

Computer System Fundamentals

by Adam Ibrahim

Submission date: 09-Jan-2026 12:12PM (UTC+0000)

Submission ID: 272662790

File name: 57247_Adam_Ibrahim_Computer_System_Fundamentals_712285_1768577994.docx (1.85M)

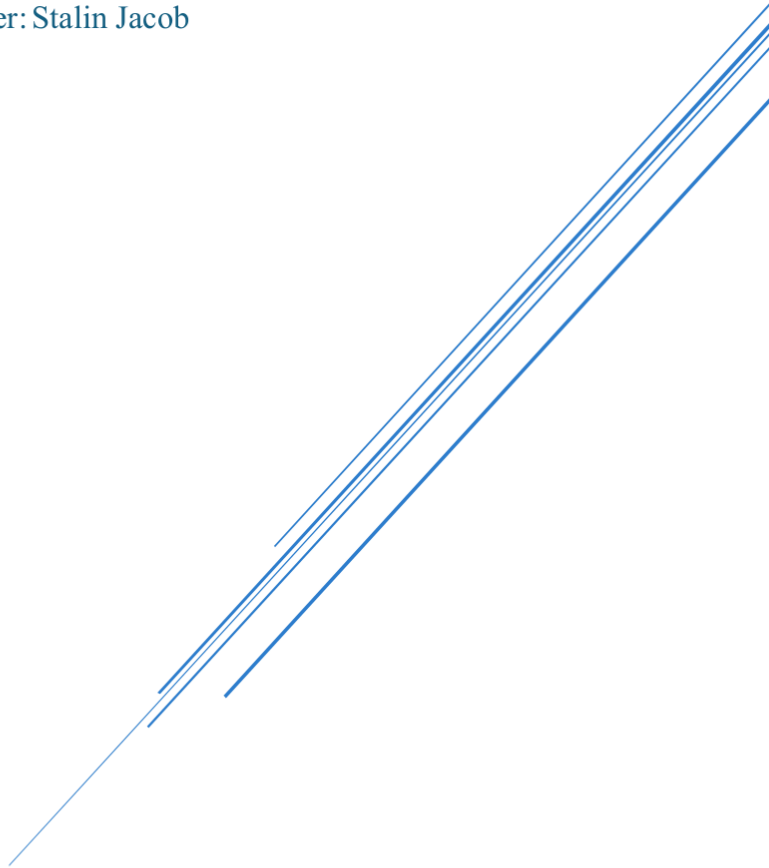
Word count: 2785

Character count: 16592

Computer Systems Fundamentals

Cyber Risk and Computer System Design

Lecturer: Stalin Jacob



Submit Date
09/01/2026



Prifysgol Cymru

Y Drindod Dewi Sant

University of Wales

Trinity Saint David

**Programme: B.Eng. (Hons) Electrical and Electronic
Engineering**

Module: Computer Systems Fundamentals

Module code: ACCA4028

Student name: Adam Ibrahim

Student ID Number: 2406034

Table of contents

Table of contents	2
Task 1	3
Introduction.....	3
Custom Desktop Computer Specification.....	3
Component Justification and Alternatives	4
CPU and Motherboard	4
RAM	4
Graphics Card (GPU).....	4
Storage	5
Power, Cooling, and Accessories	5
Connectivity ports and System Options.....	5
Operating System and Software.....	5
Peripherals.....	5
Shopping List and Total Cost.....	6
Task2	8
Introduction.....	8
Risk Identification and Impacts	8
Table of Prioritization Cybersecurity Risks	9
Embedded Devices with Default Passwords and Old Firmware	9
Insecure International Suppliers	9
Outdated Operating Systems on Engineering Workstations	10
Lack of Cybersecurity Training	10
Risk Prioritisation	10
Holistic Cybersecurity Strategy	10
Incident Response Plan	11
Cybersecurity Standards and Alignment.....	11
Conclusion	12
References.....	13

Task 1

Introduction

This report explains the design of a custom desktop computer that meets the needs of an Electrical Engineer working from home. The engineer needs to operate complex engineering software which includes SolidWorks Electrical, PSpice and LabVIEW while performing standard work duties that include creating reports and presentations and managing budgets and participating in video calls. The system needs to operate at high speed while providing dependable performance and complete security protection and simultaneous program execution without performance degradation. The components listed below were carefully chosen to match these requirements, and each one is justified in detail [1] [2].

