Government of Western Australia
North Metropolitan TAFE

Lab 3

Qualification national code and title	Transition to Cyber Security
Unit/s national code/s and title/s	VU23217 – Recognise the need for cyber security in an organisation

Assessment type (☑):

☐ Questioning (Oral/Written)
☐ Practical Demonstration
☐ 3rd Party Report
☒ Other – Project/Portfolio *(Part of assessment task 1)*

Assessment Resources:

- PC
- Google
- Computer components PowerPoint

Assessment Instructions:

Instructions to the assessor:
This lab is a part of Assessment Task 1 portfolio, it is a practical lab based on the performance criteria requirements of the unit. Each student should be given a copy of this lab to complete either in class or out of class. As the student completes each section of this lab you should verify, check off and sign off the section (Use this document as the observation checklist). Use the assessor section at the bottom to provide feedback to the student if required.
See the instructions to the student section for the remainder of the instructions.

Instructions to the student:
This lab consists of short answer questions where you will be asked to research and answer questions relating to cyber security. You are encouraged to use the documentation in the resource section to help you work on the requirements.
Time:
Approximately 60 minutes

Due date:
This lab is part of assessment 1 and inherits its due date.

Submission instructions:
When the lab is complete, submit the assessment via Blackboard.

Reasonable adjustment:
Should there be difficulty with reading technical manuals relating to disability of language and literacy levels you are encouraged to use online video tutorials similar to the following:

- https://www.youtube.com/watch?v=HBP8_LqBj44

The lab can be delivered in combination with support software like “Cortana” to help verbalise the tasks. Tasks may also be re-phrased by the assessor if required. If there are issues with resources (e.g. Blackboard/Routers) the lab can be modified to suit assuming it does not compromise its original intent.

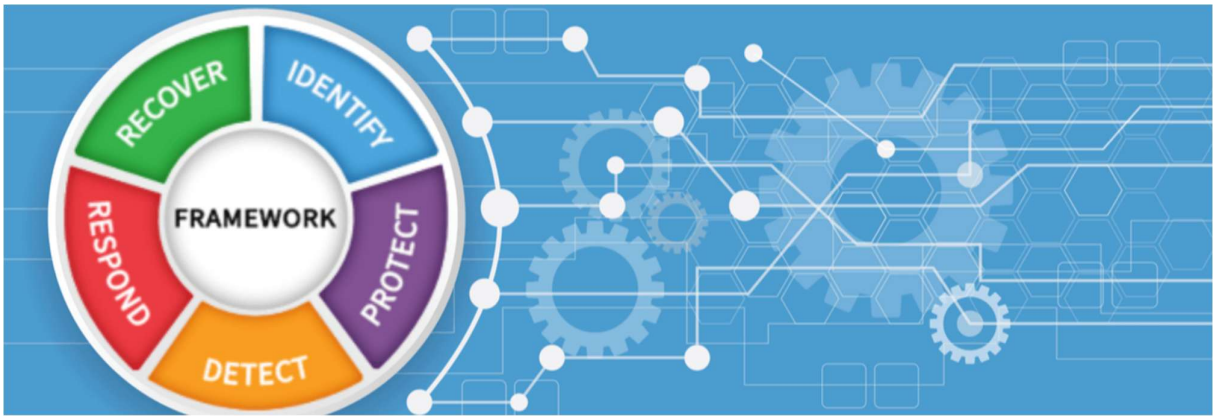
Government of Western Australia
North Metropolitan TAFE

Lab 3

Qualification national code and title	Transition to Cyber Security
Unit/s national code/s and title/s	VU23217 – Recognise the need for cyber security in an organisation

1. The NIST CSF

The American NIST framework is very well known. In this section we explain the various aspects of the framework.



1.1 Briefly explain what the NIST CSF is?

The National Institute of Standards and Technology (NIST) created the NIST Cybersecurity Framework (CSF) as a series of recommendations to assist businesses in managing and lowering cybersecurity threats. By offering an organized method based on the five essential tasks of Identify, Protect, Detect, Respond, and Recover, it helps businesses to improve resilience, fortify their cybersecurity posture, and match security initiatives with corporate goals.

1.2 List the core components of the NIST CSF?
Framework Core, Implementation Tiers, and Profiles are the three main parts of the NIST Cybersecurity Framework. While Implementation Tiers indicate maturity levels and Profiles match cybersecurity operations with business goals, the Framework Core delineates five functions: Identify, Protect, Detect, Respond, and Recover.

