

ICTICT451 Comply with IP, ethics and privacy policies in ICT environments

ICTICT443 Work collaboratively in the ICT industry

**BSBXCS404 Contribute to cyber security risk management**

Learner version

# Working In ICT Assessment 2

Portfolio

**Disclaimer:** This resource was developed by Holmesglen Institute of TAFE in 2024 for the State of Victoria (Department of Education and Training) for educational purposes, is © State of Victoria (Department of Education and Training) and is available under a Creative Commons Attribution Non-commercial 4.0 International [(CC BY-NC 4.0)](https://creativecommons.org/licenses/by-nc/4.0/) license.

**The license does not apply to:** Trademarks or branding, including the Victorian Government logo and any unattributed content supplied by third parties



Learner version

# Working In ICT Assessment 2

Portfolio

|  |  |
| --- | --- |
| Learner information | |
| **Learner name:** Van Minh Le | **Learner ID:** 100693330 |
|  | |

|  |  |
| --- | --- |
| Section A – Program/course details | |
| **Qualification code:** ICT40120 | **Qualification title:**  Certificate IV in Information Technology (Web Development)  Certificate IV in Information Technology (Programming)  Certificate IV in Information Technology (Gaming Development) |
| **Unit code:**  **Working in ICT**  ICTICT451  ICTICT443  BSBXCS404 | **Unit title:**  Comply with IP, ethics and privacy policies in ICT environments  Work collaboratively in the ICT industry  Contribute to cyber security risk management |
| **Pre/co-requisites:** N/A | |
|  | |

|  |  |  |  |
| --- | --- | --- | --- |
| Section B – Assessment task details | | | |
| **Assessment number: 2** of 2 | **Semester/year:** 1/2025 | | **Due date:** Session 15 |
| **Duration of assessment:** 6 sessions | | **Assessment task results:** This assessment task will be marked as:  Ungraded result: satisfactory or not yet satisfactory | |
|  | | | |

|  |
| --- |
| Section C – Instructions to learners |
| Assessment task description:  **Part 1 – Knowledge Questions**  This assessment requires learners to answer a range of knowledge questions related to this subject. Some of these questions are more technical and ask learners to discuss or explain terminologies while other questions are more holistic or bigger picture focused.  **Part 2 – Portfolio**  For this assessment task you will be required to plan and develop a risk management report for a mock organization as part of a team. Your risk management report must address the problems noted in the scenario and issues. Learner is indvidually required to create a risk management report in relation to their research, risk analysis and feedback.  This assessment task is comprised of the following parts:  1. Part A – Group Discussion, Findings & Protocols  As a group you will discuss and research the scenario  2. Part B – Risk Management Report  Individually you will need to develop a Risk Management Report 3. Part C – Evaluation a Feedback You will organise a time to have your teacher evaluate and provided feedback on your report.  4. Part D – Review  As part of the review you will need to implement the feedback from your teacher  Your risk management report must address the problems noted in the scenario and issues below.   * This assessment task does not focus on your technical skills. * ***Read the instructions and scenario facts very carefully.***   **Part A – Group Discussion, Findings & Protocols**  To complete this task, you will need to form a group consisting of two to four members and conduct group discussion on the various aspects of the scenario and risk management. You will also need to develop two communication and cybersecurity protocols for your teams. The protocols should be recorded in a document and made available to all team members.  You will then coordinate with your assessor to schedule a time for a direct observation session. The observation must take place in a classroom or hybrid setting. If some team members are participating via WebEx, ensure that the team provides a WebEx meeting link to all members, including the assessor. It is essential that everyone has their webcam switched on and clearly identifies themselves by showing their Student ID card or Driver's License.  During the observation, the assessor may ask individual group members to elaborate on their answers or provide additional information. The assessor will provide real-time constructive feedback, highlighting effective elements and offering suggestions or recommendations to enhance their responses on the discussed topics.  **In preparation for the group discussion prior, you will need to complete the following:**   * **EACH member must choose a Risk Register in Section 3 of the Template Report (Sections 3.1 to 3.4).** * **EACH member must make preliminary determinations on what WALLETX risks might be relevant to their risk register, and solutions to control these risks.** * **On holding the group discussion, each member must present their findings and collaborate on how best to allot the different risk types.**   To prepare for the meeting each team member must complete **Group Discussion section below as a team.**  **Scenario**  Based in Melbourne, WALLETX is a successful and growing online Australian cryptocurrency exchange company, allowing Australian digital consumers to buy and sell any cryptocurrency listed on its’ website. Founded in 2014, just after many of the large US crypto exchanges, it has grown extremely quickly into a company of 40+ employees, a customer base of over 300,000 people, who have over their history traded billions of dollars in cryptocurrencies including Bitcoin and Ethereum.  You have recently been hired by the Chief Executive Officer (CEO), Ellen Husk, to head up the new mixed operations team of **“Risk & Technologies”**. This team was determined as ***ESSENTIAL*** by the Board owing to a recent audit conducted by ASIC, which found WALLETX in breach of several compliance requirements: a symptom of wider issues in WALLETX.  Your role will be to work as a team with your fellow peers and develop a comprehensive risk management report to deal with the recent issues that have befallen WALLETX as found by ASIC and described below in “**Issues**”.  **Objectives**   * Create a new Risk & Technologies operation team * Develop a comprehensive risk management report * Identify issues in terms of compliance requirements   **Issues**  A. Risk Management System  As described by Ms Husk, WALLETX have never had a formal risk management system, nor do they have they ever operated with a dedicated risk manager. Commonly, to get around any Board requests on risks affecting WALLETX, they have made the Lead Accountant, Tony Beasley, copy a template risk register from the internet and partly populate it with the most obvious risks.  Ellen notes that on closer inspection, she commonly saw that the Lead Accountant often delegate all the risk management tasks to their accounting intern, fresh out of high school. Concerningly, she never saw the accountant (or their intern) ever consult with any head of division like the Lead Developer, Cleve Hobs, or Head of Cyber Security, Miles Zeckerbern.  B. Work Health Safety  During your initial risk assessment, you have been provided with a guided tour of the office of WALLETX by Tony (Lead Accountant), which leases one level in a modern high-rise in Melbourne’s CBD.  At the start of the tour, at the ground level, you walk through the lobby and find it relatively easy to make it to the lifts, as commented by Tony, “no stress about passes, the security guard here is always off to find the next best coffee place – he’s a laugh!” You briefly note as you make your way to the lifts, that there is a lack of “EXIT” signs and that the fire escape plan is nearly falling off the wall. Finally, you ask Tony why there is security tape & barriers across the emergency stairwell. He replies “oh some of the lower floors recently had some things stolen by perps breaking into their level via the stairwell. Apparently, the lock is pretty flimsy. No stress though – I seriously doubt a crook is so fit as to get up 20 flights of stairs and pinch one of our computers!”  Up on Level 20, Tony gives you a detailed tour of the WALLETX office, with 75% of the floorspace dedicated to open-plan workspaces. Additionally, there are four meeting rooms, a communal kitchen area and a storage space. During the open-plan workspace walkthrough, one of your colleagues nearly trip over a power cord, where you note that most workspaces seem to “overflow” onto the footpath with wires, folders and “stuff”. The kitchen is kept very tidy, although the power points all seem to be located directly above the sink. The storage space is a mess, with a clear leak in one of the exposed pipes and a lack of any lighting making it near impossible to see anything in the room.  You finish your tour in the main meeting room and have a seat on the very lush and expensive board chairs. Tony, on seeing your nod of approval, comments “they’re nice right! Luckily, I ended the tour in the main board room, the chairs in Meeting Room 4 are awful. I think one of our devs, Lucy Sharp, actually fell off one the other say.” On noting your look of alarm, he pacifies “oh don’t worry, she’s a real trooper. She’s had a couple of falls in this place over the last few weeks but bounces back like nothing happened … not sure where she is today though.”  C. Regulatory & Compliance  Whilst in the meeting room, you have a chat to Tony about the current state of WALLETX. On completion of your tour, you also asked to have a chat with the Lead Developer, Cleve, and Head of Cyber Security, Miles, about their teams and any issues. They noted the following:   * Security guard is not versed in Crimes Act 1958, as he is searching customers as they enter/leave the premises * There is an internal network drive, known as "The Crypt", where terabytes of illegally downloaded music and media is stored for IT staff to use amongst themselves * ​Several emails have been received by the IT support desk, complaining that they cannot delete their WALLETX accounts and/or remove their personal data from the system * On viewing the website, the WALLETX logo on appearance, looks alarmingly similar to the "Meta" trademarked logo * Devices are running outdated patches creating vulnerabilities * ​Many of the company computers are running "jailbroken" patented software to avoid paying proprietary licensing fees. As put by Cleve, "it's an ingenious way of keeping our overheads down.   D. IT & Cyber Security  The Lead Developer, Cleve, and Head of Cyber Security, Miles, tell you they have concerns with respect to their IT infrastructure security and adequate Cyber Hygiene at WALLETX. Specifically, they mention the following which has been flagged to them previously as an IT & Cybersecurity issue, amongst others.   * No firewall software is being used on the company computers * Employees are sharing passwords with each other * There is currently no anti-malware software being used in the company * All servers and devices are running different and outdated operating systems   **Other Details**   * Once you are assigned a team it is an opportunity to figure out each other strengths and weaknesses. This will help you plan out responsibilities. * You may ask for further information or clarity on aspects of the Scenario & Issues from the teacher, to allow you to better fill out the Risk Management Report.   As you are working in teams you will have opportunities to collaborate with others throughout the process. This would include collaboration with fellow team members, client, teachers, peers.  To build the report the team can use information gathered in the Cyber Hygiene and Risk Assessment Report (Provided in Brightspace) plus information gathered research conducted into risk policies and security frameworks (i.e. ISO 27001, NIST Framework): |
|  |

