Information Security Management System Framework for the University of Colombo

A dissertation submitted for the Degree of Master of Science in Information Security

N.D. Suduwella
University of Colombo School of Computing
Sri Lanka
2019

DECLARATION

The thesis is my original work and has not been submitted previously for a degree at this or any other university/institute. To the best of my knowledge it does not contain any material published or written by another person, except as acknowledged in the text.

Student‘s Name : **N.D. Suduwella**
Registration Number : **MIS/2015/021**
Index Number : **15770212**

Student's Signature : ..... *Date* : .....

This is to certify that this thesis is based on the work of **Mr. N.D. Suduwella** Under my supervision. The thesis has been prepared according to the format stipulated and is of acceptable standard.

Certified by :
Supervisor’s Name : **Dr. Buddy Liyanage**

Supervisor's Signature : ..... *Date* : .....

ACKNOWLEDGMENT

Information Security Management System Framework is a new thing in Sri Lanka. Therefore, getting the support from all stakeholders of the University is a challenging task. To achieve my goal of introducing ISMS for the University of Colombo wasnt that difficult due to educated stakeholders of the University. First, I must thank Professor Lakshman Dissanayake, The Vice Chancellor of the University of Colombo, for his valuable support and encouragement to introduce the ISMS framework for the University of Colombo. Then I had lengthy conversations with the Registrar and the Bursar of the University of Colombo about the proposing project. All administrative officers had given their full of support to succeed my project. Also, I was given essential support by Director UCSC, Professor KP Hewagamage and Deputy Director Dr. Ajantha Atukorale to get the recommendation and approval from the meeting of the Planning and Development Committee. Then I had some meetings about my project with Dr. Kasun De Zoysa and Dr. Chamath Keppetiyagama, where they gave me some great ideas to include in my thesis report and these ideas help me to motivate and follow the right path. I should like to thank Mr. Kenneth Thilakarathne and Dr. Buddy Liyanage for their tremendous support in completing my project and driving me along the right path. Dr. Buddy Liyanage had given online support where I needed information security expertise and his experience helped me a lot. Finally, I would like to thank my brother for helping me complete my final thesis report and the University of Colombo administrative staff who shared their knowledge and experience with me.

ABSTRACT

Information Security is an important and serious factor for any organization. Previously the focus has been on Information Technology security and the implementation of such security mechanisms were assumed to be the responsibility of the IT department and technical experts. However, this trend is changing due to new aspects of business processes and business aspirations in a digital world. The integration of business activities together has made information more vulnerable, not just the Information Technology used to process the information. To address such situations, IT security controls themselves are not enough to mitigate vulnerabilities to an organization. To address such situations, a worldwide international standard was required. The ISO 27000 family of security standards was developed to help organizations to protect their important assets. Furthermore, many developed countries have developed their own versions of security standards. In Sri Lanka we currently do not have any local standardization to assist in protecting local businesses and organization which are regularly subject to security incidents and vulnerable to information security risks. The main idea was to have an Information Security Management System for the University of Colombo, and thereby develop a localized security standard aligned to the laws and regulations of the government of Sri Lanka. By helping small organizations to use a local standardization, based on local laws and regulations provides the opportunity for such organizations to secure themselves without having to spend vast amounts trying to obtain international standardization.

Due to limited time offered to complete the project, this Information Security Management System framework is intended to provide a suitable risk assessment and a risk treatment plan to address identified hazards. It will reduce the risks arising from critically identified vulnerabilities that University system has and go towards eliminating any unacceptable security practices within some administrative departments. In this thesis, the main concentration and effort was given to the creation of an Information Security Incident Management system for the University of Colombo staff instead of creating systems to manage all risks observed when doing the risk assessment. The ISMS project will help the University of Colombo achieve a level close to the

international standard regarding information security and assist in growing the quality of work. The ISMS would provide the ongoing opportunity for the University to keep the system under constant review and apply modern technologies and new techniques with the recommendation of Information Security Steering Committee.

Contents

List of Figures

List of Tables

List of Abbreviations

CCIS	Centre for Contemporary Indian Studies
CGU	Career Guidance Unit
CIA	Confidentiality, Integrity, Availability
CIUC	Confucius Institute of University of Colombo
CSHR	Centre for the Study of Human Rights
DNS	Domain Name System
DPC	Department Procurement Committee
HETC	Higher Education for the Twenty-first Century
ISSC	Information Security Steering Committee
IATRS	Institute of Agro-Technology and Rural Sciences
IBMBB	Institute of Biochemistry, Molecular Biology and Biotechnology
IEC	International Electrotechnical Commission
IHRA	Institute of Human Resource Advancement
IIM	Institute of Indigenous Medicine
IOUC	International Office University of Colombo
IRP	Incident Response Plan
IRQUE	Improving Relevance and Quality of Undergraduate Education
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology

LMS	Learning Management System
NEREC	National Education Research & Evaluation Centre
NILIS	National Institute of Library & Information Sciences
NOC	Network Operations Centre
PC	Personal Computer
PDCA	Plan, Do, Check, Act
PwC	PricewaterhouseCoopers
RMU	Research & Management Unit
RTP	Risk Treatment Plan
SDC	Staff Development Centre
SPARC	Social Policy Analysis & Research Centre
SPC	Sri Palee Campus
SANS	SysAdmin, Audit, Network and Security
UCSC	University of Colombo School of Computing
UOC	University of Colombo
UPS	Uninterrupted Power Supply

Chapter 1

INTRODUCTION

Concerns about the security of electronic networks and information systems as well as the number of increased network users and the value of their involvement have increased. Several factors have been combined to bring information and communication security to the top of the organizational policy agenda. Some widely reported viruses have been released on the Internet, causing extensive damage through information destruction and denial of access to the network [2]. Such security problems are not confined to individual but spread quickly across the network. Recently most countries experienced a ransom-ware attack globally, which was one of the major cyber-attack ever happened on this planet.

