Higher Nationals - Summative Assignment Feedback Form

Student Name/ID	M.M.M AASHIK /E230667		
Unit Title	**Unit 05: Security**		
Assignment Number	5	**Assessor**	MR.LAHIRU
Submission Date	20.12.2024	**Date Received 1st submission**	
Re-submission Date		**Date Received 2nd submission**	

Assessor Feedback:

LO1. Assess risks to IT security

Pass, Merit & Distinction Descripts	P1 ☐	P2 ☐	M1 ☐	D1 ☐

LO2. Describe IT security solutions.

Pass, Merit & Distinction Descripts	P3 ☐	P4 ☐	M2 ☐	D1 ☐

LO3. Review mechanisms to control organisational IT security.

Pass, Merit & Distinction Descripts	P5 ☐	P6 ☐	M3 ☐	M4 ☐	D2 ☐

LO4. Manage organisational security.

Pass, Merit & Distinction Descripts	P7 ☐	P8 ☐	M5 ☐	D3 ☐

Assessor Feedback:		
Grade:	**Assessor Signature:**	**Date:**
Resubmission Feedback: • Please note resubmission feedback is focussed only on the resubmitted work		
Grade:	**Assessor Signature:**	**Date:**
Internal Verifier's Comments:		
Signature & Date:		

* Please note that grade decisions are provisional. They are only confirmed once internal and external moderation has taken place and grades decisions have been agreed at the assessment board.

Pearson
Higher Nationals in
Computing

Unit 5: Security

M.M.M AASHIK SEC
E230667

General Guidelines

1. A Cover page or title page – You should always attach a title page to your assignment. Use previous page as your cover sheet and make sure all the details are accurately filled.
2. Attach this brief as the first section of your assignment.
3. All the assignments should be prepared using a word processing software.
4. All the assignments should be printed on A4 sized papers. Use single side printing.
5. Allow 1" for top, bottom , right margins and 1.25" for the left margin of each page.

Word Processing Rules

1. The font size should be **12** point, and should be in the style of **Time New Roman**.
2. **Use 1.5 line spacing**. Left justify all paragraphs.
3. Ensure that all the headings are consistent in terms of the font size and font style.
4. Use **footer function in the word processor to insert Your Name, Subject, Assignment No, and Page Number on each pag**e. This is useful if individual sheets become detached for any reason.
5. Use word processing application spell check and grammar check function to help editing your assignment.

Important Points:

1. It is strictly prohibited to use textboxes to add texts in the assignments, except for compulsory information. eg: Figures, tables of comparison etc. Adding text boxes in the body except for the before mentioned compulsory information will result in rejection of your work.
2. Avoid using page borders in your assignment body.
3. Carefully check the hand in date and the instructions given in the assignment. Late submissions will not be accepted.
4. Ensure that you give yourself enough time to complete the assignment by the due date.
5. Excuses of any nature will not be accepted for failure to hand in the work on time.
6. You must take responsibility for managing your own time effectively.
7. If you are unable to hand in your assignment on time and have valid reasons such as illness, you may apply (in writing) for an extension.
8. Failure to achieve at least PASS criteria will result in a REFERRAL grade .
9. Non-submission of work without valid reasons will lead to an automatic RE FERRAL. You will then be asked to complete an alternative assignment.
10. If you use other people's work or ideas in your assignment, reference them properly using HARVARD referencing system to avoid plagiarism. You must provide both in-text citation and a reference list.
11. If you are proven to be guilty of plagiarism or any academic misconduct, your grade could be reduced to A REFERRAL or at worst you could be expelled from the course

STUDENT ASSESSMENT SUBMISSION AND DECLARATION

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

Student name: **M.M.M. AASHIK** **E230667**		Assessor name: **MR.LAHIRU**
Issue date:	Submission date: **20.12.2024**	Submitted on:
Programme: **BTEC Higher National Diploma in Computing**		
Unit: **Unit 5 - Security**		
Assignment number and title: **Managing Network Security for Colombo Advanced College**		

Plagiarism

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

Student Declaration

Student declaration

I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.

Student signature: E230667 Date:

Assignment Brief

Student Name /ID Number	M.M.M. AASHIK/E230667
Unit Number and Title	Unit 5- Security
Academic Year	2024/25
Unit Tutor	
Assignment Title	**Managing Network Security for Colombo Advanced College**
Issue Date	
Submission Date	20.12.2024
IV Name & Date	

Submission Format:

The assignment submission should be in the form of the following:

Formal Presentation: A 10-minute presentation (10–20 slides as a guide, with supporting speaker notes) to communicate an evaluation of your investigation to a non-technical audience. This should highlight key information regarding the range of IT security risks that organizations in Sri Lanka face and the IT security solutions available. The presentation will also include an assessment of current organizational security procedures and an evaluation of both the physical and virtual security countermeasures presented.

Briefing Paper: Produce a briefing paper that reviews the principles and the benefits of an ISMS used in an organization like Colombo Advanced College and analyze the process of implementing such a system.

Process Review Document: A review document (1,000–1,500 words) assessing the existing risk assessment procedures in a selected Sri Lankan organization. This document should summarize standard risk management approaches and demonstrate how implementing IT security should align with the organization's policies.

Written Report: A report (1,000–1,500 words) reviewing a security incident and recommending a suitable security policy for the organization. The policy should include all stakeholders to ensure an audit trail can be identified. The report will evaluate the suitability of selected security tools to meet the needs of the business.

All work must be supported with research and referenced using the Harvard referencing system. Use appropriate headings, paragraphs, and subsections.

Unit Learning Outcomes:

LO1 Assess risks to IT security.

LO2 Describe IT security solutions.

LO3 Review mechanisms to control organizational IT security.

LO4 Manage organizational security.

Assignment Brief and Guidance:

Scenario

You have been employed as a Junior Network Security Specialist for TechSecure Solutions (Pvt) Ltd., a leading provider of network security solutions for a variety of clients across different sectors in Sri Lanka. TechSecure Solutions offers a range of services, including:

- Security audits of organizational networks
- Recommendations for improving network security
- Implementation of network security solutions
- Planning and designing Information Security Management Systems (ISMS) for organizations
- Continuous monitoring and incident response
- Compliance with international security standards like ISO/IEC 27001

Client Background: Colombo Advanced College

One of your prominent clients is Colombo Advanced College, a large educational institution specializing in ICT, engineering, and business studies with over 2,500 students and 150 staff members. The college has multiple departments, including Computer Science, Electrical Engineering, Business Management, and Bioinformatics, each with dedicated labs and resources. The institution has a central data center that houses critical applications, student records, research data, and administrative functions.

Recent Incident:

Recently, Colombo Advanced College experienced a ransomware attack that led to a significant loss of data, causing major disruption in academic and administrative activities. The attack exploited vulnerabilities in the college's outdated network infrastructure and lack of robust security policies.

Your Task:

You have been tasked with reviewing the current risk assessment procedures and developing a comprehensive security policy to prevent future incidents. This involves conducting a thorough security audit, identifying vulnerabilities, and recommending appropriate security measures tailored to the college's needs.

Detailed Requirements:

Security Audit and Risk Assessment:

- Conduct a comprehensive security audit of the college's network infrastructure, including servers, workstations, and network devices.
- Assess the current security measures in place, such as firewalls, intrusion detection systems (IDS), antivirus software, and access controls.
- Identify potential vulnerabilities and threats, including malware, phishing attacks, unauthorized access, and physical security breaches.

Development of a Security Policy:

- Create a detailed security policy that addresses identified risks and vulnerabilities. This should include guidelines for data protection, user access management, incident response, and regular security audits.
- Develop procedures for handling sensitive information, including encryption standards, data backup protocols, and secure communication methods.
- Design a disaster recovery plan outlining steps to restore operations in case of a security breach or data loss.

Implementation of Security Measures:

- Recommend and implement advanced security solutions, such as next-generation firewalls, endpoint protection platforms, and multi-factor authentication (MFA).
- Set up network segmentation to isolate critical systems and minimize the impact of potential attacks.
- Implement regular patch management processes to ensure all systems are up to date with the latest security updates.

Training and Awareness Programs:

- Develop and conduct training sessions for staff and students on cybersecurity best practices, including recognizing phishing attempts, safe internet usage, and secure password management.
- Create awareness campaigns to promote a culture of security within the college, emphasizing the importance of individual responsibility in maintaining a secure environment.

Continuous Monitoring and Improvement:

- Establish a continuous monitoring system to detect and respond to security incidents in real-time.
- Regularly review and update the security policy and procedures to adapt to evolving threats and technological advancements.

- Conduct periodic security drills and simulations to test the effectiveness of the incident response plan.

Future Prospects:

As part of the long-term strategy, Colombo Advanced College is considering the implementation of a hybrid learning model, integrating more online and remote learning options. This transition will require additional security measures to protect online learning platforms, secure remote access, and ensure the privacy of students and faculty members.

Activity 1: Formal Presentation

Produce a formal presentation (with supporting notes) on a review of the range of IT security threats that are faced by an organization like Colombo Advanced College, describe and evaluate the range of countermeasures, both physical and virtual.

Your presentation should include a section on security risks, including:

- A discussion of the different types of security risks to Colombo Advanced College and similar organizations.
- An assessment of the organizational security procedures presented in the given scenario.
- An analysis, with reasons, of the benefits of implementing network monitoring systems.

Your presentation should go on to discuss a range of security countermeasures for the identified risks, including the following:

- A discussion of the potential security impact of incorrect configuration of:
    - Firewall policies
    - Third-party VPN clients and servers.
- A discussion, using a specific example from either your research or the Colombo Advanced College scenario, of how implementing each of the following can improve network security:
    - A De-Militarized Zone (DMZ)

- A Static IP
- Network Address Translation (NAT).

- A proposal for a method to assess and treat IT security risks.
- An evaluation of the range of countermeasures that can be employed to ensure that an organization's integrity is not compromised. Organizational integrity could be either Data Security or Operational Continuance. Make sure you include both physical and virtual security countermeasures.

Support any points you make in the presentation with well-chosen examples from any research you have carried out on related sectors or security scenarios.

Activity 2: Briefing Paper

Produce a briefing paper that reviews the principles and the benefits of an ISMS used in an organization like Colombo Advanced College, and analyze the process of implementing such a system.

Your paper should include a section on an ISMS framework, including the following:

- An examination of the key principles of an ISMS and its relevance to the successful operation in Colombo Advanced College.
- An analysis of the benefits that an effective ISMS can have on Colombo Advanced College.
- An assessment and critical analysis of the elements and processes required for Colombo Advanced College to establish and maintain a more robust ISMS, ensuring that the key principles are met.
- A justification of the steps required for Colombo Advanced College in order to implement an ISMS.

Support any points you make in the presentation with well-chosen examples from any research you have carried out on related sectors or ISMS scenarios.

Activity 3: Process Review Document

Produce a process review document that assesses the current mechanisms and legislation for data security within an organization.

Your review should include the following:

- A review of the current risk assessment procedures in Colombo Advanced College.
- An explanation of data protection processes and regulations applied to Colombo Advanced College.
- A summary of an appropriate risk-management strategy or applied ISO standard and its application to IT security at Colombo Advanced College.
- An analysis of the possible impact on security at Colombo Advanced College, following the results of an IT security audit.
- A recommendation, with supported reasons, on how the IT security at Colombo Advanced College can be aligned with its organizational policy. Detail explicitly the security impact if there is a misalignment.

Support any points you make in the report with well-chosen examples from any research you have carried out on related sectors or ISMS scenarios.

Activity 4: Written Report

Present a written report to appraise an ISMS for Colombo Advanced College and design a suitable security policy, based on the supplied evidence and operational requirements.

Your report should include the following:

- A plan of the design of an ISMS for Colombo Advanced College, including an implementation map, taking into consideration functional and non-functional requirements of the digital systems.
- A suitable security policy, including the main components of a disaster recovery plan for the college.
- Identification and discussion of the stakeholders and their roles in implementing a security audit.

- Justification, with reasons, for the designed security plan, including the selected physical, virtual, and policy elements.
- An appraisal of and justification for the planned ISMS design, against the new IT security landscape in Colombo Advanced College, auditing the different stages of the process followed.
- An analysis of the relationship between ISO and international ISMS standards and the establishment of an effective ISMS for Colombo Advanced College.
- An evaluation of the suitability of the tools used in the security policy designed for Colombo Advanced College in terms of how it meets their needs.
- A critical examination of the advantages and disadvantages of the planned ISMS for the college, against key and international standards.

Support any points you make in the report with well-chosen examples from any research you have carried out on related sectors or projects, as well as the existing scenario and any associated documentation.

Learning Outcomes and Assessment Criteria

Pass	Merit	Distinction
LO1 Assess risks to IT security		**LO1 and LO2** **D1** Evaluate a range of physical and virtual security measures that can be employed to ensure the integrity of organisational IT security.
P1 Discuss types of security risks to organisations. **P2** Assess organisational security procedures.	**M1** Analyse the benefits of implementing network monitoring systems with supporting reasons.	
LO2 Describe IT security solutions		
P3 Discuss the potential impact to IT security of incorrect configuration of firewall policies and third-party VPNs. **P4** Discuss, using an example for each, how implementing a DMZ, static IP and NAT in a network can improve network security.	**M2** Propose a method to assess and treat IT security risks.	
LO3 Review mechanisms to control organisational IT security		**D2** Recommend how IT security can be aligned with an organisational policy, detailing the security impact of any misalignment.
P5 Review risk assessment procedures in an organisation. **P6** Explain data protection processes and regulations as applicable to an organisation.	**M3** Summarise an appropriate risk-management approach or ISO standard and its application in IT security. **M4** Analyse possible impacts to organisational security resulting from an IT security audit.	

Pass	Merit	Distinction
LO4 Manage organisational security		
P7 Design a suitable security policy for an organisation, including the main components of an organisational disaster recovery plan. **P8** Discuss the roles of stakeholders in the organisation in implementing security audits.	**M5** Justify the security plan developed giving reasons for the elements selected.	**D3** Evaluate the suitability of the tools used in the organisational policy to meet business needs.

Content

Benefits of Colombo advanced college

Impact of improper configurations of VPN, Firewall and how it will affect to Colombo advanced college

Summary

Importance of the DMZ, static IP and NAT in a Network

Demilitarized Zones

Advantages and Disadvantages of DMZ

Uses to the Colombo advanced college and its students by using Demilitarized Zones

Static IP

Advantage Disadvantage

Uses to the Colombo advanced college and its students by using Static IP

Network Address Translation (NAT)

Types of NAT

Advantage Disadvantage

The benefits of Network Address Translation (NAT) for Colombo Advanced College and its stakeholders.

Summary

It security

Risk management to treat IT security risk

Some Actions to Prevent the Physical, Virtual Risks

Several actions and techniques to reduce the risks of the Colombo advanced college faces in the physical and virtual world

Tools

Some Security Measures Physical Risks

Some Security Measures for Virtual Risks

Importance of a Layered Security Approach for Colombo Advanced College

Commitment to Continuous Monitoring and Improvement

Activity 02

CIA TRIANGLE

Types of Confidentiality Violations

Techniques for maintaining confidentiality

Techniques for Maintaining Integrity

Relevance to Colombo Advanced College

Benefits Effective Information Security Management System (ISMS)

An assessment and critical analysis of these elements and processes

Processes Required

Critical Analysis

A justification of the steps required for Colombo Advanced College

Activity 03

What is risk assessment procedure?

Review of Current Risk Assessment Procedures at Colombo Advanced College

Areas for Improvement

Change Management

The Stages of Change Management

Network change management

Some crucial techniques that may be applied in network change management

Penetration Testing

Advantages of pen testing

Pen Testing Tools

Data Protection Processes and Regulations at Colombo Advanced College

Data protection laws

Risk-Management Strategy and ISO Standards for Colombo Advanced College

Analysis of the Possible Impact on Security at Colombo Advanced College after an IT Security Audit

Determine the holes in your current systems and procedures

The effects of the security audit on the security of Colombo advanced collage

Recommendation for Aligning IT Security at Colombo Advanced College with Organizational Policy

Purpose of the IT security organizational policy

Some Importance of the IT security organizational policy

Some ways to protect the policy

How IT Security align with Organizational Policy

To align IT security with the organizational policies at Colombo Advanced College, the following steps are recommended:

Security Impact of Misalignment at Colombo Advanced College

Preventing Misalignment

Security tools which will help organizational policies

Justifications for chosen tools

Penetration Testing and security audit's suitability for inclusion in an organizational policy

Activity 04

Plan for Designing an ISMS for Colombo Advanced College

Implementation Map

Benefits of the Plan

Suitable Security Policy for Colombo Advanced College

Organizational Security Policy

Security Policy for Colombo Advanced College

Some Standard which are support Colombo advanced college Security Policies

Disaster Recovery plan

STEPS IN DISASTER RECOVERY PLAN

Some types of disasters that organizations can plan for include the following

Types of disaster recovery plans

Main Components of the Disaster Recovery Plan for Colombo Advanced College

Stakeholders and Their Roles in Implementing a Security Audit

Justification for the Designed Security Plan for Colombo Advanced College

Conclusion

Appraisal and Justification of the Planned ISMS Design for Colombo Advanced College

Stages of the ISMS Process

Justification against the New IT Security Landscape

An Analysis of the Relationship between ISO Standards and International ISMS Standards in Establishing an Effective ISMS for Colombo Advanced College

The Relationship between ISO and International ISMS Standards

Establishing an Effective ISMS Using ISO Standards

Benefits of ISO-Aligned ISMS for Colombo Advanced College

Evaluation of the Suitability of Tools in the Security Policy Designed for Colombo Advanced College

Key Tools in the Security Policy and Their Suitability

How These Tools Meet Colombo Advanced College's Needs

The Assets of Colombo Advanced College

Critical Examination of the Advantages and Disadvantages of the Planned ISMS for Colombo Advanced College

Advantages of the Planned ISMS

Disadvantages of the Planned ISMS

Evaluation against Key and International Standards

Acknowledgement

I needed the assistance and advice of several reputable people to complete my task successfully. I'd like to start by thanking ESOFT for providing me with a welcoming workspace where I could finish my task. I'm very happy that the assignment is finished. I want to express my gratitude to **Mr Lahiru** for her helpful instructions for assignments throughout my semester. Finally, I'd like to share my sincere appreciation to all of the family members and classmates who helped me a lot in finalizing this project within the limited time. **THANKYOU SO MUCH!!!**

M.M.M. AASHIK
E230667

Task 01

Introduction

Colombo Advanced College, a leading educational institution specializing in ICT, engineering and business studies, recently faced a major cybersecurity incident in the form of a ransomware attack. This attack disrupted academic and administrative activities and exposed critical weaknesses in the college's network infrastructure and security policies. As a Junior Network Security Specialist at TechSecure Solutions (Pvt) Ltd., a reputable network security services provider in Sri Lanka, I was tasked with helping the college strengthen its cybersecurity framework. TechSecure Solutions specializes in conducting security audits, designing Information Security Management Systems (ISMS) and implementing advanced security measures in accordance with international standards such as ISO/IEC 27001. This task includes assessing the risks affecting the college's IT systems and identifying vulnerabilities. And design a comprehensive security strategy to protect critical applications, student data, research data and administrative functions. This also includes implementing proactive measures, creating training programs and implementing continuous monitoring systems to ensure long-term protection against ever-evolving cyber threats. The goal is to equip Colombo Advanced College with a robust security plan tailored to its specific needs, thereby preventing future incidents and protecting its academic and administrative operations.

Overview of Colombo Advanced College and the Recent Ransomware Attack

Colombo Advanced College is a leading educational institution in Sri Lanka specializing in ICT, Engineering and Business Studies. With a large student population of over 2,500 students and 150 staff members, the college operates several departments including Computer Science, Electrical Engineering, Business Management and Bioinformatics. Each department has its own dedicated laboratories and resources, while the operations of the facility rely heavily on its central data center. This data center houses critical resources such as student data, research data, academic applications and administrative systems. Recently, the university suffered a ransomware attack that caused significant disruption. The attack exploited weaknesses in the college's outdated network infrastructure and lack of a comprehensive security framework. This led to data loss, delays in academic and administrative processes, and reputational damage. Ransomware attacks encrypt sensitive data and demand a ransom for its release, leaving institutions in a position where operational recovery is costly and time-consuming. The incident highlights the urgent need for Colombo Advanced College to strengthen its cybersecurity posture to protect its digital assets and ensure business continuity.

SECURITY RISK

A computer security risk encompasses anything within your computer system that has the potential to harm or steal your data or allow unauthorized access without your consent or awareness. Various factors contribute to computer risks, and one common category is malware, a broad term used to describe various forms of malicious software. While computer viruses are frequently thought of, there are several types of malicious software that can pose security risks, including worms, ransomware, spyware, and Trojan horses etc…. Additionally, risks can emerge from misconfigurations of computer products and unsafe computing practices. Let's delve deeper into these aspects.

Importance of Addressing Network Security for Educational Institutions

According to educational institutions, Colombo Advanced College is targeted by cyberattacks due to its sensitive nature of the data. This includes personal data of students and staff, academic research and administrative data. Addressing network security allows Colombo Advanced College to maintain the integrity, confidentiality, and availability of its systems, creating a safe and reliable environment for teaching and research. By implementing security framework, the institution can protect its assets, prevent future incidents such as ransomware, viruses, worms, etc.

- Protection of sensitive data

Institutions process a large amount of confidential information, such as personal data, financial transactions and research data. A breach of this data can result in identity theft, financial fraud or intellectual property theft.

- Business continuity

Digital platforms are an integral part of modern education, supporting online learning, administration and research. A cyberattacks can disrupt these systems, delay academic schedules, and erode trust between students and stakeholders.

- Compliance with regulations

Many countries, including Sri Lanka, have data protection laws that require organizations to protect sensitive information. Failure to comply with these regulations can lead to legal consequences and financial penalties.