Custom Desktop Computer Specification

The computer system provides users with both excellent operational speed and extended system durability. The PCS Spectrum II Compact ARGB Mid Tower Case supports mATX boards through its design which maintains airflow while allowing users to adjust the RGB lighting effects. The system operates with an Intel Core Ultra 7 265KF processor which contains 20 processing cores to handle complex academic tasks and multiple tasks at once at 5.5GHz speed. The ASUS PRIME B860M-K motherboard enables users to install DDR5 memory, and it features PCIe 5.0 for high-speed data transfer operations. It includes 32GB Corsair Vengeance DDR5 5200MHz RAM. The ASUS TUF GeForce RTX 5070 Ti OC 16GB runs all high-resolution and graphics-intensive tasks without any issues. The system components work together to provide users with a seamless gaming experience and stylish design and effective study capabilities.

Component	Specification
Case	PCS SPECTRUM II COMPACT ARGB MID TOWER CASE (PWM) mATX
Promotional Item	Pick 1 of 4 games (e.g., Battlefield 6) with qualifying Intel® products
Processor (CPU)	Intel® Core™ Ultra 7 265KF (20-Core, up to 5.5GHz, 30MB Cache)
Motherboard	ASUS® PRIME B860M-K (mATX, LGA1851, DDR5, M.2 PCIe 5.0)
Memory (RAM)	32GB Corsair VENGEANCE DDR5 5200MHz CL40 (2 x 16GB)
Graphics Card	16GB ASUS TUF GEFORCE RTX 5070 Ti OC (2 x HDMI, 3 x DP)
1st M.2 SSD Drive	1TB CORSAIR ELITE MP600 NVMe PCIe M.2 SSD (7000 MB/s Read, 6200 MB/s Write)
DVD/BLU-RAY Drive	Not Required
Power Supply	CORSAIR 1500W HXi SERIES ATX 3.1 & 5.1 PCIe Modular 80 PLUS® Platinum
Power Cable	1 x 1.5 Metre IEC C19 USA Power Cable
Processor Cooling	PCS Frost Flow 240 Series ARGB High Performance Liquid Cooler
Thermal Paste	Standard Thermal Paste
Sound Card	Onboard 6 Channel (5.1) High-Definition Audio
Network Card	Onboard 2.5Gbe LAN Port
Wireless Network Card	None or Onboard Wi-Fi (Motherboard Dependent)
USB/Thunderbolt	Min. 2 x USB 3.0 & 2 x USB 2.0 (Back) + Min. 2 Front Ports

Operating System	Windows 11 Home 64 Bit
OS Language	United Kingdom - English
Recovery Media	Windows 10/11 Multi-Language Recovery Image
Office Software	Microsoft, Anti-virus
Anti-Virus	Norton 360 inc. Game Optimizer
Browser	Microsoft® Edge
Monitor	IYYAMA XUB2792QSU-B6 27" WQHD, DVI, HDMI, DP, 2560x1440, 100Hz
Monitor Cable	2m DisplayPort Adapter Cable - DP to DVI
Keyboard & Mouse	PCS specialist GS-813 RGB Gaming Keyboard & Mouse Bundle
Headset	CORSAIR VOID WIRELESS V2 Gaming Headset - Carbon
Webcam	Elgato Face Cam Neo - 1080p60 Full HD

Component Justification and Alternatives

CPU and Motherboard

The Intel Core Ultra 7 265KF and ASUS PRIME B860M-K were selected because they provide top-notch performance together with dependable operation and advanced features which will maintain their value in the future. The Ultra 7 265KF processor contains 20 cores which enable it to deliver better performance than Intel Core i7 models from previous generations and most AMD Ryzen 7 processors during gaming and multitasking and when running complex applications. The system operates current software at high speeds without any performance degradation. The ASUS PRIME B860M-K supports DDR5 memory and PCIe 5.0 technology which delivers faster data transfer rates and better hardware compatibility for future devices than previous motherboard specifications.

