New Zealand Diploma in System Administration Level 6

NET602: Network Services

Assessment/Aromatawai - Assessment 1 v2.3

Case Study

	Submission	FER1	FER2
Result	Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Date	Click or tap to enter a date.	Click or tap to enter a date.	Click or tap to enter a date.
Assessor's Signature			

Student Name	Click or tap here to enter text.
Student ID	Click or tap here to enter text.
Student Signature	
Assessor	Click or tap here to enter text.

Assessor's Feedback

Submission

Click or tap here to enter text.

FER1

Click or tap here to enter text.

FER2

Click or tap here to enter text.

Assessment Instructions and Guidelines for Submission

Task Completion

- All tasks must be completed to receive a mark. Submissions with incomplete or missing tasks will be marked as Incomplete and not entitled to further FER.
- Any storage media (flash drive, disk, etc.) submitted must be virus free. Media containing malware or content that cannot be run directly will be marked as a Fail.
- Submissions will be judged based on completeness, correctness and clarity. Please refer to the assessment schedule for more details.

Format

- All written submissions must:
  - Be formatted in size 11 Arial font;
  - Have 1.15 line spacing**;**
  - Include a title page with the candidate's name, class and Aspire2 student ID clearly printed.
- All pages and printouts must include the candidate's Aspire2 student ID in the footer.
- You may need to attach the task cover sheet found on Canvas to the front of the final submission of your task (Please confirm with your tutor).

Submission

- All written work will be submitted via Turnitin in your Canvas LMS course unless otherwise specified.

Due Date

- Refer to your Canvas LMS course for specific due dates.

Competency-based Assessment Resubmission and Re-enrolment

- Students will have an opportunity to provide further evidence twice.
- To be eligible for a FER the student must make a reasonable attempt at the questions/tasks in the assessment.
- *Reasonable* is to be defined as a response that at the very least attempts to address the question/task.
- Where the student does not make a reasonable attempt at ALL questions/tasks they will not achieve and will be required to re-enrol in the paper.
- A fee of $250 is payable for the second FER.
- The need for further evidence from the students will be noted on the assessment as "FER" and dated.
- When the further evidence is deemed adequate the "FER" notation will be crossed out, initialled and dated.
- If a student is still deemed not yet competent after the second FER they will be required to re-enrol in the paper. A fee will apply for re-enrolment and details will be available in the Programme Handbook, and students will be informed of them at the start of the program.

- Additional FER's are at the discretion of the Head of Faculty.

Reconsideration of Assessments and Appeals

- Students have the right to a reconsideration of assessment or appeal if they believe an assessment has been incorrectly marked or graded.
- The request for reconsideration must be made in writing to the Head of Faculty within five (5) working days of the return of the assessment. A fee of $40 per assessment applies.
- Students must be informed that, as a result of the reconsideration of assessment, their result may be unchanged, raised or lowered.
- The reconsidered result will be recorded as the final result. Students retain the right to appeal this result.

Plagiarism

- By submitting your assignment, you agree to the Aspire2 Education policy on 'Academic Dishonesty and Plagiarism'. Assignments completed using unfair means or plagiarised material will receive a FAIL grade.
- All tasks must be done in your own words and referenced using APA 7th edition.

Feedback

- You may request feedback from your lecturer to verify the accuracy of your marks.
- Any feedback and grading results will be available in the Canvas LMS within the timeframe specified by your Programme Handbook.

Assessment Criteria

Course Aims

The objective of this course is to provide learners with knowledge and skills on the implementation of advanced networking principles and protocols.

Graduate Profile Outcome (GPO)

1. Plan and use services, technologies, and tools to automate the deployment and management of devices, applications, and infrastructure by way of scripts to automate standard systems procedures.
2. Apply professional and ethical practices with integrity to meet the industry wide expectations of a responsible IT professional, in accordance with legal, regulatory, and organizational requirements.