- Preserving reputation

Educational institutions thrive on trust. A cybersecurity breach can damage an institution’s reputation, making it difficult to attract students, faculty, and funding.

- Preventing financial losses

The costs associated with recovering from a cyber-attack include compensation, system restoration, legal fees, and possible fines. Preventive measures are often more effective than recovering after an attack. (salvinge, 2024)

IT security consists of two areas

1. **Physical Security**

Physical security is the safeguarding of people, hardware, software, network information, and data from physical acts, invasions, and other events that might harm an organization or its assets. Protecting a business's physical security entails safeguarding it against threat actors as well as accidents and natural catastrophes such as fires, floods, earthquakes, and extreme weather. Physical security risks destroying servers, devices, and utilities that enable company operations and procedures. Having said that, humans are a significant aspect of the physical security threat.

2. **Information Security**

InfoSec is another term for information security. It encompasses techniques for managing the procedures, technologies, and regulations that safeguard both digital and no digital assets. When implemented properly, information security may improve an organization's capacity to avoid, detect, and respond to threats. (Anon., 2021)

Types of Security Risks to Colombo Advanced College and Similar Organizations

✓ **Malware**

Malicious software, encompassing ransomware, spyware, and viruses, falls under the category of malware. A mere click by an unsuspecting user can result in the installation of harmful software on the system. Malware can disrupt network access, pilfer data via spyware, and render the system non-functional. (Anon., 2021)

I. Ransomware

This is a type of malicious software (malware) that blocks or encrypts your files or computer system, making them inaccessible. The attackers then demand payment (a ransom) in exchange for restoring access. It can cause serious disruption, especially in organizations, by targeting important data and systems.

II. Spyware

It is a type of malware designed to surreptitiously monitor and collect information about your online activities, such as your browsing habits, passwords, or personal data, without your knowledge? This stolen information is often sent to third parties or used for malicious purposes, such as identity theft.

III. Viruses

These are malicious programs that attach themselves to legitimate files or programs and spread when those files or programs are opened or executed. They can damage or delete data, slow down systems, and disrupt operations. Viruses can spread rapidly across networks, posing a significant threat to individuals and higher education institutions.

- ✓ **Data Breaches**

Data breaches are one of the biggest security concerns for educational institutions like Colombo Advanced College. They can seriously damage an institution's reputation, disrupt academic and administrative operations, and compromise sensitive information, including student and staff data. The individuals or entities responsible for these attacks are called threat actors, which can include unidentified external attackers or malicious insiders.

- ✓ **Anonymous attacker**

Anonymous attackers are external individuals who can exploit vulnerabilities in university systems. They can obtain login credentials through phishing or other illegal means and bypass user account protection. Using advanced techniques such as software exploits, they can infiltrate the university network, especially when public or unsecured Wi-Fi connections are involved.

- ✓ **Data Leaks**

Data breaches pose a significant security threat to Colombo Advanced College. They often come from people you trust, including current or former staff members and trusted partners. These individuals may abuse their access to compromise IT assets, exfiltration sensitive academic or administrative data, or introduce malware into the university network. Common methods include the use of unauthorized USB storage devices or the exploitation of poor internal security practices, which can cause significant damage to an institution's reputation and operations.

- ✓ **Misconfiguration**

One of the most common cloud security vulnerabilities is misconfiguration, which can lead to significant data exposure in the cloud. Inadequate employee training and awareness of cloud security contribute to these misconfigurations. Encrypting data during network transfers is essential to prevent man-in-the-middle attacks. These are potential risks that can affect Colombo Advanced College's cloud computing solution.

- ✓ **Phishing Attacks**

Phishing attacks are a type of cyberattacks in which attackers pose as a legitimate organization or person to trick individuals into providing sensitive information such as usernames, passwords, or financial information. These attacks often occur through fake emails, text messages, or seemingly trustworthy websites, tricking the victim into clicking on malicious links or attachments. Once the victim provides their information, the attacker can use it for fraud, identity theft, or other malicious purposes. (Anon., 2024)

- ✓ **Unauthorized Access**

Unauthorized access is the act of accessing a system, network or data without authorization. It happens when an individual bypasses security measures, such as passwords, encryption or access controls, to access sensitive information or resources. This can happen through hacking, exploiting vulnerabilities or other means and can result in the theft, manipulation or damage of system data. Unauthorized access is illegal and poses significant security risks to organizations and individuals.

- ✓ **Outdated Systems and Software**

Outdated software and systems are technologies that are no longer regularly updated or supported by the manufacturer or developer. This includes devices, applications, and operating systems that lack the necessary security updates or patches for vulnerabilities. Outdated software and computer systems are more

vulnerable to cyberattacks because hackers can exploit known vulnerabilities that have not been patched. Additionally, using outdated software makes it more difficult to add new features, improve existing features, or comply with security regulations.

- ✓ **Weak Passwords and User Errors**

  Weak passwords and user errors refer to situations in which individuals use easily guessed or inappropriate passwords, such as simple words, short phrases, or common patterns, which allow attackers to more easily gain unauthorized access. User errors occur when people make mistakes, such as forgetting to log out of their accounts, clicking on phishing links, or misusing their login credentials. These factors can compromise security and increase the risk of unauthorized access to sensitive information or systems.

- ✓ **Distributed Denial of Service (DDoS) attacks.**

  A denial of service (DDoS) attack is a cyberattacks in which multiple compromised systems are used to flood a target system, such as a website or server, with excessive traffic, overwhelming it and making it unavailable to users.

- ✓ **Data Loss or Theft**

  Data loss or theft refers to the unauthorized deletion, destruction, or loss of sensitive information, whether through accidental means or intentional theft. This can occur when data is stored incorrectly, lost due to system crashes, or stolen by cybercriminals through hacking, phishing, or physical theft of devices. Data theft generally involves unauthorized access to confidential information, which can be used for malicious purposes, such as identity theft, financial fraud, or corporate espionage. Data loss can also result from poor data management practices or inadequate security measures.

- ✓ **Inadequate backup systems**

  Inadequate backup systems refer to the absence or weakness of adequate measures to regularly and securely back up critical data. When backup systems are inadequate, they may fail to provide reliable recovery options in the event of data loss, system failure, or cyber-attacks. This may be due to insufficient backup frequency, lack of secure storage, or failure to test backup restoration processes. Without robust backup systems, an organization risks losing valuable data forever, which can lead to operational disruptions and significant financial and reputational damage.

Physical Security Risks

- ✓ **Natural Hazards**

Colombo Advanced College's urban and coastal location exposes it to natural disasters such as floods, earthquakes, and tsunamis, which could cause significant physical damage to the college's infrastructure and completely disrupt its systems. While these events cannot be prevented, mitigation measures, such as robust disaster recovery planning, off-site backups, and reinforced physical structures, can help protect the college and minimize their impact on academic and administrative operations.

- ✓ **Theft of Data or Equipment**

This refers to either unauthorized entry or the improper utilization of files, leading to the sharing or copying of files without consent, or the theft of computing devices that store the data.

- ✓ **Malicious Damage or Loss of Sensitive Items**

This type of physical security threat occurs when an individual gains unauthorized access to sensitive items, such as confidential academic records, research data, or administrative documents. The individual might create duplicates of these items and distribute them without authorization or destroy the originals. Both scenarios pose a serious risk to the college's operations, as they compromise sensitive information, potentially exposing it to unauthorized parties and causing reputational and operational harm.

Current security mechanisms used by Colombo Advanced College

1. Firewall

- ☐ Implemented to monitor and control incoming and outgoing network traffic.
- ☐ Protects the university network from unauthorized access and external threats.

2. Antivirus and endpoint protection

- ☐ Ensures that all equipment, including laboratory and administrative computers, is protected from malware, viruses, and ransomware.
- ☐ Regular updates are implemented to combat new threats.

3. Data Encryption

- ☐ Sensitive data, such as student records and administrative documents, are encrypted both in transit and at rest to prevent unauthorized access.

4. Access Control Systems

- ☐ Role-Based Access Controls (RBAC) restrict access to critical systems and databases based on user roles and responsibilities.
- ☐ Multi-factor authentication (MFA) is used for critical systems to improve access security.

5. Monitoring Network

- ☐ Continually monitor network traffic to detect and respond to unusual activity or potential breaches.
- ☐ Use intrusion detection systems (IDS) to alert administrators of potential threats.

6. Secure Email Gateway

- ☐ Protects against phishing attacks and malicious email content by filtering and blocking malicious emails.

7. Backup and Disaster Recovery

- ☐ Regular data backups are performed and stored in secure locations to ensure data recovery in the event of a cyberattacks or system failure.
- ☐ A disaster recovery plan is in place to quickly restore operations.

8. Physical Security

- ☐ Secure access to server rooms and IT infrastructure using smart card systems or biometric authentication.
- ☐ CCTV cameras installed in critical areas for surveillance.

9. Regular security audits and penetration testing

- ☐ Periodic reviews of security measures to identify vulnerabilities and proactively address them.
- ☐ External penetration testing is conducted to simulate attacks and improve defences.

10. User Awareness Training

- ☐ Faculty, staff and students are trained in cybersecurity best practices to prevent social engineering attacks and accidental data breaches.

SECURITY PROCEDURE

What is Security Procedure?

A security procedure is a predefined and systematic series of actions aimed at carrying out a particular security task or objective. These procedures are typically structured as a step-by-step process, ensuring a consistent and repetitive approach to achieving a specific outcome. (Hathaliya, 2020)

1. Security Audit

A security audit entails a thorough evaluation of your organization's information system, typically gauging its security levels against an audit checklist that includes industry best practices, externally defined standards, or government regulations. (Martin, 2022)

How It Works?

A security audit functions by examining whether your organization's information system complies with a set of either internal or external regulations related to data security. Internal criteria encompass your college IT policies, procedures, and security controls, while external criteria involve federal regulations like HIPAA and SOX, along with standards from ISO and NIST. During a security audit, a comparison is made between your college's real-world IT practices and the applicable standards, pinpointing areas that require improvement and remediation.

To guarantee the protection of student data, meet federal mandates, and prevent potential fines, including Colombo advanced college, must conduct regular security assessments. Staying compliant with ever-changing federal regulations such as HIPAA and SOX is imperative to avoid penalties. Therefore, Colombo advanced college must conduct periodic security audits to stay updated on any emerging standards and ensure the company's adherence to them. (Sahoo, 2024)

2. Penetration Testing

A penetration test, often referred to as a pen test, is a sanctioned, simulated assault conducted on a computer system to assess its security. Penetration testers employ the same tools, tactics, and procedures as potential attackers to identify and illustrate the business ramifications of system vulnerabilities. These tests typically replicate a range of potential attacks that could pose a risk to a business. They evaluate the system's ability to withstand attacks from both authorized and unauthorized sources, as well as across various system roles. When appropriately scoped, a pen test can thoroughly investigate any facet of a system. (content79qw, 2024)

How It Works?

Penetration testers employ tools, strategies, and methodologies akin to those used by attackers to pinpoint vulnerabilities and weak spots within a college network. Consequently, conducting penetration testing aids in the identification of vulnerabilities and loopholes in network security, facilitating the enhancement of network security measures, and safeguarding data against unknown attackers.

Here are some pen test tools:

- Metsasploit
- Aircrack
- NMAP
- WireShark

College can use test access without security measures and comply with laws such as PCI DSS, HIPAA, and GDPR. Penetration tests rediscover vulnerabilities in previous security systems, such as electronic devices, configuration and coding standards, architectural analysis, and vulnerability testing. Through these actions, college can improve their security by detecting known and undetected software vulnerabilities. Penetration Te sting can simulate attacks against multiple systems, following the tactics used by most criminals. By doing this, it allows college to detect and prevent threats, ultimately protecting them.

3. Risk Management

Risk management involves the systematic procedure of recognizing and evaluating potential risks, along with developing strategies to mitigate or govern these risks and their potential consequences for an organization. Risks encompass the possibility of experiencing losses or harm and can originate from various sources, including legal responsibilities, natural calamities, unforeseen events, managerial oversights, or cybersecurity vulnerabilities. (Gibson, 2023)

Steps in risk assessment procedure

I. Risk Identification

Identify and explain potential risks that could affect Colombo Advanced College. These risks can include financial challenges, operational disruptions (such as issues with IT systems or supply chains), project-related obstacles, uncertainties in institutional planning, and external market threats. Document these risks

systematically, either in a risk register or through appropriate documentation methods, to ensure proactive management and mitigation.

II. Risk Analysis

Analyze the risk factors and record potential effects to determine the likelihood that a new danger will occur.

III. Risk Assessment and Evaluation

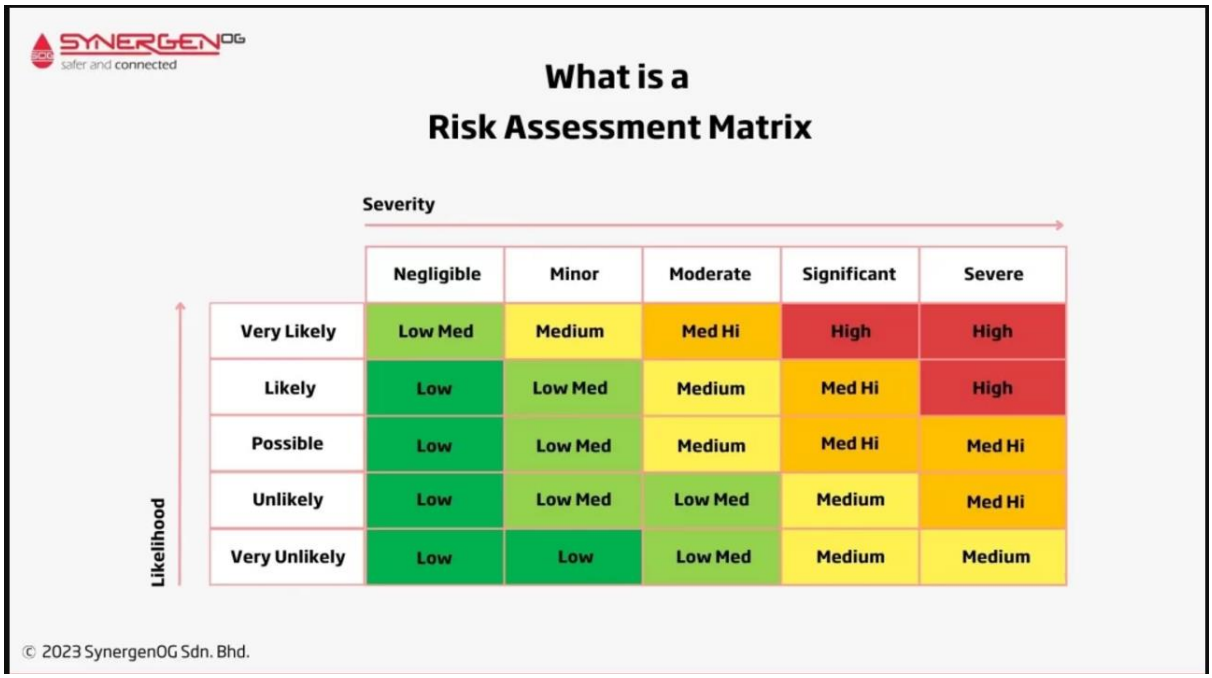
Determine the size of a risk through internal audits and risk assessments. Additionally, you must evaluate what amount of risk is acceptable and what requires quick attention.

IV. Risk Mitigation

You can move forward with a risk response strategy to reduce or control the risk once you've established the importance and priority of the issue.

V. Risk Monitoring

Risks and metrics must be regularly tracked to ensure that risk mitigation strategies are effective or to alert you if a risk grows to be a greater danger.



The risk matrix approach

Objective

Identify, assess, prioritize and mitigate IT security risks at Colombo Advanced College using a risk matrix.

I. Risk Identification

The first step is to catalo all potential IT security risks. These may include

- ❖ Ransomware attacks
- ❖ Phishing attempts
- ❖ Unauthorized access
- ❖ Data breaches
- ❖ System downtime due to outdated software or hardware

II. Create a risk matrix

A risk matrix is used to classify and prioritize risks based on two factors

1. Probability: The likelihood that a risk will occur (e.g., rare, unlikely, possible, likely, almost certain).

2. Impact: The severity of the consequences if the risk materializes (e.g., trivial, minor, moderate, major, catastrophic).

Risk levels

- Low (green)
  Monitoring required; minimal intervention required.
- Medium (yellow)
  Action required; addressed within a reasonable time.
- High (red)
  Requires immediate action to mitigate the risk.

III. Analyze and prioritize risks

- **Assess likelihood**
  Use historical data, threat intelligence reports, and system vulnerability scans.
- **Assess impact**
  Determine how each risk affects critical systems, data integrity, confidentiality, and availability.
- **Assign risk levels**
  Place each risk on the matrix to prioritize actions.

IV. Develop a treatment plan

For each identified risk, assign a treatment strategy based on its priority

- Avoid
  Eliminate activities or processes that lead to high-risk scenarios (e.g., stopping unsupported software).

- Mitigation
  Implement controls to reduce the likelihood or impact (e.g., implementing multi-factor authentication).

- Outsourcing
  Risks associated with outsourcing through insurance or third-party agreements (e.g., data retention with a secure provider).

- Recognition
  For low-priority risks, recognize and monitor without active intervention.

VI. Monitor and Reassess

- Continuously monitor risks using automated tools, such as security information and event management (SIEM).
- Perform regular audits and risk assessments. Update the risk matrix as new threats emerge or systems change. (deRitis, 2022)

Risk Matrix for Colombo Advanced College

Risk	Likelihood	Impact	Priority	Treatment Plan
Ransomware Attack	Likely	Catastrophic	High	Implement endpoint protection, staff training, and regular backups.
Phishing Attempt	Almost Certain	Major	High	Deploy email filtering, MFA, and awareness campaigns.

Unauthorized Access	Possible	Moderate	Medium	Use access control systems and conduct regular privilege reviews.
System Downtime	Likely	Moderate	High	Upgrade hardware and establish a disaster recovery plan.

The security challenges described above highlight several vulnerabilities at Colombo Advanced College.

- **Lack of proactive measures**

Firewalls and antivirus software are essential for network security, but if they are not updated regularly, they can be ineffective against new and evolving threats. Without proactive updates and monitoring, attackers can exploit known vulnerabilities to gain unauthorized access or deploy malware. The lack of a formal incident response plan can leave an organization unprepared for security breaches or emergencies. In the event of a cyberattacks or system compromise, lack of preparation can result in longer recovery times, greater data loss, and greater damage to operations and reputation.

- **Inadequate access controls**

Multi-factor authentication (MFA) and proper segmentation of user roles are essential for securing sensitive data and systems. Without MFA, users who rely on a single password are at greater risk of having their accounts compromised. Similarly, the lack of role-based access controls increases the risk of unauthorized users accessing sensitive resources or information that they should not be able to see or modify.

- **Vulnerable labs**

Shared resources, especially in computer labs, are vulnerable to unauthorized installation, access, and data theft. Without strict access control measures, users can install malware or change system settings. This makes the network more vulnerable to attack and compromises the integrity of academic and administrative data stored on these systems.

- **Weak backup systems**

In the event of data loss due to cyberattacks, hardware failure, or accidental deletion, robust backup systems are essential for rapid recovery. Outdated or inadequate backup protocols, such as infrequent backups or a lack of secure backups, can delay recovery times and result in permanent data loss. The lack of reliable backups compounds the consequences of a security incident and can seriously disrupt operations, especially for academic institutions where data integrity is paramount.

Addressing these issues requires regular updates to security software, implementing multi-factor authentication, implementing appropriate access control policies, securing shared lab resources, and ensuring stable and reliable backup systems. To ensure the safety and continuity of operations.

Network Monitoring Tools for the Colombo advanced college

Monitoring a computer network continuously for errors or flaws to maintain network performance is known as network monitoring, which is also sometimes referred to as network management. Although the two concepts are identical in practice, network monitoring can be thought of as a subset of network management technically. A network's endpoints, such as servers and workstations, as well as routers, switches, firewalls, load balancers, and other devices, are all included in the data that network monitoring gathers and reports on. The gathered information is filtered and examined to spot various network issues.

Benefits of Network Monitoring Tools

Real-time threat detection

Network monitoring systems can immediately detect unusual activity or traffic patterns, helping to identify threats such as ransomware or malware attacks before they become serious. Early detection reduces the risk of a large-scale breach.

Early detection and mitigation of security risks

Network monitoring tools can help businesses quickly detect and manage security risks. These technologies monitor network activity and can detect suspicious or unauthorized activity. Network administrators can act quickly to resolve any security issues by alerting them. Early detection and action can reduce the effects of a breach and help prevent cyberattacks.

Improved response time

With real-time alerts and notifications, security teams can act quickly to mitigate threats, minimize damage, and prevent incidents from spreading. This leads to faster resolution of security incidents.

Detailed reporting

Network monitoring systems record all activities, providing comprehensive data that can be analyzed for insights during investigations or audits. These logs are useful for identifying vulnerabilities and understanding the purpose of security events.

Mitigating Insider Threats

By monitoring user behaviour on the network, the system can detect any suspicious insider activity, such as unauthorized access to sensitive data, helping to prevent data breaches or sabotage within the organization.

Improved Compliance

Many regulatory standards (e.g., ISO/IEC 27001) require organizations to maintain an audit trail of their network activities. Network monitoring systems help meet these requirements by ensuring that all activities are recorded and accessible for compliance purposes.

Proactive problem identification

Network monitoring systems can identify potential problems, such as server overloads, network congestion, or hardware failures, before they cause system downtime. This proactive approach ensures smoother operations and avoids downtime.

Faster problem resolution

When network problems occur, monitoring systems provide detailed diagnostics, helping IT teams quickly identify the root cause and resolve issues more effectively. This helps reduce downtime and improve service continuity.

