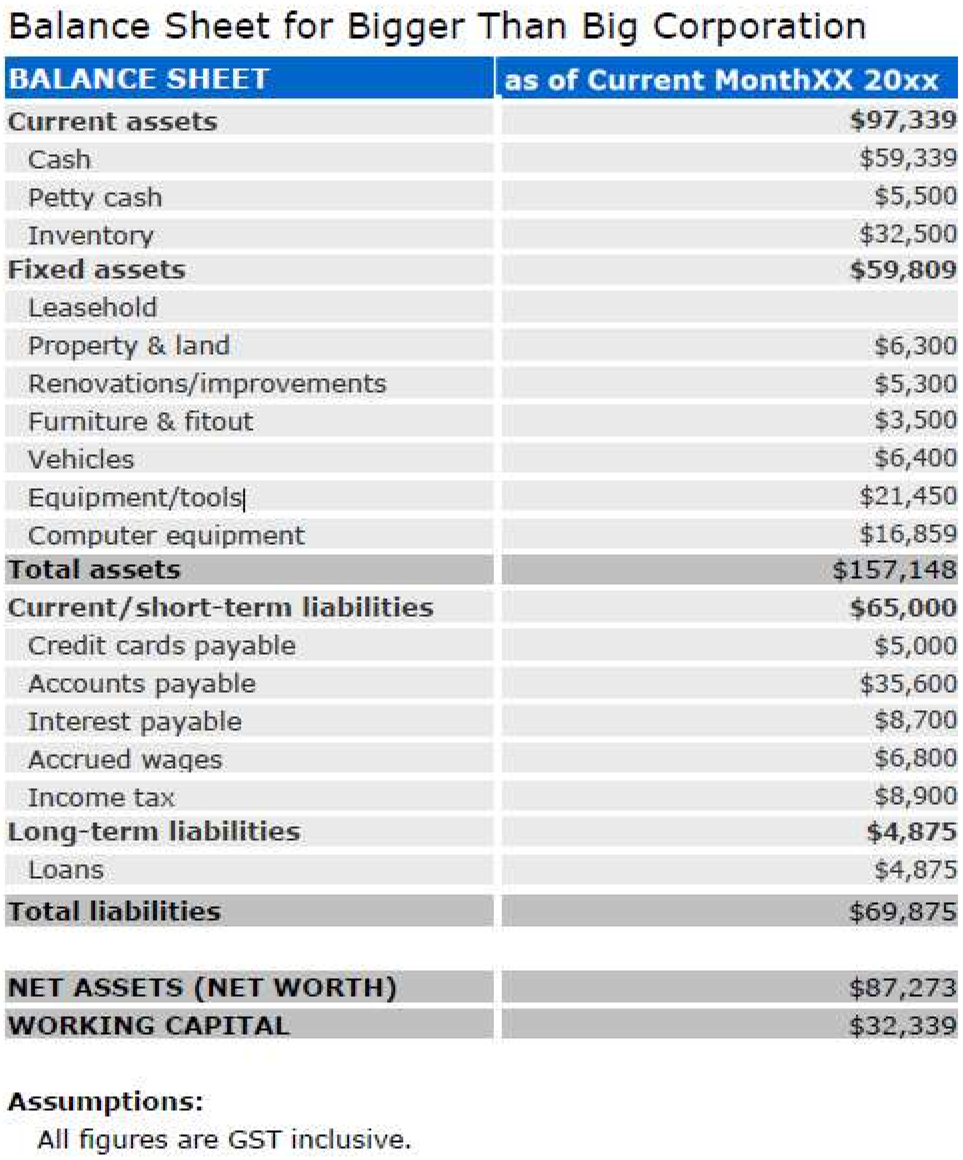
b. Payroll summary for the current month: there is no specific template for the payroll summary; however, this document must reflect the details provided in the submitted timesheets.

Ensure that the payroll summary includes all three (3) persons required:

- The student's
- Keira Hoystead
- Chris Kohler

c. Balance sheet for the current month: Students must correctly enter the details provided in the attached Bigger Than Big Balance Sheet. They may use any software or template to generate their report.

