**INTRODUCTION**

The purpose of this report is to provide a detailed review of the IT security audit conducted of the computing laboratories on the 1st floor of King William Building. Our team conducted this audit in accordance with the requirements of the British Computer Society (BCS). The audit was conducted with the goal of assessing the current state of the IT security in the laboratories, identifying any potential security risks, and providing recommendations for improving the security of the computing laboratories.

This report will begin with an overview of the audit task, providing details of the audit team, the time frame of the audit, and the guidance and instructions that were provided. This will be followed by a description of the scope of the audit task and the resources that were available for the audit, including personnel and systems. The report will then present the results of the audit, followed by a discussion of the findings, recommendations for improving the security of the laboratories, and a conclusion.

The audit team consisted of five individuals: a Chief Auditor, an Auditor, a Reviewer, a Security Analyst, and a Technician. The Chief Auditor was responsible for providing overall guidance and direction for the audit, while the other team members were responsible for specific tasks. The time frame of the audit was two weeks, and the guidance and instructions provided by the Chief Auditor were based on the relevant sections of the ISO 27002:2013 standard.

The scope of the audit was to review the security measures in place in the computing laboratories on the 1st floor of King William Building. The audit team had access to the relevant documents and resources, as well as personnel and systems. The personnel involved in the audit included the team members, as well as other staff from the university. The systems used for the audit included the university's security systems and tools, as well as the audit team's own tools and software.

The audit team conducted a thorough review of the IT security measures in place in the computing laboratories, and identified any potential security risks. The team's findings were presented in the report, along with recommendations for improving the security of the laboratories. The report also provided a conclusion and recommendations for further action.

This report provides a detailed review of the IT security audit conducted of the computing laboratories on the 1st floor of King William Building. The audit team's findings and recommendations are presented in the report, along with a conclusion and recommendations for further action.

**BACKGROUND**

The background of this report is the IT security audit conducted of the computing laboratories on the 1st floor of King William Building. The audit was conducted by a team of five individuals, including a Chief Auditor, an Auditor, a Reviewer, a Security Analyst, and a Technician. The Chief Auditor was responsible for providing overall guidance and direction for the audit, while the other team members were responsible for specific tasks.

The audit task for this report is to assess the current state of the IT security in the computing laboratories on the 1st floor of King William Building. The audit team was tasked with conducting a thorough review of the IT security measures in place in the laboratories, and identifying any potential security risks. The audit team was also tasked with providing recommendations for improving the security of the laboratories.

The time frame of the audit was two weeks, and the guidance and instructions provided by the Chief Auditor were based on the relevant sections of the ISO 27002:2013 standard. The scope of the audit was to review the security measures in place in the computing laboratories on the 1st floor of King William Building. The audit team had access to the relevant documents and resources, as well as personnel and systems.

The personnel involved in the audit included the team members, as well as other staff from the university. The systems used for the audit included the university's security systems and tools, as well as the audit team's own tools and software. The audit team conducted a thorough review of the IT security measures in place in the computing laboratories, and identified any potential security risks.

The audit team also had access to the relevant personnel, systems, and documents, which were provided by the university. These included the university's security policies, procedures, and guidelines; the university's IT security systems and tools; and the university's audit logs.

Furthermore, the audit team had access to the relevant personnel, systems, and documents, which were provided by the university. These included the university's security policies, procedures, and guidelines; the university's IT security systems and tools; and the university's audit logs. Additionally, the audit team had access to the relevant personnel, systems, and documents, which were provided by the university. These included the university's security policies, procedures, and guidelines; the university's IT security systems and tools; and the university's audit logs.

In summary, the background of this report is the IT security audit conducted of the computing laboratories on the 1st floor of King William Building. The audit was conducted by a team of five individuals, with the guidance and instructions provided by the Chief Auditor based on the relevant sections of the ISO 27002:2013 standard. The scope of the audit was to review the security measures in place in the computing laboratories on the 1st floor of King William Building. The audit team had access to the relevant personnel, systems, and documents, which were provided by the university.

**METHODOLOGY**

The audit team agreed on a number of practical techniques and methods to perform the security audit of the computing laboratories on the 1st floor of King William Building. The techniques used by the audit team are discussed as follows;

**Interviewing staff and users**

Interviewing staff and users is an important part of conducting a security audit, as it allows auditors to gain a better understanding of how the IT system is being used and how security controls and policies are being implemented. Interviews provided insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified. During the audit, the team can interview staff, users and other stakeholders to gain an understanding of their knowledge, experience and understanding of IT security.

The team can use semi-structured interviews in order to gain a better understanding of the security controls and procedures in place, as well as any potential weaknesses that may be identified. The team can also ask questions about any security incidents that may have occurred and how they were handled. Interviews can also provide an understanding of the organization’s security culture and how it affects the implementation of security controls and policies.

