|  |  |  |  |
| --- | --- | --- | --- |
| **Qualification details** | | | |
| **Training Package Code and Title:** | **ICT - Information and Communications Technology (Release 5)** | | |
| **Qualification National Code and Title:** | ICT40120 Certificate IV in Information Technology | **State code:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Assessment Title** | **AT2 Risk Management Project** | | |
| **Unit National Code & Title** | BSBXCS404 Contribute to cyber security risk management | | |
| **Date Due** |  | **Date Received** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Student Name** | Richard Pountney | **Student ID** | 30007736 |
| **Student Declaration** | I declare that the evidence submitted is my own work:  RBP  ………………………………………….. | | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Assessor Name** | **Jeff Xie** | | | |
| **Assessment Decision** | Satisfactory | | Not Yet Satisfactory | |
| **Assessor Signature** |  | | **Date** |  |
| **Is student eligible for reassessment (Re-sit)?** | No | Yes | **Reassessment Date:** |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Feedback to student** | | | |
| *Via Blackboard (LMS) – Please check [Grade] section.* | | | |
| **Feedback from student** | | | |
| *Via Blackboard (LMS) – Please use [Comment] section during submission.* | | | |
| **Student signature** |  | **Date** |  |

|  |
| --- |
| **Assessment Instructions** |

|  |  |
| --- | --- |
| **TO THE ASSESSOR** | |
| Type of Assessment | Project |
| Duration of Assessment | 3 Class Sessions (Week 6-8) |
| Location of Assessment | Classroom |
| Conditions | Learners are required to complete the required tasks in class and submit the required documentation electronically via Blackboard |
| Elements and Criteria | As detailed in the assessment plan |

|  |  |
| --- | --- |
| **TO THE STUDENT** | |
| Purpose of Assessment | You are required to show you can:   * Contribute to recommending risk management strategies that mitigate cyber security risk * Support implementation of approved risk management strategies in response to risk * Review and revise implemented risk management strategies |
| Allowable Materials | Blackboard (Topic by topic) will include the following: Weekly Readings, Class notes, and Weekly Activities. |
| Required Resources | Computer with:   * Internet Access * Word processing software * Access to Learning Management System (LMS) * Access to encryption and authentication protocols/software * Access to WAP with enterprise security support * Network topology/diagram software |
| Reasonable Adjustment | 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. |
| Assessment Submission | All questions and activities must be attempted.  Use of research tools and peers in formulating answers are acceptable – but work submitted must be your own work.  Final project documentation is to be uploaded to the appropriate area in the Blackboard course created for this unit.  If you are marked as NYS (Not Yet Satisfactory) on your first attempt, you will be provided with another opportunity to re-attempt the assessment at the discretion of the lecturer. |
| Project contents | This project consists of the following tasks:   * Consult with stakeholders to determine scope of risk management appropriate to organisation and industry * Review relevant critical cyber risk management strategies appropriate to level of risk * Assist in developing suitable cyber security response options according to organisational policies and procedures * Present options for risk management strategies for approval within scope of own role * Document approved risk management strategies * Support communication of approved risk management strategies to required personnel * Contribute to monitoring cyber security risk according to selected risk management strategies * 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 * 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 |

Your assessor will use the following checklist to assess your understanding of the issues and participation and communications skills for this competency.

| **Did the candidate demonstrate the ability to do the following:** | **Yes** | **No** | **Assessor Comments:**  *(This section must contain lecturer’s notes/comments)* |
| --- | --- | --- | --- |
| **Activity 1 – Identify and recommend risk management strategies** |  |  |  |
| * Consult with stakeholders to determine scope of risk management appropriate to organisation and industry |  |  |  |
| * Review relevant critical cyber risk management strategies appropriate to level of risk |  |  |  |
| * Assist in developing suitable cyber security response options according to organisational policies and procedures |  |  |  |
| * Present options for risk management strategies for approval within scope of own role |  |  |  |
| * Document approved risk management strategies |  |  |  |
| **Activity 2 – Support implementation** |  |  |  |
| * Support communication of approved risk management strategies to required personnel |  |  |  |
| * Contribute to monitoring cyber security risk according to selected risk management strategies |  |  |  |
| * 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 |  |  |  |
| **Activity 3 – Review and revise** |  |  |  |
| * 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 |  |  |  |

