| MODULE NAME: | MODULE CODE: |
|---|---|
| INFORMATION SECURITY | ISEC6311 |

**ASSESSMENT TYPE: ASSIGNMENT 1 (PAPER ONLY)**

**TOTAL MARK ALLOCATION: 100 MARKS**

**TOTAL HOURS: 10 HOURS**

*By submitting this assignment, you acknowledge that you have read and understood all the rules as per the terms in the registration contract, in particular the assignment and assessment rules in The IIE Assessment Strategy and Policy (IIE009), the intellectual integrity and plagiarism rules in the Intellectual Integrity Policy (IIE023), as well as any rules and regulations published in the student portal.*

**INSTRUCTIONS:**

1. ***No material may be copied from original sources, even if referenced correctly, unless it is a direct quote indicated with quotation marks. No more than 10% of the assignment may consist of direct quotes.***
2. ***Make a copy of your assignment before handing it in.***
3. *Assignments must be typed unless otherwise specified.*
4. *All work must be adequately and correctly referenced.*
5. *Begin each section on a new page.*
6. *Follow all instructions on the assignment cover sheet.*
7. *This is an individual assignment.*

## Referencing Rubric

Providing evidence based on valid and referenced academic sources is a fundamental educational principle and the cornerstone of high-quality academic work. Hence, The IIE considers it essential to develop the referencing skills of our students in our commitment to achieve high academic standards. Part of achieving these high standards is referencing in a way that is consistent, technically correct and congruent. This is not plagiarism, which is handled differently.

Poor quality formatting in your referencing will result in a penalty **of a maximum of ten percent being deducted from the percentage awarded**, according to the following guidelines. Please note, however, that **evidence of plagiarism in the form of copied or uncited work (not referenced), absent reference lists, or exceptionally poor referencing, may result in action being taken in accordance with The IIE's Intellectual Integrity Policy (0023)**.

Markers are required to provide feedback to students by indicating **(circling/underlining) the information that best describes the student's work.**

**Minor technical referencing errors: 5% deduction from the overall percentage** – the student's work contains **five or more errors** listed in the minor errors column in the table below.

**Major technical referencing errors: 10% deduction from the overall percentage** – the student's work contains **five or more errors** listed in the major errors column in the table below**.**

**If both minor and major errors** are indicated, then 10% only (and not 5% or 15%) is deducted from the overall percentage. The examples provided below are not exhaustive but are provided to illustrate the error

| **Required:**<br>**Technically correct referencing style** | **Minor errors in technical correctness of referencing style**<br>**Deduct 5% from percentage awarded** | **Major errors in technical correctness of referencing style**<br>**Deduct 10% from percentage awarded** |
|---|---|---|
| Consistency<br>• The same referencing format has been used for all in-text references and in the bibliography/reference list. | Minor inconsistencies.<br>• The referencing style is generally consistent, but there are one or two changes in the format of in-text referencing and/or in the bibliography.<br>• For example, page numbers for direct quotes (in-text) have been provided for one source, but not in another instance. Two book chapters (bibliography) have been referenced in the bibliography in two different formats. | Major inconsistencies.<br>• Poor and inconsistent referencing style used in-text and/or in the bibliography/ reference list.<br>• Multiple formats for the same type of referencing have been used.<br>• For example, the format for direct quotes (in-text) and/or book chapters (bibliography/ reference list) is different across multiple instances. |
| Technical correctness<br>Referencing format is technically correct throughout the submission.<br>Position of the reference: a reference is directly associated with every concept or idea.<br>For example, quotation marks, page numbers, years, etc. are applied correctly, sources in the bibliography/reference list are correctly presented. | **Generally, technically correct with some minor errors.**<br>• The correct referencing format has been consistently used, but there are one or two errors.<br>• Concepts and ideas are typically referenced, but a reference is missing from one small section of the work.<br>• Position of the references: references are only given at the beginning or end of every paragraph.<br>• For example, the student has incorrectly presented direct quotes (in-text) and/or book chapters (bibliography/reference list). | **Technically incorrect.**<br>• The referencing format is incorrect.<br>• Concepts and ideas are typically referenced, but a reference is missing from small sections of the work.<br>• Position of the references: references are only given at the beginning or end of large sections of work.<br>• For example, incorrect author information is provided, no year of publication is provided, quotation marks and/or page numbers for direct quotes missing, page numbers are provided for paraphrased material, the incorrect punctuation is used (in-text); the bibliography/reference list is not in alphabetical order, the incorrect format for a book chapter/journal article is used, information is missing e.g. no place of publication had been provided (bibliography); repeated sources on the reference list. |
| **Congruence between in-text referencing and bibliography/ reference list**<br>• All sources are accurately reflected and are all accurately included in the bibliography/ reference list. | **Generally, congruence between the in-text referencing and the bibliography/ reference list with one or two errors.**<br>• There is largely a match between the sources presented in-text and the bibliography.<br>• For example, a source appears in the text, but not in the bibliography/ reference list or vice versa. | **A lack of congruence between the in-text referencing and the bibliography.**<br>• No relationship/several incongruencies between the in-text referencing and the bibliography/reference list.<br>• For example, sources are included in-text, but not in the bibliography and vice versa, a link, rather than the actual reference is provided in the bibliography. |
| **In summary:** the recording of references is accurate and complete. | In summary, at least **80%** of the sources are correctly reflected and included in a reference list. | In summary, at least **60%** of the sources are incorrectly reflected and/or not included in reference list. |