The balance sheet submitted must show the following details:



Balance Sheet for Bigger Than Big Corporation

BALANCE SHEET	as of Current MonthXX 20xx
Current assets	**$97,339**
Cash	$59,339
Petty cash	$5,500
Inventory	$32,500
Fixed assets	**$59,809**
Leasehold	
Property & land	$6,300
Renovations/improvements	$5,300
Furniture & fitout	$3,500
Vehicles	$6,400
Equipment/tools|	$21,450
Computer equipment	$16,859
Total assets	**$157,148**
Current/short-term liabilities	**$65,000**
Credit cards payable	$5,000
Accounts payable	$35,600
Interest payable	$8,700
Accrued wages	$6,800
Income tax	$8,900
Long-term liabilities	**$4,875**
Loans	$4,875
Total liabilities	**$69,875**
NET ASSETS (NET WORTH)	$87,273
WORKING CAPITAL	$32,339

Assumptions:

All figures are GST inclusive.

Note: This balance sheet is generated using the template from business.gov.au

Write your responses in the spaces provided below.

Task 8: Key Performance Indicators (KPIs) and Corporate Governance

Case study Scenario

You have received the following email from your supervisor, Chris Kohler:

Good morning,

Something seems unusual with Bigger Than Big's finances. I can't pinpoint the cause of the problem yet. We had a pretty good financial standing last year, so I figured keeping the same accounting team this year would maintain that performance. I guess not. I'm surprised at the results because our client base is steadily increasing.

To my knowledge, we haven't changed or added any new equipment in the office. The company car is in great shape and isn't due for an overhaul or any sort of major change until next year.

I'm hoping you can help me out with this. Can you evaluate the situation and see how it's affecting our numbers? Then, please get back to me with your findings as soon as possible.

Thanks,

Chris Kohler

Bigger Than Big Corporation

Em: ChrisKohler@BTBC.org.au
Ph: 0145 589 987

Access the company's statement of financial position from this link:

Bigger Than Big Statement of Financial Position

- Username: uplearner
- Password: upeducation@123

For this assessment, 20xx refers to the current year while 20xx-1 refers to the previous year and so on.

1. Evaluate the company's financial performance by indicating at least three (3) observations from Bigger Than Big's Statement of Financial Position.
2. Explain the possible causes of each observation by relating them to the performance of the employees in the Accounting Operations Division.

   In your explanation, determine whether or not the employees have fulfilled the internal control procedures required in their work area.

   ***Guidance:** You may refer to your responses from Task 4.*
3. Based on corporate governance requirements from industry-based practices, specify three (3) ways the company's financial performance can be improved or how this level of performance can be maintained.
4. Write your responses in an email to Chris Kohler using the template below.

   ***Guidance:** There is **no need** to send an actual email.*

Marking guide

The student must write an email to Chris Kohler based on their review of Bigger Than Big's Statement of Financial Position. Responses and wording will vary; however, they must cover the discussion points in the benchmarked template below.

Write your responses in the spaces provided below.

(Approximate word count 400 -500 words)

To:	Chris Kohler
Subject:	Any appropriate subject header
Message:	

The student's email content must cover all of the following discussion points:

- At least three (3) observations from Bigger Than Big's Statement of Financial Position based on their evaluation.
- An explanation of the possible causes of each observation by relating them to the performance of the employees in the Accounting Operations Division. In their explanation, it must be determined whether or not the employees have fulfilled the internal control procedures required in their area of work.

Responses should include three or more of the following:

- Net Profit is lower than in the past two years. The Net Profit of 20xx is less than half of 20xx-1's.
- The company's Net Assets / Total Equity has declined for two (2) years.
- The company's Total Liabilities have increased from 20xx-1, which is suspicious since there is no new equipment, according to the supervisor.
- The Accounts Payable has almost doubled in 20xx from 20xx-1. Georgia may have left these accounts unmonitored.
- Bank Overdraft is greatly increased over the years – more than doubled in 20xx from 20xx-1. It is possible that Byron has not properly monitored the bank transactions.
- There are fewer inventories in 20xx than in 20xx-1 and 20xx-2. This can be a negative thing, as that means the company is lacking in inventory. But this can also be a positive thing, as this can mean fewer stocks on hand and less waste.
- It is possible that because the staff has remained the same for a long period, there has been a lack of check and balance.
- There may be inappropriate or unethical activity going on among the members of the Accounting Operations Division.