Managing Growing Networks

As collage expand their networks, they become more difficult to manage and secure. Network monitoring systems provide the visibility needed to monitor the performance and security of new devices, applications, and services, ensuring they are seamlessly integrated into the network.

Improved Network Performance

The potential of network monitoring tools to improve network performance is one of their most significant benefits. These tools monitor network traffic and identify any bottlenecks or performance issues that can then be resolved to enhance network performance. By identifying and resolving performance issues, network monitoring tools can help to ensure that the network operates at its peak efficiency and reduce the likelihood of downtime.

Increase Resource Efficiency

Tools for network monitoring can help businesses use their resources more effectively. By analyzing network traffic and identifying patterns in resource usage, these technologies can help businesses optimize their network resources to ensure they are being used effectively. This optimization can aid in reducing unnecessary spending. (Mather, 2022)

Importance of network monitoring

- Cost savings are gained by minimizing downtime and accelerating repair by aiding with root cause investigation or showing network parts that are over- or underutilized. Instead of continually seeking for faults, network resources may be focused on beneficial projects.

- Performance issues can be identified before they disrupt business operations or harm the customer experience.
- Network security may be improved by identifying unusual traffic or unfamiliar devices connecting to the network. These might be early warning signs of a cyberattackor ransomware attempt
- Early detection of use spikes such as login storms or seasonal traffic surges allows network managers to take corrective measures to ensure that consumption is not harmed.
- Rogue program use can be detected. Each unit may wish to follow a certain set of apps, and network monitoring can determine which programs and users are doing what on the network. (Mather, 2022)

Some Network Monitoring Tools

1. **Solar Winds Network Performance Monitor**

SolarWinds Network Performance Monitor is a comprehensive network performance monitoring solution that uses SNMP to monitor device status. It has the ability to automatically find network devices linked to your network. Utilize the dashboard to keep a close eye on the performance and availability of all connected network devices.

Key Features:

- SNMP monitoring
- Intelligent network maps with Net Path
- Automatically discovers connected network devices
- Create Wi-Fi heat maps
- Network packet analysis
- Alerts system
- Report System

2. **Auvik**

Auvik is a cloud-based network monitoring system that incorporates a number of system management features. When you open an account and access the package through a Web browser, the installation process begins on your computer. The Auvik program can oversee and centralize the monitoring of numerous sites. The suite is therefore perfect for WAN monitoring. A network discovery procedure is the first step in the service offered by Auvik. This automatically fills in all of the fundamental data required for the monitor to function. The ongoing discovery service will detect when new devices are connected to the network.

Key Features:

- Automated setup
- Network mapping
- Configuration management
- Resource utilization alerts

Security Counter measures

Virtual Private Network (VPN)

Virtual private network is referred to as VPN. Through the use of a virtual private network (VPN), a secure and encrypted connection can be established over a less secure network, such the internet.

A virtual private network (VPN) uses a public network, such the internet, to extend a private network. The name solely alludes to the fact that it is a virtual "private network," meaning that a user can join a local network while seated at a distance. To provide a secure connection, it employs tunnelling technologies. (Geeksforgeeks, n.d.)

Your IP address is hidden by a VPN by passing it through a remote server that has been set up specifically for that purpose and is managed by the VPN host. Thus, if you use a VPN to access the internet, the VPN server is inferred to be the data source. This implies that neither your ISP nor other outside parties can see the websites you visit or the information you send and receive online. Your data is filtered by a VPN,

which changes it all to "gibberish." Even if someone managed to get their hands on your data, it would be useless.

VPN Types

I. Site-to-Site VPN

A site-to-site VPN connects two or more networks together over the internet. This type of VPN is **often used by companies with multiple locations.** (Anon., 2023)

Benefits of Site-to-Site VPN to Colombo advanced college

- Site-to-Site VPNs create secure connections over the public internet by creating tunnels between various locations. It preserves secrecy and guards against unauthorized access to sensitive data.
- Site-to-Site VPNs make use of the current internet infrastructure, doing away with the requirement for specialized leased lines or pricey gear. They are thus an affordable option for tying together several sites.
- Site-to-Site VPNs are scalable, enabling collage to quickly add or remove locations as their network requirements change. It offers flexibility for college whose activities change over time or whose customer base grows.
- Site-to-Site VPNs allow remote access to programs and resources on various sites. Remote workers can safely connect to the corporate network, increasing productivity and teamwork.

II. Remote Access VPN

Users can connect to a private network from a distance using a remote access VPN. Staff that need to access corporate resources from a remote location frequently utilize this kind of VPN. (Anon., 2023)

Benefits of Remote Access VPN to Colombo advanced collage

- Employees can securely connect to the college network from off-site locations with the help of remote access VPNs. It encrypts the connection to safeguard privacy and safeguard critical information.
- Employee mobility is increased via remote access VPNs, which also boost productivity. They get access to college resources, software, and information just as they were there in person.
- Remote Access VPNs make use of the existing internet infrastructure, therefore they don't require specific remote access solutions. They are therefore a sensible choice for college with telecommuting or remote workers.
- Remote Access VPNs are extremely simple to set up and operate, especially with user-friendly client software. Access policies, user authentication, and security controls can all be centrally managed by IT administrators.

Firewall

A firewall is a network security tool that guards against unwanted network access. To find and stop threats, it examines incoming and outgoing communications using a set of security rules. Physical hardware, digital software, software as a service (SaaS), and virtual private clouds can all be used as firewalls. Both private and professional environments employ firewalls, and many devices—including Mac, Windows, and Linux computers—have one built in as standard equipment. They are frequently regarded as a crucial element of network security.

How firewall works?

To prevent attacks, firewalls thoroughly examine incoming traffic based on pre-defined criteria and filter traffic coming from unprotected or suspect sources. Firewalls protect traffic at a computer's entrance point, known as ports, where data is exchanged with external devices. Consider IP addresses to be homes, and port numbers to be rooms within the house. Only trustworthy persons (source addresses) are permitted to enter the home (destination address), and those within the house are only allowed to access particular rooms (destination ports), depending on whether they are the owner, a child, or a visitor. The owner has access to any room (any port), whereas children and visitors have access to a limited number of rooms (particular ports).

Types of firewalls

Type of firewall		Advantages	Disadvantages
Packet filtering firewalls	Inline packet filtering firewalls operate at junction points where equipment such as routers and Switches. These firewalls, however, do not route packets; instead, they Evaluate each packet received to a set of predefined criteria, such as the authorized IP addresses,	Because they analyze network packets at the IP and port levels, packet filtering Firewalls are simple and efficient. They have minimal latency and may be used on both hardware and Software firewalls. They are also inexpensive.	Because these firewalls lack deep inspection capabilities, they are vulnerable to sophisticated attacks that hide dangerous material within seemingly innocent packets. They may also Offer limited support for complicated protocols and may not provide strong user authentication.
Circuit-level gateway	Circuit-level gateways monitor TCP handshakes and other network protocol session initiation Messages as they are established across the network between the local and remote hosts to determine whether the session being initiated is legitimate – whether the remote system is considered trusted. They do not, however, check the packets	By monitoring TCP handshakes, circuit-level gateways provide a better level of security than packet filtering. They are simple to set up and might be useful for managing outbound connections.	They have limited application-layer inspection capabilities, making them unsuitable for comprehensive threat detection. Circuit-level gateways also have difficulty with protocols that employ dynamic port assignments and are unable to guard against application-specific vulnerabilities.
Gateway at the application level	This type of device, which is technically a proxy and is sometimes known as a proxy firewall, serves as the network's only entrance and exit point. Application-level gateways filter packets not just by the service for which they are intended (as stated by the destination port), but also	Deep packet inspection and content filtering are provided by application-level gateways, often known as proxy firewalls. They can impose stringent application-specific restrictions, hence increasing security. They also serve as	Because of the additional processing required for content inspection, these firewalls might increase delay. Scalability might be a difficulty, as not all applications and protocols are supported. It might be difficult to configure and manage them.

	by other criteria such as the HTTP request string. While gateways that filter at the application layer provide Significant data protection, they can have a significant impact on network speed and can be difficult to operate.	middlemen, concealing internal network information.	
Stateful inspection firewall	State-aware devices not only evaluate each packet, but also keep track of whether or not it is part of an existing TCP or other network session. This provides stronger security than either packet filtering or circuit monitoring alone, but at a higher cost to network performance. The multilayer inspection firewall is another version of stately inspection that considers the flow of transactions in progress across several protocol layers of the seven-layer Open Systems Interconnection (OSI) architecture	The benefits of packet filtering and application-level gateways are combined in stateful inspection firewalls. They keep track of the state of active connections, allowing for better security policy enforcement and performance.	While they are more sophisticated than packet filters, they may still be vulnerable to application-layer assaults. They can be resource-intensive, affecting network performance, and may necessitate more complicated configuration
Virtual firewall	To monitor and secure traffic across physical and virtual networks, a virtual firewall is typically deployed as a virtual appliance in a private cloud (VMware ESXi, Microsoft Hyper-V, and KVM) or public cloud (Amazon Web Services or AWS, Microsoft Azure, Google Cloud Platform or GCP, Oracle Cloud Infrastructure or OCI). A	Because virtual firewalls are versatile and adaptable, they are ideal for virtualized and cloud settings. They are simple to deploy and maintain using software interfaces, and they can adapt to changing network circumstances	They rely on the underlying virtualization infrastructure and might be vulnerable if not sufficiently protected. In high-traffic virtual environments, performance might be an issue.

	virtual firewall is frequently used in software-defined networks (SDN).		
Cloud-based Firewall	Cloud native firewalls are updating the way apps and workload infrastructure are secured at scale. Cloud native firewalls, with their automatic scaling features, allow networking and security operations teams to operate at breakneck speed. The Benefits of Cloud Native Firewalls are Security that is adaptable and elastic, Capability to serve many tenants and intelligent load balancing.	Because cloud-based firewalls provide centralized control and are available from anywhere, they are ideal for scattered and remote settings. They can enable quick scalability and benefit from the security knowledge of cloud providers.	Relying on internet access might be risky since outages can impair firewall functionality. When employing third-party cloud-based solutions, data privacy and compliance risks may arise. Configuration complexity and pricing might differ between suppliers.

Few common firewall configuration mistakes you need to avoid.

- ⊕ **Failure to establish rules**

The first, and most simple, error is just starting your firewall without modifying any of the default settings. In many circumstances, these defaults will be set to 'any to any' status, enabling traffic to arrive and depart from any source or destination. It is normal for security teams to start with open access while assessing the system's needs and tightening them up as they go, but neglecting to apply. Restrictions to 'any to any' communication can leave firms extremely susceptible to attack.

- ⊕ **No updating rules on a regular basis**

Once you have regulations in place, they must be evaluated on a regular basis to ensure they are up to current and still serve their purpose. Keeping an eye on this is critical to the efficient operation of your network, since as organizations develop and new regulations are implemented, they may efficiency and should always be considered in maintenance planning. However, if any changes are begin to overlap or even become contradictory. Duplicate rule deletion increases performance and required to solve such concerns, it is critical that they are implemented consistently across the network to avoid any sections becoming obsolete. Set up a clear plan for network assessments and be proactive about implementing adjustments to solve this.

- ⊕ **Ignoring cloud traffic**

The days of the firewall defining a defined network boundaries are past. In today's increasingly cloud-based security environment, where many more users and apps connect remotely, a defence- in-depth

strategy in which the firewall is only one component of a hybrid security system should be the standard. However, if your firewall setup is still built on old-school, on-premise ways, it can harm productivity for individuals who rely on cloud services while also putting you at danger.

- **Opening up your access controls too much**

The way you establish roles for different users is crucial in keeping your network safe, and the general guideline is that you should only give someone the access they need to complete their job. However, many experts begin with open permissions and gradually restrict them as they understand more about the network's requirements. Inverting this technique, beginning with a zero-trust attitude and progressively increasing rights as needed, provides network managers with a considerably more secure option.

- **Unreliable authentication**

Large, wide networks with various sites are frequently more vulnerable to attack owing to discrepancies in their defenses, and one area that must be prioritized to minimize this is authentication. This can be a handy backdoor if some sites utilize router configurations that do not adhere to key requirements. As a result, it's critical to have a centralized authentication system in place and to verify that it's implemented uniformly across the network.

- **Misapplication of port forwarding rules**

Port forwarding rules for remote access to assets are critical nowadays, but if not correctly configured, they can be another simple route into a network. The simplest approach to permit remote access is to set up blanket restrictions, but this leaves an open door. Instead, to prevent leaving the door open for hackers, limit communication to specified ports or from whitelisted IP addresses. (Anon., 2024)

Benefits of Colombo advanced college

- Auditing and logging capabilities. Administrators can use the event logs kept by firewalls to spot patterns and enhance rule settings. Rules should be changed constantly to stay up with ever-evolving cybersecurity risks. As soon as new dangers are identified, vendors create updates to address them.

- Filtration of traffic. A firewall can filter traffic in a single home network and notify the user of intrusions. Since cable modems and other always-on connections use static IP addresses, they are particularly helpful in these situations. A firewall makes sure that only intended and harmless internet content gets through.

- Restricting and preventing access. In order to prevent illegal use, firewalls can be used to restrict and deny access to specific websites and online services. For instance, a firm can install a

firewall to prevent access to problematic websites, ensuring that staff follow corporate guidelines when using the internet.

- Remote access with security. Through the deployment of a virtual private network (VPN) or other secure remote access technology, firewalls can enable secure remote access to a network.

Impact of improper configurations of VPN, Firewall and how it will affect to Colombo advanced college

Colombo Advanced College, an educational institute specializing in information security and data management, can face significant challenges due to inadequate VPN (Virtual Private Network) configurations and firewalls. Setting up a VPN is essential to establish a secure connection between the Colombo Advanced College network and remote users or devices. However, improper VPN configuration can expose the institution's network to threats, such as data breaches and unauthorized access, which can lead to data loss and damage the institution's reputation. . Inadequate user authentication in VPN settings can create a vulnerable entry point for attackers. Likewise, firewalls, which serve as essential security measures to monitor incoming and outgoing network traffic, must be properly configured to ensure network protection. If firewall configurations are incorrect, they can leave the network vulnerable to data breaches, malware infections, and attacks. For example, weak firewall rules can allow hackers to enter the network, while overly strict configurations can block legitimate traffic and affect employee productivity.

Incorrect VPN configurations and firewall settings can pose significant risks to Colombo Advanced College, including loss of revenue, reputational damage, and legal and regulatory consequences. To protect against ever-evolving threats, it is imperative that Colombo Advanced College ensures proper installation and regular updates of its VPN and firewall. Establishing a secure, industry-standard business network may require investing in qualified IT professionals or establishing partnerships with reputable security vendors.

Briefing

Incorrectly configured VPN

A third-party VPN service, if configured incorrectly, can open backdoors in the network, allowing unauthorized access and exposing sensitive data. Weak authentication methods or inappropriate tunneling protocols can leave traffic vulnerable to interception. To mitigate this risk, it is important to use secure VPN protocols such as OpenVPN, implement strong multi-factor authentication (MFA), and ensure that appropriate configurations are applied to prevent leaks and unauthorized connections.

Firewall Policies

A poorly configured firewall rule can block legitimate traffic or allow unauthorized access, which can create security vulnerabilities. If a firewall rule allows all incoming traffic on a certain port, attackers can exploit this open port and gain unauthorized access to systems. To avoid it, it is essential to implement strict firewall rules based on the principle of least privilege, ensuring that only necessary traffic is allowed.

Importance of the DMZ, static IP and NAT in a Network

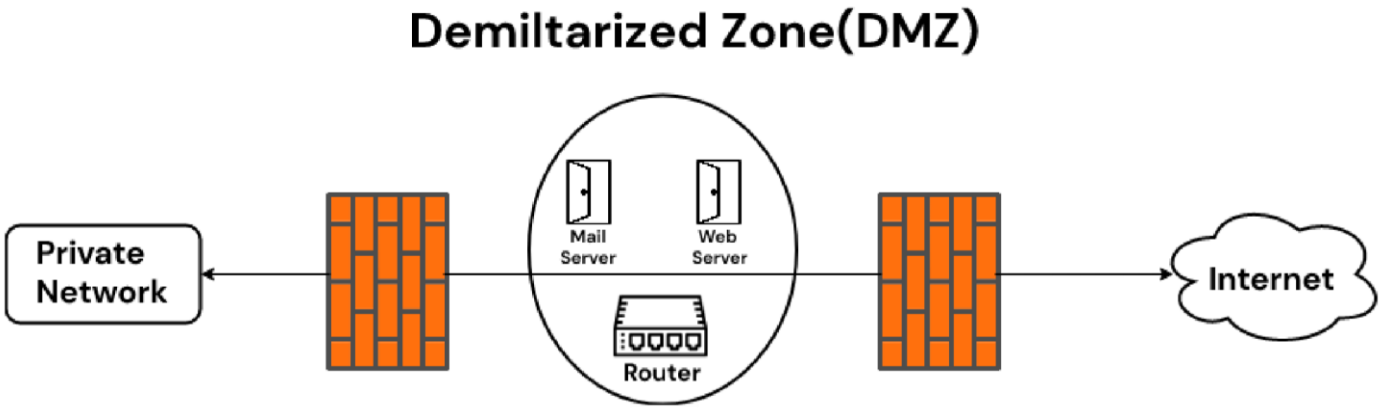
Demilitarized Zones

Cybersecurity makes use of demilitarized zones, or DMZs. DMZs are frequently seen on corporate networks and are used to divide internal networks from the internet. To protect a corporation against dangers from outside sources, a DMZ is often set up on the internal network of the college.

A DMZ can be a useful tool for network security, despite the word sounding unfavourable.
A company's private and public networks' trusted and untrusted networks are separated by the DMZ. The DMZ serves as a protective barrier that prevents outside users from accessing the organization's data.

Outside users and public networks send requests to DMZ to access a college 's data or website. The DMZ schedules sessions on the public network for this kind of request. It is unable to start a session on the exclusive network. Web pages in DMZ are corrupted if malicious activity is attempted there, but other data is secure.

The purpose of a DMZ is to give access to an untrusted network while maintaining the private network's security. Although using DMZ with a firewall is not required, it is a superior strategy.



Advantages and Disadvantages of DMZ

Advantages	Disadvantages
• By separating internet-facing services from the internal network, a DMZ improves network security. If the DMZ is penetrated, this separation reduces the chance of a direct assault on important internal resources.	• Creating and maintaining a DMZ may be difficult, particularly in big and dynamic networks. Configuring firewalls, access controls, and routing rules correctly necessitates experience.
• The DMZ can host Internet-facing services such as web servers, email servers, and DNS servers. If an attacker obtains access to these servers, their access to the internal network is limited, limiting the possible harm	• Managing servers and services in the DMZ increases administrative burden. To protect the security of the DMZ, regular updates, patches, and security settings must be maintained.
• Firewall rules and access policies may be used to closely manage access to the DMZ, allowing companies to determine which traffic is permitted and which is banned. This fine-grained management increases network security overall.	• Creating and maintaining a DMZ may be expensive. Organizations must invest in new hardware, like as firewalls and intrusion detection/prevention systems, as well as spend money for continuous maintenance.

• Only relevant ports and protocols are accessible to the internet when services are placed in the DMZ. This minimizes the attack surface and makes finding vulnerabilities more difficult for attackers. • It is simpler to monitor and log traffic entering and exiting the DMZ, which aids in the discovery of suspicious behavior and simplifies forensic investigation in the case of a security issue.	• If the DMZ infrastructure or security mechanisms are compromised, the DMZ can become a single point of failure, resulting in a security breach that affects both the DMZ and the internal network. • Depending on the network design and traffic volume, routing traffic through the DMZ may cause latency and performance bottlenecks, negatively harming the user experience for internet-facing services

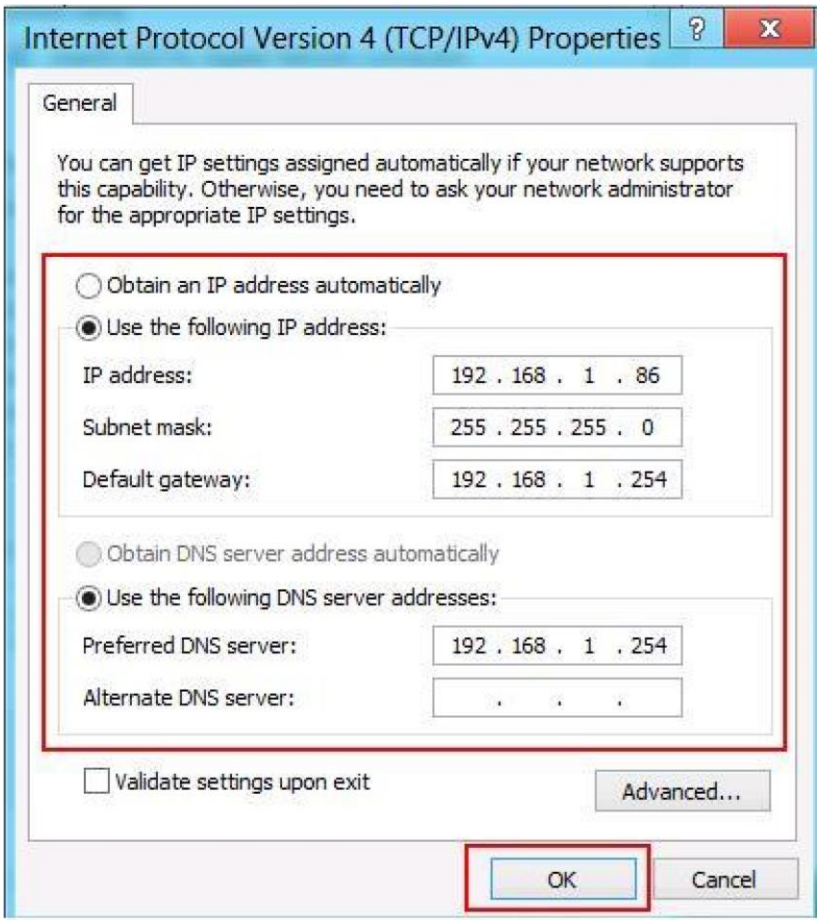
Uses to the Colombo advanced college and its students by using Demilitarized Zones

Demilitarized Zones (DMZs) are crucial for enhancing the security and functionality of Colombo advanced college and its students by using Demilitarized Zones. These DMZs serve as an essential security layer in the college network architecture. Colombo advanced college can separate and protect important assets and services via DMZs. They help to ensure that student-facing systems, such as online learning platforms and administrative portals, are protected against unauthorized internet access and cyberattacks.

