ACHIEVEMENT EXEMPLAR 2022

2

NZQA
NEW ZEALAND QUALIFICATIONS AUTHORITY
MANA TOHU MĀTAURANGA O AOTEAROA

QUALIFY FOR THE FUTURE WORLD
KIA NOHO TAKATŪ KI TŌ ĀMUA AO!

COMMON ASSESSMENT TASK

Level 2 Digital Technologies and Hangarau Matihiko 2022

91898 Demonstrate understanding of a computer science concept

Credits: Three

Achievement Criteria		
Achievement	**Achievement with Merit**	**Achievement with Excellence**
Demonstrate understanding of a computer science concept.	Demonstrate in-depth understanding of a computer science concept.	Demonstrate comprehensive understanding of a computer science concept.

Type your School Code and 9-digit National Student Number (NSN) into the space below. (If your NSN has 10 digits, omit the leading zero.) It should look like "123-123456789-91898".

There are three questions in this document. **Choose ONE question to answer.**

You should aim to write **800–1500 words** in total.

Your answers should be presented in 12pt Times New Roman font, within the expanding text boxes, and may include only information you produce during this assessment session. Internet access is not permitted.

Save your finished work as a PDF file with the file name used in the header at the top of this page ("SchoolCode-YourNSN-91898.pdf").

By saving your work at the end of the examination, you are declaring that this work is your own. NZQA may sample your work to ensure that this is the case.

INSTRUCTIONS

There are three questions in this assessment, on the topics of:

- Artificial intelligence (page 3)
- Computer security (page 8)
- Complexity and tractability (page 13).

Choose only ONE question to answer. Note that parts (b), (c), and (d) of the question include options for you to choose from.

Read all parts of your chosen question before you begin. Do not repeat information in different parts of the assessment.

EITHER: **QUESTION ONE: Artificial intelligence**

(a)   (i)   Name a **specific** New Zealand-based company or organisation that uses artificial intelligence.

    (ii)   How does this organisation use artificial intelligence?

    (iii)   What are at least TWO advantages of this organisation using artificial intelligence?

(b) Choose TWO of the following to answer:

- What common issues are found when developing an artificial intelligence solution?
- Give an example of how an artificial intelligence is trained.
- How can you evaluate the effectiveness of an artificial intelligence?

Choice (1) – (copy and paste below)

Response

Choice (2) – (copy and paste below)

Response

(c)   Choose ONE of the following to answer:
- What positive effects might artificial intelligence bring in the future?
- What negative effects are artificial intelligences currently having on people?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

Response

Weak AI refers to systems that are programmed to accomplish a wide range of problems but operate within a predetermined or predefined range of functions. Strong AI, on the other hand, refers to machines that exhibit human intelligence.

Source (adapted): http://www.differencebetween.net/technology/difference-between-strong-and-weak-ai/

(d) Choose ONE of the following to answer:

- Organisations have a choice of developing "weak AI" or "strong AI". Explain why an organisation may choose one over the other. What are the risks and opportunities for an organisation changing from "weak AI" to "strong AI"?

OR

- The Turing test originated in 1950. How likely is it that your chosen organisation's artificial intelligence would pass the test?
  Discuss how relevant the test is in evaluating the effectiveness of your chosen organisation's artificial intelligence.

Choice (copy and paste below)

Response

This page has been deliberately left blank.

OR: QUESTION TWO: Computer security

(a) (i) Name a **specific** New Zealand-based company or organisation that has had **issues** with computer security.

> �▬

(ii) What were the issues this organisation had with computer security?

> ▬▬ has had issues with phishing, ddos and brute force attempts and getting passwords. These are a few of the attacks ▬▬ has had directed towards them.

(iii) What are TWO steps the organisation took to deal with these issues?

> They have had to take different approaches to deal with different attacks. Phishing attacks are one of the most common type of attacks they will receive because they are super easy to do. Phishing is most commonly sending an email to someone with the intent of getting their information by impersonating a company most commonly google. Phishing fails basically 99% of the time because people have started getting better at recognizing them. but when there a scammer sends email to a large company with thousands of employees it is almost certain to get at least 1 of them and that would be bad because the attacker could gain access to all of ▬▬'s data and information. This has happened at ▬▬ before but the employee went straight to the IT department and they deactivated all of their accounts and changed their passwords.
>
> Firewalls are a great tool to stop incoming ddos and brute force attacks because they monitor and filter all incoming data on your home network and blocking any unwanted attacker from being able to access the information in your home network basically being able to see and steal everything you do online and they would even be able to send stuff onto your computer. Firewalls are a great way to stop attacker stop getting anything from you and all companies should have them.

(b) Choose TWO of the following to answer:
- What are common issues all individuals or organisations have with computer security?
- What steps can an organisation take to protect its computer security?
- What are the signs an individual might recognise that help them identify they are being targeted by a scammer?