Learning Outcomes/Tīpako

LO1. Plan and design network solutions to meet organizational requirements using principles of information design and automated system procedures.

LO3. Apply professional and ethical practices in the analysis of IT security solutions to protect and secure assets.

Task Mapping/Mahere Mahi	Learning Outcome/Tipako
1.1 Project plan	LO1
1.2 Analyze the current network infrastructure	LO1
1.3 Calculate IP address	LO1
2.1 Selection of hardware and software components	LO1
2.2 Design a proposed network infrastructure diagram	LO1
3.1 Security risk analysis and security solution	LO3
3.2 Design a network diagram for a secure network-level access solution.	LO1
4.1 Printer Function Automation	LO1
4.2 Backup Management Process Automation	LO1
5.1 Professional and ethical practices	LO3

Student Undertaking

I have read and understood the assessment instructions given above. I understand that I will be given zero marks and will be reported to the disciplinary committee if I am found cheating or engaging in any academic misconduct.

Student Name: Click or tap here to enter text.

Student Signature:

Date: Click or tap to enter a date.

Case Scenario

TechCo Solutions is a medium-sized technology consulting firm. It provides IT services and solutions to clients from various industries. Currently, it has approximately 18 employees across four departments. The network setup employed by TechCo Solutions is a simple and flat configuration, lacking robust security measures, and is maintained on-premises. Employees working remotely use desktops or laptops connected to the organizational network but there are no extensive security protections in place for these workers and their connections to that network.

Currently, the company deals with sensitive and confidential information in its daily operations, such as software code, development data, customer data, financial information, and employee information. For future growth, the company emphasizes a hybrid network approach, combining on-premises infrastructure with secure cloud solutions. This strategy ensures that sensitive information can be accessed and stored through its internal network while also leveraging the scalability and flexibility of cloud services. As a result, maintaining data privacy and implementing robust security measures within the premises and in the cloud is crucial for the company. This approach aligns with the company-specific operational strategy to maintain its data, infrastructure, and network services within its current building while accommodating future growth and enhancing security.

Departments and Users

Departments	No. of Users
Development	6
Operations	6
Administration	2
Sales	4

In response to the management's plans for business expansion, the team has raised concerns regarding security. To address these concerns, the company has made the decision to strengthen the current network infrastructure in terms of both security and scalability. The initiative aims to ensure that the network is protected against potential threats while also accommodating the future growth of the business.

