**TEESSIDE UNIVERSITY - SCHOOL OF COMPUTING, ENGINEERING AND DIGITAL TECHNOLOGIES**

**ICA 1 SPECIFICATION (30%)**

|  |  |
| --- | --- |
| **Module Title:**  Networks & Security | **Module Leader: Nauman Israr** |
| **Module Code: CIS1008** |
| **Assignment Title:**  ICA 1- Risk Assessment (30%).  Undertake a security risk assessment for a system without direct supervision and propose basic remediation advice. | **Deadline Date: 26 April 2023**  **Feedback Due : 26 May 2023** |
| **Deadline Time: 4:00;** PM |
| **Submission Method: Online via Blackboard Ultra** |

**~~Central Assignments Office (Middlesbrough Tower M2.08) Notes:~~**

* ~~All work (including CDs etc) needs to be secured in a plastic envelope or a folder and clearly marked with the student name, number and module title.~~
* ~~An Assignment Front Sheet should be fully completed before the work is submitted.~~
* ~~When an extension has been granted, a fully completed and signed Extension form must be submitted to the SCM Reception.~~

# Online Submission Notes:

# Please follow carefully the instructions given on the Assignment Specification

# When Extenuating Circumstances (e.g. extension) has been granted, a fully completed and signed Extenuating Circumstances form must be submitted to the School Reception or emailed to scedt-assessments@tees.ac.uk.

# FULL DETAILS OF THE ASSIGNMENT ARE ATTACHED INCLUDING MARKING & GRADING CRITERIA

**Assessment Criteria**

All parts of the component must contain your name and student ID

***Scenario:***

An trading floor Support centre employs 700 staff. They have recently expanded and as a result, need to move to a new building. A building has been identified but has no network. This means that before they can make a move a whole, new network service needs to be designed and implemented in the new building. Existing Network comprises of the following elements:

***Existing Network:***

* Desktop machines are running a mixture Windows seven SP2, Windows 11 and Ubuntu 18 as an Operating System.
* Servers are running Windows 2016 with Domain controller.
* Wireless Access Points uses WPA2.
* Subnets are class-based IPv4.
* Main Layer two Protocol is Spanning Tree.
* The main routing protocol is RIP v1.
* Physical layer cabling is CAT 5e.
* Open source web server and anti-virus software are in use.
* Servers and key network infrastructure are located on the ground floor.
* Full and incremental backups are stored on a server located on the ground floor.
* Key network services use a single 15 character password for authentication.
* USB and external adaptors are allowed.
* Executables files are automatically blocked by the email server (MS Exchange).
* Non used network ports are blocked.
* End users are not permitted to install software.
* Network Hardware is provided by Cisco and only accessible to the IT technicians but can be accessed via a network (Access via the network is password protected.).
* Remote access to network equipment is via telnet.
* End users have basic IT knowledge.

**Task :** Undertake a security risk assessment for the given network and propose remediation advice

# Products:

* ICA 1 (30%): Security Risk Assessment for the given scenario(existing network), Deadline: 26 April 2023
  + Identifies critical security risks of the existing network (e.g. likelihood and impact).
  + Record risk using appropriate tools (e.g. risk register: [Corporate-Risk-Register-Template-Example.jpg (3307×2338) (examples.com)](https://images.examples.com/wp-content/uploads/2018/07/Corporate-Risk-Register-Template-Example.jpg)).
  + Advice on how to resolve or mitigate against identified risks.

Note: Word count limits for ICA 1 is 1000 words.

**Appendix**

**Learning Outcomes**

|  |
| --- |
| Module Learning Outcomes |
| **Personal and Transferable Skills**   1. Produce supporting documentation that effectively summarises key information, adopting a professional approach. 2. Identifying network security risks and their remediation. 3. Apply the fundamentals of network design, deciding on appropriate hardware, protocols and software.   **Research, Knowledge and Cognitive Skills**       4. Demonstrate an understanding of the role of networks and security in modern IT environments.       5. Design a network to meet specified business requirements and select appropriate network technologies and topologies.       6. Undertake a security risk assessment for a simple system and propose basic remediation advice.       7. Evaluate to what extent a network design meets specified business requirements and/or objectives.  **Professional Skills**        8. Work autonomously with limited direction to produce a network design for a given scenario.       9. Discuss the ethical, social and legal issues surrounding the management of a modern networked environment.  **Learning Outcomes Degree Apprenticeship:**  C1 : Critically analyse a business domain in order to identify the role of information systems, highlight issues and identify opportunities for improvement through evaluating information systems in relation to their intended purpose and effectiveness  C4 : Undertake a security risk assessment for a simple IT system and propose resolution advice. Can identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. Cloud services).  C13: Analyse common vulnerabilities in computer networks including unsecure coding and unprotected networks.  C14: Evaluate various roles, functions and activities related to technology solutions within an organisation.  C16: Deliver a technology solutions project accurately consistent with business needs.  C29: Perform under pressure  C30: Take a thorough approach to work  SE2: Undertake analysis and design to create artefacts, such as use cases to produce robust software designs.  SE6 Deliver software solutions using industry standard build processes, and tools for configuration management, version control and software build, release and deployment into enterprise environments.  **Marking Criteria** |

|  |  |  |
| --- | --- | --- |
| **Part 1- Risk Assessment (1000 words)** | | **Marks** |
| Identifies risks | To obtain maximum marks you need to :-   * Identifies risks with key chrematistics (e.g. likelihood and impact) | 34% |
| Record risk | To obtain maximum marks you need to :-   * Record risk using appropriate tools (e.g. risk register) | 33% |
| Mitigate | To obtain maximum marks you need to :-   * Advice on how to resolve or mitigate against identified risks. | 33% |
| **Total** | | **100%** |