Additionally, DMZs offer secure connections between the college's primary IT systems, data centers, and external systems while being protected by a single firewall. This not only enhances data security but also ensures reliable connectivity, allowing the college to continue providing uninterrupted services to students and staff. Simply put, DMZs serve as a strategic security architecture that strengthens the network, safeguarding sensitive academic and administrative data while maintaining student and staff trust in the face of evolving cybersecurity threats.

Static IP

A static IP address is a 32-bit number that serves as a computer's Internet address. This address is often given by an Internet Service Provider (ISP) and is displayed in dotted-quad format. Just as humans use phone numbers to connect to a phone, IP addresses act as distinctive identifiers for connected devices, enabling computers to identify and communicate with one another on the Internet. Additionally, information like the IP address, hosting company, and geography can be revealed. Static IP addresses are manually specified for a device and never change, in contrast to dynamic IP addresses, which are given by a DHCP server.



Advantage	Disadvantage
• The fundamental benefit of a static IP address is its consistency and stability. It stays the same, enabling remote management of services and access to devices easier	• Static IP addresses are frequently more expensive than dynamic IP addresses. • Configuring a static IP address might be more difficult, particularly for non-technical people. You must manually specify the IP address, subnet mask, gateway, and DNS servers.

• A static IP address makes remote access to a device or service easier. You always know where the gadget is. • It is required for the hosting of websites, email servers, and other internet services. It enables you to keep a constant online presence. • Because DNS records do not need to be updated as frequently with static IPs, some users may notice quicker DNS resolution. • Static IP addresses can improve security by enabling you to use more granular access control lists (ACLs) and firewalls. When the IP address does not change, it is easier to administer security policies.	• It is not ideal for equipment that must regularly switch between networks. Laptops and cellphones, for example, are frequently issued dynamic IP addresses to facilitate this mobility. • If your pool of accessible IP addresses is small, providing static IP addresses to all devices may result in wasteful resource allocation. • Because static IPs are fixed, if the address is known, they may be more vulnerable to targeted assaults. • Static IP addresses need regular maintenance and changes. If modifications are required, they must be manually setup, which might take time.

Uses to the Colombo advanced college and its students by using Static IP

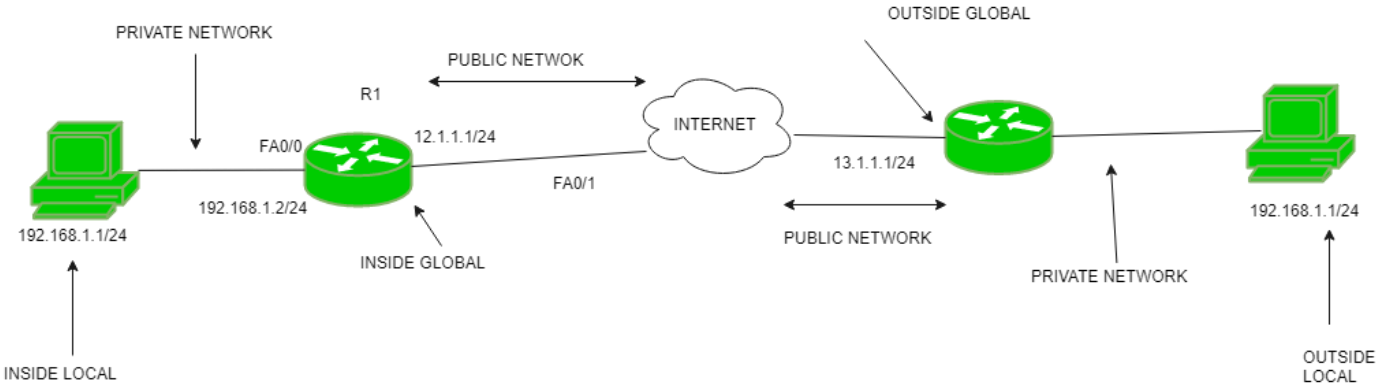
The adoption of static IP addresses by **Colombo Advanced College** provides numerous advantages for the institution and its stakeholders. The college's extensive network infrastructure, which includes data centres, departmental labs, and administrative offices, requires dependable connectivity, which static IPs ensure. Static IPs are highly beneficial for maintaining secure VPN and MPLS connections between these facilities, enhancing data security and reliability.

Static IPs also enable the college's core systems, such as the student information system, learning management system, and research databases, to communicate effectively with other internal systems and external academic or administrative partners. This supports the wide range of services provided by the college, including online classes, remote access to educational resources, and efficient administrative processes.

The college's ability to provide uninterrupted and secure educational and administrative services is strengthened by the reliability and consistency of static IP-based communication. The robust network infrastructure and secure communication channels ensure the confidentiality and accessibility of critical academic and administrative data, benefitting students, staff, and external collaborators.

Network Address Translation (NAT)

A public IP address is required to access the Internet, while a private network may use an IP address. Network Address Translation (NAT) is a technique that allows multiple devices on a private network to access the Internet from different IP addresses. This involves changing the local IP address to a global IP address and vice versa, enabling network connectivity to the local host. NAT also changes the port number by replacing the host's port number with another port number in the packet sent to the port. At the same time, the IP address and access code are recorded in the NAT message. NAT usually runs on a router or firewall. (Anon., 2021)



(Anon., 2018)

Types of NAT

1. Static NAT

This creates a one-to-one mapping between local and global addresses between a single unregistered (Private) IP address and a legally registered (Public) IP address. This is typically employed for hosting websites. These are not utilized in businesses since a public IP address is required to give Internet access for the numerous devices that require it. Assume that if there are 3000 devices that require Internet access, the company will need to purchase 3000 public addresses, which will be highly expensive.

2. Dynamic NAT

Rather of using the same IP address each time, this NAT cycles over a pool of public IP addresses. As a result, each time the router translates a local address to a public address, the router receives a

new address.

3. Port Address Translation

NAT overload is another name for this. This allows for the conversion of numerous local (private) IP addresses to a single registered IP address. To identify the traffic, or which traffic comes from which IP address, port numbers are employed. Since thousands of individuals can connect to the Internet using just one genuine global (public) IP address, this is the method that is most usually utilized.

Advantage	Disadvantage

• Multiple devices on a local network can share a single public IP address thanks to NAT. This preserves the small pool of usable IPv4 addresses, which were running out owing to the internet's fast development. • NAT functions as a firewall by concealing the internal IP addresses of local network devices from the public internet. This adds security since incoming internet traffic cannot directly access devices on the local network unless particular port forwarding rules are specified. • Organizations can employ private IP address ranges within their internal networks, which can be updated or modified without disrupting external connections, thanks to NAT. This adaptability makes network administration easier. • NAT devices may be set up to split incoming traffic among numerous internal servers, increasing service efficiency and availability. • NAT can be used as a bridge between IPv4 and IPv6, allowing IPv6-enabled devices to connect with the largely IPv4 internet.	• NAT adds complexity to network installations, especially when several internal devices must connect with external services. Managing NAT rules may be tricky, resulting in possible misconfigurations and troubleshooting issues. • Certain peer-to-peer apps and services can be hampered by NAT because it frequently makes it difficult for external devices to begin connections with devices on the local network. This has the potential to impact online gaming, video conferencing, and other applications. • NAT devices must process and translate network traffic, which adds latency and uses CPU resources. This can cause performance problems in high-traffic scenarios. • Scaling NAT can be difficult. The complexity of NAT installations and potential address conflicts can rise as more devices are added to a network. • Because it can interfere with the encapsulation and routing of VPN traffic, NAT can cause problems with some types of Virtual Private Networks (VPNs).

The benefits of Network Address Translation (NAT) for Colombo Advanced College and its stakeholders.

NAT serves as a vital security and routing function in the college's extensive network infrastructure. NAT helps the college protect public IP addresses by allowing multiple internal devices, such as departmental computers, lab systems, and administrative machines, to share a single public IP address. This approach not only increases network efficiency but also reduces operational costs.

NAT strengthens the college's defenses against potential external threats by hiding internal IP addresses from outsiders, adding an extra layer of security to its network. While accessing the college's resources, such as the learning management system, online class platforms, or administrative portals, students and staff benefit from the NAT-enabled secure and reliable connection, which ensures the protection of sensitive academic and personal data.

NAT is essential in maintaining the integrity and functionality of Colombo Advanced College's network, ultimately fostering a safe and efficient environment for learning and administration, while enhancing user satisfaction and trust in the college's digital systems.

Summary

- Ω DMZ (Demilitarized Zone): A DMZ is a network segment that separates services from the internal network. Public services such as web servers, mail servers, and DNS servers are placed in the DMZ so that even if these services are compromised, the internal network remains protected. In a university, hosting a website on a DMZ server prevents direct access to sensitive internal systems, such as student databases. This configuration reduces the risk of attackers gaining direct access to internal resources.
- Ω Static IP: A static IP address is a fixed, unchanging IP address assigned to a device. This simplifies the creation of precise security rules, such as firewall rules and access control lists (ACLs), since the device is always identified by the same IP address. In critical university systems, such as a student database, there may be a static IP address with access control rules configured to allow connections only to specific internal IP addresses, providing an additional layer of security protection against unauthorized access.
- Ω NAT (Network Address Translation): NAT is used to hide the internal IP addresses of a network so that they are not exposed to the outside world. This adds a layer of privacy and security by making it difficult for attackers to identify and target individual devices on the network. In a collage, when a student in a computer lab accesses a website, the internal IP of the lab computer is masked by the external IP of the router. This prevents attackers from directly targeting lab computers from the outside, reducing the risk of external threats.

IT SECURITY

IT security involves safeguarding information, particularly during its processing. The primary goal of IT security is to prevent unauthorized third parties from tampering with data and systems. Essentially, it aims to protect socio-technical systems, which encompass both people and technology within companies or organizations, as well as their data, from harm and potential threats. This protection extends not only to digital information and data but also encompasses the physical security of data centres and cloud services.

Information technology (IT) security pertains to the strategies, technologies, and personnel employed to safeguard an organization's digital resources. The primary objective of IT security is to shield these assets, which include devices and services, from potential disruptions, theft, or exploitation by unauthorized individuals, often referred to as threat actors. These threats can originate from both external and internal sources and may vary in nature, ranging from malicious actions to accidental incidents.

A robust security strategy employs various methods to reduce vulnerabilities and address diverse cyber threats. Detecting, preventing, and responding to security threats necessitates the implementation of security policies, software solutions, and IT services. (Anon., 2024)

Risk management to treat IT security risk

The statement highlights the importance of risk management for a higher education institution in Colombo. Anything that can threaten the business, whether physical or electronic, is a risk. These risks can have negative consequences, such as financial loss, damage to reputation or loss of student confidence.

It is necessary to use various strategies to eliminate or reduce risks. These risk treatments or strategies are at the heart of risk management at Colombo advanced College. Risk management is a set of measures taken to reduce risks and ensure that the college can continue to operate normally in the face of challenges.

Colombo Advanced College may face many threats, both physical and online. Physical hazards include workplace accidents that can result in property damage, property damage, or even death. A cyberattacks that results in data theft, ransomware, or other malicious activity, on the other hand, may be considered a virtual risk.

Various processes and treatments can be implemented to reduce these risks. When filing a property damage claim, you can reduce the risk of personal injury. Routine inspection procedures can be used to identify and resolve potential problems before they occur. By monitoring user activity, for example, by tracking the use of company devices by staff, cybersecurity threats can be mitigated. In addition, you can ensure that essential data is always available in the event of a system failure by implementing backup techniques.

These tactics help Colombo Advanced College manage and overcome risks. By using a comprehensive risk management plan, the organization can identify potential risks, assess their significance, and develop mitigation strategies. To reduce risks and ensure the long-term sustainability of the organization, every tertiary university in Colombo must take proactive measures.

Some Actions to Prevent the Physical, Virtual Risks

1. Educate Employees, student, staff about Cyber Attacks

Most employees and students and staff lack confidence in dealing with ransomware attacks. Every college member should possess a basic understanding of ransomware, including its common methods of propagation, signs of detection, and the appropriate contacts to reach out to. They should also be informed about how to respond if their actions inadvertently trigger a ransomware attack.

2. Update and patch operating systems and software

Attackers invest significant effort in identifying exploitable weaknesses, and IT professionals should take similar precautions to the malware and ransomware threats. While common vulnerabilities and exposures are regularly addressed, keeping systems updated and obtaining software updates from trusted sources can substantially mitigate exposure to vulnerabilities.

3. Implement a Firewall to Protect the System

A firewall serves as a protective barrier for your device against internet-based threats like data-driven malware. It manages the flow of data between your device and servers and routers in the online environment, continuously scrutinizing this data for potential risks. Through this process, it helps to the unauthorized remote access, data breaches, and similar security threats.

Accessing our network is a formidable task for hackers, as they must overcome the firewall. Using two different hardware firewalls within our network makes bypassing them nearly impossible.

4. Protecting Data from Theft

A good way to prevent data theft or the creation of sensitive data is to adopt a "clean desktop" policy. The policy requires employees to clear their desks at the end of each work day and store all information securely, reducing the amount of time-sensitive information left in a vulnerable location. It's also important to enable employees to manage sensitive data after use. Implementing access control is important to prevent unauthorized access to your site and prevent data theft.

5. Disaster Recovery Plan

A disaster recovery plan (DR) is a document that outlines clear procedures issued by the company to deal with unexpected events such as natural disasters, power outages, cyber-attacks, and other related events. It includes strategies to reduce the impact of a disaster and allow the organization to maintain normal operations or quickly restore critical operations.

6. Implement CCTV cameras and biometric devices

Biometric scanners capture personal biometric data to establish your identity, typically using fingerprints or other unique characteristics as access keys. These scans are cross-referenced with stored data in a database for verification, ensuring that only authorized individuals can access secured systems. Additionally, CCTV cameras not only oversee workplace activities but can also provide valuable evidence, collectively reinforcing our ability to ensure college security.

Several actions and techniques to reduce the risks of the Colombo advanced college faces in the physical and virtual world

Tools

1. Penetration Testing

A Penetration test (pen test) is an authorized simulated attack on a computer system to assess its security. In order to identify and illustrate the financial effects of a system's vulnerabilities, penetration testers employ the same tools, strategies, and procedures as attackers. The majority of assaults that potentially endanger an organization are often simulated during penetration examinations. They can assess a system's resilience to

attacks from legitimate and illegitimate places as well as from a variety of system functions. A pen test can probe any area of a system with the appropriate scope. (content79qw, 2024)

2. **Security Audit**

A Security audit is a thorough evaluation of your company's information system; often, this evaluation compares the security of your system to a checklist of industry best practices, externally imposed standards, or governmental legislation. (Martin, 2022)

3. **Risk Management**

Risk management is the process of identifying and evaluating hazards as well as developing a strategy to reduce or control such risks and their possible effects on a company. Risk is the possibility of suffering loss or harm. Legal responsibility, natural disasters, accidents, poor management, and cybersecurity threats are just a few of the sources of risk. (Gibson, 2023)

Some Security Measures Physical Risks

1. **Educate student, staff About Cyber Attacks**

Most student, staff are unclear about how to respond to ransomware assaults. Everyone must have a basic understanding of ransomware, including an understanding of how it normally spreads and how to spot the warning signs. If their actions result in the execution of ransomware, they must be informed of who to notify, any suspicions they may have, and what to do.

2. **Implement a Firewall to Protect the System**

Firewall serves as a barrier or shield to keep out internet-based virus threats that are data-based. Your device exchanges data with servers, routers, and other devices in cyberspace. These data are monitored by firewalls to determine whether they are secure. We can prevent data breaches, unauthorized remote access, and other issues because of this technique. In order to access our network, hackers must get past the firewall, which is difficult to do. It's also impossible if we utilize two distinct types of hardware firewalls to protect our network.

3. **Disaster Recovery Plan**

Disaster recovery (DR) plan is a formal document developed by an organization that provides step by-step instructions on how to handle unanticipated events like natural disasters, power outages, cyber-attacks, and other disruptive situations. The strategy includes tactics for reducing disaster consequences so that a business may carry on or quickly resume essential operations. (Yasar, 2024)

4. Implement CCTV cameras and biometric devices

Scanners that capture biometric information from your body are used to identify you. Your fingerprints or other unique features serve as entry points into the guarded system since scan results are compared to details stored in a database to ensure authenticity. Because CCTV cameras help to monitor workplace activities and can also be a source of pertinent evidence, unauthorized people are unable to access anything without authorization as a result. These factors allow us to ensure the security of the college.

5. Turn off the Drivers

Floppy disks, USB ports, and other methods of connecting external drives can be disabled or uninstalled if you don't want copying college data to removable media. Cutting the connections alone might not be sufficient to deter tech-savvy staff. Some organizations go so far as to cover ports with glue or other materials to permanently restrict their use, despite the fact that there are software ways that disallow it. If your computer still has floppy drives, you can lock out other diskettes by using a disk lock like the one from SecurityKit.com.

Some Security Measures for Virtual Risks

1. Update and Patch Operating Systems and Software

Attackers work hard to identify holes that can be exploited. To avoid malware and ransomware, IT professionals must follow similar security measures. Even though widespread flaws and exposures are frequently patched, updating systems and installing software from trustworthy sources can significantly lower vulnerability exposure.

2. Protecting Data from Theft

Implementing a "clear-desk" strategy is one of the best ways to stop document theft or accidental disclosure of sensitive information. Sensitive documents are less likely to be left in risky locations when a clear-desk

policy is in place, which requires that all desks be cleaned and all materials be put away at the end of each workday. Additionally, you must ensure that your staff members delete any sensitive information after utilizing it. To prevent theft of documents and unauthorized access to your college, access control must be implemented.

3. Use a Virtual Private Network (VPN)

A VPN can help safeguard your security and privacy by masking your IP address and encrypting your internet activity. This is especially important if you're utilizing public Wi-Fi because it's vulnerable to cyber-attacks.

4. Enable Two Factor Authentication

Two-factor authentication (2FA) adds an additional layer of security to all accounts. You must provide a code in addition to your password to access your account with 2FA. As a result, hackers will find it far more difficult to assess your accounts.

5. Often Backup Your Data

Your college should either manually backup every piece of information to an external hard drive or the cloud or just set up automated backups to guarantee that your data is stored safely. Your information will be safe with you in this way, even if your systems are compromised. It won't hurt to evaluate all internal communications to ensure that no single point of failure may erase months or years' worth of historical data, even if many software packages that handle sensitive data already have this feature by default.

Encryption

Is the process of scrambling the original message (text)into a meaningless format at the sender using a key (secret)then the encrypted text (cipher text) is added to the public network to be delivered to the receiver

It may be read by (accessed by) the hackers from the public network while it is also collected by the specific receiver

It is not meaningful for the hackers but the receiver decrypts it using the key into the meaningful original text. The sender and the receiver should exchange the key (secret) before the communication continuous which should not be known to the other parties

- **Symmetric key encryption**

- **A symmetric key encryption**

Symmetric key encryption

Symmetric key encryption uses the same key is used at the sender and the receiver to encrypt and decrypt the electronic database. If you encrypt a zip file and then decrypt with the same key, you are using symmetric encryption. Symmetric encryption is also called "secret key" encryption and the key must be kept secret from third parties. The entities communicating via symmetric encryption must exchange the key so that it can be used in the decryption process and their for the exchange method medium such as (SMS, telephone call, physical meetings) can be used by the sender and the receiver to share the same key.

A symmetric key encryption

A solution for the problem of the symmetric key encryption. A symmetric key encryption can be classified as

- **Public key encryption**
- **Private Key encryption**

Public key encryption

Public key are knows to all which can be announced on website. This is the key used for encrypting or signing the message

Private Key encryption

Secret which must only be known by the owner of the private key. At fast the receiver should register for the public key and private key. When a registering for public key encryption the public and private key issued which are having a connection among them the system knows the matching set of public and private key. There are some public key encryption software to support to the encryption and decryption activity. Whenever text is encrypted using a public key it can only be decrypted using the matching private key of the public. No other private key can decrypt the message. Receiver must register for the public key encryption and to obtain public and private key.

✓ Digital signature

Digital signature is a replacement for the traditional signature in the digital medium which is legally accepted to provide the authentication. When using digital signatures it is a must to provide the specific public key of the person to the receiving party to carry out the verification. The agreed text is encrypted using the private of the sender and create the digital signatures. It is added to the document an exchange it with the receiver the receiver maintain the list of public key of the sender.

Importance of a Layered Security Approach for Colombo Advanced College

A layered security approach, also known as defence in depth, involves implementing multiple layers of security controls to protect an organization's assets Colombo Advanced College. This approach is essential due to the college's complex operations and the increasing complexity of cyber threats.

- **Enhanced protection against multiple threats**

Ω Each layer of the security framework addresses different types of risks, providing comprehensive protection against malware, phishing, unauthorized access, and data breaches. Where firewalls can block external threats, endpoint security solutions protect individual devices.

- **Minimize single points of failure**

Ω By using multiple layers of protection, a failure in one layer does not expose the entire network. If a malicious email bypasses spam filters, another layer of antivirus or user training can prevent it from causing damage.