RAM

The 32GB Corsair VENGEANCE DDR5 5200MHz CL40 RAM received selection because it delivers excellent performance together with dependable operation at a reasonable cost. The system operates at a higher level of performance because it contains 32GB of memory which enables it to run modern games and handle intense multitasking and resource-intensive applications. The 5200MHz DDR5 speed provides reliable performance for basic computer tasks because it runs at a speed below the highest DDR5 speed.

Graphics Card (GPU)

The 16GB ASUS TUF GeForce RTX 5070 Ti OC received selection because it provides premium performance at a reasonable price point relative to other available graphics cards. The new model provides superior performance to the RTX 3060 Ti because it generates superior results through its ability to produce higher frame rates and maintain steady performance at 1440p ultra settings in modern games, but its high price makes the 5070 Ti a more suitable option for users who need top-notch performance at affordable rates. The ASUS TUF OC variant provides users with improved cooling performance and pre-overclocked settings which help maintain stable performance under heavy system usage.

Storage

The storage configuration follows a design which combines high operational speed with reliable system operation. The system features a 1TB Corsair Elite MP600 NVMe PCIe M.2 SSD which provides read performance at 7000 MB/s and write performance at 6200 MB/s. The system achieves fast boot times and immediate file and program access because of its high-speed performance.

Power, Cooling, and Accessories

The power supply system maintains system stability through its cooling components and additional accessories which also help to extend the system's operational lifespan. The Corsair 1500W HXi Platinum PSU provides additional power capacity which exceeds standard system needs while delivering clean efficient power to support high-performance CPU and GPU operations and future system growth. The system operates at its highest point which reduces stress when it needs to handle heavy loads. The PCS Frost Flow 240 ARGB liquid cooler maintains CPU temperatures at safe levels during intense operations which results in better long-term system performance.

Connectivity ports and System Options

The port and system option selection process focused on improving operational efficiency while building systems which would operate continuously for long durations. The front and rear of the device provide multiple USB 3.0 and USB 2.0 ports which enable users to connect their peripherals, and storage drives and accessories through direct connections without needing adapters. The system enables users to access Wi-Fi for network connection, which provides alternative networking options when traditional cables fail to work. Integrated 5.1-channel high-definition audio improves sound quality for media and meetings.

Operating System and Software

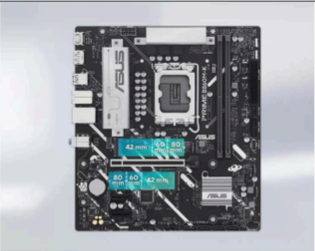
Windows 11 Home operating system was based on its ability to deliver a contemporary platform which maintains stability and security for academic tasks and gaming activities and general computing needs. The system contains built-in security features which perform scheduled software updates to protect the system from potential security threats. Users can perform their document and presentation creation tasks with dependable professional work efficiency through the use of authorized office software programs.

Peripherals

5 The peripherals were chosen to improve comfort, communication, and usability. The gaming keyboard and mouse provide users with quick control responses, and the Corsair wireless headset produces outstanding audio quality which works well.

Shopping List and Total Cost

6

Component	Specification	Estimated Price (£)	Image
Case	PCS Spectrum II Compact ARGB mATX	£75	
CPU	Intel Core Ultra 7 265KF	£420	
Motherboard	ASUS PRIME B860M-K	£160	
RAM	32GB Corsair Vengeance DDR5 5200MHz	£95	
Graphics Card	ASUS TUF RTX 5070 Ti 16GB	£850	
SSD	1TB Corsair MP600 NVMe	£90	Crucial P510 1TB PCIe Gen5 NVMe M.2 SSD 