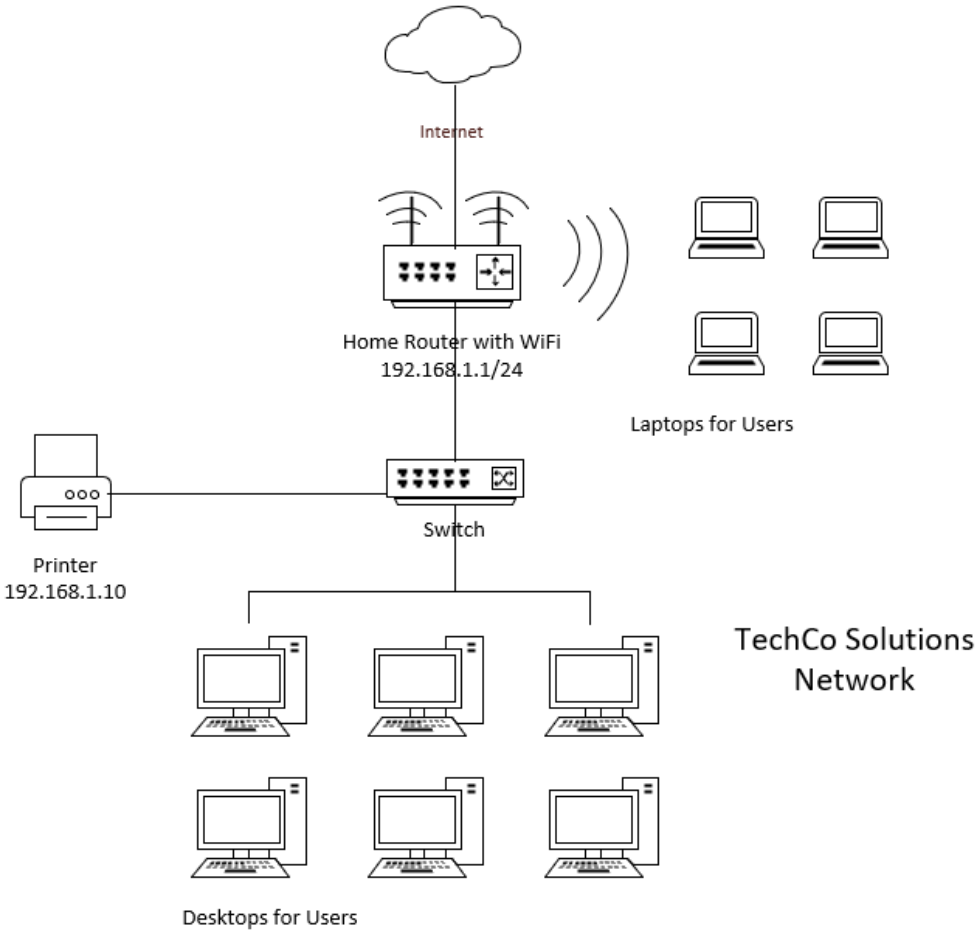
Business Requirements:

1. The company requires a hybrid network solution that is scalable to accommodate the company's growth and evolving business needs. It should support up to 80 users.
2. The company requires a secure solution to enable employees to access company resources remotely when they are working from home. It should ensure data confidentiality and integrity.
3. The network solution must be designed to retain and store information on the local premises for several reasons: data security and control, legacy systems compatibility and customization needs. By doing so, the organization can have direct control over its data and resources, achieve faster access and potentially enhance security.

Technical Requirements:

1. The company seeks centralized management of network services, including user accounts and access control.
2. The company requires secure file and printer sharing, promoting collaboration and data integrity.

3. The network solution should include security measures to protect sensitive data from unauthorized access, data breaches, and cyber threats.
4. Secure Wi-Fi access for each department.
5. The company needs secure access to its on-premises infrastructure from public networks as it is planning to host several legacy ERP systems and CRM systems on its premises.
6. Automation is required for on-premises components, specifically in printer management and backup procedures. This automation will contribute to efficient and reliable project deployments.



Current Infrastructure:

1. **Network Equipment:**
   - **Router:** Basic home router with Wi-Fi, providing general connectivity but lacking advanced security and management features.
   - **Switch:** Basic 8-port switch, which is insufficient for departmental segregation and lacks advanced network management capabilities.
2. **Printing and Storage:**
   - **Printer:** Inkjet black and white printer, suitable for low-volume printing but lacks advanced features for secure and efficient document management.
3. **Computing Devices:**

- **Desktops and Laptops:** Various computers and laptops used by employees, with no centralized management or advanced security controls.

4. **Servers:**
   - **None:** No dedicated servers are currently in use for hosting applications, data storage, or managing network services, impacting scalability and centralized management.
5. **Data Storage:**
   - **Local Storage:** No dedicated storage solutions in place for handling sensitive and confidential information, which poses risks to data security and access.

As a network administrator, you are tasked to design a secure network solution that focuses on on-premises components and incorporates various network services. The company recognises the benefits and importance of automated system procedures in ensuring efficient and reliable project deployments. While your team members are working on the cloud components, you will be responsible for planning, designing, organizing, documenting, and presenting the on-premises solutions using automated procedures for printer management and backup operations. The collaborative effort, with a hypothetical team member handling the cloud components, aims to create a secure hybrid network solution that aligns with the organization's requirements and future growth plans.