- **Security tailored to different areas**

Ω The diverse environment of Colombo Advanced College, which includes laboratories, administrative systems and online learning platforms, requires specific security measures tailored to each segment. Network segmentation, as part of a layered approach, ensures that critical resources, such as student data, are isolated from publicly accessible systems.

- **Improve incident prevention**

Ω Even if attackers penetrate a layer, additional defenses slow their progress, allowing the IT team to detect and contain the threat before it spreads. Intrusion detection systems (IDS) and network monitoring tools can flag unusual activity for immediate action.

- **Compliance with standards**

Ω Many security frameworks, such as ISO/IEC 27001, emphasize a layered approach to meeting compliance requirements. Implementing such a strategy demonstrates the college's commitment to international security standards.

- **Adaptability to ever-changing threats**

Ω Cyber threats are constantly evolving, and an evolving approach can be updated incrementally without overhauling the entire system. This makes the university's security infrastructure more adaptable and cost-effective in the long run.

Commitment to Continuous Monitoring and Improvement

Continuous monitoring and improvement is essential to maintain the security of the Colombo Advanced College network, especially in a dynamic environment with users and technology.

- **Real-time threat detection and response**

Continuous monitoring allows the IT team to detect suspicious activity in real time, such as unauthorized access or unusual data transfers. Tools like security information and event management (SIEM) systems can aggregate data from across the network for better visibility.

- **Adapt to ever-changing threats**

Cyber threats evolve rapidly, and continuous monitoring helps identify new vulnerabilities and attack patterns. By analyzing incident data and trends, the college can proactively adjust its defenses.

- **Minimize downtime**

Rapid detection and resolution of issues reduces the impact on academic and administrative operations, ensuring minimal disruption. When this happens, monitoring systems can flag an overloaded server before it goes live, avoiding downtime.

- **Regulatory advice and reporting**

Continuous monitoring supports compliance with data protection rules by maintaining an audit trail of security activities. This helps the institution demonstrate accountability and prepare for external audits.

- **The informed decision**

Regular analysis of security measures provides actionable insights to improve policies, processes and technologies. It helps the institution efficiently allocate resources to address the most critical risks.

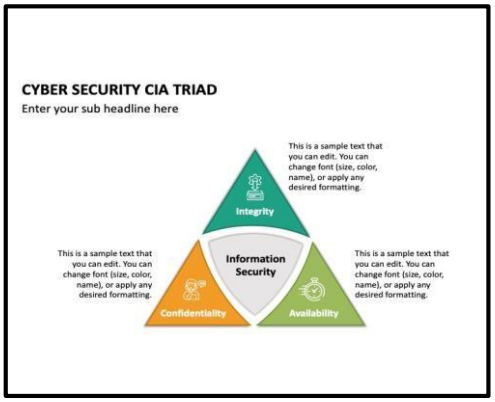
- **Promote a culture of safety**

Continuous monitoring promotes an ongoing safety dialogue among students, staff, and administrators. Regular updates on potential threats and best practices encourage everyone to contribute to a safer environment.

Activity 02

CIA TRIANGLE

The CIA Triad, consisting of confidentiality, integrity, and availability, is a fundamental framework in information security. While it's not the only framework available, it provides a straightforward approach to considering data security, whether it pertains to digital or physical information. This triad serves as a valuable tool for college looking to enhance and sustain their security measures while ensuring that essential tasks can still be carried out. Whether you're involved in computer systems, customer service, or overall management, the CIA Triad can guide you in achieving both security and operational efficiency.

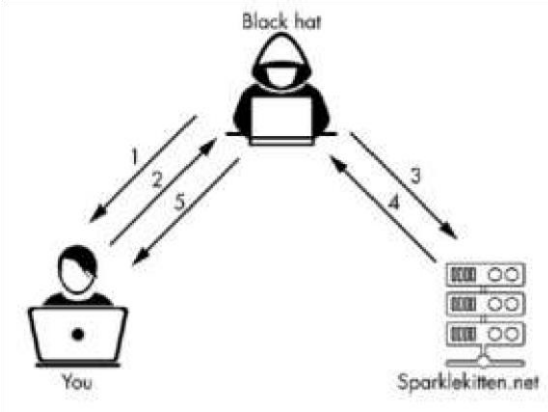


1. Confidentiality

The initial element of the triangle, which is confidentiality, focuses on preventing unauthorized individuals from gaining access to sensitive information. This involves protecting data from malicious actors and limiting access to authorized person within a college. Confidentiality shares similarities with privacy. For example, when you send an email, you specify who should receive its content. The security of your email relies on measures associated with confidentiality. These security techniques encompass items like tokens, locks, passwords, two-factor authentication, biometrics, and more.

Types of Confidentiality Violations

- **Network Reconnaissance**



Reconnaissance, often known as collecting information, is divided into two types: active and passive. Interacting directly with the target is an example of active reconnaissance. It is vital to understand that the target may capture IP addresses and log activities throughout this procedure. The large amount of information available on the internet is used for passive reconnaissance. Because one is not interacting directly with the target when doing passive reconnaissance, the target has no method of knowing, registering, or logging activities. The goal of reconnaissance is to gather as much information as possible about a target (Anon., 2023)

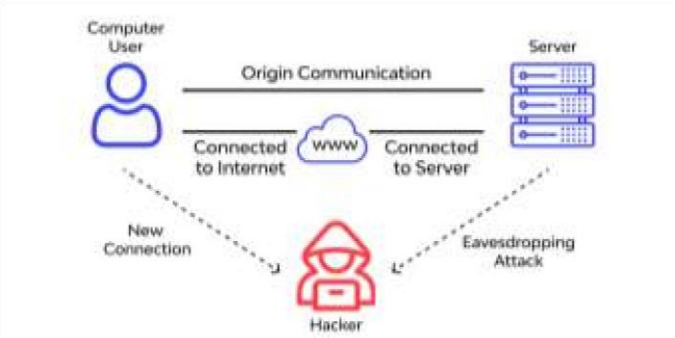
- **A weak password or a failure of the authentication mechanism to encrypt data**

A cryptographic failure is a significant web application security flaw that exposes sensitive application data due to a faulty or non-existent cryptographic algorithm. Passwords, patient health data, company secrets, credit card information, email addresses, and other sensitive user information are examples.

- **Human mistakes or carelessness**

Human error in a security environment refers to inadvertent acts - or lack of action - by staff and users that originate, propagate, or allow a security breach to occur. This includes a wide variety of acts, from downloading a malware-infected file to forgetting to use a secure password, which is why it can be tough to solve. We utilize a rising number of products and services in our more complex and intricate work settings, and we have usernames, passwords, and other things to remember for each of them. This all adds up, and when staff or student are not given with alternate, secure options, they begin to take shortcuts to make life simpler for themselves. As if struggling to make the proper decisions wasn't enough, end-users also have to contend with the continual threat of cyber criminals influencing their decision-making. Social engineering is increasingly being utilized in all forms of security breaches to abuse workers' capacity to pass over data or credentials directly into the hands of bad actors without them having to create a single line of malware code or software exploit.

- **Electronic eavesdropping**



When a hacker intercepts, deletes, or alters data being transferred between two devices, this is referred to as an eavesdropping attack. To access data in transit between machines, eavesdropping, also known as sniffing or snooping, relies on unencrypted network interactions.

Techniques for maintaining confidentiality

- **Implement a policy of confidentiality.**

A confidentiality policy specifies how employees should handle private material to maintain its security. By establishing clear instructions for users, you avoid second-guessing, reduce the risk of data breaches due to human error, and maintain regulatory compliance.

- **Encrypt your data**

One of the best ways to protect data confidentiality is encryption. Simply put, encryption is a process that uses an algorithm to turn data into an unreadable format. Only authorized people can decrypt the data and read it. To everyone else, encrypted data is intelligible. A virtual private network is an effective and convenient tool that leverages encryption technology, and there is a wealth of options available. By simply utilizing a free VPN, you can ensure that your data remains indecipherable to third parties. This helps your college to maintain confidentiality and even enables authorized people to access your college network remotely without putting sensitive data in jeopardy.

- **Restrict data access**

College may guarantee data confidentiality by limiting who has access to non-public information, documents, and files, among other things. Access control should always be based on the concept of

least privilege, which implies that only those who need to know should have access to data. After all, the smaller the chance of a data leak, the fewer persons who have access to the data.

- **Training for workers**

Offering workers a good guidance regarding privacy issues both at a basic org-wide level and as per the nature of their role.

2. Integrity

It is important to ensure that information is accurate, consistent and reliable, this is called data integrity. Data integrity means that data remains unchanged and reliable, preventing unnecessary changes (intentional or unintentional). There are many ways to protect data integrity, including using access controls, monitoring data changes, and protecting data during transmission or storage. Going back to our email example, when you send an email, you want the message you send to be the same as the recipient. For example, if a third party intercepts an email and makes unauthorized changes to its content, the integrity of the information may be lost.
These are the security control which is maintaining the integrity of the data

- Encryption
- User Access Control

Techniques for Maintaining Integrity

- **Input data should always be validated.**

Before allowing input data into your data storage system, it should always be verified. Validation is the process of ensuring that data is valid and valuable. Data should be reviewed for correctness regardless of its source, whether it be data from application end users, internal systems, or other sources.

- **Maintain an Audit Trail**

It is critical to keep an audit trail mechanism in place that can monitor the source of data changes. It is critical to understand the source of a data breach, the documents or data that may have been accessed, and how the breach occurred. An audit trail should be established automatically so that persons do not have access to tamper with the audit trail's results. It should also be able to track data events such as create, delete, update, and so on, as well as the time the events happened and the person who initiated them. A well-managed audit trail may be quite useful when investigating a data breach.

- **Implement Access Controls**

Data access should be strictly regulated to ensure that only those with the necessary authorizations have access to data. A least-privileged security paradigm should be utilized, with access allowed solely on a need-to-know basis. Broad access, such as administrative control over whole systems, should be rare. Staff should only have access to data that allows them to fulfill their specified job tasks. Data should be segregated such that unwanted access is virtually eliminated.

- **Always keep a backup of your data.**
  It is critical to have frequent, dependable, and timely backups of data systems to guarantee that data can be retrieved in the case of data loss. Hardware failure, software problems, and even ransomware attacks can all cause data loss. A backup procedure assures that your company does not suffer from irreparable data loss.
- **Always keep a backup of your data.**

It is critical to have frequent, dependable, and timely backups of data systems to guarantee that data can be retrieved in the case of data loss. Hardware failure, software problems, and even ransomware attacks can all cause data loss. A backup procedure assures that your college does not suffer from irreparable data loss.

3. Availability

The concept of availability states that those who require access to data can do so without compromising its integrity or confidentiality. You want the people who received the email you sent to be able to view it and perhaps even save it for later use. This can be challenging because the other two elements of the triad might compete for availability. Limiting access to data is among the best methods to protect it. If you work in information security, you may have encountered resistance concerning information accessibility from clients or colleagues. Virtualization, failover, redundancy, and other information security methods are used to lessen threats to the availability of data. (Anon., 2023)

Colombo advanced college has the option to the CIA Triad approach for securing student data. By utilizing this method, the college can ensure the confidentiality of data through measures like two factor authentication and encryption. Additionally, they can uphold data integrity and availability by implementing the techniques mentioned by the author. This approach enables Colombo advanced college to gain a comprehensive understanding of organizational risks by analyzing and addressing potential threats, vulnerabilities, and attacks within each component of the triad.

Relevance to Colombo Advanced College

Implementing an ISMS supports the successful operation of the college by protecting its most valuable information assets, such as student records, research data, and administrative processes. It helps prevent disruptions caused by cyberattacks, builds trust among stakeholders, and ensures that the college complies with legal requirements. Additionally, as the college moves toward hybrid learning models, an ISMS ensures the security of online platforms and remote access, maintaining the institution's reputation and operational efficiency.

Benefits Effective Information Security Management System (ISMS)

- **Protection of sensitive data**

An ISMS system protects critical information such as student records, financial information and research data. By implementing strong security measures, the college can prevent data breaches and unauthorized access.

- **Reducing cybersecurity threats**

The IT security management system helps identify and mitigate risks such as ransomware, phishing and malware attacks. This reduces the likelihood of incidents that can disrupt academic and administrative activities.

- **Improve business continuity**

With a clear disaster recovery and incident response framework, the university can quickly recover from security breaches or system outages, ensuring minimal downtime for students and staff.

- **Regulatory Compliance**

An ISMS helps universities meet legal and regulatory requirements, such as data protection laws. Compliance helps avoid legal penalties and enhances the university’s reputation for trust and professionalism. Compliant with ISO/IEC 27001.

- **Support for hybrid learning models**

As universities expand their online learning platforms, an ISMS ensures secure access for students and faculty, protects virtual classrooms, and protects personal data during remote sessions.

- **Improved Trust and Reputation**

A strong information security management system demonstrates the institution's commitment to information security, which fosters trust among students, parents, and academic partners. It reinforces the institution's reputation as a safe and trustworthy organization.

- **Proactive Risk Management**

By identifying vulnerabilities and implementing regular audits, an information security management system enables the organization to address security issues before they become serious problems.

- **Encourage a culture of safety**

An assessment and critical analysis of these elements and processes

- **Ω Risk Assessment Framework**

A systematic approach to identifying, analyzing and prioritizing risks. The college should regularly assess vulnerabilities in its infrastructure, such as outdated systems and shared laboratory resources, to determine potential threats such as ransomware and unauthorized access.

- **Ω Policies and Procedures**

Clearly defined security policies tailored to the needs of the college, including data protection, access control, acceptable use, and incident response. These policies ensure consistency and provide guidance for staff and students to follow.

- **Ω Access Control Mechanisms**

Implemented role-based access control (RBAC) and multi-factor authentication (MFA) to restrict access to sensitive systems and data based on job responsibilities. This reduces the risk of unauthorized access.

- **Ω Technological protection measures**

Implementation of advanced tools such as firewalls, intrusion detection and prevention systems (IDPS), encryption technologies and endpoint protection platforms. These tools help protect the network and sensitive data against external and internal threats.

- **Ω Incident response plan**

A comprehensive plan that includes procedures for identifying, reporting and responding to security breaches. Regular incident simulations allow staff to know how to respond in an emergency.

- **Ω Regular training and awareness programs**

Train staff and students on cybersecurity best practices, such as recognizing phishing attempts, managing strong passwords, and avoiding insecure downloads. Awareness reduces the risk of user error.

- **Ω Ongoing monitoring and auditing**

Monitoring tools that detect unusual activity in real time, combined with regular audits to assess ISMS effectiveness. These processes allow for adaptation to evolving threats.

- **Ω Backup and Disaster Recovery Systems**

Powerful backup protocols that ensure critical data is stored securely and can be restored quickly. A disaster recovery plan minimizes downtime and ensures continuity in the event of a cyber-attack or system outage.

Processes Required

1. **ISMS planning and scoping**
Define the scope of the ISMS to include all services, laboratories and digital systems. This ensures that no critical area is left unprotected.

2**. Asset identification and classification**
Catalogue all assets, including data, hardware and software, and classify them based on importance and sensitivity.

3**. Risk management and mitigation**
For each identified risk, the institution must have a treatment plan. This may include applying security patches, segmenting networks, or adopting stricter authentication protocols.

4**. Regular review and updates**
The ISMS must evolve to remain relevant. Periodic reviews of security policies, risk assessments, and technology tools ensure that the system adapts to new threats and changes in university operations.

5. **Documentation and Record Keeping**
Maintain detailed records of risk assessments, incidents, audits, and compliance actions. This data promotes accountability and is essential for regulatory audits.

Critical Analysis

The success of an information security management system at Colombo Advanced College depends on how well these elements and processes are implemented and maintained. The main challenge is to balance the technical, administrative and cultural aspects of security.

- ⊕ **Cultural change**
  While tools such as firewalls and encryption can mitigate external threats, user awareness and policy compliance are equally important. However, fostering a security-conscious culture can take time and requires sustained effort.

- ⊕ **Resource allocation**
  Upgrading outdated systems and implementing advanced tools will require significant investment. It is essential to balance costs with security priorities to avoid leaving critical areas vulnerable.

- ⊕ **Continuous improvement**

Cyber threats are dynamic and ISMS must be proactive rather than reactive. Continuous monitoring, training and system improvement are essential to maintain the effectiveness of the ISMS.

A justification of the steps required for Colombo Advanced College

To successfully implement an Information Security Management System (ISMS) at Colombo Advanced College, the institution needs to follow a series of well-structured steps. These steps are essential to ensure that the system effectively protects sensitive data, minimizes risks, and supports the college's academic and administrative functions.

Define the goals and purpose

The institution must decide on the objectives of the ISMS and the areas it will cover. For example, protecting student data, protecting research data and ensuring uninterrupted access to IT systems. Scoping helps focus efforts on the most critical systems and assets.

For what? Without clear objectives, efforts can be scattered and important assets can be vulnerable.

Conduct a risk assessment

A thorough assessment is needed to identify potential risks, such as outdated software, weak passwords, or insecure networks in labs. Each risk should be assessed based on its likelihood of occurrence and the degree of harm it could cause.

Why? Understanding risks helps you prioritize issues that require immediate attention and resources.

Develop security policies

The college should establish rules and guidelines to manage security. This includes data access policies, password creation, software updates, and incident management such as data breaches.

Why? Clear policies ensure that everyone knows their role in maintaining security and reduce the risk of human error.

Implement security controls

Based on the risk assessment, the institution should introduce measures to reduce risks. This may include firewalls, encryption, multi-factor authentication, and regular backups. Network segmentation and the use of a DMZ for publicly accessible systems can also improve protection.

Why? Security controls are practical tools that protect facility systems from threats.

Train staff and students

It is essential that everyone is informed about cybersecurity best practices. Training should cover recognizing phishing emails, creating strong passwords, and using shared resources safely in labs.

Why? Many security breaches occur due to simple mistakes. Training helps reduce these risks.

Monitoring and auditing of systems

The institution should continuously monitor its systems for unusual activity and perform regular security audits to identify and correct vulnerabilities.

Why? Threats are constantly evolving, so ongoing monitoring ensures that the ISMS remains effective.

Create an Incident Response Plan

There should be a detailed plan for responding to security incidents, such as data breaches or ransomware attacks. The plan should include steps to contain the problem, recover lost data, and prevent future occurrences.

Why?

Rapid and organized responses can minimize the damage caused by a security incident.

Maintain and Update ISMS

The ISMS should be reviewed and updated regularly to adapt to new security challenges, technological advances, and changes in the institution.

Why? A static system can quickly become outdated, leaving the facility vulnerable to new threats.

Activity 03

What is risk assessment procedure?

The systematic process of discovering, evaluating, and controlling risks and hazards is known as a risk assessment. A competent individual determines the steps that need to be taken to reduce or eliminate risk in the workplace in every given circumstance. One of the key elements of a risk analysis is risk assessment. Risk analysis is a multi-step process with the goal of identifying and analyzing all potential risks and problems that could be harmful to the business. This is a continuous procedure that is updated as required.

These ideas are related and adaptable on their own. (Hathaliya, 2020)

Review of Current Risk Assessment Procedures at Colombo Advanced College

Risk assessment at Colombo Advanced College is a process designed to identify, analyze and address security threats that may impact its operations. However, the recent ransomware attack has revealed gaps in current procedures, signalling the need for improvement.

A. Risk Identification

The College performs basic risk identification processes, focusing on common threats such as malware, phishing and unauthorized access. However, the scope appears to be limited, with less attention paid to advanced threats such as distributed denial of service (DDoS) attacks or insider risks.

B. Vulnerability analysis

The college looks for vulnerabilities in its systems, including outdated software and weak passwords. However, there does not appear to be a comprehensive assessment of all network equipment, labs, or critical systems, leaving blind spots in the infrastructure.

C. Lack of regular updates

Risk assessments are not conducted frequently enough to monitor new threats. The lack of regular reviews means that new emerging risks can go unnoticed until they cause significant damage.

D. Limited risk prioritization

Although the college recognizes some risks, there is no systematic process for prioritizing them based on their likelihood or potential impact. This can lead to resources being spent on minor issues while critical vulnerabilities are not addressed.

E. Insufficient documentation and monitoring

The results of the risk assessment are not always well documented or integrated into a continuous monitoring system. It is therefore difficult to verify whether the identified risks have been effectively mitigated.

F. Lack of a global policy

Current procedures do not appear to be in line with international standards such as ISO/IEC 27001. Without a clear framework, the risk assessment process lacks structure and depth. Areas for improvement

To improve the risk assessment process, Colombo Advanced College should adopt a more structured approach, including:

- Regularly scheduled assessments to stay on top of evolving threats.
- A comprehensive assessment of all systems and infrastructure, including laboratories and administrative resources.
- Implement a risk prioritization framework to address the most critical vulnerabilities first.
- Integrate the results into a continuous monitoring system for real-time threat detection.
- Align with international standards to ensure a comprehensive and effective process.

Change Management

This process of assessing, identifying, comprehending, managing, and reporting on the risks that a change management program, business effort, or project will face during the course of the change implementation is known as project change management risk assessment and mitigation.

This should be done alongside a project management risk management assessment that looks at project deployment because the two go hand-in-hand when it comes to project success. (Iacoviello, 2024)

The Stages of Change Management

1. Request for the change
2. Impact Analysis
3. Approve or Deny
4. Implement Change
5. Review and reporting

Network change management

Colombo Advanced College adopts a structured approach to enterprise risk management (ERM) to identify, evaluate, and prioritize risks that could impact its academic and operational goals. As part of ERM, network change management plays a critical role in addressing risks associated with changes to the college's network infrastructure. This ensures that updates and modifications are carried out securely and effectively, minimizing disruptions to educational and administrative activities while safeguarding critical systems and data.

Some crucial techniques that may be applied in network change management

- Change Control procedure

For effective network change management, a formal change control procedure must be established. This procedure outlines the procedures for submitting, approving, testing, and putting modifications to the network into effect. It guarantees that all modifications are approved, evaluated, and documented, minimizing the possibility of mistakes or failures.