|  |
| --- |
| Section D – Conditions for assessment |
| ****Unit application:****   * This is an individual task. * You must meet all criteria listed in the marking guide to be satisfactory in this task. * You must submit all required working files, documentation, and any other assets that may be required in a zipped file, including the completed and signed coversheet, where necessary. The assessment must be completed and submitted electronically to Brightspace by the due date. If this is not possible, you must contact your assessor to gain written approval for an alternative arrangement for submitting the assessment. * If not successful within the enrolment period as per Holmesglen assessment procedure, you will be requested to resubmit within 7 days of receiving feedback. You will have the opportunity to resubmit if any part of the assessment is deemed unsatisfactory (you are permitted TWO (2) resubmission per assessment task). Resubmissions must be submitted by the resubmission due date provided by your teacher. * This task is open book. You may use the internet for research purposes only. All answers must be in your own words. Where a quote is used, you must cite the information source. * If you feel you require special allowance or adjustment to this task, please discuss with your assessor within one week of commencing this assessment. Any change to assessment arrangements must be reviewed by the Education Manager and approved by the Head of Department. * You can appeal an assessment decision according to the Holmesglen Assessment Complaints and Appeals Procedure. * You are expected to dedicate time to develop this assessment task both in and out of the classroom. * Leaner must contribute to and abide by organisational standards including intellectual property, privacy laws, and plagiarism and academic honesty. Further information is detailed at: https://holmesglen.edu.au/Students/Student-Resources/ |
|  |

|  |  |
| --- | --- |
| Equipment/resources learners must supply: | Equipment/resources to be provided by the RTO: |
| **Learners opting to BYOD laptop or intending to learn remotely will require access to:**  Holmesglen Computer Classroom:  data projector, whiteboard, computer with double screens, mobile Cisco Spark Board, Conference camera  HP Z1 Entry Tower G5  • Dual Displays 24” HP Monitor  • CPU: Intel Core i7-9700K @ 4GHz  • Motherboard: 8591  • RAM 32GB  • 1TB SSD  • OS: Windows 10  This will vary as CAIT upgrades computer rooms.  • Internet connection  Applications available at ZENworks and Holmesglen MyHorizon and also free to download via url below:  • Brightspace (Learning Management System) access - https://holmesglen.brightspace.com/  • 365 Microsoft office suite also can be downloaded via https://portal.office.com - free to Holmesglen students  • LinkedIn Learning – https://www.linkedin.com/learning/  • WebEx - https://holmesglen.webex.com/  • 7Zip or an equivalent compression utility - https://www.7-zip.org/download.html  • Google Chrome – recommended web browser  • OneDrive - https://www.microsoft.com/en-ww/microsoft-365/onedrive/online-cloud-storage - free to download  • The relevant legislation/regulation and using policies, procedures, processes available in Brightspace course offering - Resources | **This is a blended learning course and as such a remote learner will access their own computer equipment as per the specification provided. The Institute will provide the following:**  Learners opting to BYOD laptop or intending to learn remotely will require access to:  A MAC or PC/laptop with the following minimum specification:  Quad Core CPU  • CPU with minimum 4GHz processor or faster  • RAM 16GB  • 200GB of storage  • Windows 10 OS, or virtual machine installed with Windows 10 OS (available free from https://developer.microsoft.com/en-us/windows/downloads/virtual-machines/ or https://www.microsoft.com/en-us/evalcenter/evaluate-windows-10-enterprise)  • Monitor 24" (PC only, dual monitor optional but preferred)  • Headset with microphone (webcam optional but preferred)  • Access to reliable internet connection (ADSL or cable connection desirable)  Applications are available at Holmesglen MyHorizon and also free to download via url below:  • Brightspace (Learning Management System) access - https://holmesglen.brightspace.com/  • MyHorizon - https://myHorizon.holmesglen.edu.au - free to download  • 365 Microsoft office suite also can be downloaded via https://portal.office.com - free for all Holmesglen students  • LinkedIn Learning – https://www.linkedin.com/learning/  • WebEx - https://holmesglen.webex.com/  • 7Zip or an equivalent compression utility - https://www.7-zip.org/download.html  • Google Chrome – recommended web browser https://www.google.com/  • OneDrive - https://www.microsoft.com/en-ww/microsoft-365/onedrive/online-cloud-storage - free to download   * • The relevant legislation/regulation and using policies, procedures, processes available in Brightspace course offering - Resource |

|  |  |  |
| --- | --- | --- |
| Section E – Assessment questions/criteria | | |
| **Assessment number:** 2 | | **Assessment title:** Portfolio |
| **Unit code:**  **CWEB4 - Working in ICT**  ICTICT451  ICTICT443  BSBXCS404 | **Unit title:**  Comply with IP, ethics and privacy policies in ICT environments  Work collaboratively in the ICT industry  Contribute to cyber security risk management | |
|  | | |