Task Instructions

Task 1.1

Develop a project plan for deploying the proposed secure network solution.

- The plan must have a start date, end date, responsibilities, tasks and subtasks, milestones, risks and post-deployment support.
- The timeline for the project is 6 weeks.
- The plan should be presented using any project management tool.

Task 1.2

Conduct an analysis of the current network infrastructure to identify issues and determine the hardware and software requirements necessary to address these issues effectively. The analysis should be based on both business and technical requirements.

1. **Analyse the Current Network Infrastructure: r**eview the current network setup to identify issues and areas for improvement.
2. **Define Requirements:** based on business and technical requirements, identify and list the hardware and software needed to address the identified issues.
3. **Justify Requirements: p**rovide explanations and justifications for each component to fulfil the business and technical requirements effectively.

Task 1.3

You have been assigned the task of subnetting the office network, which currently has the IP address 192.168.1.1/24. The network consists of multiple departments with different numbers of hosts. Your task is to calculate the new network range and subnet mask for each department using a standard /24 subnet structure.

- The calculation should include the Network ID, Broadcast ID and IP range.
- Create a subnet based on the following table:

Subnets	No of IP
Development	50
Operations	30
Administration	20
Sales	10
Server	6

Task 2.1

Select the appropriate hardware and software components to address the identified network issues identified in Task 1.2 and meet the defined requirements for TechCo Solutions. Each component must include its specification, cost, quantity, and justification. The budget for this task is between NZD 15,000 and NZD 23,000.

1. **Select Hardware Components**:
   - Provide detailed specifications, costs, and quantities for each hardware component.
   - Justify the choice of each hardware component based on how it addresses the network issues and meets the requirements.
2. **Select Software Solutions:**
   - Provide detailed specifications, costs, and quantities for each software component.
   - Justify the choice of each software solution based on how it addresses the network issues and meets the requirements.

Task 2.2

Develop a detailed network infrastructure diagram that illustrates the proposed secure network solution for TechCo Solutions utilizing the subnetting information from Task 1.3.

1. **Design the Network Diagram**
   - **Components**: Include all selected hardware and software in the diagram.
   - **Connections**: Show how each component connects to the network.
   - **Subnetting:** Integrate the subnetting scheme derived in Task 1.3, showing how IP addresses are allocated across different network segments.
2. **Label Components**
   - **Clear Labels**: Label each component according to industry practice, ensuring that the purpose and function of each item are clear.
   - **Security Measures**: Show where security measures are implemented in the network.
3. **Document the Diagram**
   - Presentation: Ensure that the diagram is clear, well-organized, and visually appealing. Use appropriate software tools to create the diagram.

Task 3.1

Identify potential vulnerabilities and security threats and propose suitable security mechanisms using a defence-in-depth approach.

1. **Identify Vulnerabilities and Threats**
   - Review the update network structure in Task 2.2 to identify at least three potential vulnerabilities or security threats.
   - Clearly describe each identified issue and its potential impact on the network.
2. **Propose Security Mechanisms**
   - For each identified threat or vulnerability, propose a specific security mechanism.
   - Explain how the mechanism addresses the issue and integrates with the overall network solution.
   - Detail how the mechanism enhances network security and supports the defence-in-depth strategy.
   - List out the hardware or software to use in the current network infrastructure with specification and costs and justification for the product.
3. **List Hardware and Software for Proposed Security Mechanisms**
   - Specify the hardware or software required for the proposed security mechanisms.
   - Provide detailed specifications and costs for each listed item.
   - Explain why each hardware or software component was chosen to enhance overall security.

Task 3.2

Implement the proposed security mechanisms from Task 3.1 into the network diagram to enhance the overall network security for TechCo Solutions.