- Automated testing

This method is essential for managing network change. To simulate network changes and check for any potential problems or conflicts, software tools are used. This method guarantees thorough testing of changes and reduces the possibility of mistakes or failures.

- Rollback Strategy

For managing network change, a rollback strategy is crucial. A rollback strategy explains what should be done if a change causes unanticipated problems or conflicts. If necessary, it guarantees that the network can be swiftly put back in its original state.

- Communication

Managing network transformation requires effective communication. It entails explaining the specifics of the change to all parties involved, including management, network administrators, and end users. It guarantees that everyone is informed about the change, is aware of its effects, and may offer feedback or voice any concerns.

- Documentation

One of the most important methods for managing network change is documentation. It entails recording every change, together with its justification, its implementation process, and any testing or verification that was carried out. It guarantees that modifications can be monitored and audited, and that any problems or conflicts can be found and handled right away.

Penetration Testing

The term "pen test" or "pen test" is frequently used in ethical hacking. It is a type of cyber-attack that is mostly carried out to evaluate the security of a system. People frequently mistake the vulnerability assessment exam for the penetration test, also known as a pen test.

The practice of assessing a software application or system to see if it complies with requirements and to find any flaws is known as software testing. Both physical labor and mechanized tools are acceptable. In order to assess the security of a computer system, network, or online application, penetration testing, commonly referred to as "pen testing," simulates a cyber-attack. Penetration testing's objectives are to find security holes that an attacker could exploit and to make suggestions for plugging those holes. (content79qw, 2024)

Advantages of pen testing

- Ω A penetration test can be performed to identify any weaknesses in the system that could be exploited.
- Ω The hazards posed by the vulnerabilities are also identified.
- Ω It can be used to assess the consequences and propensity for an attack.
- Ω It can aid in evaluating the efficacy of security measures.
- Ω It can assist in prioritizing corrective actions.
- Ω It can guarantee the security of the system.
- Ω It may be used to evaluate the security of any system, regardless of its size.
- Ω It can be used to identify undiscovered weaknesses in systems.
- Ω It can be used to evaluate how well security controls are working.
- Ω It can be used to inform staff members of security risks.

Pen Testing Tools

1. Nmap: It is a security scanner and network investigation tool. It can be used to locate hosts, services, and security flaws on a network.

2. Nessus: It is a scanner for vulnerabilities. It can be used to identify weaknesses in programs and systems.

3. Wireshark: It is a packet analyzer. It can be used to capture and analyze network traffic.

4. Burp Suite: It is a tool for testing web application security. Finding security flaws in online apps can be done using it.

Data Protection Processes and Regulations at Colombo Advanced College

1. Data Encryption

Sensitive information, such as student data and financial data, should be encrypted during transmission and storage to prevent unauthorized access.

2. Access Control

Only authorized personnel have access to specific data based on their role. This is possible through strong password policies, multi-factor authentication (MFA), and user role segmentation.

3. Regular Backups

Data is regularly backed up and stored securely in multiple locations. This ensures that data can be quickly recovered in the event of an incident, such as a ransomware attack or system crash.

4. Compliance with legal standards

The College complies with local and international data protection laws, such as the Sri Lanka Data Protection Act and the GDPR (if applicable to international students). These laws require secure data processing, transparency, and user rights regarding personal data.

5. Incident response plan

A structured plan is in place to manage data breaches, ensuring rapid action to minimize damage and to notify affected parties as required by law.

6. Data minimization

Only necessary data is collected and stored, reducing the risk of exposure. This is in line with regulatory principles for responsible data management.

7. Employee training

Staff and faculty are trained in data protection practices, such as recognizing phishing attempts and protecting student information, to prevent human error.

8. Monitoring and auditing

Regular audits and real-time monitoring of data access and use help identify potential breaches or abuses, ensuring compliance with data protection rules. By implementing these measures, Colombo Advanced College can ensure the security and confidentiality of its critical information, protect itself from legal liabilities, and maintain trust with its stakeholders.

Data protection laws

Data Privacy Laws

Data privacy rules control the gathering and utilization of personal information. They are made to guarantee that data is only gathered and utilized for lawful purposes in order to protect people's privacy. People have the right to access and update their own personal data under data privacy legislation.

Data Security Laws

Data protection regulations are in charge of safeguarding personal information. They are made to guard against unapproved access to or usage of personal information. In accordance with data security rules, organizations must take precautions to prevent the loss or theft of customer data.

1998 Data protection act

The Data Protection Act 1998 (DPA, c. 29), enacted by the UK Parliament, was created to safeguard personal information kept on computers or in a well-organized paper filing system. It adopted rules on the storage, handling, and transfer of data from the European Union (EU) Data Protection Directive of 1995.

Individuals had legal rights to manage information about themselves under the 1998 DPA. The vast majority of the Act did not apply to residential use, including maintaining a personal address book [1]. Subject to certain exceptions, anybody who holds personal data for other reasons is required by law to adhere to this Act. To guarantee that information was treated lawfully, the Act established eight data protection principles.

2018 Data protection act

The European Union (EU) implemented the General Data Protection Regulation (GDPR), a data protection regulation, on May 25, 2018. The 1995 EU Data Protection Directive is replaced by this one. For people in the EU, the GDPR establishes a new norm for privacy protection and data management. No matter where the organization is based, it applies to all organizations that process personal data of EU persons.

General Data Protection Regulation (GDPR)

A rule of the European Union (EU) that went into effect on May 25, 2018, is known as the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) updates the 1995 Data Protection Directive and enhances and expands upon the EU's existing framework for data protection.

The GDPR outlines the requirements for firms doing business in the EU regarding the collection, processing, and storage of personal data. In relation to their personal data, it also introduces new rights for individuals. To guarantee that data controllers follow the GDPR, it also establishes enforcement procedures.

A Data Protection Officer (DPO) must be appointed by any organization that handles personal data. The DPO is in charge of making sure the company complies with the GDPR.

A notification stating the following must be given to persons by companies processing personal data:

- The data controller's name and contact information
- The objectives of the processing of personal data
- The recipients of the personal data, or the groups of recipients
- The rights granted to people under the GDPR, such as the right to view their personal data and the right to complain to the supervisory authority
- The length of time that the personal data will be kept on file, or, if that isn't practicable, the standards used to establish that time frame.
- Whether the provision of personal data is required by law, by contract, or as a condition of entering into a contract, as well as whether the person is required to disclose the personal data and what would happen if they didn't.

Risk-Management Strategy and ISO Standards for Colombo Advanced College

To protect its IT systems and data, Colombo Advanced College requires a well-structured risk management strategy, guided by internationally recognized standards such as ISO 31000 for Risk Management and ISO/IEC 27001 for Information Security.

1. Risk Identification

The first step is to identify potential risks such as ransomware, unauthorized access, data theft or system crashes. This includes assessing external threats (such as cyber-attacks) and internal vulnerabilities (such as weak passwords or outdated systems).

2. Risk Assessment

Once risks are identified, they are rated based on their likelihood and impact of a ransomware attack on student data would be classified as high and require immediate attention.

3. Risk Management

Based on the assessment, risks are mitigated through measures such as firewalls, antivirus software, data encryption, and staff training. Risks that cannot be eliminated are managed or transferred (e.g. Through cyber insurance).

4. Implementing the ISO/IEC 27001 Standard

This standard provides a framework for implementing an information security management system (ISMS).

Systematic security practices

Colombo Advanced College's systematic security practices ensure consistent data protection through comprehensive policies and procedures that comply with legal standards. This includes advice on sensitive data management, access management, incident response and disaster recovery. Standardised processes such as data backup, encryption and access control are regularly reviewed and updated to respond to evolving threats and technological advances, fostering a culture of accountability and creating a secure academic environment.

Regular audits

Colombo Advanced College emphasizes regular audits and continuous monitoring to ensure strong security measures, regulatory compliance and timely resolution of security issues. This helps the university stay proactive in combating cyber security threats and promotes security awareness among staff and students.

Compliance

Advanced College Colombo prioritizes compliance with legal and regulatory requirements, such as the Personal Data Protection Act of Sri Lanka, to protect sensitive academic and administrative information. The College implements policies and procedures to protect data from unauthorized access, conducts regular audits, invests in training programs, and aligns its practices with international standards such as ISO/IEC 27001 to enhance its reputation as a secure academic institution and build trust among stakeholders.

5. ISO 31000 for Risk Management

The ISO 31000 standard helps an organization establish a formal risk management process

Integration

The integration of risk management into all organizational processes.

Evaluation

Regular review of risk controls to ensure they remain effective as threats evolve.

6. Monitoring and improvement

Continuous monitoring ensures that the risk management strategy is updated to address new vulnerabilities and threats while maintaining a strong security posture.

Analysis of the Possible Impact on Security at Colombo Advanced College after an IT Security Audit

Security Audit

A security audit is a comprehensive assessment of the physical, procedural, and technological security measures in your business that demonstrates how well you safeguard your data and staff. Audits serve as a kind of litmus test for the effectiveness of your current security protocols. They assist you in creating a baseline of 18 DRP that highlights your strengths and areas for development. (Martin, 2022)

Security audits may identify inadvertent compliance lapses at **Colombo Advanced College**. Noncompliance could result in the loss of student trust, operational downtime, and potentially fines or penalties related to regulatory requirements, which audits are designed to help prevent. The compliance framework for the college should align with applicable standards, such as the Sri Lanka Personal Data Protection Act (PDPA), ISO/IEC 27001, or other relevant education and data protection guidelines. Integrating these standards into the college's audit process allows for a systematic comparison of compliant versus non-compliant processes and provides actionable steps for returning to compliance efficiently.

Below are some of the most common IT compliance standards, and their auditing requirements.

I. ISO Compliance Audits

The goal of ISO 27001 is to give modern businesses a uniform framework for managing information and data. An essential component of ISO 27001 is risk management, which makes sure businesses or non-profits are aware of their advantages and disadvantages.

The ISO 27001 certification process is generally divided into three steps:

A. The company engages a certification authority to carry out a fundamental information security management system (ISMS) evaluation using the company's supporting documents.

B. The certification body carries out a more thorough assessment and evaluates the organization's ISMS against the numerous ISO 27001 components. The organization must demonstrate that it appropriately followed all policies and procedures. The choice of whether to provide certification rests with the lead auditor.

C. The certifying body conducts post-audits to make sure that compliance is managed continuously.

II. HIPAA Audits

Organizations that manage or process personal health information (PHI) are subject to the USA Health Insurance Portability and Accountability Act (HIPAA). It establishes limitations and Guidelines for how to use and safeguard PHI. Patients have the right to examine and request corrections of their health information and medical records under the HIPAA Privacy Rule.

HIPAA audits are carried out by the Office for Civil Rights (OCR) of the Department of Health and Human Services (HHS) to determine whether the law is being followed.

A random sample of Covered Entities and Business Partners (the two types of companies covered by HIPAA) is subject to routine, ongoing audits by the OCR. Even if an entity was not chosen at random for an audit, the regulator may become interested in it as a result of a security incident or complaint.

A college must reply to the OCR audit within 10 days if it is chosen for a HIPAA audit. This means that enterprises must make early preparations, including setting up security measures as well as creating paperwork and proof of compliance.

Determine the holes in your current systems and procedures

Security audits reveal gaps where better systems and greater training could address well-known security problems. There is a direct correlation between your risk and the chance of a significant security event and the number of security gaps you have.

Systematically minimize risk

Your chances of discovering potential vulnerabilities increase if you make your audits repeatable and regular rather than occasional or reactive. Vulnerability scans, departmental audits, and penetration testing are three tried-and-true auditing procedures that can help you organize your procedure and ensure that all security bases are covered.

The effects of the security audit on the security of Colombo advanced collage

Security vulnerability identification

The infrastructure, policy, and practices of an organization's IT systems can all be found to have security flaws and weaknesses during an IT security audit. The audit may identify risks that the college was unaware of but that attackers could exploit.

Suggestions for Improvements

After identifying security flaws, the IT security audit may offer recommendations for improving the college security protocols. This may entail changing procedures and rules, updating software, or implementing new security technologies.

Higher Reputation

By conducting an IT security audit and updating its security protocols, the college can improve its standing with students, staff, and other stakeholders. This can lead to a rise in trust and confidence about the college.

Improve the Awareness of Security Risks

An IT security audit can raise awareness of security threats within the college as well as the significance of maintaining strong security procedures. With increased staff awareness regarding security dangers, this can support the development of a safety organizational culture.

Better Compliance

A corporation may benefit from an IT security audit to help it adhere to legal and regulatory standards. The audit may identify any instances where the college is not adhering to the appropriate security standards and make recommendations on how to do so.

Ongoing Monitoring and Continuous Improvement

Following the audit, continuous monitoring processes may be put in place, helping to detect potential threats in real-time. Real-time monitoring enables faster detection and mitigation of security threats, reducing the risk of a successful attack and increasing overall network resilience.

Potential Disruption to Operations during Remediation

Addressing audit findings may require system downtime or disruptions to normal operations, such as updating software, improving network segmentation, or deploying new security solutions. While this may temporarily affect operations, the long-term benefits of a more secure network will outweigh the disruption, preventing more severe security breaches in the future.

Strengthened Trust and Reputation

Demonstrating commitment to robust security through an audit and subsequent improvements helps build trust with students, staff, and external stakeholders. A strong security posture improves the institution's reputation, making it more attractive to potential students, faculty, and partners, as they feel confident their data is well-protected.

Recommendation for Aligning IT Security at Colombo Advanced College with Organizational Policy

An organization's IT assets and resources must be accessed and used in accordance with the policies laid out in its information technology (IT) security policy. The organization's culture is modelled by its employees' attitudes toward their information and work in effective IT security policy, which serves as the foundation for regulations and procedures. (Pantelakis, 2024)

Purpose of the IT security organizational policy

IT security policies can help organizations maintain the confidentiality, integrity, and availability of systems and information. These three principles make up the CIA triad

- Maintaining asset confidentiality entails guarding them from unwanted access.
- Consistency guarantees that data and systems can only be changed in ways that are approved by the company.
- Availability denotes that trusted users always have access to the data and systems they need.

Some Importance of the IT security organizational policy

1. Information security rules specify what is expected of student in a college in terms of security.
2. Information security policies should reflect the managerial attitude toward security and represent the risk appetite of a college management.
3. Information security policies offer guidance on which a control architecture to protect the college from external and internal risks can be established.
4. Information security policies provide as a framework for a college's moral and legal obligations.
5. Information security policies serve as a means of holding people accountable for adhering to the required information security behaviours.

Some ways to protect the policy

1. Verify that the policy complies with all applicable laws.
2. Establish clear punishments and uphold them
3. Educate your staff
4. Be careful to employ organizational resources without changing the policy.

How IT Security align with Organizational Policy

IT security and organizational policy are closely associated since IT security policies are a part of the wider organizational policies.

Organizational policies frequently encompass a wide range of topics, including workplace behaviour, operational procedures, legal compliance, and information security. IT security policy pertains to the organization's digital assets, which include data, networks, and systems.

To align IT security with the organizational policies at Colombo Advanced College

organizational policies	Impact
Integration of IT security in the mission and objectives of the institution IT security should be considered an essential part of the institution's overall mission, which is to provide a secure learning and administrative environment. The security strategy should be explicitly aligned with the broader educational, research and administrative goals of the institution. By ensuring that IT security policies are considered an integral part of the institution's vision, they will be more easily accepted by all departments.	If IT security is not aligned with the institution's mission, security measures may not be funded or ignored, leading to increased vulnerability to cyber threats, data loss and a negative impact on the structure of the institution.

Ensuring consistency between IT and institutional security policies All institutional policies (e.g. data protection, acceptable use and access control policies) should be consistent with IT security practices. This includes ensuring that data protection and privacy policies, as well as compliance with international standards such as ISO/IEC 27001, are integrated into the overall governance framework of the institution. Clear guidelines should be established for user behaviour, data access and how sensitive information is handled.	Non-harmonization can result in conflicting policies, where staff may not be aware of or follow security protocols. This can lead to data breaches, non-compliance with regulatory requirements and significant financial and reputational damage.
Regular security training and awareness programs	Without this alignment between training programs and security policies, individuals may inadvertently bypass security protocols or fail to recognize threats, leaving the institution vulnerable to attacks such as phishing or social engineering.
All staff and students should receive regular training in IT security, including the proper handling of sensitive data, recognizing phishing attempts and the importance of strong passwords. This will ensure that everyone understands how their actions directly affect the institution's network and data security.	
Develop a centralized incident response and disaster recovery plan The institution should establish a formalized and centralized incident response and disaster recovery plan that is regularly reviewed and updated. This plan should be closely aligned with the institution's IT security strategy and overall risk management policies.	Without a comprehensive incident response plan, the organization may react too slowly or ineffectively to a security breach, which can result in further damage, data loss, and operational disruption.
Continuous monitoring and evaluation	If monitoring efforts are not aligned with organizational policy, threats may go

A continuous monitoring system should be established to detect and respond to threats in real time. In addition, regular security audits should be conducted to assess the effectiveness of current IT security measures and their alignment with institutional objectives.	unnoticed and the university's response to security incidents may be delayed, potentially leading to system outages, data breaches, and loss of trust among stakeholders.

Align access control policies with organizational roles and needs Information security access controls should be consistent with the university's hierarchical structure, ensuring that students, staff, and faculty have access only to the data and resources necessary for their roles.	Lack of adherence to access controls can result in unauthorized access to sensitive data or systems, increasing the risk of data theft, internal sabotage, or accidental data exposure.

Security Impact of Misalignment at Colombo Advanced College

If Colombo Advanced College's IT security measures are not aligned with its organizational policies, critical challenges can arise

1. Widening gaps
These gaps create security vulnerabilities where critical areas of the network are not adequately protected. This increases the risk of cyber-attacks, such as ransomware, data breaches, and denial-of-service attacks, putting sensitive university operations and information at risk.

2. Inconsistency
Failure to comply with data protection regulations and standards, such as ISO/IEC 27001, can result in legal penalties, fines, and reputational damage. It can also affect an institution's ability to obtain partnerships and accreditations.

3. Operational disruption
Inconsistent security practices can lead to ineffective incident responses, causing disruptions and disruptions to educational and administrative services. This affects the availability of resources for students and staff and delays key processes.

4. Loss of Trust

Stakeholders, including students, faculty, and partners, may lose confidence in the institution's ability to secure their data. Loss of trust can damage the institution's reputation, leading to lower enrollment, reduced cooperation, and negative public perception.

5. Financial and Resource Pressures

Inappropriate policies may require reactive spending for adjustments, system redesign, or additional resources, leading to unanticipated financial stress and inefficiencies.

Diversion Prevention

1. Policy integration

Align IT security measures with organizational policies and ensure they are enforced clearly and consistently.

2. Advisory Board

Regularly review compliance with industry standards and data protection regulations.

3. Stakeholder Engagement

Train staff and students on the importance of policies and their role in maintaining security.

4. Continuous Improvement

Conduct periodic reviews of policies and systems to adapt to evolving threats. By addressing these areas, Colombo Advanced College can minimize risks, maintain operational efficiency, and build stakeholder trust.

Security tools which will help organizational policies

1. Penetration Testing

An authorized simulated attack is carried out on a computer system as part of a penetration test (pen test) to assess its security. In order to identify and illustrate the financial effects of a system's vulnerabilities, penetration testers employ the same tools, strategies, and procedures as attackers. The majority of assaults that potentially endanger an organization are often simulated during penetration examinations. They can assess a system's resilience to attacks from legitimate and illegitimate places as well as from a variety of system functions. A pen test can probe any area of a system with the appropriate scope.

2. Security Audit

A Security audit is a comprehensive assessment of your organization's information system; typically, this assessment measures your information system's security against an audit checklist of industry best practices, externally established standards, or federal regulations.

Justifications for chosen tools

Security audits and penetration testing should both be a part of a sound cybersecurity plan since they each have specific advantages for safeguarding a college's digital assets. In order to identify weak points and vulnerabilities in a system or network, penetration testing, also known as ethical hacking, replicates actual cyber-attacks. One of its key traits is its proactive nature. By simulating potential threats, organizations can identify vulnerabilities before malicious actors do, allowing them time to patch and fortify their defenses. Penetration testing provides crucial information about the security posture of the college, aiding in resource allocation and efficient prioritization to address vulnerabilities. Additionally, it encourages a culture of continual security growth by highlighting issue areas and offering helpful remedial assistance.

On the other hand, security audits are comprehensive evaluations of the college's entire security system, including policies, processes, and controls. The comprehensive approach of security audits is its key advantage. Along with the technical components of security, they also assess the administrative and human aspects of it. This ensures that the college follows accepted procedures and standards in the sector. Security audits assist in risk management and evaluation since they can identify governance and compliance flaws. They are useful for demonstrating an organization's commitment to security to stakeholders, staff, and regulatory bodies.

Security audits and penetration testing are valuable tools in the cybersecurity toolbox, to sum up. While penetration testing is practical and technical, focusing on identifying vulnerabilities in systems and networks, security audits provide a comprehensive examination of an organization's security posture, including policies, processes, and compliance. Together, these processes help college maintain stakeholder confidence, regulatory compliance, and proactive data and asset security.

Penetration Testing and security audit's suitability for inclusion in an organizational policy

1. Scope

Every component of the organization's security architecture should be covered by the security audit's broad scope. It should include a review of the organization's policies, procedures, and controls as well as the technical security measures in place.

2. Actionability

The security audit should produce concrete recommendations for improving the college security procedures. The recommendations should be prioritized based on how significant the risks are and how they will impact the organization.

3. Confidentiality

The security audit should be performed in a confidential setting to secure the organization's sensitive data. The audit report should be protected from unauthorized access and only accessible by authorized individuals. The organizational policy determines who is authorized and who is not Penetration testing and security audits should be a part of every corporate cybersecurity policy.