**Overall Feedback** about the consistency, technical correctness and congruence between in-text referencing and bibliography:

.................................................................................................................................................................................................

.................................................................................................................................................................................................

## Case study

The advent and adoption of advanced information technology tools are gaining momentum worldwide, and the banking industry is capitalizing on it. The banking industry has always been regarded as one of the most stringent due to the nature of its business,  services and vulnerability, therefore, in order to survive, it had to adhere to various industry standards, code of conduct, government regulations, auditing requirement and so on. Nevertheless, for centuries, their services areare still gained momentum; providing secure banking services to their client worldwide. Traditionally, clients would be 'going to the bank' for whatever services that they want. Today the use of ICT made it possible to bank wherever the client is. Not only the client would be banking from the comfort of their homes or the place they choose to be at the time of interaction, but they can also do so at any given time.

No need to highlight the type of confidential information banks would be collecting from their respective clients in order to comply with various regulations, but they are also expected to protect the integrity of that information as long as they have them, they perceive flexibility of client being able to gain access to their asset from the remote distance brings to light to the question of information security, data encryption, authenticity, data validation, and authorization.

Not too long ago, one of the newest banks in the Republic of South Africa decided to only provide their services online, meaning no direct physical contact with the bank staff members, SimunyeBank as it is known, does not have any branches, all their customer relied on the internet for services, from their initial account application to the cash deposit or withdrawal, all is done via the internet or at various kiosk and ATM scattered around the country major public places and commercial centers.

Interest client can call their call centers for human voice assistance, but most of the time, a client can download their applications and use them as they choose to without any time or location limitation. The bank employs thousands of employees most of them worked from their respective homes, and provide their services to a customer using a virtual private network (VPN) connection which is a secure and encrypted internet line.

After 4 years of operation, as per regulation, internal audit schedule must take place ahead of banking regulator ones, the company noticed that most of their clients are young people between the age of 16 to 40 years old, mostly college-educated, and professional, although their financial figure looks or may be positive, the bank estimates that there is a pool of senior citizen out there looking for a reliable and trustworthy bank for their immense financial capital, tapping into this market could increase their revenue.

Technically speaking, the headquarter of SimunyeBank is located at Sandton, Gauteng, but the ITC technical division is located in Sunninghill. The bank also heavily relied on a number of outsourcing service providers, software vendors, independent contractors, both locally and abroad and so on. Some of these service providers are located outside of South Africa and speak foreign languages.

A couple of years ago, another well-known bank, which is also licensed to operate in South Africa was a victim of ransomware from an unknown individual who was requesting financial compensation to release their grips on their systems, their customers were left for days without access to their internet banking systems, an employee at the branch could not log in to the intranet, those at the head-quarter could not be viewed or monitored transactions at various branches countrywide, originally, it was described as a 'mass-attack', but some experts describe it as a 'targeted-attack' since many other banks in the country were not victimised. For failing to pay the requested reason, many customer private information were found unencrypted on the foreign-based website, as a result, the institution came under various scrutinise, from the state banking regulator, customer launching lawsuit against them, potential customer avoiding them and so forth, at the end they lost public trust and interest.