1. **Update the Network Diagram**
   - **Security Mechanisms:** Integrate the security mechanisms proposed in Task 3.1 into the network diagram, clearly showing their placement and configuration.
   - **Components and Connections:** Ensure that all components and connections reflect the enhanced security measures.
2. **Label Security Enhancements**
   - **Clear Labels:** Label each security mechanism in the diagram according to industry practice.
3. **Document the Updated Diagram**
   - **Presentation:** Ensure that the updated diagram is clear, well-organized, and visually appealing. Use appropriate software tools to create the diagram.

Task 4.1

According to the specified requirements, an automated procedure is needed to handle printer functions, intending to automate tasks related to printer functions and streamline the printer deployment process within a Windows environment using PowerShell. The assigned tasks are as follows:

- Create a PowerShell script to install and configure printer management features on the designated server.
- Select appropriate cmdlets and modules to create and configure Group Policy Objects (GPOs).
    - Customize the scripts to target specific Organizational Units (OUs) such as "Staff", "Management", or "Account", and link corresponding GPOs for efficient deployment of printer.
- Utilize the Graphic User Interface (GUI) to dynamically assign printers to specific OUs.
- Conduct thorough testing of the PowerShell scripts in a controlled environment to ensure correct printer assignment to OUs and successful printer sharing via GPOs.

Task 4.2

Next, you are tasked to automate the backup management process in a Windows Server environment, ensuring regular backups of critical data and system configurations. An automated procedure intends to streamline the backup process, scheduled and configured to meet the organizational requirements effectively. The assigned tasks are as follows:

- Research and select appropriate PowerShell cmdlets/modules for managing Windows backup.
- Create a PowerShell script to configure and schedule Windows backups with the following specifications:
    - Customizing the script to target specific directories, such as the entire C drive for backup.
    - Adapt the script to schedule backups after office hours.
    - Specify the network path for storing backup files.
- Test the PowerShell scripts in a controlled environment to ensure the correct configuration of backup settings.
- Validate that the scheduled backups occur after office hours, are stored on the specified network path, and include the entire C drive.

Task 5.1

Discuss three professional and ethical practices that the IT administrator and the team should adopt to ensure data privacy and protect user information. Provide an example related to the case scenario and discuss how each practice addresses the concern. Additionally, propose strategies to effectively manage legal considerations and adhere to NZ data protection regulations to ensure that overall ethical practices are established for the network solution.

Task 6.1

Assemble and submit your documentation.

- Each item must be clearly labelled with the appropriate task number.
- Ensure that you include the assessment instrument, with all verification signed by your tutor.
- Submitted content/documentation must:
    - Maintain consistent formatting throughout the document.
    - Be well-structured and organized with clear headings and subheadings to guide the reader.
    - Include a cover page and table of contents.
    - Incorporate visual elements and labels appropriately.
    - Be presented in a way that is easily comprehensible and visually appealing.

Evidence and Judgement Statements

Learning Outcomes	LO1. Plan and design network solutions to meet organizational requirements using principles of information design and automated system procedures. LO3. Apply professional and ethical practices in the analysis of IT security solutions to protect and secure assets.
Documentation	The student has provided all the required documentation. Note: All the documentation must be submitted with suitable screenshots. Steps must be explained properly where necessary andcomments should be provided if any selection must be made from a given batch of options.