Power Supply	Corsair 1500W HXi Platinum	£420	
CPU Cooler	PCS Frost Flow 240mm AIO	£85	
Operating System	Windows 11 Home 64-bit	£100	
Monitor	iiyama 27" 1440p 100Hz	£210	
Keyboard & Mouse	PCS RGB Bundle	£29	
Headset	Corsair VOID Wireless V2	£110	

Webcam	Elgato Face Cam Neo	£159.99		
Total price	£2803.99			

Task2

Cybersecurity Risks and Their Impacts

Introduction

The evaluation process of this task assesses manufacturing company cybersecurity threats while showing an effective method to decrease their security vulnerabilities. The organization operates through connected IT systems which perform business functions and OT systems which run production operations thus making it more vulnerable to threats including phishing attacks and malware incidents and insecure embedded devices and outdated workstations and supply chain vulnerabilities. The potential risks will result in system failures which cause business interruptions and data destruction and financial losses and endanger human safety.

Risk Identification and Impacts

The manufacturing company functions as an essential which maintains critical infrastructure systems. The three security elements of confidentiality and integrity and availability need equal attention because they protect designs and intellectual property and prevent unauthorized changes to firmware/configurations and maintain production operations. The audit identified three main risks which will affect operational performance and preserve data accuracy. The system faces two major security risks because its firewall rules have not been updated and the network lacks proper segmentation. The system becomes vulnerable to unauthorized access which allows attackers to move between IT and OT networks which increases the danger of ransomware attacks and production system failures.

Table of Prioritization Cybersecurity Risks

Priority Level	Cybersecurity Risk	Reason for Priority
1 (Highest)	Outdated firewall rules and lack of network segmentation	This allows attackers to move freely between corporate and operational systems, which could quickly disrupt production and compromise sensitive designs.
2	Embedded devices with default passwords and outdated firmware	These devices are easy targets and control critical equipment. Exploiting them can lead to operational failure or manipulation of machinery.
3	Outdated operating systems on engineering workstations	Unpatched systems are highly vulnerable and can expose valuable intellectual property and engineering files to malware or attackers.
4	Insecure international suppliers	Supply chain risks have high impact but usually develop more slowly. Weak supplier practices can introduce hidden vulnerabilities in components.
5 (Lowest)	Lack of staff cybersecurity training	Although quite common and it can be addressed quickly through training programmes.

Embedded Devices with Default Passwords and Old Firmware

Another major issue lies in the embedded devices used in the company's production environment. Most devices continue to operate with their original factory passwords while running outdated versions of their operating system. The system vulnerabilities allow attackers to quickly access equipment while they can change system settings which causes disruptions to operational activities. The security of embedded devices becomes vulnerable to attacks which could enable attackers to use these devices as entry points to access more sensitive areas of the organization. Given their importance in controlling machinery and processes, this risk also carries a high impact and likelihood.

Insecure International Suppliers

The company depends on international suppliers who provide components, but these suppliers lack secure development methods and proper quality control systems. The organization faces supply chain threats because tampered components and firmware with hidden backdoors exist in its system.

Outdated Operating Systems on Engineering Workstations

Multiple engineering computers continue to operate with outdated operating systems which have lost their security update support. The systems remain exposed to malware and software exploits which attackers can discover through public sources. The risk faces a high probability of exploitation, yet it would result in less severe consequences than a full network breach.

Lack of Cybersecurity Training

The absence of staff cybersecurity training has already resulted in phishing incidents. The lack of fundamental security awareness among staff members creates an environment where cyber attackers can successfully target them because employees will either believe fake emails or download harmful files or expose their account passwords. System attacks which result from human errors create average system disruptions, yet organizations need to focus on employee training because such incidents occur regularly [3].

Risk Prioritisation

The main security threat emerges from networks that lack proper segmentation and use outdated firewall configurations because these weaknesses allow attackers to access both business and industrial networks. The following devices need immediate attention because they use their default passwords and their firmware versions are no longer supported. The development process faces a major risk because its fundamental engineering workstations run with outdated systems which introduce security weaknesses. Supply chain issues rank below these because they develop over longer periods, while the lack of employee training, although common, can be quickly improved with proper programmes [4].