While security has become a key challenge for policymakers, it is becoming increasingly complex to find an adequate policy response. Only a few years ago, Security of computer systems was limited to large organizations and focused on access controls. Initiating a security policy was a comparatively simple task. Because of a variety of developments in the broader market context, this situation has now changed considerably, including liberalization, convergence and globalization. End-user terminals such as PCs, mobile phones, etc. have become an active element in the network architecture and can be connected to various networks [2].

An information security management system provides an organization to keep their business on track without worrying about any failure due to security incidents where it would reduce and mitigates security incidents. An Information Security Management System (ISMS) provides information to be shared whilst ensuring it's protection.

Statistically equipment theft is a real problem, the most damaging aspect is the loss of data and software. Sources of damage such as computer viruses, computer hacking and denial of ser-

vice attacks have become more trivial, more determined and increasingly practical.The internet exposes organizations to an increased risk of improper access to networks, corruption of data and the introduction of viruses. The percentage of organizations reporting hacking incidents has trebled, with telephone systems as a new target. Not all infringements result from crime, as well as inadvertent misuse and human error. Virus infections are still the single most prevalent form of abuse. It is just as destructive as crime, are threats like fire, system crashes, and power cuts [2].

Poor staff supervision and lack of proper procedures for authorization are often highlighted as the main causes of security incidents. Companies vary in their approach to preventing security breaches, some prohibit everything, making mundane access tasks difficult, others are not sufficient and permit access to all by all, exposing themselves to a high degree of risk. Efficiency in business depends on the right balance, and this is where standards can help.

Dependency on information systems and services means that organizations are more sensitive to security threats. Interconnecting and sharing information resources between public and private networks boost the difficulty of obtaining access control. The trend for distributed computing has depleted the effectiveness of central, specialist control.

1.1 University Perspective

The University relies mostly on manual procedures for handling and processing information that support many of its activities. Information shared and managed by the University needs to be adequately secured to protect against the consequences of breaches of confidentiality, failures of integrity, disruption of availability and failure to comply with legal, statutory or regulatory requirements.

The core principles of information security are confidentiality, integrity and availability, and it is vital that we have the ability to protect these three aspects of information security regard to the University information assets.

University of Colombo is the leading and number one university in Sri Lanka for a number of reasons. But the University doesn't have proper mechanism to protect important assets of the business process. Neither Sri Lankan university has a proper method to secure its critical assets.

University of Colombo has several administrative departments to achieve their common goals. These different departments have different goals that will be added together to achieve the University's future goals. The main goal of the university is to provide students with quality education.

Information security steering committee

Information security steering committee helps to identify all stakeholders of the organization and which would help to apply information security in to the business model of the organization. The steering committee should communicate with all stakeholders in-order to create a proper framework for the organization.

Organizations are becoming increasingly aware that it could expose them to unsustainable risk if they fail to implement successful security management processes.

The steering committee works are very high demands, where they should coordinate security strategies, examine working processes, and identifying the required information security expenses to reduce any risk by applying adequate security controls [3].

Information security steering committee is the main body which is responsible for protecting the assets of the organization from security incidents.

Establishment of information security steering committee recommended by the planning and development committee of the University of Colombo. Then the committee decided to obtain permission and approval from the Senate Committee to appoint the required people to the Information Security Steering Committee.

List of administrative departments of the University

- Academic Establishment.
- Academic & Publication.
- Finance Division.

  Accounts.

Supplies.

Payments.

Salaries.

Research & Management Unit (RMU).

Shroff.

- Capital Works & Planning.
- Examination Branch.
- General Administration.
- Student & Staff Affairs
- Network Operations Centre (NOC)
- Non-Academic Establishment

All of these departments have critical data or information that is either supported by the information security triad (CIA) or a combination of such aspects as confidentiality, integration and availability. But it will be based on how critical, impact and likelihood the data will be when talking about securing those.

1.2 Importance of Information Security

Information could be any kind such as hard files, storage, network systems, computer systems, employees, strategic plans. Therefore, protecting sensitive data is more essential to the organization. Information security maintenance and up to date improvement would help any organization to keep their business competitive in the global market.

Some computer systems may not design well enough to support technical security controls to be implemented. Therefore, such systems must be controlled through management and administrative controls. Information security management is necessary to have careful planning and all stakeholders support. It may require consultancy supports from outside the University.

- It is applicable to all administrative departments of the University
- It is applicable to any type of information or data

- It is applicable to protection of any type of information or data

High-level management Support of the ISMS

ISMS proposal was submitted to the planning and development committee meeting. Before submission of the proposal, had some lengthy conversations with stakeholders of the University of Colombo such as vice chancellor, Registrar, Bursar, Librarian and top-level administrative officers. After submitting to the meeting, the proposal was given to the Director, UCSC to examine and come with his consent about the ISMS proposal. Then it was examined by some senior lecturers of the UCSC and finally recommended to proceed the proposal. Planning and development committee decided to have an information security steering committee to initiate the ISMS framework.

Specific problem going to address within the project

While the University of Colombo is a large university, this project will be focused on ISMS for Administrative works of the University. Where it is centralized at the College house premises of the University.

There are persistent issues at every department. Where some of those issues specific to departments and others are common to all departments. No proper working procedures were the biggest issue in the current university system. It's really improper when things don't happen in a precise procedure. Everyone gets frustrated, people who are working and people who are seeking their service. This issue is mainly due to government regulations and procedures, and changes made by government are not fast enough to adopt changes in global technology. Some government procedures are very old, and those procedures need to be refined, but they don't happen at all. This is really the disaster at all government offices, not just the university system.