These procedures are necessary to guarantee a solid security posture for a college.

On the other hand, thorough risk management and legal compliance are supported by security audits. The fact that security audits are covered by the policy shows how dedicated the college is to maintaining a strong governance system. This is essential in industries with strict compliance requirements, such as healthcare (HIPAA) and banking (PCI DSS). Security audits ensure that the college complies with these demands, assisting it in avoiding legal and financial issues.

Additionally, the policy should outline the exact objectives, deadlines, and responsible parties for conducting penetration tests and security audits. This openness ensures that these processes are followed consistently and that the results are used appropriately to strengthen security precautions.

The incorporation of security audits and penetration testing into corporate policy offers a proactive and responsible approach to cybersecurity. By demonstrating a commitment to solid security, risk management, and compliance, these measures also increase the organization's resistance to evolving cyber threats.

Activity 04

Plan for Designing an ISMS for Colombo Advanced College

1.ISMS design objectives

The ISMS (Information Security Management System) of Colombo Advanced College aims to protect the confidentiality, integrity and availability of the college's digital systems and data. It will meet the functional and non-functional requirements to ensure a secure and efficient academic and administrative environment.

Implementation Guide

1. **Assessment and Preparation**

Understand the Purpose

- ☐ **Identify Key Assets**

Start by cataloguing critical assets, including student data systems, research databases, administrative software, and any other digital or physical resources essential to academic and operational functions. These assets form the foundation of what the ISMS protects.

- ☐ **Set Boundaries**

Determine the scope of the ISMS by determining which systems, processes, and services are affected. Prioritize critical systems and sensitive data, ensuring they are aligned with the university's goals and risk management priorities. Clearly defined boundaries help simplify implementation and focus efforts on high-impact areas.

Conduct a risk assessment

- ☐ **Identify vulnerabilities, threats, and risks**

Conduct a detailed analysis of the university's digital systems to detect potential vulnerabilities (outdated software, weak passwords) and identify external and internal threats (ransomware attacks, insider threats). Assess the risks associated with these vulnerabilities and threats.

- ☐ **Prioritize risks based on potential impact**

Rank identified risks based on their likelihood and the potential harm they could cause, such as loss of sensitive student data or system outages. This prioritization allows mitigation efforts to be focused on the most critical risks, thereby ensuring optimal resource allocation.

Create leadership and support

- ☐ **Form an ISMS implementation team**

Assemble a dedicated team of IT staff, faculty representatives, and administrators to bring diverse perspectives and expertise. This team will oversee the design, implementation, and management of the ISMS.

- ☐ **Obtain management approval and allocate resources**

Obtain senior management commitment and support to ensure that the project has the authority and funding necessary for a successful implementation. This includes the allocation of financial resources, tools and personnel to address identified risks and maintain the effectiveness of the ISMS.

ISMS design and development

Define policies and controls

- ☐ **Write comprehensive policies**

Develop policies that specifically address access control, data protection, incident response, and disaster recovery. For example, an access control policy can ensure that only authorized faculty and staff have access to student data, while data protection policies mandate encryption of sensitive information in transit and at rest

- ☐ **Establish clear roles and responsibilities**

Define specific responsibilities for managing IT security, such as assigning an IT security manager to oversee compliance and response efforts. When this happens, assign faculty representatives to ensure alignment between IT policies and academic requirements.

1. **Functional Requirements**

Secure Access through Multi-Factor Authentication (MFA)

Implement multi-factor authentication for all critical systems, including student portals, administrative applications, and research databases, to ensure that only authorized personnel have access to them, thereby reducing the risk of unauthorized access or data breaches.

Data Encryption for Information at Rest and in Transit

Encrypt all sensitive data, including student data and financial information, both when stored in databases and when transmitted over the university network. This ensures confidentiality and prevents data breaches during transmission.

Automated Backup with Off-Site Storage

Automate regular backups of systems and key data by storing them in an off-site location, such as a secure cloud platform. This approach minimizes the risk of data loss due to cyberattacks, hardware failures, or natural disasters.

2. Non-functional Requirements

System Scalability

Design systems that effectively accommodate institutional growth, especially as student numbers increase and hybrid learning models are adopted. The infrastructure must support additional users, increased data storage requirements, and more concurrent users without significant performance degradation.

System Reliability with Minimal Downtime

Ensure that the facility's IT systems are highly reliable, with redundancy and failover systems in place to minimize downtime. Implement quick recovery solutions to restore services quickly, especially during critical periods such as exams or registrations.

Compliance with international standards and data protection laws

Ensure that all systems, policies and procedures comply with internationally recognized standards such as ISO/IEC 27001 for information security management. Comply with data protection laws, including GDPR or local equivalents, to protect the personal data of students and teachers.

1. Network Security Measures

Implement firewalls, intrusion detection/prevention systems (IDS/IPS), and endpoint protection

Implement advanced firewalls to monitor and control inbound and outbound network traffic. Implement IDS/IPS to detect and prevent malicious network activity, ensuring early identification of potential cyber threats. Use endpoint protection software on all devices (staff computers, student laptops, and mobile devices) to prevent malware and unauthorized access.

Segment networks to isolate critical systems

Create network segments to separate critical systems (such as student data, research databases, and administrative applications) from less sensitive areas such as staff workstations or public websites. This helps limit access to sensitive information and reduce the impact of potential attacks.

2. Access Controls

Implement role-based access controls (RBAC)

Use RBAC to restrict access to systems based on user roles within the institution. For example, only authorized faculty and administrative staff should have access to student records or grading systems, while students should only have access to their own personal information. Regularly review and update these access controls to ensure they are consistent with the evolving structure of the institution.

Use static IP addresses and network address translation (NAT)

Assign static IP addresses to critical systems such as servers to ensure they are secure and easy to identify. Use NAT to hide internal network addresses and prevent direct access from external sources, adding an extra layer of security.

3. Data Protection Mechanisms

Introduce encryption protocols for sensitive data

Implement strong encryption protocols (such as AES-256) to protect sensitive data, both at rest (stored in databases) and in transit (when data is transferred across networks). This ensures that even if the data is intercepted, it remains unreadable to unauthorized users.

Establish data classification procedures

Implement a data classification system to prioritize the protection of critical assets such as student data, faculty personal information, and research data. Classify data based on sensitivity and establish guidelines for who can access and modify each category. Highly sensitive data requires tighter access controls, while less sensitive information may be subject to fewer restrictions.

Monitoring and Testing

Continuous Monitoring

Use network monitoring tools to detect and respond to threats in real time

Implement advanced network monitoring solutions that can track traffic in real time across all network segments, detecting anomalies or unusual patterns that may indicate cyber threats such as unauthorized access, malware, or denial-of-service attacks. These tools should be able to send immediate alerts to the IT team for rapid response. Schedule regular security audits to assess compliance with the Information Security

Management System (ISMS)

Schedule periodic security audits to assess the compliance of facilities with the Information Security Management System (ISMS). These audits should focus on verifying compliance with security policies, identifying potential security vulnerabilities, and ensuring that sensitive data and systems are properly protected. Audit results drive security strategy improvement.

Testing and simulation

Run penetration tests to identify vulnerabilities

Conducting regular penetration tests to simulate potential cyber-attacks and identify vulnerabilities in the university infrastructure. This includes web application testing, network protection and access controls. Penetration test results should guide the implementation of corrective measures to strengthen security defenses.

Conduct disaster recovery exercises to prepare for incidents

Conduct disaster recovery exercises to test the effectiveness of the university's recovery plans in response to various incidents such as ransomware attacks or data breaches. These exercises involve key IT staff, administration, and faculty to ensure smooth coordination during an actual disaster. Regular practice improves readiness and minimizes downtime during real-life incidents.

Maintenance and Improvement

Review and update policies

Regularly update ISMS policies to address evolving threats and regulatory changes

Continuously review and revise information security management system (ISMS) policies to adapt to new security threats, evolving technologies and changing regulatory requirements. This includes ensuring that policies are aligned with national and international standards such as ISO/IEC 27001, as well as any changes in data protection laws or cybersecurity best practices. Regular policy updates will ensure that the university's security posture remains relevant and strong.

Training and awareness

Provide regular training sessions for staff and students on cybersecurity best practices

Organize periodic cybersecurity training sessions for staff and students. These sessions should cover topics such as identifying phishing emails, using the Internet safely, managing passwords, and reporting suspicious activity. The training will help the campus community understand their role in maintaining security and follow best practices for protecting sensitive information.

Promote awareness campaigns to ensure a culture of security across the college

Initiate ongoing cybersecurity awareness campaigns throughout the college. These campaigns can include posters, emails, and online materials that encourage secure practices, such as strong passwords and multi-factor authentication. Creating a culture of security ensures that everyone on campus understands the importance of information security and is vigilant in protecting themselves from threats.

Benefits of the Plan

1. Functional Outcomes

• Protecting Sensitive Academic and Administrative Data

The information management system ensures that critical data, such as student records, faculty information, and academic research, are protected from unauthorized access and potential breaches. By implementing rigorous security controls, the College can maintain the confidentiality, integrity, and availability of sensitive information.

• Ensures system reliability

The plan ensures that all university systems, including learning platforms, student management systems, and administrative applications, remain operational and resilient to cyber threats. It reduces the likelihood of system outages, ensuring the continued availability of services for staff, students, and faculty.

• Supports regulatory compliance

The information security management system ensures that the college adheres to national and international data protection regulations (such as GDPR, local data protection laws and standards such as ISO/IEC 27001). Compliance with these regulations mitigates the risk of legal and financial penalties while strengthening the college's reputation as a responsible institution.

2. Non-functional outcomes

Builds trust among stakeholders

Through strong security measures, the college demonstrates its commitment to protecting personal and academic data, which fosters trust among students, staff, parents and external partners. This trust is essential for maintaining a positive reputation and attracting new students and faculty.

Improves system scalability

The information security management system is designed to support the future growth of the institution. As the institution grows and adopts new technologies or educational models (e.g., blended learning), the security framework will evolve accordingly to ensure that new systems are securely integrated.

Minimize disruptions during security incidents

Information security management and incident response system recovery protocols help minimize disruptions during security breaches or system outages. Readiness ensures that the institution can respond quickly to incidents, reducing downtime and mitigating the impact of security threats on academic and administrative operations.

Suitable Security Policy for Colombo Advanced College

Organizational Security Policy

The important assets in an organization that need to be safeguarded should be listed in the security policy. This could encompass the college's network, physical structure, and other things. It must also describe any potential risks to such things. If the document focuses on cyber security, internal dangers could be mentioned, such as the potential for irate employees to steal sensitive data or spread an internal virus over the college's network. The system could also be compromised by a hacker from outside the college, who could then alter, steal, or lose data. And finally, physical harm to computer systems is a possibility.

The possibility that the threats will really materialize must be assessed once they have been identified. The college must decide how to stop those dangers. A few protections include implementing specific staff policies as well as robust network and physical security. A strategy for what to do in the event that a danger really materializes is also necessary. Everyone in the organization should receive a copy of the security policy, and the procedure for protecting data must be constantly reviewed and updated when new employees join the team.

Security Policy for Colombo Advanced College

- **Physical Security Policy** – This policy outlines standards to ensure physical access control to the college's resources, including guidelines for visitor management, access restrictions to sensitive areas (like server rooms), and overall security oversight to safeguard against unauthorized access.
- **Password Policy** – This policy sets the guidelines for creating strong passwords, specifying requirements for password complexity, the frequency of password changes, and the circumstances under which multi-factor authentication (MFA) should be implemented for access to critical systems (e.g., student databases, learning management systems).
- **Access Control List (ACL)** – This policy specifies the systems, data, and information that can be accessed by different users within the college. It outlines how access is granted, monitored, and revoked, ensuring only authorized personnel or students can view or modify sensitive data such as student records, grades, or research materials.
- **Bring Your Own Device (BYOD) Policy** – This policy governs when and how faculty, staff, and students can use their personal electronic devices (e.g., smartphones, laptops) for work or study purposes within the college. It ensures that devices are secured and compliant with college IT standards before being allowed access to internal networks or systems.
- **Backup Procedures** – Given the significant amount of critical academic and administrative data held by Colombo Advanced College, this policy mandates the regular backup of essential data (such as student records, research, and academic materials) to ensure its availability in case of system failures or cyberattacks. Backups are conducted on a weekly basis, with off-site or cloud storage for additional protection.

- **Data Classification Policy** – This policy sets the framework for categorizing data based on its sensitivity and value. It provides guidelines for protecting critical assets, such as student records, financial information, and research data. The policy also specifies rules for labeling data, restricting access based on roles, and ensuring the secure transmission and preservation of data.

Some Standard which are support Colombo advanced college Security Policies

1. ISO/IEC 27001

This international standard establishes, implements, maintains, and continuously improves an information security management system (ISMS). It offers a methodical approach to handling sensitive data and maintaining its availability, confidentiality, and integrity.

2. HIPAA

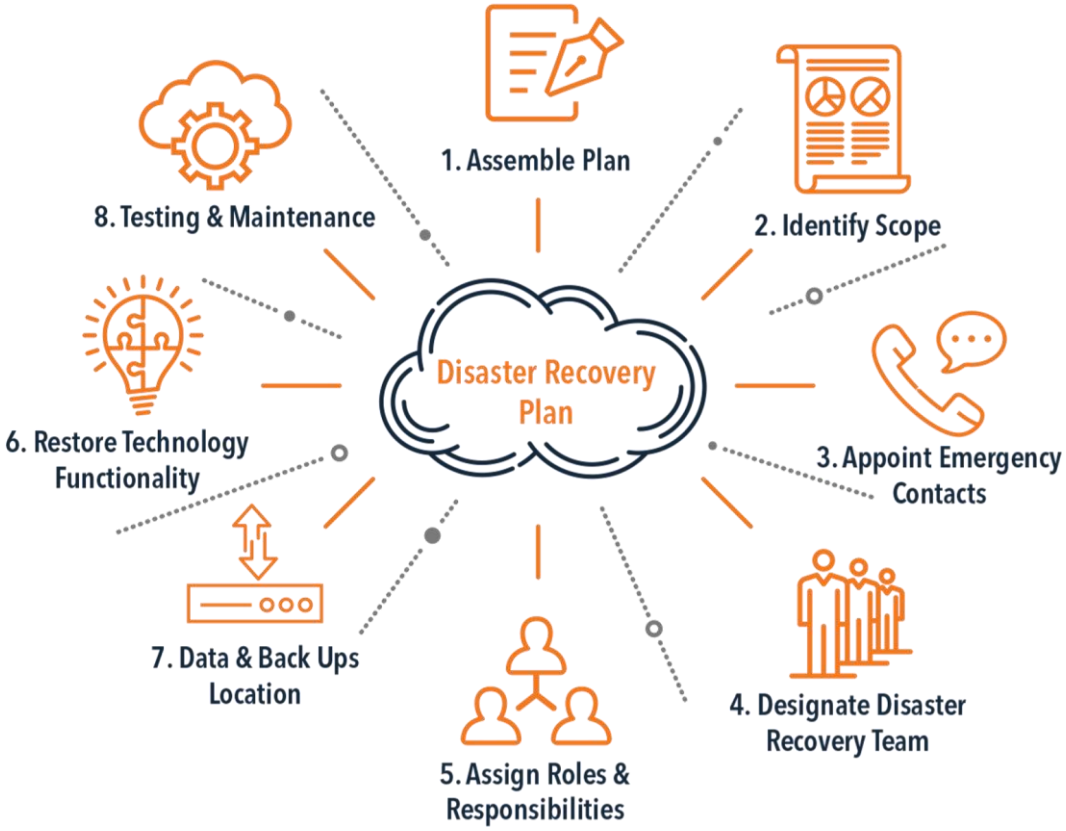
The Health Insurance Portability and Accountability Act is a federal statute that specifies principles for preserving patient information privacy and security. It outlines specifications for securing patient data, putting in place access limits, and disclosing security events.

Disaster Recovery plan

A disaster recovery plan (DRP) is a written, organized strategy that outlines how a company can quickly restart operations following an unanticipated occurrence. A business continuity plan (BCP) must include a DRP. It is used in relation to organizational components that are dependent on an effective information technology (IT) infrastructure. A DRP seeks to assist an organization in resolving data loss and recovering system functioning so that it can function even if it functions at a low level following an incident. The disaster preparedness strategy comprises of actions to lessen the consequences of a disaster so that the company can carry on with operations or swiftly restart mission-critical tasks. (Yasar, 2024)

STEPS IN DISASTER RECOVERY PLAN

1. Create your disaster recovery contingency planning team
2. List all names and contact details
3. Determine a chain of command
4. Consider your risk assessment
5. Plan B
6. Protect your college data
7. Testing



Disaster Recovery Plan

A disaster recovery plan (DRP) is a written, organized strategy that outlines how a company can quickly restart operations following an unanticipated occurrence. A college continuity plan (BCP) must include a DRP. It is used in relation to organizational components that are dependent on an effective information

technology (IT) infrastructure. A DRP seeks to assist an organization in resolving data loss and recovering system functioning so that it can function even if it functions at a low level following an incident.

The disaster preparedness strategy comprises of actions to lessen the consequences of a disaster so that the company can carry on with operations or swiftly restart mission-critical tasks. A study of college processes and continuity requirements is typically part of a DRP. An enterprise frequently conducts a business impact analysis (BIA), a risk analysis (RA), and develops recovery targets before creating a comprehensive strategy.

An organization must specify its data recovery and protection policies as cybercrime and security breaches become more complex. Rapid incident response can minimize downtime as well as financial and reputational losses. DRPs also assist firms in adhering to regulations while offering a clear path to recovery. (Yasar, 2024)

Some types of disasters that organizations can plan for include the following:

- application failure
- communication failure
- power outage
- natural disaster
- malware or other cyber attack
- data center disaster
- building disaster
- campus disaster
- citywide disaster
- regional disaster
- national disaster
- multinational disaster

Types of disaster recovery plans

DRPs can be modified to fit a certain setting. The following are some particular sorts of plans:

Virtualized disaster recovery plan- Through the use of virtualization, DR may be implemented more quickly and easily. In a virtualized environment, fresh virtual machine instances may be created in a matter of minutes, and high availability enables application recovery. Testing is also more convenient, but the plan needs to demonstrate that programs can be run in DR mode and resume regular operations within the RPO and RTO.

Network disaster recovery plan - The more sophisticated the network, the more challenging it is to create a plan for network recovery. A thorough, step-by-step rehabilitation technique must be provided, tested thoroughly, and kept up to date. Information related to the network, such as its performance and networking personnel, should be included in the plan.

Cloud disaster recovery plan - Cloud DR methods can include everything from simple file backups to full replication. Cloud disaster recovery (DR) can be time, space, and money-effective, but maintaining the disaster recovery plan calls for effective administration. The location of both real and virtual servers must be known to the manager. The plan must address security, a problem that plagues the cloud frequently but may be resolved through testing.

Data center disaster recovery plan - This kind of strategy focuses solely on the infrastructure and building of the data center. A data center DRP's operational risk assessment is a crucial component. It examines important elements such building positioning, power supply and protection, security, and office space. The strategy needs to cover a wide range of potential outcomes.

Main Components of the Disaster Recovery Plan for Colombo Advanced College

The first step in creating a disaster recovery plan (DRP) is to define its scope. The college must identify which systems, applications, and data are crucial to its operations, such as student record systems, academic platforms, and administrative data. These should be prioritized for recovery in case of a disaster. Without a clear understanding of what needs to be protected, it's impossible to plan recovery activities effectively.

Next, positions and responsibilities should be clearly defined across the entire college. Every staff member, including both academic and administrative personnel, needs to understand their role during a disaster. This ensures everyone knows their duties and can act promptly when needed. Clear responsibility assignment helps the college respond quickly and effectively.

The third important element is creating processes and procedures for handling critical situations. The college needs to develop and document these processes in advance. This includes identifying potential risks and outlining the steps to take to minimize them. These procedures should cover both technical actions, such as restoring systems, and non-technical actions, like decision-making and communication strategies.

Communication planning is also vital for a successful disaster recovery plan. The college should establish a communication strategy for before, during, and after a disaster. This involves determining which channels will be used, who the key people are for communication, and how often updates should be given. A well-structured communication plan ensures everyone remains informed and aligned throughout the recovery process.

Finally, the DRP should be regularly tested to identify any weaknesses and improve the plan. Testing helps ensure that all procedures work as expected and that any gaps in the plan are addressed before a real disaster occurs. In conclusion, Colombo Advanced College can develop an effective disaster recovery plan by focusing on five essential components: scope, roles and responsibilities, processes and procedures, communication planning, and regular testing.

Stakeholders and Their Roles in Implementing a Security Audit

Stakeholders	Roles	Importance
IT Department	Perform technical assessments of network infrastructure, servers, and endpoints. Provide detailed information on the current state of systems and configurations. Implement post-assessment audit recommendations, such as	As the primary custodians of the college's digital infrastructure, the IT team ensures that the audit identifies all relevant security gaps and addresses them effectively.

	software updates or configuration changes.	
College Management and Leadership	Approve and allocate resources to conduct the audit. Define the strategic objectives of the security audit, ensuring they are consistent with the institution's mission and objectives. Review audit findings and make decisions on prioritizing security investments.	Their leadership ensures that the security audit receives the necessary funding and aligns with the organization's priorities.
External Security Auditors or Consultants	Conduct an impartial assessment of the university's security posture. Provide expertise in identifying vulnerabilities and recommending best practices. Provide a detailed audit report with actionable information.	External auditors bring objectivity and specialized knowledge that may not be available internally, increasing the reliability and rigor of the audit.
Academic and administrative staff	Participate in surveys or interviews to identify potential security issues in daily operations. Adhere to enhanced post-audit security protocols, such as password policies or tighter access controls.	Their collaboration ensures that the audit captures the impact of security policies on actual operations and user behaviour.
Students	Provide feedback on challenges or weaknesses in student systems, such as learning management platforms or lab computers. Follow the security instructions presented after the audit.	Students are the primary users of many university systems and can highlight problems such as unauthorized access to resources or phishing attempts.
Legal and Compliance Team	Ensure that the audit complies with applicable regulations, such as data protection laws or ISO/IEC 27001 standards	Their participation ensures that audit and follow-up actions protect the college from legal and regulatory risks.