**PART 1 - KNOWLEDGE QUESTIONS (Written Response)**

**Provide your responses in the boxes below each question.**

|  |  |
| --- | --- |
| Question 1. | Satisfactory response |
| You are required to contribute to the code of ethics.  Please refer to the Supporting documents section of this document. You are required to contribute by filling in the missing statement points under each heading. Please write you answer in red.  This policy must include the following topics with at least three (3) points per category:  1. Privacy and confidentiality (with Managers and also students)  2. Copyright procedures for all assessments  3. Ethical behaviour as a designer in class  4. WHS procedure and issues  5. Communication strategy and class behaviour | Yes  No |
| Answer:  ***Please answer this question as per the supporting document - Classroom Code of Ethics.* 1. Privacy and confidentiality.**  - Don't take photos of other students, manager or their work, without permission.  - Don't share logins or ask for others log in details information.  - Don't share any confidential or private information of other people on social media.  - Don’t give out personal information of other students to others without their permission.  - Do not give names or documents without the other person’s permission.  **2. Copyright procedures for all assessments.**  - Don't copy other students work or assessment.  - If you're using another person's material, don't try to pass it off as your original work and make sure to add a reference part in your work that clearly states the sources.  - Respect copyright owners e.g. use citations/credit content creators where necessary.  - If applicable, apply fair use when using copyrighted materials.  - Check the copyright information regarding materials if you plan to use it.  **3. Ethical behaviour as a designer in class.**  - Give respect to others.  - Follow teacher's instructions.  - Don't answer phone calls in class – excuse yourself and go outside.  - Make reasonable efforts to punctual.  - Speak appropriately in class; avoid using curse words.  **4. WHS procedure and issues.**  - Set up workstations correctly – correct heights, lighting, chairs.  - Keep the classroom clean and tidy – place rubbish in bins.  - Follow WHS signs.  - Report any potential hazard.  **5. Communication strategy and class behaviour.**  - Email your teacher if you are absent.  - Respectfully communicate with each other.  - Allow others to speak and do not talk over others.  - Don't send inappropriate texts or emails to each other.  - Do not answer your phone in the middle of class. | Comment: |

|  |  |
| --- | --- |
| Question 2. | Satisfactory response |
| You are to update the MotionWeb Studio’s privacy policy, to be in line with organisational IP requirements.  The template policy can be found on Brightspace. Please attach the completed privacy policy to your submission and confirm below that you have done this. | Yes  No |
| Answer: Yes. I attached MotionWeb Studio’s privacy policy to my submission. | Comment: |

|  |  |
| --- | --- |
| Question 3. | Satisfactory response |
| What are (3) different communication tools and technology to support teams working collaboratively in virtual environments? | Yes  No |
| Answer:  **1. Live Communication Platforms (e.g., Microsoft Teams, Zoom, Slack)**  - Helps build trust and relationships among team members.  - Set up systems for teamwork.  - Allow real-time discussions and making decisions.  **2. Collaboration & Document Sharing Tools (e.g., Google Drive, OneDrive, Notion.)**  - Provides a platform for scheduling, electronic messaging, document and data sharing.  -  Allow multiple users to edit, store, and share documents in real-time.  Help teams maintain a central location for important files and references.  Ensure cloud storage is well-organized and accessible from anywhere.  **3. Task & Project Management Tools (e.g., Trello, Asana, GitHub)**  Help teams track tasks, assign responsibilities, and manage deadlines.  Provide visibility into project progress through boards, lists, and timelines.  Ensure smooth project collaboration, especially for software development (GitHub for version control). | Comment: |

|  |  |
| --- | --- |
| Question 4. | Satisfactory response |
| List the functions and features of at least (2) communication tools & and state how it aligns with the communication strategy for teams working collaboratively in virtual environments. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 5. | Satisfactory response |
| Describe (2) communication techniques and explain how to use those techniques in the context of the communication tools listed previously. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 6. | Satisfactory response |
| Explain (2) methods of mediating conflicting perspectives in collaborative teams and how it works in the context of virtual environments. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 7. | Satisfactory response |
| Elaborate on (2) constructive feedback techniques for responding to situations which require criticism and how to effectively do that in a virtual environment. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 8. | Satisfactory response |
| Source (1) legislative and regulatory requirement relating to data protection legislation. | Yes  No |
| Answer | Comment: |