Task	Task Description	Evidence Criteria	Judgement
1.1	Develop a plan for deploying the proposed secure network solution using an automated deployment process. • The plan must have a start date, end date, responsibilities, tasks and subtasks, milestones, risks, and post-deployment support. • The timeline for the project is 6 weeks. • The plan should be presented using any project management tool.	• The student provides a plan that consists of start date, end date, responsibilities, tasks, subtasks, milestones, risks and deployment support. • The timeline for the project is within 6 weeks. • The plan must be presented using a project management tool.	• The student has provided a proposed plan using an automated deployment process including the requirements listed for 6 weeks' timeline. • The student has provided the plan using a project management tool.
1.2	Conduct an analysis of the current network infrastructure to identify issues and determine the hardware and software requirements necessary to address these issues effectively. The analysis should be based on both business and technical requirements. 1. **Analyse the Current Network Infrastructure:** • Review the current network setup to identify issues and areas for improvement. 2. **Define Requirements:** • Based on business and technical requirements, identify and list the hardware and software needed to address the identified issues.	• The student reviews the current network infrastructure to identify issues and areas for improvement. • The student defines and lists the hardware and software requirements necessary to address the identified issues based on business and technical requirements. • The student provides explanations and justifications for each hardware and software component to ensure they effectively meet the business and technical requirements.	• The student has reviewed the current network infrastructure to identify issues and areas for improvement, defined and listed the necessary hardware and software requirements based on business and technical needs, and provided explanations and justifications for each component.

Task	Task Description	Evidence Criteria	Judgement
	3. Justify Requirements: • Provide explanations and justifications for each component to fulfil the business and technical requirements effectively.		
1.3	Calculate the new network range and subnet mask for each department by /24 subnet structure. • The calculation should include the Network ID, Broadcast ID and IP range. • Create a subnet according to the requirements given in the task description.	• The student provides each step to calculate the IP range, Subnet mask, Network ID, Broadcast ID calculation using /24 for each department as per the task instructions. • The student correctly calculated the number of maximum and usable hosts for each department.	• The student has calculated the correct IP range, Subnet mask, Network ID, Broadcast ID using standard /24 subnet structure for each department as per the task instructions. • The student correctly calculated the number of maximum and usable hosts for each department.
2.1	Select the appropriate hardware and software components to address the identified network issues identified in Task 1.2 and meet the defined requirements for TechCo Solutions. Each component must include its specification, cost, quantity, and justification. The budget for this task is between NZD 15,000 and NZD 23,000. 1. **Select Hardware Components**: • Provide detailed specifications, costs, and quantities for each hardware component. • Justify the choice of each hardware component based on how it addresses the network issues and meets the requirements. 2. **Select Software Solutions**: • Provide detailed specifications, costs, and quantities for each software component. Justify the choice of each software solution based on how it addresses the network issues and meets the requirements.	• The student provides a list of appropriate hardware and software components used at enterprise level. • The student provides detailed specifications, costs, and quantities for each hardware and software components. • The student justifies the choice of each hardware and software components based on how it addresses the network issues and meets the requirements. • The student ensures that the total cost of selected hardware and software components falls within the budget range of NZD 15,000 to NZD 23,000.	• The student has provided the appropriate hardware and software components to implement the proposed plan with its specification and cost.

Task	Task Description	Evidence Criteria	Judgement
2.2	Develop a detailed network infrastructure diagram that illustrates the proposed secure network solution for TechCo Solutions utilizing the subnetting information from Task 1.3. 1. **Design the Network Diagram**: • **Components**: Include all selected hardware and software in the diagram. • **Connections**: Show how each component connects to the network. • **Subnetting:** Integrate the subnetting scheme derived in Task 1.3, showing how IP addresses are allocated across different network segments. 2. **Label Components**: • **Clear Labels**: Label each component according to industry practice. • **Security Measures**: Show where security measures are implemented in the network. 3. **Document the Diagram**: • **Presentation**: Ensure that the diagram is clear, well-organized, and visually appealing. Use appropriate software tools to create the diagram.	• The student develops a detailed network infrastructure diagram illustrating the proposed secure network solution for TechCo Solutions utilizing the subnetting information from Task 1.3. • The student includes all selected hardware and software in the diagram. • The student shows how each component connects to the network. • The student integrates the subnetting scheme derived in Task 1.3, displaying the allocation of IP addresses across different network segments. • The student labels each component clearly according to industry practice. • The student shows where security measures are implemented in the network. • The student ensures that the diagram is clear, well-organized, and visually appealing, using appropriate software tools to create the diagram.	• The student developed a comprehensive network infrastructure diagram for TechCo Solutions, incorporating all hardware and software components, connections, IP address allocations from Task 1.3, and security measures, with clear and industry-standard labelling.