There are no clear procedures on behalf of the University and mostly nobody knows which is the best way to do related work. Sometimes the same work is done in numerous ways. There are many examples.

- Applying for leave (Foreign leave, study leave, medical leave, etc.)
- Payments for service providers (Building contractors, utility providers, IT services, etc.)
- Requesting, recommendation and approving processes

- Requesting services from internal departments (IT department, maintenance department, general stores, etc.)
- Vehicle arrangements
- Reservation of Board Rooms
- Recruitment exams

Accessing the University premises and assets needed to look as main security threat of the University. Because there is no exact way to track or monitor human activities. Access to premises should only be permitted for certain people. There must be an ID system for everyone who access and use University premises. At least there should be a way to track and monitor people accessing administrative departments. There should be an identification system to track who is accessing the Administrative building and the main building of the college house. University has issued university identification cards to all staff members, but only very few people wear it. They should wear it when they're at the University premises.

Virtual access to University assets should be monitored and there should be a proper mechanism to track suspicious activities to reduce and protect important virtual data.

1.3 Objectives

The main objective of this project is to do the appropriate work efficiently and effectively. All procedures should be easy to understand and carefully followed. Everything will be documented and refine in a timely manner. Adequate technology changes could be implemented quickly enough to match other top-ranking global universities around the world. Expecting somewhat higher quality of service and production due to the University's work efficiency.

Due to time constraints, the ISMS Framework had to narrow down to process identification, risk assessment and to establish an information security incident management system for the University of Colombo administrative office staff members.

1.4 Research Problem

Summary of The University of Colombo Information Security breaches and incidents occurred within last five years.

Security incident / Year	**Damage / Level of Damage**	**How did the incident handle?**
Examination branch hard disk failure on a windows PC-2015	Loss of examination data and marks - High	Had to re-enter all those data again using hard copies of examination marks and other things. It took more than a week to re-enter all those data.
Major hard disks and server failure on the web server-2013	Loss of web server database, users, templates and other important assets - High	Had to re-arrange the web server from the scratch
Fiber cable damage of the main ring network due to renovation of the Mathematics building - 2014	Loss of network redundancy of the University - Low	It was bit difficult to find the right place where the fiber was damaged and fixed it. This incident resulted somewhat financial loss for the University
Power failure at the College house premises, University of Colombo - 2014	No internet connection for most of the faculties in the University and most important works had to hold till the power is back on - Medium	It was beyond the control of the University
Core network switch (Layer 3 network switch) failure at the Network Operations Centre (NOC) - 2014	No internet connection for most part of the University - Medium	Had to replace a new network switch with desired configuration

One of the core network switch failure (Layer 3) at the Faculty of Arts due to lightning - 2015	No internet connection for the entire faculty - Low	Replaced network switch with desired configurations
Fiber cable damage of the network due to maintenance of the access road at the faculty of science - 2015	No internet connection for the Marshall office and the Medical Centre of the University - Low	Had to fix the damaged fiber cable
Main website hacking 2014,2015,2016	Unavailability of the University of Colombo website - Medium	Re-established the website after finding the hackers invention part and fixed those bugs which were used by hackers to gain the control of the University website
Unavailability of the University of Colombo web server database and user accounts - 2015	Unavailability of the University of Colombo website - Low	Had to re-configure University of Colombo web server with using the latest backup
Main proxy server failure of the University - 2014	Unavailability of the Internet connection - Low	Had re-configure main proxy server from the scratch
Botnet kind network attack - 2016	Using of University of Colombo bandwidth which shows unusual traffic on University of Colombo upstream path - High	Restrict access within the network and used better access control method only to allow needed services from outside networks
Fiber cable damage of the main ring network due to renovation of the Faculty of Arts internal road - 2016	Loss of network redundancy of the University - Low	It was difficult to locate the place where the cable has been damaged from more than one places. Financial loss for the University

Crashing firmware of the access network switches around the University-2017	Loss of network connection for period of time. No availability of network - Medium	It was due to product failure which was admitted by the supplier and agreed to change network switches whenever the University needed.
Network rack system failure at NOC - 2017	Loss of redundancy of the power supply given to servers in both server racks - Medium	Server rack failure happened due to power outage of the server rack UPS system. With the agreement, supplier has fixed it and install in the server rack.
Main website hacking - 2017	Unavailability of the University of Colombo website - Medium	Recovered it and patch those web vulnerabilities we had.
Power failure at the UOC - 2018	Loss of power supply for the server rack system. Unavailability of network for the whole University - High	This was happened when the college house had some issues on the power generator. Fixed the generator.
Firewall failure due to fluctuation of power supply after main power supply was down - 2018	Loss of network connection of the University of Colombo - High	Had to reinstall the firewall software with the help of checkpoint firewall agent
DNS server failure - 2018	Loss of access to Internet and the University of Colombo website - Medium	Reconfigure the DNS server without vulnerabilities
Faculty of arts main switch failure due to lightning - 2018	Loss of network connection at the faculty of arts - Low	Replace the switch with new layer 3 network switch

Faculty of science main switch failure due to power failure at the faculty of science mathematics building - 2018	Loss of network connection at the faculty of science - Low	Fix the power at mathematics building.
Data loss of a supplies branch desktop PC - 2018	Loss of very important and critical needed data (Unavailability of data) - High	Had to hard done the work again. Not able to recover original data.
Database Crash of the Faculty of Medicine Learning Management System - 2019	This incident results major loss to the Medical students and staff of the University - High	There were no hard Backups for the Medical Faculty LMS. Although the Backup system is running there is no scheduled backup for those valuable data of the University. Needed to fix the issue by hard coding the LMS again with old data. It only could fix up to 80 percentage of the system.