Based on corporate governance requirements from industry-based practices, at least three (3) ways on how the company's financial performance can be improved or how this level of performance can be maintained.

Responses should include three or more of the following:

- Conduct risk assessments to identify risks that correlate directly to the organisation's objects both for business and governance, such as:
    - ○ Product Quality
    - ○ Supplier performance

  - The integrity of information – confidentiality, accessibility and usability
  - Accuracy of accounting entries (precision, classification, ratification, valuation)
- Reviewing corporate governance requirements, including reporting periods, taxation payment timings, and corporate and tax laws.
- Measure financial data, including income, assets, expenditure, liabilities and equity.
- Develop processes for safeguarding assets such as insurance cover – type, cost, etc.
- Evaluate the economic and efficiency factors of controls.
- Regular reviews of current policies and procedures to identify changes or improvements.
- Reviewing the specific controls to establish if:
  - Controls are timely in responding to negative events
  - Strengths of selected controls
  - Availability of resources needed to perform the controls

Task 9: Computer and data loss prevention

Instructions:

Case-study Scenario

You receive the following email from Supervisor Chris Kohler.

Good morning,

This morning at 8:56 AM, I received a phone call from our bookkeeper, Keira Hoystead.

On her way to work this morning, she left her laptop on the train, it had slipped from her bag as she exited the carriage, and she could not retrieve it before the doors closed.

Keira informed me that the laptop was not password protected; it did not contain any sensitive files, and she feared that someone could access our systems via the computer's VPN.

- Can you advise me if our existing policies and procedures should have prevented this?
- Can you also advise of any changes to our internal control procedures that could be made to decrease the risk of this happening again?

Thanks,
Chris Kohler
Bigger Than Big Corporation
Em: ChrisKohler@BTBC.org.au
Ph: 0145 589 987

Steps

1. Based on the email message, you are to write a document to address Chris's concerns. *(250 -350 words)*
2. Using the materials you have prepared for tasks 1,2 and 3, consider the Bigger than Big Corporations existing policies :

   Bigger Than Big Policies and Procedures

   - Username: uplearner
   - Password: upeducation@123

   - Computer and Email Policy
   - Information and Records Management Policy
   - Internet Access and Computer Use Policy
3. In a separate document, summarise:
4. If and how the Bigger than Big Corporations existing policies and procedures should have prevented the loss of the computer?
5. Any changes or additions to internal control procedures are required to decrease the risk of such a loss.
6. Use the Bigger Than Big Style Guide in composing your document.

   Bigger Than Big Style Guide

7. Ensure that your document uses clear and concise language suitable for the audience and purpose.
8. Name your document FNSACC526 Case Study Task 9 Internal Control Procedures data loss prevention.pdf

Submission instructions

Submit your assessment via the LMS.

Assessment checklist:

Students must have completed all activities within this assessment task before submitting. This includes:

Student has submitted:		Yes	No
1	The Document FNSACC526 Case Study Task 9 Internal Control Procedures data loss prevention.pdf	□	□
2	Addressed how the Bigger than Big Corporations existing policies and procedures should have prevented the loss of the computer	□	□
3	Any changes or additions to internal control procedures could decrease the risk of such a loss.	□	□
4	Used the Bigger Than Big Style Guide in composing the document.	□	□

Assessment marking criteria: Task 9

Marking guide
Candidate must write a document addressed to Chris Kohler based on their review of Bigger Than Big Corporations Computer and Email, Information and Records Management and Internet Access and Computer Use Policies. Responses and wording will vary; however, they should cover the discussion points below.

Assessor instructions: All sections/questions must be completed. Refer to the template for sample answers and benchmarks.

The evidence submitted demonstrates that the student has satisfactorily (S) covered the following criteria or the evidence is unsatisfactory (U) and requires resubmission.