Task	Task Description	Evidence Criteria	Judgement
3.1	Identify potential vulnerabilities and security threats and propose suitable security mechanisms using a defense-in-depth approach. 1. **Identify Vulnerabilities and Threats:** • Review the update network structure in Task 2.2 to identify at least three potential vulnerabilities or security threats. • Clearly describe each identified issue and its potential impact on the network. 2. **Propose Security Mechanisms:** • For each identified threat or vulnerability, propose a specific security mechanism. • Explain how the mechanism addresses the issue and integrates with the overall network solution. • Detail how the mechanism enhances network security and supports the defense-in-depth strategy. • List out the hardware or software to use in the current network infrastructure with specification and costs and justification for the product. **3. List Hardware and Software for Proposed Security Mechanisms:** • Specify the hardware or software required for the proposed security mechanisms. • Provide detailed specifications and costs for each listed item. • Explain why each hardware or software component was chosen to enhance overall security.	• The student provides at least three comprehensive lists of potential vulnerabilities. • The student clearly explains the vulnerabilities with potential impact on the network. • The student proposes and provides justification for the chosen security mechanisms, illustrating how they integrate with the overall network solution. • The student provides an explanation on how the security mechanism enhances network security and supports the defense in depth strategy. • The student specifies the hardware or software required for the proposed security mechanisms. • The student provides detailed specifications and costs for each listed item. • The student explains why each hardware or software component is chosen to enhance overall security.	• The student has provided at least three suitable potential vulnerabilities and proposed the appropriate options to secure the organization's network environment within premises. • The student has discussed how proposed security measures integrate with the overall network solution and illustrated how each solution enhances network security according to the organization's requirements. • The student specified the hardware or software required for the proposed security mechanisms with specification and cost for each item. • The solutions provided are appropriate and in accordance with the industry practices.

Task	Task Description	Evidence Criteria	Judgement
3.2	Implement the proposed security mechanisms from Task 3.1 into the network diagram to enhance the overall network security for TechCo Solutions. 1. **Update the Network Diagram:** • **Security Mechanisms:** Integrate the security mechanisms proposed in Task 3.1 into the network diagram, clearly showing their placement and configuration. • **Components and Connections:** Ensure that all components and connections reflect the enhanced security measures. 2. **Label Security Enhancements:** • **Clear Labels:** Label each security mechanism in the diagram according to industry practice. 3. **Document the Updated Diagram:** • **Presentation:** Ensure that the updated diagram is clear, well-organized, and visually appealing. Use appropriate software tools to create the diagram.	• The student integrates the security mechanisms proposed in Task 3.1 into the network diagram, clearly showing their placement and configuration. • The student ensures that the updated diagram is clear, well-organized, and visually appealing. • The student uses appropriate software tools to create the diagram.	• The student has created a network-level access solution with at least three security mechanisms from task 3.1 using a network diagram. • The diagram is labelled and elaborated.
4.1	• Create a PowerShell script to install and configure printer management features on the designated server. • Select appropriate cmdlets and modules to create and configure Group Policy Objects (GPOs). • Customize the scripts to target specific Organizational Units (OUs) such as "Staff", "Management", or "Account", and link corresponding GPOs for efficient deployment of printer. • Utilize the Graphic User Interface (GUI) to dynamically assign printers to specific OUs. • Conduct thorough testing of the PowerShell scripts in a controlled environment to ensure correct printer assignment to OUs and successful printer sharing via GPOs.	• The student installs and configures Printer management using the PowerShell Command. • The student creates GPOs according to the requirements using PowerShell Script. • The student submits well-documented PowerShell scripts for printer management. • The student has tested the scripts in a controlled environment. • The student supplies screenshots validating the successful installation of the printer server, along with the addition of printers and the subsequent sharing of printers with users.	• The student has installed and configured printer management features using the PowerShell command and deployed it using GPOs according to the requirements given. • The student submits well-documented PowerShell scripts for printer management, providing clear explanations of the commands used and their functions. • The student conducts thorough testing of the PowerShell script, accompanied by screenshots to verify the installation and configuration of printers, as well as the sharing of printers via Group Policy Objects (GPOs).