|  |  |
| --- | --- |
| Question 9. | Satisfactory response |
| Source (1) notifiable data breach legislation relating to cyber security risk management. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 10. | Satisfactory response |
| Is there a comprehensive legal / regulatory framework for cyber security at an international level? Source (1) international law that has some applicability to managing cyber security between governments. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 11. | Satisfactory response |
| Detail (1) risk management strategy regarding regular organisational training. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 12. | Satisfactory response |
| Explain (1) risk management consideration regarding regular risk analysis & threat assessment. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 13. | Satisfactory response |
| Describe (3) business process design & best practice principles in relation to risk management. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 14. | Satisfactory response |
| Explain general guidelines required for updating technology in relation to a web design company. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 15. | Satisfactory response |
| List (2) reporting mechanisms for tracking organizational cyber security maturity. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 16. | Satisfactory response |
| What are suitable procedures for applying risk management strategy that are industry standard? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 17. | Satisfactory response |
| In a step-by-step process, explain the process of escalation routes regarding risk management strategies. You must include at least (5) steps. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 18. | Satisfactory response |
| **Scenario 1: Jean’s problem solving.**  Jean, a statistical database programmer, is trying to write a large statistical program needed by her company.  Programmers in this company are encouraged to write about their work and then publish their algorithms in professional journals. This is detailed in the company code of conduct.  After months of tedious programming, Jean has found herself stuck on several parts of the program. Her manager, not recognising the complexity of the problem, wants the job completed within the next few days.  Not knowing how to solve the problems, Jean remembers that a co-worker had given her source code listings from his current work and from an early version of a commercial software package developed at another company.  On studying these programs, she sees two areas of code which could be directly incorporated into her own program.  She uses segments of code from both her co-worker and the commercial software but does not tell anyone or mention it in the documentation. She completed the project and turns it in a day ahead of time.  Jean says that she is unaware of the company code of conduct.  How do you see this situation? Choose the correct answer(s) below and explain why.   1. Jean should take the day off and reward herself with a massage. 2. Jean should have waited until the deadline and not a day earlier, before turning her work in early. Now her manager may give her extra work. 3. Jean could have approached her manager about the complexity of the issue and discussed her concerns. 4. Jean needs to ask permission before using the code from her co-workers. 5. Jean needs to mention her co-workers, and the use of their code, giving them credit for their work in her documentation.   *Acknowledgement: Burmeiser, OK (2000), ‘Applying the ACS code of ethics’, Journal of Research and Practise in Information Technology. Vol. 32, no.2, pp. 107-120.* | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 19. | Satisfactory response |
| What are principles that you can use to assist current and future employees understand their obligations and the rights of others regarding intellectual property infringements in the previous question? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 20. | Satisfactory response |
| **Scenario 2: Joseph’s logo design.**  Joseph is a Melbourne based designer and has been asked to design an original logo for a local small business. He commences research and creates a few original concept designs.  After he shows his client his initial designs the client is unhappy with those concepts.  Joseph goes away and works on a new design but the client emails through an image of a logo design that they like.  The logo is of a competitor and the client wants their logo to look exactly the same, but with only a small change to the lettering only.  What should Joseph do? Choose the correct answer(s) below and explain why.   1. Joseph should just follow the instructions of the client and complete the job he can buy those new pair of shoes on sale with the money he makes. 2. Joseph should discuss his ethical concerns with his client. 3. Joseph should just design a logo he likes regardless of what the client requests or needs and disregard the email entirely. Who cares? 4. Joseph should design an original design and use the emailed logo as a reference.   Run away and curl up in a ball somewhere | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 21. | Satisfactory response |
| What would you say to your client to support your answer(s) in the previous question? Write no more than two paragraphs. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 22. | Satisfactory response |
| Where would find two (2) intellectual property and copyright in the ICT industry standards or legislation to support your answers? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 23. | Satisfactory response |
| **Scenario 3: Deedee and her data.**  Deedee has been asked to collect data from a competition to determine the demographics of the online magazine readers.  The competition terms and conditions state that information will only be used for demographic research purposes only once the competition has ended.  Deedee receives the final spread sheet with the competition entrants detailing each persons’ name, age, email, and location. The information is secure on Deedee’s computer and only she has access to that data.  Jules has asked for access to the spreadsheet so she can email each person weekly email newsletter selling online products.  There is no provision in the terms and conditions Deedee used to collect the data for other purposes other than research. It is very specific.  You find that the company privacy policy is very vague and general. It is not in accordance with Australian Privacy Principles.  Jules asks for Deedee’s log in.  What should Deedee do? Choose the correct answer below.   1. Deedee should go ahead and give Jules the access to the spread sheet. The more products Jules and Deedee can sell online means the possibility of a monthly bonus. Deedee is saving to go on vacation to Ibiza. She needs a holiday! 2. Deedee should inform Jules this is not a good decision and advises against using the data to email each customer directly. 3. Everyone in the office should have access to Deedee’s data. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 24. | Satisfactory response |
| In less than one paragraph, discuss your reasons for your answer the previous question. You may use bullet points instead. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 25. | Satisfactory response |
| Where would you find privacy standards or legislation to support your choices for the earlier question? What is the main issue here? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 26. | Satisfactory response |
| Does the privacy policy in the earlier question need to be reviewed? Why? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 27. | Satisfactory response |
| **Scenario 4: Deedee and her policy**  After the debacle above in the previous scenario, Management is impressed with Deedee’s work ethic.  She has now been asked to update the company privacy policy to be alignment with the Australian Privacy Principles.  This new policy change should then be applied to upholding competition term and conditions in future or changing them to be in accordance with the APP when appropriate.  Deedee has written a draft and the policy is now more specific, detailing the rights of all stakeholders and mentions the principles in detail.  The company code of conduct has also been reviewed and now includes the duties of staff to maintain the privacy rights of all customers along with general ethical conduct in the workplace such as professional development and good moral conduct.  Deedee interviews the staff members in her work area about the new policy update. She asks them to source the company privacy policy and code of conduct, discuss its relevance to their job and records their feedback.  After the interview she discovers the following:   * Two staff members do not actually know where to find the code of conduct or privacy policy. * Five do not understand the guidelines behind the Australian Privacy Principles * Only 2 understand the potential consequences of breaching the APPs and don’t see the big deal. * Three mention the wording is too complicated and too wordy. * 5 say the type is too small and they struggle to read the documents. * Five staff still don’t understand what this has to do with their competition terms and conditions that they email out to customers or put on raffle tickets on a regular basis. * Management have asked for all staff to undergo training in some manner and for Deedee to organize this. * You realise that customer data files have are not backed up.   What should Deedee do? Choose the correct answer(s) below.   1. Deedee should consider this a job well done. 2. Deedee should panic, take an aspirin go to bed. Let someone else deal with this rubbish. 3. Deedee should update the policy again incorporating her recorded feedback, distribute it again and revise the policy again in future? 4. Deedee should make the wording even more difficult to read because she doesn’t really understand it either. 5. Deedee needn’t worry about educating the staff about the NPP. Most staff leave the company within a few months, so why waste so much time and money? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 28. | Satisfactory response |
| If the policy were to be updated again what feedback should be considered based on the interviews on the previous question? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 29. | Satisfactory response |
| In terms of overcoming a non-compliance incident with personnel, list two (2) ways or general principles to advise staff about the location of the policy and the fact it has been updated again? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 30. | Satisfactory response |
| As an additional example of overcoming a non-compliance incident with personnel, list one (1) way or general principle to check that staff are understanding and applying the new policies and procedures? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 31. | Satisfactory response |
| Please explain briefly about your understanding of key risk management strategies, specifically to what a cyber security incident response plan is. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 32. | Satisfactory response |
| Write an analysis and review risk management methodologies and how they relate to clear organizational policies and procedures. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 33. | Satisfactory response |
| Explain what a communication plan is and how you would develop one? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 34. | Satisfactory response |
| What are some different techniques for monitoring cyber risk and describe how they work? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 35. | Satisfactory response |
| Explain what the process for reviewing the currency of risk registers? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 36. | Satisfactory response |
| List examples of organizational cyber security protocols and give a brief description of each of them. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 37. | Satisfactory response |
| Give examples of protocols for virtual ways of working, including information about those virtual platforms used and the frequency of those virtual platforms use. | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 38. | Satisfactory response |
| What are some examples of roles and responsibilities of team members in promoting collaborative work environments? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 39. | Satisfactory response |
| Describe how you could include guidelines in a policy on using collaborative communication tools? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 40. | Satisfactory response |
| Describe at least TWO (2) WHS issues / expectations when working in collaborative work arrangements? | Yes  No |
| Answer: | Comment: |

|  |  |
| --- | --- |
| Question 41. | Satisfactory response |
| Provide one example of a source where to find information on either federal or state WHS legislation, codes, regulations or standards in collaborative work arrangements? | Yes  No |
| Answer: | Comment: |

**PART 2 – PORTFOLIO**

For this assessment task you will be required to plan and develop a risk management report for a mock organization as part of a team. Your risk management report must address the problems noted in the scenario and issues.  
Learner is indvidually required to create a risk management report in relation to their research, risk analysis and feedback.

This assessment task is comprised of the following parts:

1. Part A – Group Discussion, Findings & Protocols   
As a group you will discuss and research the scenario

2. Part B – Risk Management Report   
Individually you will need to develop a Risk Management Report  
3. Part C – Evaluation a Feedback  
You will organise a time to have your teacher evaluate and provided feedback on your report.

4. Part D – Review   
As part of the review you will need to implement the feedback from your teacher  
  
Your risk management report must address the problems noted in the scenario and issues below.

* This assessment task does not focus on your technical skills.
* ***Read the instructions and scenario facts very carefully.***

**Part A – Group Discussion, Findings & Protocols**

To complete this task, you will need to form a group consisting of two to four members and conduct group discussion on the various aspects of the scenario and risk management. You will also need to develop two communication and cybersecurity protocols for your teams. The protocols should be recorded in a document and made available to all team members.

You will then coordinate with your assessor to schedule a time for a direct observation session. The observation must take place in a classroom or hybrid setting. If some team members are participating via WebEx, ensure that the team provides a WebEx meeting link to all members, including the assessor. It is essential that everyone has their webcam switched on and clearly identifies themselves by showing their Student ID card or Driver's License.

During the observation, the assessor may ask individual group members to elaborate on their answers or provide additional information. The assessor will provide real-time constructive feedback, highlighting effective elements and offering suggestions or recommendations to enhance their responses on the discussed topics.