		S	U
1	Identified the existing policies and procedures would not have prevented the loss of the computer	□	□
2	Candidates' responses can include suggested amendments to the following policies • Computer and Email Policy • Information and Records Management Policy • Internet Access and Computer Use Policy	□	□
3	Suggested amendments may include: • Prohibiting the offsite use of company computers • Mandating password protection for all computing devices • Introducing mandatory two-factor authentication for remote systems access.	□	□
4	The candidate used the Bigger Than Big Style Guide in composing the document to produce a professional document in appearance complying with the organisation's style. Ensured that the responses used clear and concise language suitable for the audience and purpose.	□	□

Task 10: Cyber security breach reporting

Instructions:

Case study Scenario

You have received another email from Supervisor Chris Kohler.

Good morning,

Some more bad news. The I.T. department informed me that bookkeeper Keira Hoystead's lost computer was briefly used to access our main server remotely morning at 09.30 AM.

A copy of the internal staff directory was downloaded before the access was detected, and our I.T. department withdrew VPN login privileges.

The I.T department manually accessed the computer while connected to the VPN and encrypt the hard drive, preventing any other access or data loss.

I.T also recorded the I.P. address of the person using the computer before the VPN activated when accessing the file. The I.P. address was 101.179.194.61

Before VPN access was withdrawn:

Staff names, home addresses, and email addresses appear to have been compromised.

I know you have been doing work with the control procedures embedded in our

- Computer and Email Policy
- Information and Records Management Policy
- Internet Access and Computer Use Policy

However, I am concerned that we have a significant breach of private information, which may require notification to staff and authorities.

I am sending a notification to all staff that the breach has occurred, with our apologies; it will state that:

- All staff email addresses and logins will be changed automatically by the I.T. department,
- Requesting staff to take steps to secure any data sources that may have links to their work email addresses.
- Staff should guard against identity theft by securing their personal information, such as date of birth etc., and updating their personal account passwords

I'm not sure if our policies adequately address what to do in the event of private information breaches or other cyber security breaches.

Can you please immediately update me on what we can do to build reporting of security or privacy breaches into our existing policies and procedures?

Please look at our **Reporting and Notification** Policies and procedures, as I know they were previously focused on reporting WHS issues.

As a pre-emptive measure, I have also attached an Information Security and Privacy Incident Notification Form. Can you please complete it for me using the information I have supplied?

Thanks,

Chris Kohler
Bigger Than Big Corporation
Em: ChrisKohler@BTBC.org.au
Ph: 0145 589 987

Steps

1. Based on the email message, you are to write a document to address Chris's concerns.
2. Using the materials you have prepared for tasks 1,2 and 3, consider the Bigger than Big Corporations existing policies :

   Bigger Than Big Policies and Procedures

   - Username: uplearner
   - Password: upeducation@123

   - Computer and Email Policy
   - Information and Records Management Policy
   - Internet Access and Computer Use Policy
   - And the Reporting and Notification Policy
3. In a separate document, summarise:
4. How the Bigger than Big Corporation can amend its existing policies and procedures to include Reporting and Notification of breaches in cyber security
5. Use the Bigger Than Big Style Guide in composing your document.

   Bigger Than Big Style Guide

6. Ensure that your document uses clear and concise language suitable for the audience and purpose.
7. Name your document FNSACC526 Case Study Task 10 Internal Control Procedures Cyber security breach.pdf
8. Complete the Information Security and Privacy Incident Notification Form