*Continue to the next page*

|  |
| --- |
| **Scenario** |
| *You are a member of the CITE MS Information Security team, you work directly under and report to the CITE MS Chief Security Officer (CSO). CITE MS has recently been engaged by South Metropolitan TAFE (SMTAFE) to do an audit on their current cyber security risk posture and recommend risk management strategies to minimise their exposure to cyberattacks.*  *SMTAFE is a Registered Training Organisation (RTO) with a campus based in Western Australia. It offers certificate and diploma level qualifications in the Vocational Education and Training (VET) sector for many subject areas including business, community services, education, information technology, health, hospitality, and many others.*  *There are currently 450 students that attend the college across a wide range of classrooms. Depending on their studies, students who require access to a computer are given access Windows 10 desktop machine and a word processor and other software applicable to their studies plus access the internet. For classes that are self-directed, all learning materials are provided in Blackboard, a learning management system, as are the assessments.* |

|  |
| --- |
| **Activity 1 – Identify and recommend risk management strategies** |
| 1.1 You are required to consult the client manager (your lecturer) to determine the scope of risk management for the client’s organisation (SMTAFE). During this discussion, you are required to ask 2 or more questions to clarify the scope of this risk management project. The questions have to be related to the industry/organisation.  Fill in the table below with details of the discussion.     |  |  | | --- | --- | | Date of Discussion: 25/11/2022 | Client Manager: Nab Yadav | | Q1: What sort of protection is being used? (e.g., Firewalls) | Response:  Firewall  Anti-Virus | | Q2: How is it monitored? | Response:  Auto Scan |  * 1. Review the attached ***AT2 Appendix A - Information Security Policy.doc*** and the risk management strategies within. Identify **at least 4 strategies** that may not be appropriate to the level of risk and justify it.  |  |  | | --- | --- | | **Strategies that are inadequate** | **Why is strategy not appropriate?** | | 1. Phone System Security There is no proper phone security system in place | If it’s running on VOIP, it can be hacked It doesn’t specify how to minimise the risks that can accrue. | | 1. Virus Protection All firewalls used at SMTAFE shall filter out incoming ActiveX and Java control viruses at the firewall. | There are more control viruses than what is said so it would be better to cover most if not all of them. | | 1. Redundancy & Backups Point 3, Monthly full backups shall be stored for a minimum of three months. | Backups should be stored for at least 6 months if not 12 months. | | 1. Passwords Policy Point 1, Minimum 6 characters | Having a minimum of 6 characters can be cracked easily. |  * 1. Recommend risk management strategies to address the issues with existing strategies that you identified above. List down the strategies with justification to describe how the recommended strategies will help reduce the risk exposure to an acceptable level.  |  |  | | --- | --- | | **Proposed Strategies** | **Justification** | | 1. I would recommend that having phone numbers saved to minimise answering a dangerous number. | To reduce the amount of dangerous numbers going through the system. This is because hackers can use a phone call to access the internet that the answer is connected to so this can be very dangerous so it would be best to only answer numbers that are recognised. | | 1. The firewall will filter out any malicious programs & there will be an anti-virus &or anti-malware program that is also protecting the systems. | There should be more than a firewall protecting the systems because a firewall can’t protect from all malicious programs so it would be best to have at least an anti-virus or an anti-malware. | | 1. Monthly full backups shall be stored for a minimum of 6 months if not 12 months. | 6 months is an adequate time because it gives enough time for it to be used if needed. | | 1. The minimum number of characters should be 10 or 12 characters. The password should have at least 1 lowercase letter, 1 uppercase letter, 1 number, and 1 special character (examples are: &, $, @). | This makes it harder to decrypt the password for anyone trying to hack the encrypted password. |  * 1. Present the proposed strategies to the client manger (your lecturer) for approval. Record the details of discussion in the table below.  |  |  |  | | --- | --- | --- | | **Date of discussion:** 2/12/2022 | **Client Manager:** Nab Yadav |  | | **Proposed Strategies** | **Feedback** | **Approved/Rejected** | | 1. I would recommend that having phone numbers saved to minimise answering a dangerous number. |  | Approved | | 1. The firewall will filter out any malicious programs & there will be an anti-virus &or anti-malware program that is also protecting the systems. |  | Approved | | 1. Monthly full backups shall be stored for a minimum of 6 months if not 12 months. |  | Approved | | 1. The minimum number of characters should be 10 or 12 characters. The password should have at least 1 lowercase letter, 1 uppercase letter, 1 number, and 1 special character (examples are: &, $, @). |  | Approved | |