Justification for the Designed Security Plan for Colombo Advanced College

Colombo Advanced College's security plan is designed to address the unique challenges facing the institution, below is the rationale for the selected physical, virtual, and policy elements

Physical Security Elements	**Rationale**	**Reason**
Controlled Access to Sensitive Areas	Areas such as servers and laboratories have critical resources. Implementing access controls such as biometric scanners or key card systems ensures that only authorized personnel can enter these areas, reducing the risk of harassment or theft.	Prevents unauthorized physical access, which could result in hardware damage, data breach, or service interruption.
Observation and control with video surveillance	Surveillance cameras monitor activity in high-risk areas, deter malicious activity, and provide evidence in the event of an incident.	Helps identify physical security breaches or abuses, ensuring accountability.
Environmental Controls	Implementing measures such as temperature and humidity control in server rooms helps prevent equipment damage due to environmental factors.	Ensures system reliability by maintaining optimal operating conditions for equipment.
Virtual Security Elements	**Rationale**	**Reason**
Firewalls and Intrusion Detection Systems (IDS)	Next-generation firewalls and IDS monitor and filter network traffic, blocking unauthorized access and detecting suspicious activity.	Protects the network from external and internal threats, such as malware and unauthorized users.
Encryption and secure communication channels	Encryption of sensitive data ensures its security during transmission and storage, especially for student data and research data.	It prevents data theft or leakage even if systems are compromised.
Endpoint protection and patch management	Advanced endpoint protection tools protect network-connected devices, while regular patch management addresses software vulnerabilities.	Reduce the attack surface by closing security gaps in devices used by staff and students.
Multi-Factor Authentication (MFA)	The addition of multi-factor authentication ensures that access to systems requires more than one password, reducing the risk of	Protect against phishing attacks and other credential-based threats.

	unauthorized access even if credentials are compromised.	
Policy elements	**Rationale**	**Reason**
Global Security Policy	Establishing clear guidelines for acceptable use, data protection, and incident response ensures consistency in security management across the college.	Provides a framework for users to follow, minimizing human error and ensuring compliance with legal standards.
Disaster Recovery Plan (DRP)	The PRA outlines procedures for recovering critical systems and data in the event of disruptions, such as ransomware attacks or hardware failures.	Ensures business continuity by minimizing downtime and reducing the impact of incidents.
User awareness training	Regular training programs teach staff and students how to recognize threats, such as phishing, and adhere to best security practices.	Human error is one of the main causes of security breaches, and awareness programs mitigate this risk.

Appraisal and Justification of the Planned ISMS Design for Colombo Advanced College

Evaluation of the planned design of the information management system

1. Compliance with College Security Requirements

The information management system is adapted to the unique environment of Colombo Advanced College, which includes

A central data center containing sensitive student data, research data and administrative systems.

A large user base of students, faculty and staff who require secure yet flexible access.

A hybrid learning model that integrates online platforms. The design emphasizes the protection of these assets by ensuring confidentiality, integrity and availability (the CIA triad).

2. Comprehensive coverage of security aspects

ISMS integrates

Risk Management

Identifies, evaluates and mitigates risks based on their likelihood and impact.

Access Controls
Implements user authentication and role-based authorizations to prevent unauthorized access.

Incident Response
Establishes clear procedures for identifying, managing and recovering from security incidents.

3. Compliance with industry standards
The ISMS is compliant with ISO/IEC 27001, which provides a structured approach to information security management and compliance with legal and regulatory requirements.

4. Adaptability to future challenges
The system is designed to evolve with emerging threats and technological advances, making it sustainable in the long term.

ISMS process steps

Steps	Process	Rationale
Risk assessment and initial audit	A comprehensive audit was conducted to identify weaknesses in the existing infrastructure, such as weak passwords, unpatched systems, and lack of disaster recovery mechanisms.	A thorough understanding of risks ensures that security measures are prioritized effectively, addressing critical issues first.
Policy and Procedure Development	Data protection, incident response, and acceptable use policies are developed to establish clear guidelines for all stakeholders.	Policies provide a foundation for consistent and enforced security practices throughout the organization.
Implementing Technical Controls	Measures such as firewalls, encryption, network segmentation, and multi-factor authentication (MFA) are in place.	These controls provide robust protection against common threats such as malware, phishing, and unauthorized access.
Training and Awareness Programs	Implement regular training for staff and students to increase awareness of cybersecurity practices.	Human error is a significant risk factor, and awareness programs reduce the likelihood of accidental breaches.
Continuous Monitoring and Improvement	ISMS includes real-time monitoring tools and mechanisms	Security is a dynamic field and continuous improvement ensures

	for regularly reviewing and updating security policies.	that the system remains effective against ever-changing threats.

The Rationale for the New IT Security Landscape

1. Ransomware Resistance
By implementing regular backups, robust access controls, and incident response procedures, ISMS minimizes the risk and impact of ransomware attacks.

2. Protection of sensitive data
Encryption and access controls protect critical student and research data, ensuring compliance with data protection rules.

3. Support for the hybrid learning model
Secure remote access solutions and monitoring tools address the growing risks associated with online platforms and remote access.

4. Compliance and Reputation Management
Compliance with ISO/IEC 27001 and other standards strengthens the university's reputation as a secure and attractive institution for students and staff.

An Analysis of the Relationship between ISO Standards and International ISMS Standards in Establishing an Effective ISMS for Colombo Advanced College

Understanding ISO and ISMS standards

The International Organization for Standardization (ISO) develops globally recognized standards, including the widely adopted ISO/IEC 27001, which focuses specifically on information security management systems (ISMS). These standards provide organizations with a structured framework to manage and protect sensitive data and ensure information security. For Colombo Advanced College, integrating ISO standards into its ISMS aligns the institution with international best practices, ensuring both compliance and enhanced security for its digital and physical assets.

The relationship between ISO and WSIS international standards

1. ISO standards as a foundation

ISO standards, particularly ISO/IEC 27001, define the fundamental principles, processes, and controls of an effective ISMS. These include risk assessment, policy development, access controls and incident response procedures.

The ISO/IEC 27001 standard is widely recognized and compatible with other international frameworks, such as NIST (National Institute of Standards and Technology) and COBIT (Control Objectives for Information and Related Technologies).

2. Interoperability and global relevance

The ISO standards ensure that Colombo Advanced College's ISMS is interoperable with other security frameworks, thus enabling compatibility in a global context.

Adherence to these standards demonstrates the college's commitment to international standards, enhancing its reputation and facilitating partnerships with global institutions.

3. Holistic approach to security

The ISO framework emphasizes a systematic approach to security by considering people, processes and technology.

This ensures that Colombo Advanced College comprehensively addresses technical, human and procedural weaknesses.

Creating an effective ISMS using ISO standards

1. Alignment with the ISO/IEC 27001 framework

- **Risk assessment**

ISO emphasizes the identification, analysis and mitigation of risks. For universities, this means addressing vulnerabilities such as outdated systems, phishing risks, and ransomware threats.

- **Policy development**

ISO mandates detailed policies on data protection, incident management, and access controls. These policies are essential for managing a university's data center, labs, and hybrid learning platforms.

- **Control implementation**

The standard requires the implementation of strong technical controls such as encryption, firewalls, and multi-factor authentication (MFA).

2. French Focus on continuous improvement

- ISO encourages regular audits and reviews to adapt the ISMS to evolving threats and technological advances.

- This is consistent with the need for universities to monitor in real time and periodically update their security policies and systems.

3. Legal and Regulatory Compliance

- ISO standards help the college comply with data protection regulations, such as the EU GDPR (where applicable) or local Sri Lankan information security laws.

- Compliance reduces legal risks and ensures the privacy and security of student and staff data.

Benefits of an ISO-compliant ISMS for Advanced College Colombo

Ω Enhanced security posture

By adopting ISO standards, the college creates a robust and systematic defense against cyber threats, ensuring the integrity of its systems.

Ω Reputation and trust

Compliance with ISO standards improves stakeholder trust, demonstrating the college's commitment to protecting sensitive information.

Ω Operational efficiency

Standardized processes minimize disruption and streamline incident response, ensuring that academic and administrative functions function smoothly.

Ω Global recognition

Alignment with ISO standards positions the college as a cutting-edge institution ready to engage with the international academic and research communities.

Evaluation of the Suitability of Tools in the Security Policy Designed for Colombo Advanced College

The security policy for Colombo Advanced College incorporates various tools and technologies to address the institution's specific IT security needs. Evaluating these tools involves assessing their effectiveness, relevance, and ability to align with the college's operational and strategic goals.

Key Tools in the Security Policy and Their Suitability

Tools	Purpose	Suitability

Firewall	Acts as a barrier between the college's internal network and external threats by filtering unauthorized traffic.	The college's central data center houses critical student, research, and administrative data. Firewalls ensure that only legitimate traffic is allowed through, protecting sensitive information from cyberattacks. Advanced configurations such as Next Generation Firewalls (NGFW) provide additional functionality such as application-level inspection, which is essential for the institution's diverse range of applications.
Intrusion Detection and Prevention Systems (IDPS)	Monitor network traffic to detect suspicious activity and block potential threats.	IDPS are particularly important for detecting anomalies, such as unauthorized attempts to access university laboratories or data centres. Real-time alerts improve response time, ensuring minimal disruption to academic and administrative operations.
Multi-Factor Authentication (MFA)	Adds an additional layer of security by requiring users to provide two or more forms of verification before accessing systems.	With over 2,500 students and 150 staff accessing the university network, multi-factor authentication significantly reduces the risk of unauthorized access, especially for sensitive areas such as student records and hybrid learning platforms.
Data Encryption	Secures data in transit and at rest, ensuring that even if data is intercepted, it is not easily accessible.	Essential for protecting research and student data. Encryption ensures compliance with data protection regulations, thus preserving the reputation of the college.
Security Solutions	to ensure data availability and rapid recovery in the event of a breach or system failure.	On-premise and cloud backups meet the college's reliability and accessibility needs. Regularly tested backups mitigate the risks of ransomware attacks, which previously caused downtime.
Security Information and Event Management	Centralize log management, correlate events, and provide actionable information to IT teams.	SIEM tools streamline monitoring across departments and university systems, reducing the time it takes to detect and respond to threats.

(SIEM) Systems.		
Endpoint Protection Platforms (EPP)	Protect individual devices from malware, phishing, and other endpoint-specific threats.	Ensures that workstations in computer labs and administrative offices are protected from malware infections. Improves overall network security by reducing device vulnerabilities.
Regular Patch Management Tools	Keep all systems and applications up-to-date with the latest security patches.	Fix vulnerabilities in outdated university systems that were previously exploited. Ensure that critical software, such as learning management systems, remains secure and functional.

How these tools meet the needs of Colombo Advanced College

1. Enhanced Security

The combination of tools provides powerful protection against external and internal threats, including malware, phishing, and unauthorized access.

2. Business Continuity

Backup and patch management solutions ensure minimal disruption to academic and administrative functions.

3. Scalability

Tools such as SIEM and cloud-based backups can adapt to the institution's expanding IT infrastructure, including hybrid learning platforms.

4. Regulatory guidelines

Encryption and access control measures ensure compliance with data protection regulations, protecting student and staff data.

5. Ease of Management

Centralized monitoring and automation reduce the workload on IT teams, allowing them to focus on strategic initiatives.

Challenges and Recommendations

Challenge

Some tools, such as SIEM systems, can require a significant upfront investment and specialized training.

Recommendation

Ensure staff training and allocate resources for a gradual implementation to maximize the effectiveness of these tools.

Challenge

Relying solely on tools without regular policy updates can lead to gaps.

Recommendation

Combine these tools with security audits and periodic updates to ensure compliance with evolving threats.
Conclusion

The Assets of Colombo Advanced College

• Computer Labs equipped with modern technology for student use.

• Student and faculty databases that store academic, personal, and financial information.

• Servers and network infrastructure that support the college's learning platforms and administrative systems.

• Security technologies – including firewalls, Virtual Private Networks (VPNs), endpoint protection, and intrusion detection systems (IDS).

• Internal communication systems, such as email servers and collaboration platforms.

In this case, the college's key asset is its student and faculty data stored in the databases, as well as the infrastructure that supports online learning platforms.

To ensure the security and availability of critical data, a comprehensive disaster recovery strategy is recommended. This should include regular and automatic data backups from the primary servers to a secondary, secure location. Backups should be frequent to minimize data loss in the event of a disaster. Additionally, a disaster recovery site with the necessary hardware and infrastructure should be established as a failover point if the primary data center is compromised.

Regular testing of the disaster recovery process is important to ensure the plan's effectiveness. This testing should involve both anticipated and unforeseen events to ensure that operations can be quickly restored to the backup servers in case of emergencies.

Backup power sources such as generators and redundant internet connections should be maintained to ensure continued operations during power outages or network disruptions. Storing backup data in a geographically

separated location, such as a cloud service, can offer extra protection in case of disasters affecting the primary datacentre.

Comprehensive documentation of the disaster recovery plan, including protocols, contacts, and equipment inventories, should be prepared and regularly updated. This will ensure that all stakeholders are well-informed and prepared to respond effectively in the event of a disaster, ensuring the continuity of the college's operations and safeguarding its vital data.

Critical Examination of the Advantages and Disadvantages of the Planned ISMS for Colombo Advanced College

Advantages of the Planned ISMS	Disadvantages of the Planned ISMS
Compliance with International Standards • The ISMS is designed to align with ISO/IEC 27001, which provides a globally recognized framework for managing information security. • Ensures adherence to legal and regulatory requirements, such as data protection laws, enhancing trust among students, staff, and stakeholders. **Structured Risk Management** • The ISMS provides a systematic approach to identifying, assessing, and mitigating risks. • Reduces vulnerabilities like ransomware and phishing attacks, which have previously disrupted operations. **Enhanced Data Protection** Implements strong encryption, access controls, and backup systems to safeguard sensitive data, including student records, research outputs, and administrative information. Supports the college's shift towards hybrid learning by securing online platforms and remote access. **Improved Incident Response** • Includes a formal incident response plan, enabling the college to respond swiftly to security breaches and minimize downtime. • Regular security drills and monitoring systems enhance preparedness.	**High Implementation Costs** • Complying with international standards such as ISO/IEC 27001 requires significant financial investment in tools, technologies, and training. • Budget constraints may hinder the complete implementation of the system. **Complexity of Implementation** • Establishing an ISMS involves multiple stages, from risk assessment to monitoring and continuous improvement, which can be time-consuming and resource-intensive. • Resistance from staff and students who are unfamiliar with security protocols may delay implementation. **Dependence on Regular Updates** • The effectiveness of the ISMS depends on continuous updates to security policies, tools, and training programs. • Neglecting these updates could lead to vulnerabilities and reduced compliance. **Potential for Overhead in Administration** • Managing an ISMS requires additional administrative effort, including

Scalability and Adaptability • The ISMS can grow with the college's evolving infrastructure, including new digital systems and hybrid learning models. • Flexible enough to incorporate emerging technologies and address evolving threats. **Promotes a Security-First Culture** • Incorporates staff and student training programs, raising awareness of cybersecurity risks and best practices. • Reduces human errors, a common vulnerability in educational institutions.	documentation, audits, and compliance checks. • For a college with limited IT staff, this could strain resources. **Risk of Misconfiguration** • Tools like firewalls, intrusion detection systems, and access controls must be configured correctly. Misconfigurations could inadvertently expose the network to threats or disrupt legitimate activities. **Initial Productivity Impact** • Implementing new security protocols, such as multi-factor authentication (MFA) or strict access controls, may initially disrupt workflows for staff and students. • Adjusting to these changes may require time and cause temporary inefficiencies.

Evaluation against Key and International Standards

Alignment with ISO/IEC 27001

- **Advantages**:
  - Provides a comprehensive framework for protecting information assets.
  - Ensures accountability through regular audits and certifications.
- **Disadvantages**:
  - Requires rigorous documentation and adherence to protocols, which may be challenging for an educational institution with diverse operations.

Comparison with NIST (National Institute of Standards and Technology)

- **Advantages**:
    - NIST standards, like the Cybersecurity Framework, complement ISO/IEC 27001 by offering detailed guidelines for technical implementation.
    - Focus on incident detection and response aligns well with the college's need for improved resilience.
- **Disadvantages**:
    - Implementing multiple standards simultaneously could increase complexity and costs.

Relevance to Colombo Advanced College

- Aligning with these standards ensures robust protection for sensitive data and continuity of academic operations.
- However, balancing compliance requirements with the institution's unique needs and budget constraints remains a challenge.

CONCLUSION

Colombo Advanced College is committed to providing excellent educational services and continuously improving its processes. The goal of this project is to improve the security system of the college, as some of the current security protocols still have weaknesses. To protect the college's assets, several security solutions can be implemented, such as firewalls, VPNs, and DMZs. The use of biometric devices, network traffic filtering, and encryption of communication channels help protect the university's systems and data from physical and cyber threats. In addition, security techniques such as penetration testing, security audits, risk analysis, and security control checks can be used to prevent unauthorized access to sensitive information. Having a disaster recovery plan in place will help protect the entire facility from all types of potential risks, both physical and digital. Colombo Advanced College complies with various laws and regulations, such as data protection laws, to ensure that strong security measures are maintained to protect institutional and student data. By implementing these security measures, protocols, and best practices, Colombo Advanced College can improve its security and better protect its assets and stakeholders from potential threats. With these safeguards, the college can continue to provide high-quality services while minimizing the risk of security issues.

References

References

Anon., 2018. *NAT.* [Online]
Available at: https://media.geeksforgeeks.org/wp-content/uploads/staticRFWE.png
[Accessed 13 12 2024].

Anon., 2021. *IT security consists of two areas.* [Online]
Available at: https://www.crowdstrike.com/en-us/cybersecurity-101/cybersecurity/it-security/#:~:text=IT%20security%20can%20be%20divided%20into%20two%20main,as%20faulty%20hardware%2C%20network%20failures%20or%20software%20glitches.
[Accessed 11 12 2024].

Anon., 2023. *availability.* [Online]
Available at: https://www.geeksforgeeks.org/the-cia-triad-in-cryptography/
[Accessed 12 12 2024].

Anon., 2023. *Types of Confidentiality Violations.* [Online]
Available at: https://www.geeksforgeeks.org/information-security-confidentiality/
[Accessed 11 12 2024].

Anon., 2023. *VPN Types.* [Online]
Available at: https://www.geeksforgeeks.org/types-of-virtual-private-network-vpn-and-its-protocols/
[Accessed 11 12 2024].

Anon., 2024. *firewall.* [Online]
Available at: https://www.fortinet.com/resources/cyberglossary/firewall
[Accessed 11 12 2024].

Anon., 2024. *IT SECURITY.* [Online]
Available at: https://www.ibm.com/topics/it-security
[Accessed 8 12 2024].

Anon., 2024. *phising attack.* [Online]
Available at: https://www.cloudflare.com/en-gb/learning/access-management/phishing-attack/
[Accessed 11 12 2024].

content79qw, 2024. *penetration testing.* [Online]
Available at: https://www.geeksforgeeks.org/what-is-penetration-testing/
[Accessed 11 12 2024].

deRitis, C., 2022. *risk matrix.* [Online]
Available at: https://www.garp.org/risk-intelligence/technology/risk-matrix-approach-221007
[Accessed 11 12 2024].

Gibson, K., 2023. *risk management.* [Online]
Available at: https://online.hbs.edu/blog/post/risk-management
[Accessed 11 12 2024].

Hathaliya, J. J., 2020. *security procedure.* [Online]
Available at: https://www.sciencedirect.com/topics/computer-science/security-procedure#:~:text=A%20security%20procedure%20is%20a%20predefined%20sequence%20of,or%20function%20in%20a%20consistent%20and%20repetitive%20manner.
[Accessed 11 12 2024].

Iacoviello, A., 2024. *change management.* [Online]
Available at: https://www.ibm.com/topics/change-management
[Accessed 4 12 2024].
Martin, C., 2022. *security audit.* [Online]
Available at: https://www.isaca.org/resources/news-and-trends/industry-news/2022/an-integrated-approach-to-security-audits
[Accessed 11 12 2024].
Mather, D., 2022. *Benefits of Network Monitoring Tools.* [Online]
Available at: https://securitygladiators.com/network/monitoring/benefits/
[Accessed 11 12 2024].
Pantelakis, A., 2024. *oraganizational policy.* [Online]
Available at: https://resources.workable.com/tutorial/policies-any-organization-should-have-plus-templates
[Accessed 11 12 2024].
Sahoo, C. K., 2024. *how it works.* [Online]
Available at: https://qualysec.com/what-is-security-audit/#:~:text=During%20a%20security%20audit%2C%20auditors%20closely%20examine%20an,planning%2C%20identification%20of%20critical%20assets%2C%20and%20risk%20evaluation.
[Accessed 11 12 2024].
salvinge, r., 2024. *Importance of Addressing Network Security for Educational Institutions.* [Online]
Available at: https://securetrust.io/blog/enhancing-network-security-in-schools-to-safeguard-against-intrusions/#:~:text=Network%20security%20is%20crucial%20for%20schools%20to%20protect,it%20important%20to%20regularly%20update%20and%20backup%20systems.
[Accessed 10 12 2024].
Yasar, K., 2024. *DRP.* [Online]
Available at: https://www.techtarget.com/searchdisasterrecovery/definition/disaster-recovery-plan
[Accessed 2 12 2024].