**In preparation for the group discussion prior, you will need to complete the following:**

* **EACH member must choose a Risk Register in Section 3 of the Template Report (Sections 3.1 to 3.4).**
* **EACH member must make preliminary determinations on what WALLETX risks might be relevant to their risk register, and solutions to control these risks.**
* **On holding the group discussion, each member must present their findings and collaborate on how best to allot the different risk types.**

To prepare for the meeting each team member must complete **Group Discussion section below as a team.**

**Scenario**

Based in Melbourne, WALLETX is a successful and growing online Australian cryptocurrency exchange company, allowing Australian digital consumers to buy and sell any cryptocurrency listed on its’ website. Founded in 2014, just after many of the large US crypto exchanges, it has grown extremely quickly into a company of 40+ employees, a customer base of over 300,000 people, who have over their history traded billions of dollars in cryptocurrencies including Bitcoin and Ethereum.

You have recently been hired by the Chief Executive Officer (CEO), Ellen Husk, to head up the new mixed operations team of **“Risk & Technologies”**. This team was determined as ***ESSENTIAL*** by the Board owing to a recent audit conducted by ASIC, which found WALLETX in breach of several compliance requirements: a symptom of wider issues in WALLETX.

Your role will be to work as a team with your fellow peers and develop a comprehensive risk management report to deal with the recent issues that have befallen WALLETX as found by ASIC and described below in “**Issues**”.

**Objectives**

* Create a new Risk & Technologies operation team
* Develop a comprehensive risk management report
* Identify issues in terms of compliance requirements

**Issues**

A. Risk Management System

As described by Ms Husk, WALLETX have never had a formal risk management system, nor do they have they ever operated with a dedicated risk manager. Commonly, to get around any Board requests on risks affecting WALLETX, they have made the Lead Accountant, Tony Beasley, copy a template risk register from the internet and partly populate it with the most obvious risks.

Ellen notes that on closer inspection, she commonly saw that the Lead Accountant often delegate all the risk management tasks to their accounting intern, fresh out of high school. Concerningly, she never saw the accountant (or their intern) ever consult with any head of division like the Lead Developer, Cleve Hobs, or Head of Cyber Security, Miles Zeckerbern.

B. Work Health Safety

During your initial risk assessment, you have been provided with a guided tour of the office of WALLETX by Tony (Lead Accountant), which leases one level in a modern high-rise in Melbourne’s CBD.

At the start of the tour, at the ground level, you walk through the lobby and find it relatively easy to make it to the lifts, as commented by Tony, “no stress about passes, the security guard here is always off to find the next best coffee place – he’s a laugh!” You briefly note as you make your way to the lifts, that there is a lack of “EXIT” signs and that the fire escape plan is nearly falling off the wall. Finally, you ask Tony why there is security tape & barriers across the emergency stairwell. He replies “oh some of the lower floors recently had some things stolen by perps breaking into their level via the stairwell. Apparently, the lock is pretty flimsy. No stress though – I seriously doubt a crook is so fit as to get up 20 flights of stairs and pinch one of our computers!”

Up on Level 20, Tony gives you a detailed tour of the WALLETX office, with 75% of the floorspace dedicated to open-plan workspaces. Additionally, there are four meeting rooms, a communal kitchen area and a storage space. During the open-plan workspace walkthrough, one of your colleagues nearly trip over a power cord, where you note that most workspaces seem to “overflow” onto the footpath with wires, folders and “stuff”. The kitchen is kept very tidy, although the power points all seem to be located directly above the sink. The storage space is a mess, with a clear leak in one of the exposed pipes and a lack of any lighting making it near impossible to see anything in the room.

You finish your tour in the main meeting room and have a seat on the very lush and expensive board chairs. Tony, on seeing your nod of approval, comments “they’re nice right! Luckily, I ended the tour in the main board room, the chairs in Meeting Room 4 are awful. I think one of our devs, Lucy Sharp, actually fell off one the other say.” On noting your look of alarm, he pacifies “oh don’t worry, she’s a real trooper. She’s had a couple of falls in this place over the last few weeks but bounces back like nothing happened … not sure where she is today though.”

C. Regulatory & Compliance

Whilst in the meeting room, you have a chat to Tony about the current state of WALLETX. On completion of your tour, you also asked to have a chat with the Lead Developer, Cleve, and Head of Cyber Security, Miles, about their teams and any issues. They noted the following:

* Security guard is not versed in Crimes Act 1958, as he is searching customers as they enter/leave the premises
* There is an internal network drive, known as "The Crypt", where terabytes of illegally downloaded music and media is stored for IT staff to use amongst themselves
* ​Several emails have been received by the IT support desk, complaining that they cannot delete their WALLETX accounts and/or remove their personal data from the system
* On viewing the website, the WALLETX logo on appearance, looks alarmingly similar to the "Meta" trademarked logo
* Devices are running outdated patches creating vulnerabilities
* ​Many of the company computers are running "jailbroken" patented software to avoid paying proprietary licensing fees. As put by Cleve, "it's an ingenious way of keeping our overheads down.

D. IT & Cyber Security

The Lead Developer, Cleve, and Head of Cyber Security, Miles, tell you they have concerns with respect to their IT infrastructure security and adequate Cyber Hygiene at WALLETX. Specifically, they mention the following which has been flagged to them previously as an IT & Cybersecurity issue, amongst others.

* No firewall software is being used on the company computers
* Employees are sharing passwords with each other
* There is currently no anti-malware software being used in the company
* All servers and devices are running different and outdated operating systems

**Other Details**

* Once you are assigned a team it is an opportunity to figure out each other strengths and weaknesses. This will help you plan out responsibilities.
* You may ask for further information or clarity on aspects of the Scenario & Issues from the teacher, to allow you to better fill out the Risk Management Report.

As you are working in teams you will have opportunities to collaborate with others throughout the process. This would include collaboration with fellow team members, client, teachers, peers.

To build the report the team can use information gathered in the Cyber Hygiene and Risk Assessment Report (Provided in Brightspace) plus information gathered research conducted into risk policies and security frameworks (i.e. ISO 27001, NIST Framework):

|  |  |  |  |
| --- | --- | --- | --- |
| Criteria for assessment | SatisfactoryYes No | | Comment |
| **The following has been submitted for assessment:** | | | |
| 1. Supplementary documentation – filled out, signed, and dated |  |  |  |
| 1. Final Risk Management Report (.pdf or docx) |  |  |  |

| **Part A - Group Discussion, Findings & Protocols (Direct Observation)** |
| --- |
| To complete this task, you will need to form a group consisting of two to four members and conduct group discussion on the various of the scenario and risk management. You will also need to develop two communication and cybersecurity protocols for your teams. The protocols should be recorded in a document and made available to all team members.  You will then coordinate with your assessor to schedule a time for a direct observation session. The observation must take place in a classroom or hybrid setting. If some team members are participating via WebEx, ensure that the team provides a WebEx meeting link to all members, including the assessor. It is essential that everyone has their webcam switched on and clearly identifies themselves by showing their Student ID card or Driver's License.  During the observation, the assessor may ask individual group members to elaborate on their answers or provide additional information. The assessor will provide real-time constructive feedback, highlighting effective elements and offering suggestions or recommendations to enhance their responses on the discussed topics.  Below are the observation components that the learner is required to demonstrate as part of this assessment. The learner only needs to demonstrate this once. If the learner is unable to demonstrate one or more of the required Observation tasks to a satisfactory level, they will be given two opportunities to demonstrate the unsatisfactory Observation task(s). |

Marking criteria: Skills to be observed during this task to the required standard