|  |
| --- |
| **Activity 2 – Support implementation** |
| 2.1 Create an email to notify end users of the approved risk management strategies and how it will affect them. Attach this email as part of your submission.    2.2 The client manager has selected 2 risk management strategies that should be prioritised based on the current risk situation. These strategies are:   * Enhancing and enforcing password policy * Installing and configuring Anti-Virus solution (windows defender is not acceptable).   You have been tasked to create a set of step-by-step instructions to guide the security team in monitoring the 2 risks above. The instructions should include detailed steps to navigate to the respective settings page as well as screenshots where necessary.  Enhancing and enforcing password policy  Step 1 – Search “Local Security Policy”  by using the computers search bar.  Step 2 – Click account policy > Click password policy.  Step 3 – double click minimum password length & change accordingly.    Installing and configuring an Anti-Virus solution (windows defender is not acceptable).  Step 1 – find an Anti-Virus & download it.  Step 2 – open the executable file that you just downloaded.  Step 3 – follow the instruction from the installation.  Each anti-virus has at least a slightly different layout so you should be able to navigate it. Especially when setting up for the first scan, this is also how you configure the anti-virus as well.  2.3 Using the provided Windows 10 VM, conduct a check on both the password policy and AV within the VM to determine if it is compliant to the proposed risk management strategies. Provide screenshots with a description to explain your results.  Password Policy:  This is showing the VM Local Security Policy, Password Policy. As shown in this image, the minimum password length is 0 characters which means that you don’t need a password to login. This puts the system at a high risk.  Anti-Virus Solution:  This is showing the VM desktop  **PLEASE TAKE NOTE:**  You need to perform the tasks on ONE of the following systems:   * Your own laptop/desktop * \*Windows 10 Virtual Machine <User ID: **Admin**|Password **Admin**> * \*Any other Virtual Machines that you got from other units.   \*You may download the Windows 10 Virtual Machine using the following link:  <https://tafewa-my.sharepoint.com/:u:/r/personal/jeff_xie_smtafe_wa_edu_au/Documents/SMTAFE/2021%20Semester%202/BSBXCS404/BSBXCS404%20AT2.zip?csf=1&web=1&e=Ol7mBf>  Please note that the file is 5.9GB and will take some time to download so please start early.  You may also use any other Virtual Machines that you have obtained from other units.  2.4 Address non-compliance by configuring the settings according to approved risk management strategies. You are required to provide screenshots to show that the configurations have been applied.  Ensure that:   * Password policy is configured and enforced according to approved standards * Third-party antivirus solution is installed * AV is set to updated and scan automatically based on the approved standards.   Password Policy:  Before change:    After Change:    2.5 After the implementation of the new risk management strategies, the team realised that employees/end users can contribute in terms of identifying potential new risks within the organisation. As such, you have been tasked to assist in establishing formal feedback processes so that there is are channels of reporting potential new risks.  Create a set of instructions for employees to provide feedback or report an incident to warn the team of potential new risks. You must include a feedback/reporting form within the document. The reporting form will need to include basic information about the risk and a list of common risks that may be present within the organisation. |

|  |
| --- |
| **Activity 3 – Review and revise** |
| 3.1 Identify benchmarks to track the effectiveness of the implemented risk management strategies. Create a list of conditions for each of the following strategies to assist the security team when they are testing the strategies. List at least 2 conditions to meet when checking for effectiveness of the respective strategies   |  |  | | --- | --- | | Implemented Strategies | Benchmarks of Effectiveness | | Password policies | 1.  2. | | Antivirus | 1.  2. |   3.2 Conduct a check on the provided Windows 10 VM after you have implemented the risk management strategies. Capture screenshots and provide a description of the results of evaluation to determine if they meet the benchmark of effectiveness provided above.  3.3 Based on the evaluation in 3.2, determine if the strategies were effective and update the strategies if necessary. If no further changes are required, update the information security plan with the approved strategies and highlight them. Ensure that all required information is updated as well, including version control. Attach the updated security policy as part of your submission. |