Holistic Cybersecurity Strategy

A manufacturing company needs to establish a full cybersecurity strategy which will defend its systems through various security layers that protect both IT and OT infrastructure. The organization needs to establish separate networks for IT and OT systems through network segmentation and firewall restrictions and DMZ implementation to prevent malware from spreading and protect production systems from attackers. Remote access security depends on VPN technology together with multi-factor authentication systems and permission settings which allow suppliers to access only what they need. The organization needs to implement patch management for all workstations and servers and embedded devices while using alternative security measures to protect its legacy systems through isolation and application allow-listing and restricted internet access. The system needs to detect abnormal system operations through its combination of endpoint protection (antivirus/EDR) and central logging and continuous monitoring capabilities. The protection of IoT devices needs organizations to maintain complete inventory records and perform software updates and password resets and disable non-active services. Organizations need two security measures which include scheduled staff training sessions and email filtering systems to defend themselves against phishing attacks. The system requires secure backup systems which need to have tested recovery plans to achieve quick system restoration and maintain business operations [3].

Incident Response Plan

The incident response plan table



Phase	Key Actions	Owner/Team
Preparation	Define IR team roles; maintain offline backups; log collection; run tabletop exercises.	IT Security + OT Leads
Detection & Analysis	Monitor alerts; confirm incident; triage affected systems	SOC / IT Security
Containment	Isolate affected segments; block indicators; disable compromised accounts.	IT + Network Team
Eradication	Remove malware; patch vulnerabilities; reset credentials; validate configurations.	IT Security + OT
Recovery	Restore from backups; verify system integrity; resume production safely.	IT + Operations
Lessons Learned	Post-incident review; update policies; improve controls; report to leadership.	CISO / Management

Cybersecurity Standards and Alignment

The proposed strategy uses multiple industry-recognized cybersecurity standards which it will implement. Organisations can use the NIST Cybersecurity Framework to develop their security system through threat identification and protection and detection and response and recovery processes. The standards of ISO/IEC 27001 enable organizations to follow established best practices for access control systems and incident response and data management procedures. The company needs to implement these standards for security practices because they will create an enhanced method to handle cyber risks which receives official recognition [3].

