|  |  |  |  |
| --- | --- | --- | --- |
| **COMP1431 (2021/22)** | **Audit & Security** | **Faculty Header ID:** | **Contribution: 50% of course** |
| **Course Leader: Dr David Chadwick** | **Practical Audit**  **of KW Labs** | **Given Out: 8 Feb 2023** | **Deadline Date;**  **Wed 22 Mar 2023** |
| **This coursework will be marked anonymously** | | | |
| This coursework should take an average student who is up-to-date with tutorial work approximately 25 hours   Feedback and grades are normally made available within 15 working days of the coursework deadline | | | |
| **Learning Outcomes:**  E. Critically appraise the use of audit techniques to ensure appropriate use of controls. | | | |

|  |
| --- |
| Plagiarism is presenting somebody else's work as your own. It includes: copying information directly from the Web or books without referencing the material; submitting joint coursework as an individual effort; copying another student's coursework; stealing coursework from another student and submitting it as your own work.  Suspected plagiarism will be investigated and if found to have occurred will be dealt with according to the procedures set down by the University. Please see your student handbook for further details of what is / isn't plagiarism.   **All material copied or amended from any source (e.g. internet, books) must be referenced correctly according to the reference style you are using.   Your work will be submitted for plagiarism checking.  Any attempt to bypass our plagiarism detection systems will be treated as a severe Assessment Offence.** |

**Coursework Submission Requirements**

* An electronic copy of your work for this coursework must be fully uploaded on the Deadline Date of using the link on the coursework Moodle page for COMP1431.
* For this coursework you must submit a single PDF document.  In general, any text in the document must not be an image (i.e. must not be scanned) and would normally be generated from other documents (e.g. MS Office using "Save As .. PDF"). An exception to this is hand written mathematical notation, but when scanning do ensure the file size is not excessive.
* There are limits on the file size (see the relevant course Moodle page).
* Make sure that any files you upload are virus-free and not protected by a password or corrupted otherwise they will be treated as null submissions.
* Your work will not be printed in colour. Please ensure that any pages with colour are acceptable when printed in Black and White.
* You must NOT submit a paper copy of this coursework.
* All courseworks must be submitted as above. Under no circumstances can they be accepted by academic staff

The University website has details of the current Coursework Regulations, including details of penalties for late submission, procedures for Extenuating Circumstances, and penalties for Assessment Offences.  See <http://www2.gre.ac.uk/current-students/regs>

# Specification

## **This coursework is to be completed as a TEAM (2 persons) piece of work. Please select your own team member from within the class.**

You are one of the MSc level trainees newly employed in IT security auditing at CyberSAFE Auditors. The Chief Auditor, Nigel Waring, is very keen on team work approaches to auditing and so, as part of the postgraduate induction programme, has divided trainees into teams of two persons. Nigel explains that each team is tasked with conducting a limited ISO27002 compliance audit of a new client’s premises and to prepare an audit report. Nigel will then select the best report to present to the client.

Nigel explains that each pair must arrange between them for the following tasks to be undertaken:

1. must meet, either in-person or by email, and allocate one person to do Secure Areas (Section4 in report) and another person to Equipment Security (Section5 in report). All other sections to be dealt with jointly.
2. must decide on their fieldwork methods, timetable and approach
3. must, as the audit progresses, keep minutes (up to 250 words each) of three work-in-progress meetings (Initial, Interim, Final). These minutes should contain the following:-

Initial: agreements, differences of opinion, allocation of tasks and duties for audit process.

Interim: agreements, differences of opinion, peer review of each other’s work to date,

Final: agreements, differences of opinion, and peer review of each other’s work and decisions on structure of final report.

1. must produce a joint audit report according to required template (see Audit Job Allocation form) and containing an Appendix A showing brief notes (no more than 250 words each) for the three work-in-progress meetings (Initial, Interim, Final).

Nigel then presents each team formally with the following documents:-

1. An Audit Job Allocation Form
2. A copy of the original letter from the client specifying the audit to be undertaken,
3. A copy of the relevant parts of ISO27002:2013 sect. 11 that Nigel wants you to use,

# Deliverables

Visit the computing laboratories on the 1st floor King William (all labs) and perform your audit using whatever practical techniques you have jointly decided upon. However, you MUST abide by the constraints specified by the client. Based on this, write a report as requested below. The report should have a minimum 3000 words, maximum 5000 words excluding any appendices/references. The report must be word-processed and **must have** the headings and sub-headings specified by the Chief Auditor in the Audit Job Allocation form.

The report must contain, on it’s header page, the following Joint Authorship statement:

*This report is a team product, reviewed through regular work-in-progress meetings, and its content integrated and jointly agreed by all authors. It represents a true statement of the team’s audit findings and conclusion.*

*Secure Areas author: <put your student number here>*

*Equipment Security author: <put your student number here>*

**Assessment Criteria**

Marks will be awarded for the report as follows:-

Title, Team Name, Recipients, Joint Authorship statement, Date, Contents 2 marks

Scope, 6 marks

Business Setting 6 marks

Practical Audit Method Employed 20 marks

Secure Areas 20 marks

Equipment Security 20 marks

Audit Conclusion 20 marks

Appendix A: Work-in-Progress Peer Review reports 6 Marks

Marks will be lost for report presentation, as follows:-

* Poor referencing (especially of internet sources): word-for-word copies of sources must be shown in quotes and be referenced. Ideas that are not original to you must be properly attributed.
* Poor presentation:
  + Poor quality of expression, spelling and grammar, referencing
  + Poor Content: lacking original thought, research, integration of topics
  + Poor integration of work amongst team members
  + Poor Application of Taught Concepts

**This coursework does not lend itself to copying from internet or other published materials. You are reminded of the University’s policy on plagiarism and cheating and that any evidence of wrongful cutting and pasting of internet sources will be passed to the Plagiarism Officer; you may then be given a zero mark for this work**.