**Observing users and processes**

Observing users and processes is another important part of the audit process, as it allows auditors to gain a better understanding of how the IT system is being used and how security controls and policies are being implemented. During the audit, the team observed users and processes in order to identify any potential security vulnerabilities or weaknesses. This can include observing user activity, such as logging into the system or accessing sensitive data, as well as observing processes, such as the implementation of security controls.

Observing users and processes can provide insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified. It can also provide an understanding of the organization’s security culture and how it affects the implementation of security controls and policies.

**Security testing**

Security testing is an important part of the audit process, as it allows auditors to identify any potential security risks or weaknesses that may exist within the IT system. During the audit, the team employed a variety of security testing techniques in order to identify any potential security risks or weaknesses. These can include vulnerability scans, penetration tests, and code reviews. These tests can identify any potential security vulnerabilities or weaknesses that could be exploited by malicious actors.

**Analyzing system logs**

Analyzing system logs is another important part of the audit process, as it allows auditors to identify any suspicious or unauthorized activity that may be occurring within the IT system. During the audit, the team analyzed system logs in order to identify any suspicious or unauthorized activity. This can include identifying any potential attempts to access sensitive data or resources, as well as any suspicious logins or access attempts. Analyzing system logs can provide insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified.

**Examining access control lists**

Examining access control lists is an important part of the audit process, as it allows auditors to ensure that only authorized users are granted access to sensitive data and resources. During the audit, the team examined access control lists in order to identify any potential security vulnerabilities or weaknesses. This included identifying any unauthorized users that may have access to sensitive data or resources, as well as any potential attempts to access sensitive data or resources. Examining access control lists can provide insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified.

**Reviewing policies and procedures**

Reviewing policies and procedures is an important part of the audit process, as it allows auditors to ensure that they are up to date and being followed correctly. During the audit, the team reviewed policies and procedures in order to identify any potential security vulnerabilities or weaknesses. This included identifying any policies or procedures that may be out of date, as well as any potential attempts to access sensitive data or resources that may not be in compliance with the organization’s policies and procedures. Reviewing policies and procedures can provide insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified.

**Performing vulnerability scans**

Performing vulnerability scans is an important part of the audit process, as it allows auditors to identify any potential security risks or weaknesses that may exist within the IT system. During the audit, the team can employed a variety of vulnerability scanning tools in order to identify potential security risks or weaknesses. These tools were able to scan a variety of potential security vulnerabilities, such as unpatched software, weak passwords, open ports, and other potential security issues. Performing vulnerability scans provided insights into the organization’s security processes and procedures, as well as the weaknesses or areas of improvement that were be identified.

**Analyzing system configurations**

Analyzing system configurations is another important part of the audit process, as it allows auditors to ensure that the IT system is secure and up to date. During the audit, the team analyzed the system configurations in order to identify any potential security vulnerabilities or weaknesses. This included identifying any outdated software or configurations that may be vulnerable to attack, as well as any potential attempts to access sensitive data or resources that may not be in compliance with the organization’s security policies. Analyzing system configurations could provide insight into the organization’s security processes and procedures, as well as any weaknesses or areas of improvement that may be identified.

**RESULTS**

The audit team conducted a thorough review of the IT security measures in place in the computing laboratories on the 1st floor of King William Building. The team's findings are presented in the report, along with recommendations for improving the security of the laboratories.

The audit team found that the university had implemented a number of security measures to protect the computing laboratories, including firewalls and antivirus software. The team also found that access control lists had been implemented, and that user accounts had been set up in order to restrict access to sensitive data and resources.

In addition, the team found that the university had implemented a number of policies and procedures in order to protect the IT systems. These included policies related to password management, access control, and data security. The team also found that the university had implemented a system of user education in order to ensure that users were aware of the security procedures and policies.

The audit team also identified a number of potential security risks and weaknesses. These included outdated software and configurations, weak passwords, and open ports. The team also found that there were a number of users with access to sensitive data and resources who did not have the appropriate training or knowledge to handle this data securely. Additionally, the team noted that the audit logs were not being reviewed on a regular basis.

Based on the findings of the audit, the team was able to provide a number of recommendations for improving the security of the computing laboratories. These included the implementation of additional security measures, such as two-factor authentication and encryption; the implementation of additional policies and procedures; and the regular review of the audit logs. The team also recommended the implementation of user education and training in order to ensure that users are aware of the security procedures and policies. Finally, the team recommended the use of security tools and software in order to identify potential security risks and vulnerabilities.

**DISCUSSION**

The audit team conducted a thorough review of the IT security measures in place in the computing laboratories on the 1st floor of King William Building. The team's findings are presented in the report, along with recommendations for improving the security of the laboratories.