Table 1.1: Summary of Information Security Incidents

The implementation of the Information Security Incidents Reporting and Management System would help to mitigate above security incidents in the future, thus it would help to reduce the damage by taking care of security incidents as early as possible. Further investigation into international standards and related documents is essential to create a comprehensive ISMS framework for the University.

Chapter 2

LITERATURE REVIEW

2.1 Adhered International standards and frameworks

Information Security Management System

An ISMS is a standardized way to protect sensitive company information. A risk management process consisting of people, processes, IT or non-IT systems and assets. It would help any organization in any sector to keep information assets secure [4].

ISO 27000 [5]

The ISO / IEC 27000 family of standards help organizations to keep information secure. Therefore, it is mandatory for any organization to use well-known international standards to manage their organizational resources and valuable information which is important to the continuity of any business type. When creating an information security framework, the best approach is to follow the best known international standard and apply it appropriately in the university administrative system [4].

ISO 31000 vs ISO 27005

ISO 31000 risk management [6]

ISO 31000 standard more directed to the risk management process, and it contains different vision, both standards address the risk management process in the similar manner.According to the ISO 31000, organizations typically determine the context and manage risk by identifying it, analyzing it, and then evaluating whether the risk should be modified by a strategic approach to meet their risk criteria. Throughout this entire process, university must communicate and

consult with stakeholders, while critically monitoring and analyzing the risk and controls that modify it, to ensure that no additional risk management approach will be required [4].

ISO 27005 risk management [6]

As for ISO 27005, information security risk management should define context, assess the risk, and address them through a clear plan for implementing recommendations and decisions.Risk management will cover all processes of an organization to cover all risks and their level of security to reduce risks to an acceptable level before taking a decision regarding exposed risks. This standard includes decisions on risk analysis and treatment as risk acceptance activities will ensure that residual risks are explicitly accepted by the University of Colombo Steering Committee. This is very important in such situations where control implementation is either eliminate or postponed for time being [4].

Risk management best practices has been changed over the time due to variety of organizational needs.The Well-known complete standardized system would help the university to manage risks effectively and efficiently. ISO 31000 could be considered as the main standard, which provides overall guideline for managing a risk in a proper systematic way. ISO 270005 is a particular standard that helps the ISO 31000 by providing better way of managing risks.

According to these cons and pros of ISO 31000 and ISO 27005, decided to use ISO 27005 risk management methodology instead of ISO 31000 methodology. Where ISO 27005 standard provide better comprehensive risk management process and this is the standard we should apply when doing a risk management for first time. We could use ISO 31000 standardization after establishing a risk management system through ISO 27005 standard, where we could implement a proper risk management procedure with better approach on strategic point of view. Both standards will help to have a complete risk management system.

2.2 Sample projects

The University of Waikato, New Zealand has created an Information Security Standard framework based on ISO 27000 and the law of the government of New Zealand [7]. They used structural framework method, this documentation would help the University of Colombo to design better framework.

The University of Arizona has an Information Security Steering Committee that covers all important stakeholders and involves their top management decision-makers. The Steering Committee of the University of Arizona is composed of high-level administrators representing the strategic interests of the entire university. They meet regularly (Quarterly) to provide guidance on strategic directions, oversee the University road map, provide recommendations on the most pressing priorities, and generally provide advice and support to the University team [8].

ISMS research paper was published by the Laurea University of Applied science in Finland. The researcher found those security management systems may required to learn about laws and regulations of global, country and sector, which your organization falls to. They also found that there are different standards for information security management, and it is essential that we select the most appropriate one for our organization [9].

2.3 Information Security Incident Reporting and Management

Due to time constraints of the project, more effort given on the information security incident reporting and management unless concentrating on all other departments of the University. It is very much essential as many information security incidents were reported recently. ISMS project is a massive project if you follow the right standards and procedures. Considering these facts and time of the project, focus was made to solve the most valuable aspect of the University of Colombo's information security.

Recently, there have been numerous information security incidents reported. The University of Colombo suffered a great loss of assets and time to recover from those incidents and the damage was invaluable to the University. Table 1 shows some of the security incidents reported in recent years. And there are the same kind of incidents happening over and over again.

Chapter 3

METHODOLOGY

3.1 Scope

Scope of this is an Information Security Management System for administrative activities of the University of Colombo. Where main concern would be on Administrative and Financial activities of the University. In this project, all non-academic and administrative staff of the University will be considered and their related works. Risk management will only base on ISO 27005 standard where it will not consider ISO 31000 standard.

Information collection

All required information gathered from each administrative departments of the university. Had small meetings with heads of departments to explain purpose and benefits of having a security framework for the University. Required information gathered to create procedures and processes by having interviews with staff of the administrative departments. All gathered information signed off by heads of departments to ensure accuracy and the quality.

Selecting Controls

When risks and security requirements were identified, risk treatment plan should be enforced to use suitable controls mitigate identified risks. This selection criteria will be finalized and review by the Information Security Steering Committee [10].

3.2 Evaluation criteria

Project will be evaluate using information security risk assessment and risk treatment plan document of the propose ISMS framework for the University of Colombo administrative and financial activities. Planning and Development committee meeting minutes will be attached due to there were no Information Security Steering Committee established yet. Information security steering committee establishment is late due to security and other procedures of the University of Colombo. Information security framework will be signed off by Vice chancellor of the University of Colombo. With Vice chancellors signature on it will legalize the security framework documentation and to use it in the University of Colombo [11].

