Government of Western Australia
South Metropolitan TAFE

Delivery and Assessment Plan (DAP)
QD020102

Qualification Details		
Training Package Code & Title	ICT - Information and Communications Technology (Release 6.0)	
Qualification National Code & Title		State code:
ICT40120 Certificate IV in Information Technology (Networking)		AC10

Units of Competency (UoC) detailed in this DAP | Cluster : Cyber Security	
Unit National code and title	State Code
BSBXCS404 Contribute to cyber security risk management	OBO73

Duration of Training/location and group details					
Group Details	**Thornlie CIV-Prog-stage-2 & Dip-Prog-stage-1 & CIV-Games-stage-2 (Semester 2, 2022)**				
Start date	22/07/2022	End date:	09/0122022	Session Times:	Friday 9:00-10:00
Location	Thornlie Campus, Room 8G31			Lecturer:	Nabin Yadav
Group Details	**Thornlie CIV-Networking-stage-1 (Semester 2, 2022)**				
Start date	22/0172022	End date:	09/12/2022	Session Times:	Friday 12:30-13:30
Location	Thornlie Campus, Room 8G22			Lecturer:	Suganya Devi Ramalingam
Group Details	**CIV Genral (Semester 2 2022)**				
Start date	04/10/2022	END DATE:	07/12/2022	Session Times:	Wednesday 08:30-12:30
Location	Thornlie Campus, Room8G31			Lecturer:	Samad Abdus
Mode of delivery	☒ Face to face ☐ On-the-job	☐ Flexible ☐ Other		☐ Combination (describe) *See study requirements*	

Individual study requirements	Students are provided with 20 hours of instructor lead tuition and classroom based activities. In addition, students are expected to complete 15 hours of prescribed activities, self-study/assignmentsfor this unit in their own time outside of class time. **Virtual Classrooms** The mode of delivery may change from face-to-face delivery to a Virtual Classroom in order to meetthe COVID-19 social distancing requirements. If the delivery mode changes to Virtual Classroom, your lecturer will use Blackboard Collaborate to conduct classes as per your usual timetable. Students are expected to attend these sessions as withstandard face to face classes. Blackboard Collaborate allows the lecturers to communicate with the whole group using voice and/orvideo and to communicate with individual students using break out sessions. Where students need todo group activities this can also be achieved using break out sessions. Virtual Classroom sessions can be accesses via Internet from home. Where students are unable to access the internet from home please contact your lecturer as you may be able to access the internetfrom the college library or other computing facilities at the college.

Pre-requisite requirements

Nil

Lecturer contact information

Lecturer: Ken Beck
Email: Ken.beck@smtafe.wa.edu.au

Lecturer: Toby Dinnigan
Email: Toby.dinnigan@smtafe.wa.edu.au

Lecturer: Miraz Islam
Email: Miraz.islam@smtafe.wa.edu.au

Lecturer: Suganya Devi Ramalingam
Email: Suganya.Ramalingam@smtafe.wa.edu.au

Lecturer: Nabin Yadav
Email: Nabin.yadav@smtafe.wa.edu.au

Required resources, texts, equipment you will need

Computer with

- Internet Access
- Word processing software
- Blackboard Access
- USB/HDD
- Office 365 subscription (provided by College)

- Computer with the ability to virtualise operating systems
- Virtualisation Software
- Operating System software as prescribed in course content

Students will be provided with necessary templates and guides prior to commencing assessments as required.

Occupational Health and Safety (OHS) arrangements/requirements:

Learners are expected to follow health, safety and well-being requirements and must ensure they do not endanger themselves, others or equipment used in this course.

No specific OHS requirements pertinent to the learning and assessment activities in the cluster. It is recommended enclosed footwear is worn to protect feet from office chairs.

Additional Information

The following information is to be read in conjunction with the “Current Students” section of the website.

Recognition of Prior Learning (RPL) / Credit / Credit Transfer

You are encouraged to speak to your lecturer about the possibility of recognition of prior learning if you believe you have any existing skills and knowledge that may be formally recognised towards the unit or qualification you are undertaking.

If you have previously completed qualifications or units speak to your Lecturer regarding the possibility of credit or credit transfer.

Assessment Rules and Appeals Process

If your first submission is deemed not satisfactory you will be allowed one further attempt. This is to be negotiated with your lecturer. You are entitled to appeal if you are not satisfied with the assessment process or outcome. The appeal must be lodged within two weeks of receiving the assessment information or outcome. In the first instance, approach your lecturer for information about the process, or check the ‘current students’ section of the SM TAFE website.

Absences

If you are unable to attend any class or assessment session you must inform your lecturer as soon as possible.

If you miss an assessment due to illness, please provide your lecturer with a medical certificate in order to negotiate an alternate time for the assessment.

Reasonable adjustment in the assessment process:

In some circumstances, adjustments to assessments may be made for you. If you require support for literacy and numeracy issues; support for hearing, sight or mobility issues; change to assessment times/venues; use of special or adaptive technology; considerations relating to age, gender and cultural beliefs; format of assessment materials; or presence of a scribe you need to inform your lecturer.