**Grading Criteria**

The grades for the sections will be amalgamated into an overall grade for the entire coursework.

A: 70–100% Professional piece of work with excellence in all given assessment criteria.

B: 60-69% Professional piece of work good in all given assessment criteria, possibly excellent in some.

C: 50-59% Professional piece but with some omissions/inaccuracies/inappropriate deductions.

D: 40-49% Marginal Fail in academic assessment criteria lacking in thoroughness as professional report.

E: 35-39% Definite Fail as an academic exercise and not acceptable as a professional piece of work.

F: 0-34% Fail: work that is unacceptable both academically and as a professional piece.

**AUDIT JOB ALLOCATION**

TO: Trainee Auditor Team FROM: Nigel Waring (Chief Auditor)

DATE: 1st February 2023 REF: GreLab/Feb2023

SUBJECT: Audit of University of Greenwich King William 1st Floor Computing Laboratories

Your report will be delivered electronically by close of business on the required date.

Please find enclosed documents for your attention:-

* + - * Copy of original letter from the client dated 22nd January 2023.
* Copy of ISO27002:2022 section 7.

I envisage that these documents will be useful to the team in this audit job although it may not be possible to fully address some o22f the control criteria specified in the required ISO sections.

In view of the fact that the University is a new client to us and we wish to build a good business relationship with them for the future, please also include in your audit any related issues concerning the 1st Floor King William Computing Laboratory not necessarily covered in the above guidelines but which you think should be communicated to the client as a matter of urgency.

Your final report MUST have the headings as shown below and which follow the CyberSAFE Auditors standard method of reporting.

One page showing Title, Recipients, Date, Joint Authorship statement

One Page showing Contents Page (with section headings and page numbers)

Section 1: Scope (no more than 250 words)

Section 2 : Business Setting (no more than 250 words)

Section 3 : Practical Audit Method Employed

Section 4 :Secure Areas

4(a) Expected Controls,

4(b) Observed Controls and Comments

Section 5 : A.11.2: Equipment Security

5(a) Expected Controls,

5(b) Observed Controls and Comments

Section 6 : Audit Conclusion

6(a) Overall conclusion based on relevant GAP analyses

6(b) Recommendation for Immediate and Future Management Action

References

Appendix A: Minutes of Work-in-Progress meetings (Initial, Interim, Final).

Other appendices

Please approach this job with planning, thoroughness, fair allocation of tasks, and good record-keeping. Keep to the headings above and most of all to the deadlines. All of these things are a measure of our professionalism as an auditing company (and also of you personally) and they are the criteria by which the client will assess us as a future business partner.



Nigel Waring

CEO CyberSAFE Auditors plc

Romney Road

Greenwich

London SE10 9LS

22nd January 2023

Dear Mr Waring,

The Department of Computing and Mathematical Sciences (CMS) requires you to undertake a security audit of computing resources used by students in all the computing laboratories on the first floor of the King William Building. The scope of the audit is to cover the physical and environmental security of the physical assets in the labs themselves as per ISO27002:2022 section 7.

However, the university has specified two constraints that must be adhered to by all of your participating fieldwork auditors. Constraint 1 is that auditors must not converse either verbally or in writing with any member of the university staff of any grade. Constraint 2 is that auditors must approach from a point of view consistent with that of an average (not highly technical) student. Consequently, the audit need not investigate at the operating systems level nor the actual network servers themselves. In fact, to be as authentic as possible and not cause alarm or disruption, it would be desirable for auditors to pose as typical students and fulfil the audit requirements without alerting the technical staff in any way.

We would welcome your commencement of the audit as soon as possible on receipt of this documentation and look forward to receiving your audit report as agreed by close of business on the required date.

Yours Sincerely,

L. Clancy

Manager CMS Support

Queen Mary Building

|  |  |
| --- | --- |
| **ISO27002(2022) section: 7** | **Physical Controls** |
| ***Secure areas*** | ***Objective:* To prevent unauthorized physical access, damage and interference to the organization’s premises and information**. |
| 7.1  Physical security perimeter | Control:Security perimeters ( walls, gates, reception) shall be used to protect areas that contain information and information processing facilities. |
| 7.2  Physical entry controls | Control:Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access. |
| 7.3  Securing offices, rooms and  facilities | Control: Physical security for offices, rooms, and facilities shall be designed and applied. |
| 7.4  Physical Security Monitoring | Not required for this audit |
| 7.5  Protecting against external  and environmental threats | Not required for this audit. |
| 7.6 Working in secure areas | Control: Physical protection and guidelines for working in secure areas shall be designed and applied. |
|  |  |
|  |  |
| ***Equipment security*** | ***Objective:* To prevent loss, damage, theft or compromise of assets and interruption to the organization’s activities.** |
| 7.7  Clear desk/screen policy | Not required for this audit. |
| 7.8  Equipment siting and  protection | Control: Equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access. |
| 7.9  Assets off-premises | Not required for this audit. |
| 7.10  Storage Media | Not required for this audit. |
| 7.11  Supporting utilities | Control: Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities. |
| 7.12  Cabling Security | Control: Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. |
| 7.13  Equipment Maintenance | Not required for this audit. |
| 7.14  Disposal/reuse of equipment | Not required for this audit. |
|  |  |
|  |  |