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| In this assessment task you will be performing the following activities: | Date 1SatisfactoryYes No | | Date 2Resubmission  if applicableSatisfactoryYes No | | Date 3Resubmission if applicableSatisfactoryYes No | | Comment |
| 1. Has formed group and determined the roles and responsibilities they have for the project. |  |  |  |  |  |  |  |
| 1. presented their findings and collaborate on how best to allot the different risk types. |  |  |  |  |  |  |  |
| 1. identified and described at least (2) communication tools and technology are available to support your team to working collaboratively in a virtual environment. |  |  |  |  |  |  |  |
| 1. identified and discussed (2) communication protocols for the team to work collaboratively in virtual environments that help achieve team objectives. |  |  |  |  |  |  |  |
| 1. discussed and developed (2) cyber security protocols for your team to work collaboratively in virtual environments, in according with organisational cyber safety procedures. (The protocols should be recorded in a document and made available to all team members.) |  |  |  |  |  |  |  |
| 1. identified and discussed industry standard benchmarks and / or models to track effectiveness of risk management strategies. |  |  |  |  |  |  |  |
| 1. discussed and developed (2) protocols for your team to share knowledge collaboratively in a virtual environment according to the scenario’s work details and your team objectives. (The protocols should be recorded in a document and made available to all team members.) |  |  |  |  |  |  |  |
| 1. Chosen a risk register in section 3 of the Template Report |  |  |  |  |  |  |  |
| 1. made a preliminary determination on what WALLETX risks might be relevant to their risk register, and solutions to control these risks. |  |  |  |  |  |  |  |
| 1. worked collaboratively with their team and discussed at least one problem outlined in the scenario and a potential solution to mitigate or resolve the issue. |  |  |  |  |  |  |  |
| 1. presented their findings and collaborate on how best to allot the different risk types. |  |  |  |  |  |  |  |
|  |  | |  | |  | |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Part B** | | **Risk Management – This is an individual task**  Individually you will need to develop a Risk Management Report | | | | | | | | | | | | | |
| **Instructions**  **Develop a Risk Management Report**  This component requires that you have developed a risk management report. The risk management report must be completed individually  How you choose to develop your action plan is up to you, **provided you use the template in the supporting documentation located at the bottom of this document**. Your action plan must cover the major sections of the report including:   * Executive summary * Section 1: Introduction * Section 2: Risk Assessment Methodology * Section 3: Risk Analysis * Section 4: Summary of Findings * Section 5: Recommendations & Actions   **Present Report to Facilitator**  You will need to organise a time to present your report to your facilitator. Your action plan must use the template in the supporting documentation and must be completed as instructed. | | | | | | | | | | | | | | | |
|  | | | | | | | **Satisfactory** | | | **Comment** | | | | | | |
| **Yes** | | **No** |
| **The following has been included in assessment:** | | | | | | | | | | | | | | | | |
| 1 | Learner has submitted Assessment Risk Management Report using required Template which defines purpose and scope of risk assessment and risk assessment methodology used. | | | | | | ☐ | | ☐ |  | | | | | | |
| 2 | Learner has stated in Assessment Risk Report Risk Model used ISO 27001 or NIST to conduct risk assessment | | | | | | ☐ | | ☐ |  | | | | | | |
| 3 | Learner determined risk assessment by using appropriate standards ISO 27001 or NIST | | | | | | ☐ | | ☐ |  | | | | | | |
| 4 | Learner has contributed to monitoring cyber security risk according to selected risk management strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 5 | Learner has assisted in determining compliance with implemented cyber risk mitigation strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 6 | Learner has assisted in developing at least two suitable cyber security response options according to organisational policies and procedures | | | | | | ☐ | | ☐ |  | | | | | | |
| 7 | Learner has documented approved risk management strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 8 | Learner has assisted in establishing feedback processes that provide warning of potential new risks according to organisational requirements | | | | | | ☐ | | ☐ |  | | | | | | |
| 9 | Learner has identified benchmarks to track effectiveness of risk management strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 10 | Learner has supported evaluation of effectiveness of implemented strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 11 | Learner has updated risk management strategies with new information as required | | | | | | ☐ | | ☐ |  | | | | | | |
| 12 | Learner has addressed non-compliance within scope of own role and escalate where required according to organisational policies and procedures | | | | | | ☐ | | ☐ |  | | | | | | |
| 13 | Learner has assisted in establishing feedback processes that provide warning of potential new risks according to organisational requirements | | | | | | ☐ | | ☐ |  | | | | | | |
| 14 | Learner has supported evaluation of effectiveness of implemented strategies | | | | | | ☐ | | ☐ |  | | | | | | |
| 15 | Learner has updated risk management strategies with new information as required | | | | | | ☐ | | ☐ |  | | | | | | |
| 16 | Learner has supported evaluation of effectiveness of each implemented strategy | | | | | | ☐ | | ☐ |  | | | | | | |
| 17 | Learner has managed incident response plans | | | | | | ☐ | | ☐ |  | | | | | | |
| 18 | Learner has communicated and contributed as a member of a team | | | | | | ☐ | | ☐ |  | | | | | | |
| 19 | Learner has supplied risk management report to supervisor for feedback and approval & covers all sections in required detail | | | | | | ☐ | | ☐ |  | | | | | | |
| **Part C** | | | **Evaluation and Feedback – This is an individual task** | | | | | | | | | | | | | |
| **OBTAIN FEEDBACK AND APPROVAL FROM YOUR TEACHER BEFORE PROCEEDING.**  **The following checklist is to be completed by the facilitator** | | | | | | | | | | | | | | | | |
| **Checklist (To be completed by the learner’s facilitator)** | | | | | | | | | | | | **Yes** | | **No** | | |
| 1. The learner has assisted in developing suitable cyber security response options according to organisational policies and procedures. | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has consulted with stakeholders to determine scope of risk management appropriate to organisation and industry | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has presented options for risk management strategies for approval within scope of own role. | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has determined and reported areas of potential risk and non-compliance within scope of own role and escalate where required according to organisational policies and procedures. | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has supported communication of approved risk management strategies to required personnel. | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has sought feedback from relevant personnel on team communication practices according to working collaboratively in virtual environments protocols | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has shared knowledge and information according to work details, team objectives, organisational policies and procedures. | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has supported communication of proposed risk management strategies to required personnel | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The learner has worked collaboratively with interdisciplinary teams develop cyber risk management strategies | | | | | | | | | | | | ☐ | | ☐ | | |
| 1. The leaner has shared knowledge and information according to work details, team objectives, organisational policies, and procedures. | | | | | | | | | | | | ☐ | | ☐ | | |
| **Assessor Name** | | | | *Insert Name* | **Assessor Signature** | *Insert Signature* | | **Date** | | | | | *Insert Date* | | | |
| **Part D** | | | **Review – This is an individual task** | | | | | | | | | | | | | |
| **Question 1:** | | | What was the feedback you have received on your risk management report? Record your feedback in the answer box below. | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 2:** | | | What alterations have you made to the final report and why? Update your report accordingly and attach to submission. | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 3:** | | | What areas of team protocols for working collaboratively in a virtual environment would you improve in the future? | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 4:** | | | What improvements would you make for future work protocols in virtual environments? | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 5:** | | | Review the relevant critical cyber risk management strategies listed in your risk management report and describe how they were appropriate to level of risk stated in the scenario? | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 6:** | | | Review the protocols your team utilized to support each other to working collaboratively in virtual environments. | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 7:** | | | Review the technology utilized to support your team to work collaboratively in virtual environments. | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |
| **Question 8:** | | | Review how your team complied to the team protocols to work collaboratively in a virtual environment. | | | | | | | | **Satisfactory response** | | | | | |
| Yes ☐ | | | | No ☐ | |
| **Answer:** | | | | | | | | | | | Comment: | | | | | |