Student support services

South Metropolitan TAFE has a number of services available to assist and support you while you are an enrolled student. These include:

- Disabilities support
- Language literacy and numeracy
- Aboriginal and Torres Strait Student Services
- Assistive technology

Delivery and assessment schedule

Week/ session	Topic	Link to UOC *(Element level only)*	Assessments
1-2	• Overview of cyber security risk management • Scoping of risk management according to organization and industry Session 1-2 Powerpoint slides Session 1-2 Activities (Word document) Homework – review Session 1-2 Powerpoint slides and complete session 1-2 activities – 1 hour	BSBXCS404.1 KE	
3-4	• Review relevant critical cyber risk management strategies appropriate to level of risk Session 3-4 Powerpoint slides Session 3-4 Activities (Word document) Homework – review Session 3-4 Powerpoint slides and complete session 3-4 activities – 1 hour	BSBXCS404.1 KE	
5-6	• Key risk management strategies, including: ○ regular organisational training ○ regular threat assessment ○ cyber security incident response plan ○ clear escalation routes Session 5-6 Powerpoint slides Session 5-6 Activities (Word document) Homework – review Session 5-6 Powerpoint slides and complete session 5-6 activities – 1 hour	BSBXCS404.1 KE	
7-8	• legislative and regulatory requirements relating to contributing to cyber security risk management • Understanding organisational policies and procedures, • Developing suitable cyber security response options according to organisational policies and procedures Session 7-8 Powerpoint slides Session 7-8 Activities (Word document) Homework – review Session 7-8 Powerpoint slides and complete session 7-8 activities – 1 hour	BSBXCS404.1 KE	AT1 – Knowledge Questions
9-10	• Present options for risk management strategies for approval • Document approved risk management strategies Session 9-10 Powerpoint slides Session 9-10 Activities (Word document)	BSBXCS404.1 KE	AT1 – Knowledge Questions

	Homework – review Session 9-10 Powerpoint slides and complete session 9-10 activities – 1 hour		
11-12	- Communication of approved risk management strategies to required personnel - monitoring cyber security risk according to selected risk management strategies - reviewing currency of risk register Session 11-12 Powerpoint slides Session 11-12 Activities (Word document) Homework – review Session 11-12 Powerpoint slides and complete session 11-12 activities – 1 hour	BSBXCS404.2 KE	AT2 – Risk Management Project
13-14	- Assist in determining compliance with implemented cyber risk mitigation strategies - Address non-compliance within scope of own role and escalate where required according to organisational policies and procedures - Assist in establishing feedback processes that provide warning of potential new risks according to organisational requirements Session 13-14 Powerpoint slides Session 13-14 Activities (Word document) Homework – review Session 13-14 Powerpoint slides and complete session 13-14 activities – 1 hour	BSBXCS404.2 KE	AT2 – Risk Management Project
15-16	- Identify benchmarks to track effectiveness of risk management strategies - Support evaluation of effectiveness of implemented strategies - Update risk management strategies with new information as required Session 15-16 Powerpoint slides Session 15-16 Activities (Word document) Homework – review Session 15-16 Powerpoint slides and complete session 15-16 activities – 1 hour	BSBXCS404.3 KE	AT2 – Risk Management Project
17-18	Complete AT2 – Risk Management Project Homework – Review all previous sessions and complete AT2 Risk Management Project – 1 hour	BSBXCS404.1,2,3 KE	AT2 – Risk Management Project
19-20	Resits		

Assessment 1	
Title	AT1 – Knowledge Questions
Brief Description	This assessment consists of knowledge-based questions relating to: •legislative and regulatory requirements relating to contributing to cyber security risk management •key risk management strategies, •organisational policies and procedures relating to risk management

	•industry-specific knowledge of suitable procedures for applying risk management strategy •guidelines required for updating technology •business process design principles in relation to risk management
Where	Out of Class
When	Weeks 7 - 10
Conditions	Open book

Assessment 2	
Title	AT2 – Risk Management Project
Brief Description	This assessment requires learners contribute to cyber security risk management is 2 scenarios (password and antivirus). This involves: • Activity 1: Identify and recommend risk management strategies • Activity 2: Support implementation of risk management strategies • Activity 3: Review and revise risk management strategies
Where	Out of Class
When	Weeks 11 - 18
Conditions	Open book

Delivery and Assessment Plan (DAP)

Qualification Details			
Training Package Code & Title:	ICT - Information and Communications Technology (Release 6.0)		
Qualification Code & Title:	ICT40120 Certificate IV in Information Technology	State code	BFF9

Student Declaration

I have read the delivery and assessment plan for:
Unit/s of Competency:

The delivery and assessment details have been discussed with me. I understand my role and responsibilities and agree to undertake the assessment tasks as detailed in the delivery and assessment plan.
I am aware that all assessment work I submit must be my own work and must abide by all the assessment rules set by my lecturer.
I also understand that copying directly from research sources or another student's work without acknowledgement is plagiarism. I further understand that plagiarised work (or cheating of any kind) will not be accepted and may result in disciplinary action taken against me.

#	Student name (please print)	Telephone number	Email address	Date	Signature
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					