1.3 How can an organisation use the NIST CSF?

The NIST CSF is a tool that a business can use to evaluate its present cybersecurity procedures, find weaknesses, and rank enhancements. Through constant monitoring and development, it directs the creation of risk management plans, synchronizes security measures with corporate objectives, and strengthens overall resistance to cyberthreats.
1.4 What are the benefits to an organisation in using the NIST CSF?

Organizations may strengthen resilience, lower risks, and improve cybersecurity posture by utilizing the NIST CSF. It supports regulatory compliance, encourages standardized risk management, improves communication between technical and business teams, and permits ongoing development in safeguarding vital assets and successfully handling cyber incidents.

Qualification national code and title	Transition to Cyber Security
Unit/s national code/s and title/s	VU23217 – Recognise the need for cyber security in an organisation

1.5 Is the use of the NIST CSF mandatory?

It is not required to use the NIST Cybersecurity Framework. It is a risk-based, voluntary framework intended to help businesses enhance their cybersecurity procedures. Nonetheless, it is adopted as a best practice or regulatory reference by numerous companies and government organizations.

2. The Essential 8

The Australian Essential 8 framework is not quite as well known internationally; but it serves an important purpose. In this section various questions are posed concerning this framework.

2.1 Briefly explain what the Essential 8 is all about?

The Australian Cyber Security Centre (ACSC) created the Essential 8, a collection of fundamental cybersecurity tactics, to assist businesses in reducing online dangers. Through realistic, prioritized security rules, it focuses on preventing infections, reducing breaches, and guaranteeing quick recovery.

2.2 What are some of the key elements of the Essential Eight Strategies?

To successfully prevent, limit, and recover from cybersecurity incidents, the Essential 8 Strategies include key components such as application whitelisting, patching operating systems and applications, configuring Microsoft Office macro settings, user application hardening, limiting administrative privileges, multi-factor authentication, frequent backups, and application control.

2.3 Briefly explain how an organisation can implement and make use of the Essential 8 strategy?

By evaluating present security procedures, finding weaknesses, and gradually implementing each control, a company can put the Essential 8 into practice. Strengthening defences, reducing risks, and enhancing overall cybersecurity resilience can be achieved through routinely updating systems, enforcing access rules, training personnel, and keeping an eye on compliance.

Qualification national code and title	Transition to Cyber Security
Unit/s national code/s and title/s	VU23217 – Recognise the need for cyber security in an organisation

2.4 What are some of the benefits of implementing the Essential Eight Strategies?

By putting the Essential 8 Strategies into practice, businesses may lower their cyber risks, stop malware infections, and minimize data breaches. It improves system resilience, guarantees quicker incident recovery, facilitates regulatory compliance, and offers an affordable, workable framework for enhancing operational continuity and overall cybersecurity posture.

3. The Centre for Internet Security (CIS) Controls

The CIS controls are complementary to NIST and Essential 8. Various questions are posed concerning what it is, and how it is implemented and used in an organisation.

3.1 What are the Center for Internet Security (CIS) Controls?
The Center for Internet Security created a collection of cybersecurity best practices known as the CIS Controls. They enhance overall security posture and risk management by assisting firms in prioritizing and putting defensive measures in place to stop, identify, and react to cyberthreats.

3.2 How many CIS Controls are there?

The 18 CIS Controls are arranged to assist enterprises in methodically enhancing cybersecurity. With Implementation Groups directing adoption according to company size and resources, they offer focused, doable steps for strengthening overall security posture, enhancing risk management, and thwarting cyber threats.

3.3 What are some examples of Basic CIS Controls?

Inventory and control of software and hardware assets, ongoing vulnerability management, and restricted use of administrative capabilities are a few examples of basic CIS controls. These fundamental steps assist businesses in gaining visibility and defending vital systems from online attacks.

Qualification national code and title	Transition to Cyber Security
Unit/s national code/s and title/s	VU23217 – Recognise the need for cyber security in an organisation

3.4 Why are the Center for Internet Security (CIS) Controls important for organizations?

The CIS Controls are crucial because they give businesses a list of cybersecurity measures that are prioritized and actionable. They boost security posture, support risk management, guarantee compliance, assist in preventing, detecting, and responding to threats, and successfully defend vital assets from cyberattacks.

3.5 How can organizations implement the CIS Controls?

By evaluating current security procedures, ranking controls according to risk, and gradually implementing them, organizations can put CIS controls into place. Effective defence, compliance, and enhanced resilience against changing cyberthreats are ensured by ongoing monitoring, patching, access management, staff training, and frequent audits.