Task	Task Description	Evidence Criteria	Judgement

4.2	Next, you are tasked to automate the backup management process in a Windows Server environment, ensuring regular backups of critical data and system configurations. An automated procedure intends to streamline the backup process, scheduled and configured to meet the organizational requirements effectively. The assigned tasks are as follows:
	• Research and select appropriate PowerShell cmdlets/modules for managing Windows backup.
	• Create a PowerShell script to configure and schedule Windows backups with the following specifications:
	  ○ Customizing the script to target specific directories, such as the entire C drive for backup.
	  ○ Adapt the script to schedule backups after office hours.
	  ○ Specify the network path for storing backup files.
	• Test the PowerShell scripts and GUI in a controlled environment to ensure the correct configuration of backup settings.
	• Validate that the scheduled backups occur after office hours, are stored on the specified network path and include the entire C drive.
		• The student documents the findings and selects appropriate PowerShell cmdlets/modules for managing Windows backup.
		• The student installs and configures Server backup using PowerShell commands.
		• The student submits well-documented PowerShell scripts for Server backup.
		• The student tests the PowerShell Scripts in a controlled environment.
		• The student supplies screenshots validating the successful configuration of the backup.
			• The student demonstrates proficiency in researching and identifying relevant PowerShell cmdlets/modules for Windows backup management.
			• The student develops PowerShell scripts to configure and schedule Windows backups effectively.
			• The student develops the PowerShell Script to target specific directories, such as the entire C drive for backup.
			• The student develops the PowerShell Script to schedule daily backups after office hours.
			• The student conducts thorough testing of the PowerShell scripts and GUI in a controlled environment to ensure the correct configuration of backup settings.

5.1	Discuss three professional and ethical practices that the IT administrator and the team should adopt to ensure data privacy and protect user information. Provide an example related to the case scenario and discuss how each practice addresses the concern. Additionally, propose strategies to effectively manage legal considerations and adhere to NZ data protection regulations to ensure that overall ethical practices are established for the network solution.	• The student discusses three professional and ethical practices that the team should adopt to ensure data privacy and protect user information. • The student provides appropriate examples of practices related to the case and discussed how to apply the practices to address the concern. • The student proposes at least 2 strategies to manage legal considerations for the organization and ensure the overall ethical practices are established for the network solutions. • The student assesses the incorporation of ethical considerations in the proposed	• The student has provided 3 professional and ethical practices to ensure data privacy and protect user information with examples for each. • The example provided must relate to the case and be discussed in detail. • The student has provided the strategies to manage the legal considerations and ensure that overall ethical practices are established for the network solution.

Task	Task Description	Evidence Criteria	Judgement
		strategies for the network solution. • The student evaluates the effectiveness of strategies in managing legal and compliance risks related to data protection.	
6.1	Assemble and submit your documentation. • Each item must be clearly labelled with the appropriate task number. • Ensure that you include the assessment instrument, with all verification signed by your tutor. • Submitted content/documentation must: ○ Maintain consistent formatting throughout the document. ○ Be well-structured and organized with clear headings and subheadings to guide the reader. ○ Include a cover page and table of contents. ○ Incorporate visual elements and labels appropriately. ○ Be presented in a way that is easily comprehensible and visually appealing.	• The student provides organized documentation with clear labelling and task number. • The student provides all required documentation according to the assessment instruction.	• The student has provided all required documentation. • The content of the report is presented using information design principle.