Importance of Information Security

An information security framework is a series of documented processes that are used to define policies and procedures around the implementation and ongoing management of information security controls in the University. This framework is basically a ”blueprint” for building an information security program to manage risk and reduce vulnerabilities. Information security pros can utilize these frameworks to define and prioritize the tasks required to build security into the University. Proper maintaining of security framework will result higher security level of the University assets and related works [11].

Frameworks are often customized to solve specific information security problems, just like building blueprints are customized to meet their required specifications and use. The framework that is developing for specifically to Sri Lankan government and University laws and regulations. Also, frameworks are easy to read and understand. It helps all stakeholders of the University to understand and use the framework for better usage [11].

It is the responsibility of the University senior management to sufficiently resource the system and direct the team or individual to implement the Framework for betterment of the University in the future [11]. The University's Information Security Framework is intended to:

- Ensure everyone understands the Universitys expectations around acceptable use of University information assets and IT facilities.
- Ensure everyone is aware of the several types of information which the University uses and can recognize and manage the associated range of risks and threats.

- Ensure everyone clearly understands their role and responsibilities in respect of information security management.
- Reduce the likelihood of information security breaches and information loss by ensuring information security requirements are understood at all levels of the University.
- Ensure that we could meet our statutory, regulatory and contractual obligations and any other agreed standards or approaches in respect of information security of the University [12].

Expected Benefits

- User awareness
- Compliance with required laws and regulations
- Improving confidentiality, integrity and availability
- Safeguarding critical information
- Prompt actions regarding security incidents to minimize the damage
- Meeting international benchmarks of security
- Proper procedures for all administrative works of the University
- Better backup procedures and mechanisms for hard and soft data
- Much more improved work efficiency
- Doing all related works in simplest feasible way
- Clear and complete auditing system for the University assets
- Easy to design and plan to meet University future goals [13].

Work plan

- Reviewing the current procedures of Administrative departments
- Go through all the processes included in those procedures
- Design of all administrative department processes and procedures

- Then the risk assessment will be carried out with the process owners and the steering sub-committee for each process
- According to the risk assessment report, the main steering committee will decide what to do, when to do and how to do, based on its business value and other measures
- all those procedures needed to test and refine whether we need to add more or delete some unwanted security measures within processes [13].
- It will create a comprehensive framework for administrative work at the University of Colombo, where it will be signed by the University's Vice Chancellor and sent to the Council for approval (top most decision makers)
- Finally, with the approval of the Council, we could proceed with the proposed framework

Individual responsibilities of University of Colombo employees Access to University information assets will be granted to everyone (e.g. email, teaching and learning materials, staff/student information, financial information, research information, and the systems used to process these). Every user of the University responsible to ensure they are working according to the framework. If an user fail to comply with the mandatory requirements of the framework could result disciplinary action according to the University laws and regulations [12].

Everyone is responsible for protecting the Universitys information assets, systems and IT infrastructure, and will protect likewise those belonging to third parties but used during their work at the University. Protection of university or third party information and assets may be required contractually, legally, ethically or out of respect for other individuals or organizations. Users should immediately report any breach of the University's security policies or threats to, systems or services of the University. The first steps are to inform your Head of the Department [12].

Chapter 4

DESIGN AND IMPLEMENTATION

4.1 University of Colombo Internet and Email User Policy

Introduction

The University of Colombo understands that the staff of the University have the right to access their emails and the Internet for limited personal use.

Purpose

This policy document will provide guidelines to the staff to use of computer systems and networks to carry out day to day duties in their division or a branch.

Policy

The University of Colombo employees may use the Internet for:

- Any work or work-related matters
- Limited authorized personal use

Procedures

Limited authorized personal use

Limited authorized personal use acceptable if:

- It should not affect the duties of the division or the branch.

- It should not impede with operations of University of Colombo.
- It should not breach any security boundaries of the University of Colombo.
- It should not affect on University of Colombo's computer storage capacity.
- It should not reduce University of Colombo's network performance.
- It should not result any additional expense for the University of Colombo.
- It should not breach any laws or regulations of the Country or the University.
- It should not compromise any confidentiality or privacy requirements of the University of Colombo.

Unacceptable use

- To play computer games on your work time.
- To use official email accounts on internet for personal use.
- To use and send offensive, harassing or pornographic messages.
- To visit web sites containing pornographic or criminal material unless it is related to the research or working area.
- To exchange or keep unauthorized sensitive information of the University of Colombo.
- To use internet for illegal activities such as gambling, gaming or conducting a business.
- To create or exchange advertisements using University of Colombo official email accounts and internet. [14].

4.2 Risk Assessment

Risk assessment main idea is to identify threats and risk that could harm important assets to the University. Risk assessment would analyze and evaluate those with the respective of the risk factor and the likelihood of occurring threats. After the identification of harmful threats, risk assessment would provide a threat, elimination or control criteria according to the University needs.

A risk assessment could be a thorough investigation at the organization to spot procedures, processes. Which will cause damage to essential assets of the organization. When identification method is completed, analyzing and evaluating ought to do consistent with however seemingly and severe the risk is. Once analyzing and evaluating method is completed, decide what measures ought to be apply to effectively eliminate or manage any threat from occurring. [15].

Risk Analysis

- It provides how the risks are going to treat.
- Information could be any form of data, which is essential to the organization.
- Estimated level of risk.

Importance of risk assessment

- Identifying who may be at risk.
- Identifying of validity of given security controls.
- Identifying existing security controls are up to date or refine it if possible.
- Ranking all threats and controlling those threats in critically order.
- It should be comply with laws and regulations.

Risk assessment goal

Risk assessment is victimization to gauge threats, take away or cut back the risks by adding management measures. That makes the organization's risk level is low, and it ought to increase the potency of the organization. [15].