The audit team found that the university had implemented a number of security measures to protect the computing laboratories, including firewalls and antivirus software. Firewalls are important security measures as they act as a barrier between internal and external networks, preventing malicious actors from accessing sensitive data or resources. Antivirus software is also important as it helps to protect the system from malware and other malicious code. The team also found that access control lists had been implemented, and that user accounts had been set up in order to restrict access to sensitive data and resources. These access control lists ensure that only authorized users have access to the system and that potentially malicious users are blocked from accessing the system.

In addition, the team found that the university had implemented a number of policies and procedures in order to protect the IT systems. These included policies related to password management, access control, and data security. Password management policies ensure that users are using strong and secure passwords, while access control policies ensure that only authorized users are granted access to sensitive data and resources. Data security policies ensure that data is protected from unauthorized access. The team also found that the university had implemented a system of user education in order to ensure that users are aware of the security procedures and policies. This system of user education ensures that users are aware of the security risks associated with accessing and using the IT system, as well as the measures they can take to protect their data.

The audit team also identified a number of potential security risks and weaknesses. These included outdated software and configurations, weak passwords, and open ports. Outdated software and configurations can make the system vulnerable to attack, as attackers can exploit known vulnerabilities in the software. Weak passwords can make the system more vulnerable to attack, as attackers can easily guess passwords or use brute force attacks to gain access to the system. Open ports can allow attackers to gain access to the system, as they can use the port to connect to the system without authentication. The team also found that there were a number of users with access to sensitive data and resources who did not have the appropriate training or knowledge to handle this data securely. Additionally, the team noted that the audit logs were not being reviewed on a regular basis. This can make it difficult to detect any suspicious or unauthorized activity on the system.

**RECOMMENDATIONS**

Based on the findings of the audit, the team was able to provide a number of recommendations for improving the security of the computing laboratories. These included the implementation of additional security measures, such as two-factor authentication and encryption; the implementation of additional policies and procedures; and the regular review of the audit logs. Two-factor authentication can help to protect the system from unauthorized access, as users will need to provide two pieces of information in order to gain access to the system. Encryption can also help to protect data from unauthorized access, as it prevents attackers from being able to read the data even if they gain access to the system. The team also recommended the implementation of additional policies and procedures, such as policies related to user access and data security. These policies can help to ensure that users are only accessing data and resources that they are authorized to access, and that data is protected from unauthorized access. The team also recommended the regular review of the audit logs in order to detect any suspicious or unauthorized activity on the system.

The team also recommended the use of security tools and software in order to identify potential security risks and vulnerabilities. These tools and software can be used to scan the system for potential security risks and vulnerabilities, such as outdated software, weak passwords, and open ports. Additionally, the team recommended the implementation of user education and training in order to ensure that users are aware of the security procedures and policies. This training can ensure that users are aware of the security risks associated with accessing and using the IT system, as well as the measures they can take to protect their data.

**CONCLUSION**

The audit team conducted a thorough review of the IT security measures in place in the computing laboratories on the 1st floor of King William Building. The team's findings are presented in the report, along with recommendations for improving the security of the laboratories. The audit team found that the university had implemented a number of security measures to protect the computing laboratories, including firewalls and antivirus software. The team also found that access control lists had been implemented, and that user accounts had been set up in order to restrict access to sensitive data and resources. In addition, the team found that the university had implemented a number of policies and procedures in order to protect the IT systems.

The audit team also identified a number of potential security risks and weaknesses. These included outdated software and configurations, weak passwords, and open ports. The team also found that there were a number of users with access to sensitive data and resources who did not have the appropriate training or knowledge to handle this data securely. Additionally, the team noted that the audit logs were not being reviewed on a regular basis.

Based on the findings of the audit, the team was able to provide a number of recommendations for improving the security of the computing laboratories. These included the implementation of additional security measures, such as two-factor authentication and encryption; the implementation of additional policies and procedures; and the regular review of the audit logs. The team also recommended the use of security tools and software in order to identify potential security risks and vulnerabilities, as well as the implementation of user education and training in order to ensure that users are aware of the security procedures and policies.

In conclusion, the audit team found that the university had implemented a number of security measures to protect the computing laboratories on the 1st floor of King William Building. However, the team also identified a number of potential security risks and weaknesses. The team was able to provide a number of recommendations for improving the security of the laboratories, including the implementation of additional security measures, policies and procedures, and the use of security tools and software. It is essential that the university implements these recommendations in order to ensure that the computing laboratories are secure and protected from potential threats. Additionally, it is important for the university to regularly review and update its security measures, policies and procedures in order to ensure that the IT systems remain secure and up to date.