

**COMP40001 Cloud & Cyber (APIIT-campus)**

**Group assignment**

**Notes on Plagiarism**

1. You are expected to explain the concepts in your own words or rephrase and avoid quotes as quotes will increase Turnitin matches. You are referred to the University’s regulations on plagiarism available at <http://www.staffs.ac.uk/assets/academic_misconduct_tcm44-26770.pdf>
2. If the Turnitin system detects plagiarism, it will be reported to the school and appropriate actions will be taken.

**Submission requirements**

1. The deadline is published on the Blackboard.
2. Your report - Your report can be of up to 2000 words with an overall flexibility of +10%. However, this is the absolute word count limit and any further words will be ignored i.e., NOT marked. To improve the document readability and to reduce the number of words, you can use graphs, diagrams etc.

**Word count will include the following items.**

1. All titles or headings that form part of the actual text.
2. All words that form the essay (the main body of text).
3. All words forming the titles/captions for figures, tables and boxes
4. All in-text (that is bracketed) citations
5. All directly quoted material

**Additional Guidelines:**

1. The report should be structured professionally e.g., a title page containing the title of the coursework, student name, student ID etc., table of contents (ToC), defined sections or headings/sub-headings corresponding to the marking criteria items, diagrams, citations and references, page numbers etc.
2. Text font size, image or diagrams must be readable. Margins must be sufficiently wide to allow the work to be read easily. Your report must have valid citations and references i.e., for each reference, at least 1 citation MUST exist in the body of the report. The university requirement is Harvard style. You are recommended to use a referencing tool e.g., Mendeley, Zotero etc. At least 10 references are considered as sufficient.
3. Report submission through the Turnitin system ONLY. Turnitin system will NOT accept submission after the deadline. It is strongly recommended that you attempt to submit bit early to avoid any technical difficulty or missing the deadline.
4. Paper submission or handwritten report / element will be ignored i.e. NOT marked. Any text, code etc. inserted as image will be ignored i.e. NOT marked.
5. You will be allowed to upload ONLY once to the Turnitin system. Therefore, please make sure that your coursework is free of plagiarism, and you are uploading the correct version.
6. An editable source file e.g., Microsoft docx MUST be submitted. Non-editable source file e.g., PDF is NOT allowed. Do NOT attempt to submit other file formats e.g., zip as these file formats might NOT be recognised by the Turnitin system.
7. If you have a Learning Support Statement (LSS) or Learning Support Agreement (LSA), it MUST be discussed with the module leader and any extension MUST be pre-approved by the module leader.

### **Assignment Description**

In an increasingly digital world, organizations are migrating their IT infrastructures to the cloud to leverage scalability, flexibility, and cost efficiency. However, this shift brings significant challenges in terms of cybersecurity, compliance, data protection, and incident readiness.

This assignment simulates a real-world consultancy scenario. Your team will act as cybersecurity consultants tasked with designing a secure, resilient, and compliant **cloud-based infrastructure** for a healthcare organization. You are expected to combine theoretical knowledge with hands-on implementation using **freely available tools** (such as AWS Free Tier, VirtualBox, OpenSSL, Autopsy, etc.).

The assignment is designed to meet all **four learning outcomes** of the module, with a particular emphasis on security design, implementation, incident response, and cyber forensics.

### **Task**

Working in groups, you are required to,

1. **Analyse the given business scenario** (a healthcare provider planning to move to the cloud) and **identify key security risks**, data protection needs, and operational priorities.
2. **Design a secure cloud-based architecture**, justifying your choices with respect to cloud models, services, and cybersecurity frameworks (e.g., ISO27001, NIST).
3. **Implement selected security features** using **free/open-source tools** and demonstrate their effectiveness.
4. **Incorporate digital forensic strategies** and propose an **incident response plan**.
5. Document your work in a professionally written **case study report** and submit supporting **evidence of implementation** (screenshots, config files, outputs, etc.).

### **Expected Deliverables**

Your group submission must include the following,

#### 1. Report Document (2000 words)

* Executive Summary
* Threat Landscape and Requirements Analysis
* Cloud Architecture Design
* Security Framework & Access Control
* Incident Response Plan
* Digital Forensics Approach
* Evidence and Discussion of Implementation
* Conclusion and Recommendations
* Harvard-style References

#### 2. Practical Implementation (Choose at least 4 from below)

Each with screenshots and brief configuration explanations.

* Deploy a VM using AWS Free Tier or VirtualBox
* Set up access controls (IAM / ACL / MFA)
* Configure network security (UFW, AWS Security Groups, firewalls)
* Encrypt a sample file (OpenSSL, GPG)
* Simulate system logging and monitoring (e.g., OSSEC, Splunk)
* Automate data backup and test recovery
* Perform a basic forensic investigation using Autopsy or log analysis

#### 3. Appendix

* Screenshots of tools in action
* Scripts/config files if applicable
* Contribution statement from all group members

|  |  |
| --- | --- |
| **Criteria** | **Weight** |
| **A. Needs Analysis & Threat Landscape** | 15% |
| Understanding business context, identifying data assets, risk sources |
| **B. Cloud Architecture Design** | 15% |
| Deployment model, services used, scalability, alignment with organizational needs |
| **C. Security Framework and Compliance** | 15% |
| Application of standards (ISO27001, NIST), policy design, encryption |
| **D. Access Control and Risk Mitigation** | 10% |
| Use of IAM/ACLs, backup strategies, MFA, role-based access |
| **E. Incident Response and Cyber Forensics Plan** | 15% |
| Detection, logging, containment, investigation approach |
| **F. Practical Implementation (Free Tools)** | 20% |
| Execution and evidence of at least 4 tasks |
| **G. Report Structure and References** | 5% |
| Presentation quality, clarity, grammar, Harvard referencing |
| **H. Innovation and Group Collaboration** | 5% |
| Novel approaches, balanced contribution |