Risk assessment should be done

- Before the begin of new processes.
- Before any changes applied to ongoing processes
- When new threats are identified.

Risk assessment planning

- Scope identification
- Resources identification
- Stakeholders identification
- Risk analysis measurements
- Government laws, regulations and University policies.

The risk assessment should be done by an expert team or a person who is experienced and knowledgeable about such systems. On behalf of the University, Heads of departments and co-workers who have knowledge about processes, would be ideal to deal with this risk assessment [15].

To do an assessment:

- Identify threats.
- Impact of the threat.
- Identify required controls to mitigate the risk.
- Check whether the risk has been controlled.
- Further monitoring to check controls are adequate or not.
- Keep all essential information regarding risk assessment.

Identify Threats

Overall, the main objective is to identify possible threats in an organization that are vulnerable and active. To arrange an identification of threats should need to have mix of experience and new staff members of the University. Hazards identifying team should be able to do thorough assessment on all threats which are exposed. The team should be able to list down all possible threats which are exposed and threats which could occur in near future. [15].

To ensure that all hazards are captured:

- Check all processes and procedures for possible connection for any threat
- It should include all departments and related activities.
- Check all past security incidents.
- Carefully check all working procedures to find any threat involvement presented.
- Review all working processes of the organization annually or quarterly.
- Consider outsider's monitoring system. [15].

Identifying a risk

- The work environment.
- Geographical area
- The systems which are used to do desired work.
- User awareness of staff and the students.
- Capability and knowledge of users [15].

Responsibilities

- All members of the University of Colombo are responsible for reporting an information security incident to the responsible person or department.
- It is necessary to report all incidents immediately.
- The Vice Chancellor and senior management are responsible for information security of the University.
- Deans of Faculties, Directors, Department Heads and other Line Managers are responsible for reporting, investigating and taking action in their respective departments following an information security incident.
- The NOC Director is responsible for reporting, investigating and required controls and actions taken.

- The information security team responsible for security incident reporting and management system for the University.

Prioritizing or ranking risks

The best way to determine which risk is the most vulnerable and needed to be monitored immediately is to rank potential risks. Prioritization will be based on exposure, potential and likelihood of such incidents. Risks will be ranked in ascending order through risk prioritization [15].

This risk determination is not easy or simple, because there is plenty to consider when you rank such threats. These threats must be discussed by the team or organization to determine which actions they should use or which techniques are best suited for controlling the risk. Ranking hazards require knowledge of activities, situations, important things, and perception of goals.

By evaluating the work environment with workers ' experiences, some situations could be solved. Sometimes critical or highly technological hazards need to be solved, there should be a knowledgeable team that is familiar with such cases.

Data classification is very important for any organization, where it could determine what kind of data to protect and how valuable things are. Risk ranking should be carried out after all above factors have been considered. [15].

Risk Ratings:

- High: Requires immediate reaction
- Medium: Need to be alert and further monitoring
- Low: Need to monitor

Impact Ratings:

- High: Major Impact (It's very hard to recover)
- Medium: Medium Impact (Damage is somewhat high, but in a certain period it can recover)

- Low: Minimal Impact (Damage is very low and could immediately recover)

Likelihood ratings:

- High: It's likely to happen once or twice a year
- Medium: Can be experienced once two to five years
- Low: Can occur once in a lifetime

Criticality Description Table

Description of Criticality Level	**Level of Score**	**Colour Code**
Very High	Score >25	
High	25 >= Score >20	
Medium	20 >= Score >15	
Low	15 >= Score >10	
Very Low	10 <= Score	

Table 4.1: Criticality description table

Criticality Level Table

Risk Rating	Impact	Likelihood	Criticality Level
High (10)	High (10)	High (10)	30 Very High
High (10)	High (10)	Medium (7)	27 Very High
High (10)	High (10)	Low (3)	23 High
High (10)	Medium (7)	High (10)	27 Very High
High (10)	Medium (7)	Medium (7)	24 High
High (10)	Medium (7)	Low (3)	20 Medium
High (10)	Low (3)	High (10)	23 High
High (10)	Low (3)	Medium (7)	20 Medium
High (10)	Low (3)	Low (3)	16 Medium
Medium (7)	High (10)	High (10)	27 Very High
Medium (7)	High (10)	Medium (7)	24 High
Medium (7)	High (10)	Low (3)	20 Medium
Medium (7)	Medium (7)	High (10)	24 High
Medium (7)	Medium (7)	Medium (7)	21 High
Medium (7)	Medium (7)	Low (3)	17 Medium
Medium (7)	Low (3)	High (10)	20 Medium
Medium (7)	Low (3)	Medium (7)	17 Medium
Medium (7)	Low (3)	Low (3)	13 Low
Low (3)	High (10)	High (10)	23 High
Low (3)	High (10)	Medium (7)	20 Medium
Low (3)	High (10)	Low (3)	16 Medium
Low (3)	Medium (7)	High (10)	20 Medium
Low (3)	Medium (7)	Medium (7)	17 Medium
Low (3)	Medium (7)	Low (3)	13 Low
Low (3)	Low (3)	High (10)	16 Medium
Low (3)	Low (3)	Medium (7)	13 Low
Low (3)	Low (3)	Low (3)	09 Very Low

Table 4.2: Criticality level table

Criticality Ratings:

- Very high: Immediately stop the process and carry out necessary actions.
- High: Investigate the process and implement the necessary controls as soon as possible.
- Medium: Continue the process. But to prevent further damage, the control plan must be implemented as soon as possible.
- Low: Could work on the process and should be adequately monitored to identify threats and be alert.
- Very low: Continue monitoring the threat identification process [15].