|  |  |
| --- | --- |
| Learner Acknowledgement and Cover Sheet | |
| **Academic Declaration:**  By submitting this assessment task and signing the below, I acknowledge and agree that:   1. This completed assessment task is my own work. 2. I understand the serious nature of plagiarism and I am aware of the penalties that exist for breaching this. 3. I have kept a copy of this assessment task. 4. The assessor may provide a copy of this assessment task to another member of the Institute for validation and/or benchmarking purposes. 5. For electronic submissions, by typing your name in the student signature field, you are accepting this declaration. | |
| **Learner name:** Insert name | **Learner ID:** Insert ID |
| **Submission Date:** Insert date | |
| **Learner signature:** | |
|  | |

|  |
| --- |
| Section F – Feedback to Learner |
| **Has the learner successfully completed this assessment task?** Yes No |
| **Assessor feedback (as appropriate):** Insert feedback |
| **Resubmission allowed:** Yes No  **Resubmission due date:** Insert date |
| **Assessor name:** Insert name |
| **Assessor signature:** |
|  |

# Classroom Code of Ethics

1. Privacy and confidentiality

- Don't take photos of other students or their work, without permission

- Don't share logins, or ask for others log in details

- Don't share any confidential or private information of other people on social media

2. Copyright procedures for all assessments

- Don't copy other students work

- If you're using another person's material, don't try to pass it off as your original work

- Respect copyright owners e.g. use citations/credit content creators where necessary

3. Ethical behaviour as a designer in class

- Give respect to others

- Follow teacher's instructions

- Don't answer phone calls in class – excuse yourself and go outside

4. WHS procedure and issues

- Set up work stations correctly – correct heights, lighting, chairs

- Keep the classroom clean and tidy – place rubbish in bins

- Follow WHS signs

5. Communication strategy and class behaviour

- Respectfully communicate with each other

- Don't send inappropriate texts or emails to each other  
- Email your teacher if you are absent

# Privacy Policy Template

How to use this template

The information in this template provides some base content for you to use and modify with information that relates to your specific privacy policy. Follow the steps below:

1. Replace the bold items in square brackets with your business information
2. Update content to align with your business's privacy policy
3. Create or update the privacy policy page on your website using the updated text.

# Privacy Policy

**[Your business name]** is committed to providing quality services to you and this policy outlines our ongoing obligations to you in respect of how we manage your Personal Information.

We have adopted the Australian Privacy Principles (APPs) contained in the Privacy Act 1988 (Cth) (the Privacy Act). The NPPs govern the way in which we collect, use, disclose, store, secure and dispose of your Personal Information.

A copy of the Australian Privacy Principles may be obtained from the website of The Office of the Australian Information Commissioner at [www.aoic.gov.au](http://www.aoic.gov.au)

## What is Personal Information and why do we collect it?

Personal Information is information or an opinion that identifies an individual. Examples of Personal Information we collect include: names, addresses, email addresses, phone and facsimile numbers.

This Personal Information is obtained in many ways including **[interviews, correspondence, by telephone and facsimile, by email, via our website www.yourbusinessname.com.au, from your website, from media and publications, from other publicly available sources, from cookies- delete all that aren’t applicable]** and from third parties. We don’t guarantee website links or policy of authorised third parties.

We collect your Personal Information for the primary purpose of providing our services to you, providing information to our clients and marketing. We may also use your Personal Information for secondary purposes closely related to the primary purpose, in circumstances where you would reasonably expect such use or disclosure. You may unsubscribe from our mailing/marketing lists at any time by contacting us in writing.

When we collect Personal Information we will, where appropriate and where possible, explain to you why we are collecting the information and how we plan to use it.

## Sensitive Information

Sensitive information is defined in the Privacy Act to include information or opinion about such things as an individual's racial or ethnic origin, political opinions, membership of a political association, religious or philosophical beliefs, membership of a trade union or other professional body, criminal record or health information.

Sensitive information will be used by us only:

• For the primary purpose for which it was obtained

• For a secondary purpose that is directly related to the primary purpose

• With your consent; or where required or authorised by law.

## Third Parties

Where reasonable and practicable to do so, we will collect your Personal Information only from you. However, in some circumstances we may be provided with information by third parties. In such a case we will take reasonable steps to ensure that you are made aware of the information provided to us by the third party.

## Disclosure of Personal Information

Your Personal Information may be disclosed in a number of circumstances including the following:

• Third parties where you consent to the use or disclosure; and

• Where required or authorised by law.

## Security of Personal Information

Your Personal Information is stored in a manner that reasonably protects it from misuse and loss and from unauthorized access, modification or disclosure.

When your Personal Information is no longer needed for the purpose for which it was obtained, we will take reasonable steps to destroy or permanently de-identify your Personal Information. However, most of the Personal Information is or will be stored in client files which will be kept by us for a minimum of 7 years.

## Access to your Personal Information

You may access the Personal Information we hold about you and to update and/or correct it, subject to certain exceptions. If you wish to access your Personal Information, please contact us in writing.

**[Your business name]** will not charge any fee for your access request, but may charge an administrative fee for providing a copy of your Personal Information.

In order to protect your Personal Information we may require identification from you before releasing the requested information.

## Maintaining the Quality of your Personal Information

It is an important to us that your Personal Information is up to date. We will take reasonable steps to make sure that your Personal Information is accurate, complete and up-to-date. If you find that the information we have is not up to date or is inaccurate, please advise us as soon as practicable so we can update our records and ensure we can continue to provide quality services to you.

## Policy Updates

This Policy may change from time to time and is available on our website.

## Privacy Policy Complaints and Enquiries

If you have any queries or complaints about our Privacy Policy please contact us at:

**[Your business address]**

**[Your business email address]**

**[Your business phone number]**

|  |
| --- |
| **Risk Management Report Template** Amend & alter the template in the empty fields/sections to meet the requirements outlined in the brief. |



**Risk Management Report ICT40120 Certificate IV in Information Technology  
ICTICT451 Comply with IP, ethics and privacy policies in ICT environments ICTICT443 Work collaboratively in the ICT industry BSBXCS404 Contribute to cyber security risk management**

**WALLETX**

Version 1.0

**GROUP NAME**

**Holmesglen TAFE**

[ Student 1 | Student 2 | Student 3 | Student 4 ]

0. Executive Summary

**0.1 Primary Role**

< State broad engagement role to be completed by Risk & Operations team (“students group”) >

**0.2 Key Concerns to Resolve**

< List **AT LEAST THREE (3)** specific areas of concern with regard to WALLETX’s operations >

**0.3 Summary of Recommendations**

< List **AT LEAST THREE (3)** actions that WALLETX are to take at the conclusion of this report (*you can only answer this once you have completed the report*) >

Section 1: Introduction

**1.1 Purpose of Report**

WALLETX, the online Australian cryptocurrency exchange company, requires a streamlined risk management report on the current and future risks that it faces. This report will identify key vulnerabilities and possible active issues, as well as recommendations and actions to take moving forward.