Choice (1) – (copy and paste below)

> What are common issues all individuals or organisations have with computer security?

Response

> Probably the most well-known type of cyber security is antivirus's because they come preinstalled on windows computer when you buy them most people know what they are. They are a very necessary piece of software because it can stop malware and harmful downloads it is something that everyone should have but not MacAfee which come preinstalled on most windows laptops it is just plain bad and slows down your Computer Windows defender is better than it.
>
> ▨▨▨▨ has had a lot of security threats in the past and as I'm typing this they are probably being attacked through things like ddos attacks and other means of trying to get their information. because they are a security company this is basically guaranteed to happen. I have already talked a lot about phishing attacks which are those annoying emails you probably get spammed with which are just the most super annoying thing ever yeah those a phishing attack them are made by scammers to try and take your information but they are almost always unsuccessful but the reason why scammers still use them is the sheer amount of email they can send out is bound to get somebody.

Choice (2) – (copy and paste below)

> What steps can an organisation take to protect its computer security?

Response

> Firewalls and antiviruses are great ways to protect yourself when online. Firewalls are a layer of security that will block unwanted attacks for example ddos attacks can be blocked by internet firewalls which monitor incoming traffic on your router and can block anything you don't want. Anti-viruses are great for if you have already made a mistake by downloading something you should not have. There are different types of antivirus's some check what you are downloading and stops it from finishing these are great and are also the best way of preventing yourself from getting a virus. Let's way you don't have that type of anti-virus and you accidentally do download something harmful there are antiviruses that scan everything on your computer every set amount of time Windows has this enabled by default and in my experience having downloaded a few bad things in my time on the internet I can tell you that windows defender is actually really good at its job but I would say that you should not fully trust it because it is the most common antivirus a lot of viruses can get around it using various ways which is why it's best to also have another anti-virus also installed.

(c)   Choose ONE of the following to answer:

- How can the security of computers be protected against future risks?
- What impact do peoples' attitudes and behaviour have on computer security?

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

> How can the security of computers be protected against future risks?

Response

> Hackers and scammer will always be coming up with new ways of getting through security. The best way of stopping hackers if the future is by keeping your computer up to date of the operation system you are using because these small updates are fixing security issues they may not change anything that you can see or tell but please do them they are very important in keeping your computer secure against hackers. This is something that ▆▆▆▆▆▆ has to think about when using their computer systems because they need them to be as secure as possible.

(d)   Choose ONE of the following to answer:

- Operating systems, drivers, software, and firmware all require updates. Discuss the purpose of these different updates in maintaining computer security.
- Organisations commonly have firewalls at the entry point of the internet as well as on individual computers. Discuss why these are needed to maintain computer security.

You should consider this question in the context of the organisation you wrote about in part (a).

Choice (copy and paste below)

> Organisations commonly have firewalls at the entry point of the internet as well as on individual computers. Discuss why these are needed to maintain computer security.

Response

> Firewalls are Super important because they are the main way of block any incoming attacks to the internet or computer ▆▆▆▆▆▆ is always being attacked by hacked trying to get into their systems wand without firewalls their companies would not be able to function with the amount of data being sent to their servers. Firewalls are super important for keeping your computer working.

This page has been deliberately left blank.

OR: **QUESTION THREE: Complexity and tractability**

(a) (i) Name a common example of complexity and tractability.

(ii) Explain in detail why this is an example of complexity and tractability.

(b) Choose TWO of the following to answer:

- Give a practical example where it would be good for a solution to an intractable problem not to be found.
- Give a practical example where it would be good for a solution to an intractable problem to be found.
- Give a practical example of a mechanism that can be used to partly solve an intractable problem. What are its limitations?

Choice (1) – (copy and paste below)

Response

Choice (2) – (copy and paste below)

Response

(c) Choose ONE of the following to answer:
- What are some ways that complexity or tractability can be future-proofed?
- What positive or negative effects does the field of complexity or tractability have on people?

Choice (copy and paste below)

Response

(d)   Choose ONE of the following to answer:

- A real-world "solution" to an intractable problem, such as route planning, includes a number of additional factors such as one-way streets. Discuss how effective these solutions need to be and how you can measure their effectiveness.

- The "travelling salesman problem" is easy to solve with only a small number of destinations. Discuss why this becomes intractable as more destinations are added.

Choice (copy and paste below)

Response

Achievement Exemplar 2022

Subject	Digital Technologies Level 2		Standard	91898	Total score	03
Q2	**Grade score**	**Annotation**				
(a)		The candidate chose a NZ company and gave two good issues they experienced and steps the company took to deal with the threats.				
(b)	A3	Good common issues were discussed, there was an amount of repetition from the answer to (a) but sufficient new ideas to gain an overall 03 grade.				
(c) & (d)		The Merit and Excellence answers were not detailed enough to gain a higher grade.				