Threat controlling methods

When prioritization is done, the organization or team responsible could decide how to control these threats in order to eliminate or reduce the risks for each hazard [15].

There are some hazard control metrics:

- Elimination.
- Technical controls.
- Administrative controls.
- Personal protective equipment.

Importance of assessments reviewing and monitoring

It is very important to know whether the risk assessment is carried out efficiently and effectively. It is also important to review the risk assessment periodically to ensure that your control methods are effective and efficient in managing risks [15].

Important risk assessment documents

Records and risk assessment controls taken on these risk assessments are very important for future activities. Therefore it should be stored securely and should be available whenever necessary.
Documentation of records will depend on:

- Risk level of threats.
- University's legal requirements
- Any other managerial or governmental requirements (Government Acts.).
- It should include records.
- Proper review of threats.
- Determined level of the risk.
- Controls used to manage risks.
- All reviewed and monitored hazards of the University [15].

4.3 Information Security incident reporting and management

Information Security incident reporting and management procedure are essential for any organization. It helps the organization to identify any security threats actively present, and it also helps them to take the actions and control the situation before it gets worst. There are five main aspects of a Security incident management process which are an identification, reporting, investigating, solution and keeping records. The incident management system would gradually grow with past information and rich data which ensures prompt response for the incident if you have experienced such an incident in the past. Therefore, keeping records is essential for a security incident management system.

- Information security incident identification : this step is very important for an organization where, if you couldn't identify incidents everything will be ruined thereafter. User awareness and training on security threats are mandatory for the users.
- Information security incident reporting : This phase requires some qualities from users where they should have a clear idea about security incidents and how they should react and understand the real scenario. Then they will be able to report the incident to a responsible person or a team.
- Information security incident investigation : Investigation phase starts when the incident is reporting to the responsible party where they should able to give an immediate solution and proper guidance to how they should act after the incident. Then the technical expertise people will investigate the incident further.

- Information security incident solution : This phase could be identified when the incident is reporting as well as where all required prompt actions on incidents will be given to users. Main solution would be available after thorough investigation about the incident and it will report to the relevant parties.

- Information security incident records keeping : This phase important to an organization where it may help them to avoid or prompt actions towards the same kind of incidents in the future. Where, it may reduce the time and cost to control of such events.

Goals of incident management system

- Reduce the damage or prevent further damages to critical assets
- Identifying threats and reduce re-occurrence of such events
- Improvement of user awareness and knowledge about security incidents
- Improvement of the University of Colombo reputation

”A whopping 40 percent of all investors and analysts surveyed identify cyber-threats as the single biggest threat to business, compared to just fifth in 2017. And it reached 30 percent in 2019, largely due to the engagement of threat identification and treatment plans for pre-measured information security according to the figure 4.1. Therefore, to manage security incidents within the organization, it is very important to have better reporting and management system of information security incidents [16].

”According to the SANS Institute, documenting the Incident Response Plan is especially necessary as it can be a substantial lifesaver when it comes to incident response, Both in the case of legal action for retention of evidence and lessons learned exercises to improve future incident response capabilities” [17].

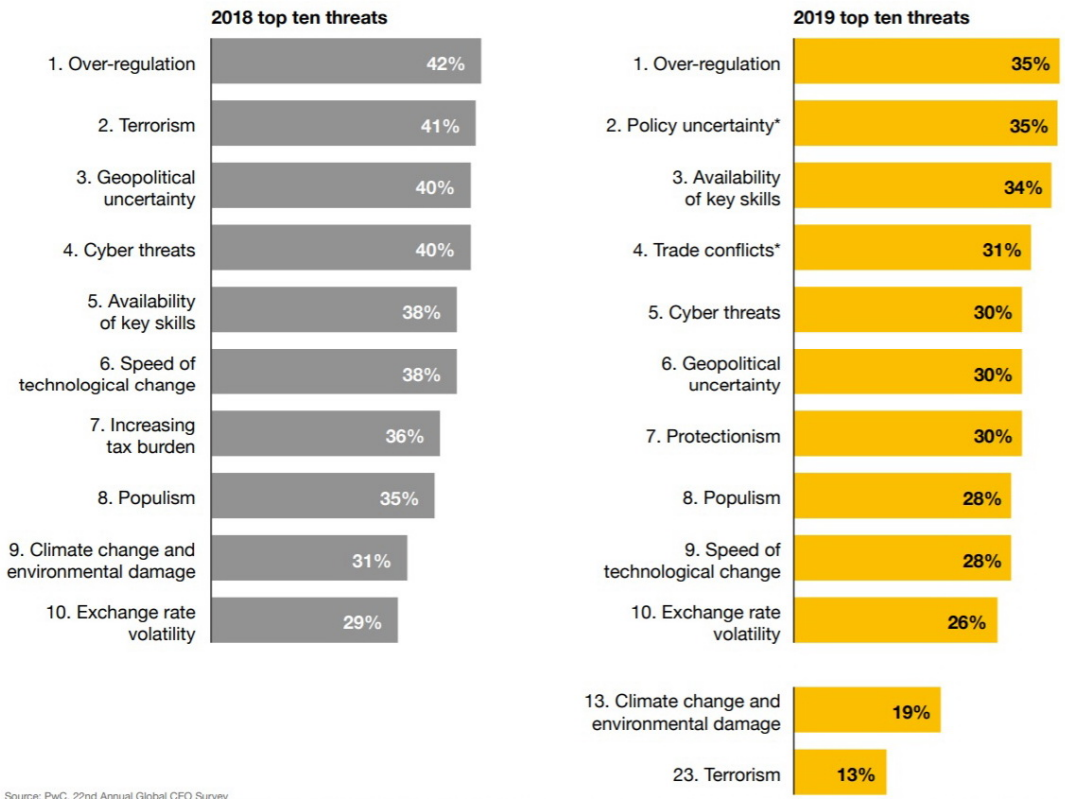


Figure 4.1: Top ten threads [1]

Incident Reporting Procedure

All active information security incidents should be reported immediately. Report active security incidents through one of the following:

- Internal extension NOC Internal extension number
- External NOC General Number
- NOC email address

4.4 Risk Treatment

Risk treatment process

Risk treatment is a significant step in the process of risk management. Risk treatment process begins when all risks are identified after completion of the risk assessment process. Risks that are not acceptable should be selected to do the risk treatment for each unacceptable risk. Risk treatment step will select one or more available options to address each unacceptable risk. Decide primarily how to reduce or mitigate all these risks [18].