**1.2 Risk & Technologies Team Members & Roles**

|  |  |  |
| --- | --- | --- |
| **Name** | **Role** | **Risk Assessment Involvement** |
| Ellen Husk | Chief Executive Officer | < Risk Assessment Involvement role > |
| Tony Beasley | Lead Accountant | < Risk Assessment Involvement role > |
| Cleve Hobs | Lead Developer | < Risk Assessment Involvement role > |
| Miles Zeckerbern | Head of Cyber Security | < Risk Assessment Involvement role > |
| < Student 1 > | Risk & Technologies | < Team role > |
| < Student 2 > | Risk & Technologies | * < Team role > |
| < Student 3 > | Risk & Technologies | < Team role > |
| < Student 4 > | Risk & Technologies | < Team role > |

**1.3 Scope of Risk Assessment**

< State the key tasks that the report will conduct a risk assessment/risk analysis against (*look to the risk registers*) and state/list **AT LEAST TWO (2)** limitations on the scope, of which the report will NOT cover >

Section 2: Risk Assessment Methodology

**2.1 Risk Model**

The risk management system adopted by WALLETX is guided by ISO/27001 and will be instructed by common risk management guidelines and standards. A qualitative methodology has been used to conduct this risk assessment, utilising judgement to categorise risks as being low, medium or high. With those risks being categorised, this report makes use of a risk assessment matrix to determine action required using appropriate controls (see below matrix model).

Table

Description automatically generated

For the purpose of determining overall risk, scoring will be applied as part of the risk assessment/treatment where ***likelihood x impact = overall risk:***

* Likelihood: [ Very Unlikely (1) | Unlikely (2) | Possible (3) | Likely (4) | Very Likely (5) ]
* Impact: [ Negligible (1) | Minor (2) | Moderate (3) | Significant (4) | Severe (5) ]
* Overall: *Rate based on matrix above*

**2.2 Risk Definitions**

Based on the risk model, this report will use the following defined terms in the context provided:

|  |  |
| --- | --- |
| **Risk Term** | **Definition** |
| Risk | < Define >  An uncertain event that may occur and impact at least one initiative deliverable. Can include mention of the cause of the risk itself. |
| Issue | < Define >  A risk that has happened & requires evaluation of impacts and urgent mitigating activities |
| Threat | < Define >  What specifically will happen if the risk is not addressed / comes to fruition |
| Control | < Define >  The strategy by which you attempt to prevent the risk from occurring |
| Response Type | You must categorise each solution into one of the following:   * (**Watch**) – risk analysis has commenced by too early / difficult to determine active solution a.k.a. *monitoring* * (**Mitigate**) – you plan to apply risk response strategies to resolve the risk * (**Accept**) – no actions can be taken to mitigate the risk & must be accepted * (**Transfer**) – transfer the risk to another owner outside the company |
| Risk Owner | Person within the company best placed to manage the risk going forward |

Section 3: Risk Analysis (Risk Registers)

The risks (*and issues*) are identified & analysed below as an incident response plan for each of the required risk categories. To the best of your ability and using fair assumptions, estimate the likelihood & impact ratings for the identified risks.

**NOTE: Fill out each register with the MINIMUM number of entries provided. An example for each register has been provided – please fill out the remaining fields based on the Scenario & Issues.**

**3.1 Risk Register – Work Health & Safety (MINIMUM THREE (3) RISKS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Identified Risk** | **Threat** | **Current Controls** | **Likelihood** | **Impact** | **Overall Risk** | **Solution** |
| Bad employee seating | Ergonomic hazard leading to injury | N/A | Likely (4) | Low Med (2) | Minor (8) | (**Mitigate**)  Conduct audit of employee seating, including age of seats.  Replace any seats that are broken OR over 10 years old. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**3.2 Risk Register – Regulatory & Compliance (MINIMUM THREE (3) RISKS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Identified Risk** | **Threat** | **Current Controls** | **Likelihood** | **Impact** | **Overall Risk** | **Solution** |
| Non-licensed software | Copyright infringement & legal liability | N/A | Minor (2) | Significant (4) | Minor (8) | (**Mitigate**)  Audit software made available by WALLETX & check licences up to date.  Setup employee training to ensure no employees are using independent software outside recommended products. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**3.3 Risk Register – IT & Cyber Security (MINIMUM THREE (3) RISKS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Identified Risk** | **Threat** | **Current Controls** | **Likelihood** | **Impact** | **Overall Risk** | **Solution** |
| Sharing of passwords | Access to secure areas / permissions    Hacker vulnerability | N/A | Very Likely  (5) | Moderate  (3) | Medium High  (15) | (**Mitigate**)  Reset all passwords, re-train staff, monitor system access. |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

**3.4 Risk Register – Risk Management System (MINIMUM TWO (2) RISKS)**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Identified Risk** | **Threat** | **Current Controls** | **Likelihood** | **Impact** | **Overall Risk** | **Solution** |
| Risk Audit | Critical systems failure  Governance sanctions | Not found | Likely  (4) | Moderate  (3) | Medium  (12) | (**Mitigate**)  Develop risk audit template that allows for components inherit risk, control of risk and detection of risk to be documented.  Audit on periodic cycle (monthly). |
|  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |

Section 4: Summary of Findings

**4.1 Major Negative Trends**

On conclusion of the risk analysis conducted by the Risk & Technologies team (*known as “< Student Team Name >”*), a range of issues have been identified which affect many areas of operations. The major identified negative trends include:

* < List **AT** **LEAST THREE (3)** major problem trends that are present within WALLETX (*try to capture* ***OVERALL*** *issues with the company, rather than specific issues listed in Section 3*) >

**4.2 Priority of Risks**

The risks captured in Section 3 are listed in order of priority, based on the risk methodology adopted by this report:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Priority** | **Identified Risk** | **Threat Source (*Affected Register*)** | **Likelihood** | **Impact** | **Risk Rating** | **Solution** |
| 1. |  |  |  |  |  |  |
| 2. |  |  |  |  |  |  |
| 3. |  |  |  |  |  |  |
| 4. |  |  |  |  |  |  |
| 5. |  |  |  |  |  |  |
| 6. |  |  |  |  |  |  |
| 7. |  |  |  |  |  |  |
| 8. |  |  |  |  |  |  |
| 9. |  |  |  |  |  |  |
| 10. |  |  |  |  |  |  |
| 11. |  |  |  |  |  |  |
| 12. |  |  |  |  |  |  |
| 13. |  |  |  |  |  |  |
| 14. |  |  |  |  |  |  |
| 15. |  |  |  |  |  |  |

***NOTE****: you are not required to include the examples provided in Section 3*

Section 5: Recommendations & Actions

**5.1 Recommendation Overview**

Based on the streamlined risk management analysis, this report recommends that < state general trends / overall issues that need to be addressed by WALLETX >.

**5.2 Immediate Actions**

Specifically, to address a large portion of these negative risk trends, the following actions should be taken immediately within the current financial year to avoid negative ASIC penalties:

|  |  |  |
| --- | --- | --- |
| **Recommendations for Risk Actions** | **Risk Owner** | **Recommended Resources** |
| Implement password policy | Head of Cyber Security | Soft/Hard copy of password policy |
| < Risk Action > | < Risk Owner > | < Resources needed to carry out action > |
| < Risk Action > | < Risk Owner > | < Resources needed to carry out action > |
| < Risk Action > | < Risk Owner > | < Resources needed to carry out action > |
| < Risk Action > | < Risk Owner > | < Resources needed to carry out action > |
| < Risk Action > | < Risk Owner > | < Resources needed to carry out action > |

**5.3 Review of Report**

Required Review of Risk Management Report Date: < insert date for review >