Conclusion

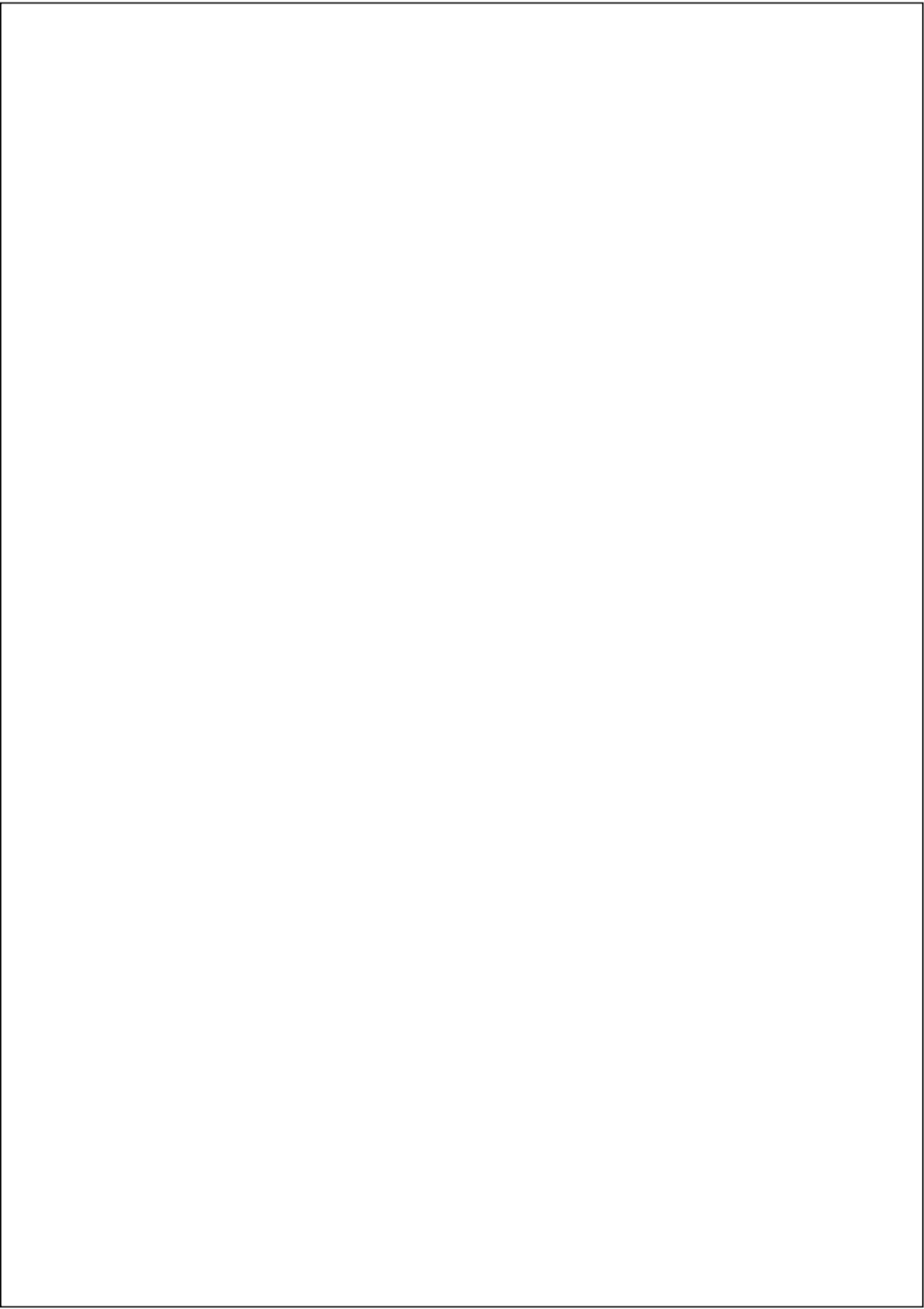
The system design fulfils all requirements for building a fast and dependable desktop computer. The CPU and motherboard and DDR5 RAM are provides quick performance for executing various tasks and demanding applications and the graphics card supports high-definition video output and complex graphic processing. The system provides flexible operation through its multiple USB ports and 2.5Gb Ethernet connection and built-in Wi-Fi functionality. The high-quality power supply and liquid cooling improve stability by delivering clean power and keeping temperatures low during long sessions. The system provides users with a smooth operating experience and allows them to upgrade their components and maintain its value throughout time which makes it an excellen



station solution.

References

- [1] W. Stallings, in *Computer Organization and Architecture*, Pearson Education Ltd , 2022, pp. 24-70.
- [2] M. M. Mano, in *Computer system Architecture* , Pearson Education , Digital Logic Circuit , pp. 1-171.
- [3] G. Johansen, "Incident response tools and techniques for effective cyber threat response," in *Digital Forensics and Incident Response : Incident Response*, Birmingham, Published by Packt Publishing Ltd, 2022, pp. 1-100.
- [4] D. a. M. G. S. Kim, in *Fundamentals of Information Systems Security* , World Headquarters Jones & Bartlett Learning, 2018, pp. 22-97.
- [5] U. M. Jiehui (Annabella) Huang, "The impact of cybersecurity risk management strategy disclosure on investors' judgments and decisions," (*J. (Annabella) Huang*), no. 1467-0895, pp. 1-17, 2024.
- [6] K. Sandhu, in *Handbook of Research on Advancing Cybersecurity for Digital Transformation*, University of New England, Australia, Published in the United States of America by IGI Global, 2021, pp. 1-61.



Computer System Fundamentals

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

74/100

PAGE 1

PAGE 2

PAGE 3



Comment 1

Good work

PAGE 4



Comment 2

It is better to number each heading



Comment 3

caption
should be added for the table, so the reader will get an idea about the table



Comment 4

It is better to include page numbers

PAGE 5

PAGE 6



Comment 5

The
font, font size, line spacing, spacing between paragraphs, spacing between
heading and paragraph should be uniform throughout the document.