Given the above, SimunyeBank is well-aware of its level of vulnerability and risk, given the nature of its service and the method of its delivery. Its chief information officer, embarked on the wide campaign to re-evaluate their threat, vulnerability and risk, starting with all their own employee, their systems, the physical environment, their internal operation, the framework guiding their business. The bank hired an external investing unit to look at their employee education, background, and past professional history since their internal audit report indicated some discrepancies. They then move to independent contractors, and then outsource service providers, it is important to note their server ran on open-source software, these service providers have access to all customer information with no or little restriction, it is also important to note that outsource service provider are not employees of the institution and therefore SimunyeBank cannot audit them nor participate in their employee recruitment drives. The report of the audit indicated a wide range of risks faced by the bank such as:

- Theft of customer information for the malicious purpose by employees, using their own medium to copy them.
- Denied of service to clients and employees since the internet is the sole means of communication.
- Limitation of VPN
- Little control over an independent contractor, outsourcing service providers, during and after hours of operation.
- Absence of service level agreement with outsource service providers to adhere to regulatory requirements.
- The internal security threat from own ICT employees, who naively planted the device on the network which facilitated external connection.

- External mass or targeted attack from hackers.
- General low-speed Internet access in the country sometimes gives the customer the impression of 'NO connectivity' while the process is still ongoing.
- Etc.

**Question 1** **(Marks: 100)**

Based on the case study above, you are expected to write an essay report which must be structured as described below.

Your report must be structured in the following approach.

| | | |
|---|---|---|
| **Q.1.1** | Executive summary | (5) |
| **Q.1.2** | Background (pay attention to local south African banking online risk only). | (5) |
| **Q.1.3** | The best approach to evaluate internal versus the external threat to IT systems | (10) |
| **Q.1.4** | The most appropriate method to deal with an outsourced staff member is concerning internal threats and system vulnerability. | (10) |
| **Q.1.5** | The role of data encryption when dealing with customers and remote workers. | (5) |
| **Q.1.6** | The possible role of cloud-based computing to deal with a case study. | (5) |
| **Q.1.7** | The impact of CIAA. | (10) |
| **Q.1.8** | Given the perceived level of vulnerability of SimunyeBank, what is the best method of implementing business continuity? | (10) |
| **Q.1.9** | The best method to deal with IT risk mitigation. | (10) |
| **Q.1.10** | Describe some of the limitations of VPN and how they can be overcome. | (10) |
| **Q.1.11** | How can CIO address some of the limitations listed in the case study given the nature of the industry and restriction of the sector regulator? | (10) |
| **Q.1.12** | Conclusion. | (10) |

## Appendix A

**Please note: Tear** off this section and **attach** it to your work when you submit it.

| | |
|---|---|
| **MODULE NAME:** | **MODULE CODE:** |
| **INFORMATION SECURITY** | **ISEC6311** |

| |
|---|
| **STUDENT NAME:** |
| **STUDENT NUMBER:** |

| **RUBRIC 1 — SKELETON OUTLINE** | **Levels of Achievement** | | | | **Feedback** |
|---|---|---|---|---|---|
| | **Excellent** | **Good** | **Developing** | **Poor** | |
| | **Score Ranges Per Level (½ marks possible)** | | | | |
| Executive summary | **5** | **4** | **2-3** | **0-1** | |

| **RUBRIC 1 — SKELETON OUTLINE [continued]** | **Levels of Achievement** | | | | **Feedback** |
|---|---|---|---|---|---|
| | **Excellent** | **Good** | **Developing** | **Poor** | |
| | **Score Ranges Per Level (½ marks possible)** | | | | |
| Background (pay attention to local south African banking online risk only). | **5** | **4** | **2-3** | **0-1** | |
| The best approach to evaluate internal versus the external threat to IT systems | **8-10** | **5-7** | **3-4** | **0-2** | |
| The most appropriate method to deal with an outsourced staff member is concerning internal threats and system vulnerability. | **8-10** | **5-7** | **3-4** | **0-2** | |
| The role of data encryption when dealing with customers and remote workers. | **5** | **4** | **2-3** | **0-1** | |
| The possible role of cloud-based computing to deal with case study. | **5** | **4** | **2-3** | **0-1** | |
| The impact of CIAA. | **8-10** | **5-7** | **3-4** | **0-2** | |

| | | | | | |
|---|---|---|---|---|---|
| Given the perceived level of vulnerability of SimunyeBank, what is the best method of implementing business continuity? | **8-10** | **5-7** | **3-4** | **0-2** | |
| The best method to deal with IT risk mitigation. | **8-10** | **5-7** | **3-4** | **0-2** | |
| Describe some of the limitations of VPN and how they can be overcome. | **8-10** | **5-7** | **3-4** | **0-2** | |
| How can CIO address some of the limitations listed in the case study given the nature of the industry and restriction of the sector regulator? | **8-10** | **5-7** | **3-4** | **0-2** | |
| Conclusion | **8-10** | **5-7** | **3-4** | **0-2** | |
| **Question 1** | | | | | **/100** |