Sample: Information Security and Privacy Incident Notification Form

Section A: General Details	
Organisation Name	the Bigger than Big Corporation
Contact name and position	Chris Kohler
phone number	0145 589 987
email address	ChrisKohler@BTBC.org.au
Describe the steps what happened	A copy of the internal staff directory was downloaded before the access was detected, and our I.T. department withdrew VPN login privileges.
When did it happen?	Today's date/09.30 AM.
When did the organisation become aware of it?	Today's date/09.30 AM.
Describe how it happened	A lost computer was used to access the internal directory.
For example: What caused it? Was it a Malicious or accidental act? Who accessed information in an unauthorised manner? Be as specific as possible. E.g., name the party or describe the nature of the party.	Accidental loss of P.C. Access may have been an accidental download by the person finding the computer or a malicious act. Accessing Person or persons unknown The I.P. address was 101.179.194.61
Describe the steps taken or proposed to contain the incident.	The I.T department manually accessed the computer while connected to the VPN and encrypt the hard drive, preventing any other access or data loss. VPN access was withdrawn:
Describe the steps taken or proposed to prevent future incidents	Policies and procedures are being reviewed to prevent computer and system access without specific access controls.
Section B: Privacy (Personal Information) Incidents	
Fill in this section if the incident relates to personal information. Please visit our website for further information on managing the privacy impacts of a data breach.	
Describe the nature of the personal information involved	Staff names, home addresses, and email addresses appear to have been compromised.
Describe the the risk of harm to the affected individuals	Identity fraud if the information were combined with other identifying information such as Date of Birth, Tax File Numbers etc
Describe the type of harm? How serious? How likely?	There is a low risk of Financial loss or reputational damage as the data accessed did not contain other identifying information.

Describe the how the affected individuals were notified about the incident?	A notification was sent to all staff that the breach had occurred, with apologies; stating: All staff email addresses and logins will be changed automatically by the I.T. department, Requesting staff to take steps to secure any data sources that may have links to their work email addresses. Advising staff to guard against identity theft by securing their personal information, such as date of birth etc., and updating their personal account passwords
If not, why? If so, how? What reactions?	Staff notified by email from Chris Kohler.

Submission instructions

Submit your assessment via the LMS.

Assessment checklist:

Students must have completed all activities within this assessment task before submitting. This includes:

Student has submitted:		Yes	No
1	The Document FNSACC526 Case Study Task 10 Internal Control Procedures Cyber security breach.pdf	□	□
2	Addressed how the Bigger than Big Corporation can amend its existing policies and procedures to include Reporting and Notification of breaches in cyber security	□	□
3	Suggested changes or additions to internal control procedures could decrease the risk of such a loss.	□	□
4	Completed the Information Security and Privacy Incident Notification Form	□	□

Assessment marking criteria: Task 9

Marking guide
Candidate must write a document addressed to Chris Kohler based on their review of Bigger Than Big Corporations Computer and Email, Information and Records Management and Internet Access and Computer Use, and Reporting and Notification Policies. Responses and wording will vary; however, they must cover the discussion points below.

Assessor instructions: All sections/questions must be completed. Refer to the template for sample answers and benchmarks.

The evidence submitted demonstrates that the student has satisfactorily (S) covered the following criteria or the evidence is unsatisfactory (U) and requires resubmission.

		S	U
1	Addressed how the Bigger than Big Corporation can amend its existing policies and procedures to include Reporting and Notification of breaches in cyber security.	□	□
2	Candidates' responses could include suggested amendments to the following policies • Computer and Email Policy • Information and Records Management Policy • Internet Access and Computer Use Policy • Reporting and Notification Policy	□	□
3	Suggested amendments could include: • Updating the policy and procedures to include the actions to take in the event of a data breach or breach of the policy. • Updating and expanding the policy and procedures to include specific requirements around breach trigger points for things such as unsuccessful password attempts, unauthorised file access, • Establishing reporting processes for senior management, the board, staff and authorities • Referencing the Corporate Compliance Policy in all policies and updating the Corporate Compliance Policy to include the importance of Cyber security measures • Referencing Reporting and Notification policies in all policies and Updating the Reporting and Notification policy to include the importance of and processes for Cyber security reporting	□	□

	- Ensure that third-party partners and service providers maintain similar Internet Access and Computer Use mechanisms or seek to do business only with those who do.		
4	The candidate used the Bigger Than Big Style Guide in composing the document to produce a professional document in appearance complying with the organisation's style. Ensured that the responses used clear and concise language suitable for the audience and purpose.	□	□
5	Candidates completed the Information Security and Privacy Incident Notification Form; responses will vary but should paraphrase the model answers in the template provided		

✓

Congratulations, you have reached the end of Assessment 2!