PAGE 7



Comment 6

A caption should be added to the table, including a table number, and the table should be referred to in the text. This will help the reader understand the context and purpose of the table.

PAGE 8

PAGE 9

PAGE 10



Comment 7

A caption should be added to the table, including a table number, and the table should be referred to in the text. This will help the reader understand the context and purpose of the table.

PAGE 11

PAGE 12



Comment 8

A caption should be added to the table, including a table number, and the table should be referred to in the text. This will help the reader understand the context and purpose of the table.

PAGE 13



Comment 9

It would have been better if the conclusion about task 2 is also included

PAGE 14

PAGE 15

GRADING FORM: CSF RUBRICS

ADAM IBRAHIM

73.50

ENGAGEMENT WITH LITERATURE

The report should be supported by credible sources on cybersecurity and computer systems design in engineering. These may include academic journals, textbooks, official guidelines, and peer-reviewed or recognised online publications. Use of recent materials (from the past five years) on cybersecurity and hardware is encouraged. Proper referencing, with in-text citations and a reference list, is essential.



Engagement with a wide range of literature, including sources retrieved independently and with strong selection of sources. Include more peer-reviewed or technical publications to enhance depth. Some technical claims are not directly supported by in-text citations. Citations and referencing require improvement

6.8

KNOWLEDGE AND UNDERSTANDING

The report should demonstrate knowledge of key cybersecurity principles and hardware specifications relevant to the scenario. Understanding should be shown through explanations of how these principles apply to real-world situations, supporting a balanced approach to risk mitigation that protects data integrity, confidentiality, and availability.



Excellent knowledge and understanding of the basic underlying concepts and principles of computer systems is evident through the description. Demonstrates a solid understanding of hardware compatibility, application requirements, and security risks. Good explanation of cybersecurity concepts, including CIA triad, segmentation, firewalls, and incident response. The analysis would be even stronger with reference to cybersecurity frameworks and more detailed explanations for hardware choices.

23

COGNITIVE AND INTELLECTUAL

The report must evaluate cybersecurity risks and hardware specifications relevant to the scenario, comparing alternatives and assessing cost-effectiveness. Logical reasoning and clear justification should support each decision, demonstrating a holistic and proportionate response to security risks.



Excellent evaluation of the underlying concepts and principles of computer systems. The report demonstrates logical reasoning in prioritising cybersecurity threats through the use of a matrix, and risk assessments are well-structured. Limited comparison with alternative components or architectures. Cybersecurity analysis could benefit from clearer risk likelihood vs impact reasoning. The report clearly demonstrates the adoption of a holistic and proportionate approach to mitigating security risks by addressing technical, organisational, and human factors, aligned with the severity and likelihood of each risk.

21.6

PRACTICAL SKILLS

Practical application of theoretical knowledge is expected, with clear demonstrations of how hardware choices are suited to the given scenarios. Solutions should be realistic, feasible, and contextually appropriate, showing a direct link between theory and practical implementation.



A very good application of a range of taught, basic methods, materials, tools, and techniques is demonstrated. The context of the application is well considered and insightful. Practical skills are evident through the selection of components for the computer. The response would benefit from a good explanation of component compatibility. PSU and GPU selection could include efficiency or workload justification. The design would also be improved by considering potential future upgrades or system scalability, which is important for long term usability.

15

TRANSFERABLE SKILLS FOR LIFE

The report should demonstrate professional communication and high-quality presentation, with well-organised sections, diagrams, and tables to convey technical content, as well as clarity and fluency in technical writing.



The report exhibits a high level of structure and coherence. The presentation is clear, contributing to a very good overall quality. It demonstrates strong transferable skills for both life and professional practice. Proofreading is recommended to further improve the quality of the document and to address inconsistent formatting (line spacing, headings, and tables). Additionally, some grammatical repetition and long sentences reduce clarity, and tables lack captions and are not always referenced in the text.

7.1