Risk Treatment Plan

- The University should identify assets, risks involvement, damage and required controls to mitigate any threats.
- This should be in the University security policy and it should clearly mention how you are going to manage risks.

This plan could clearly identify in the plan do check act cycle of the information security. Where it links all four phases of the cycle [18].

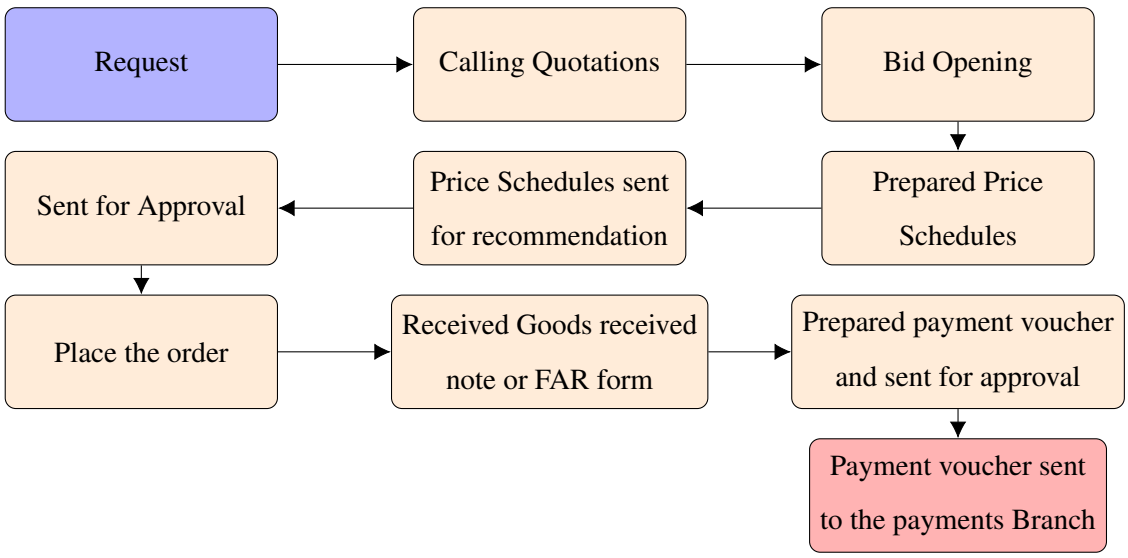
4.5 Working procedures and processes of the University of Colombo

Note: These processes and procedures have been validated by respective heads of departments and signed attestation has attached in Appendix C

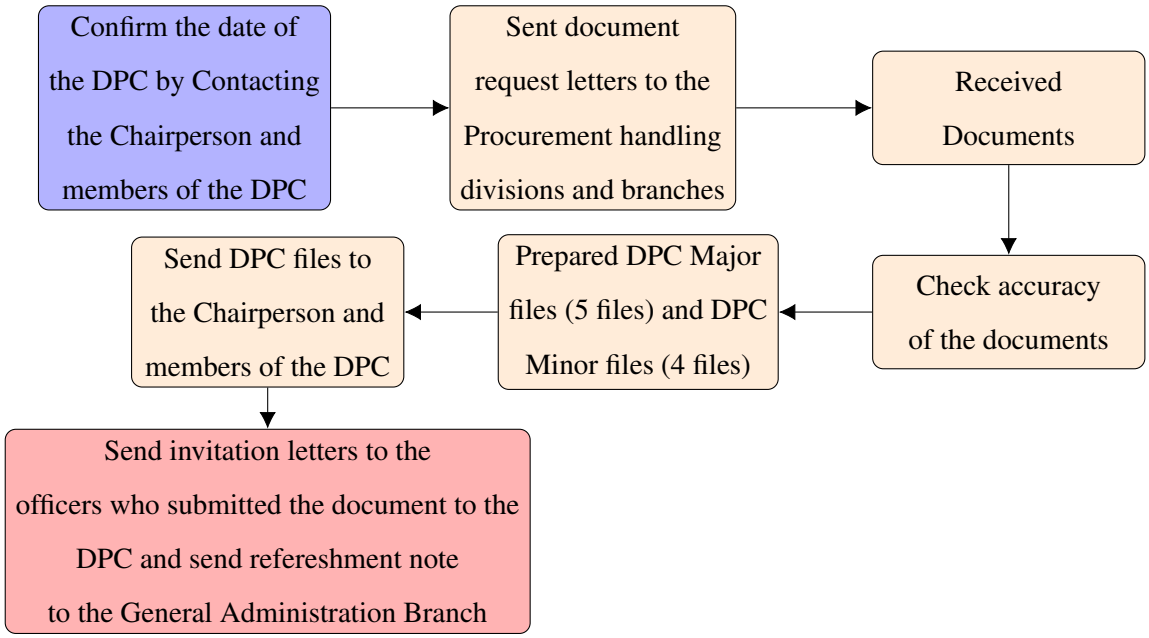
Administrative Departments

Finance Division

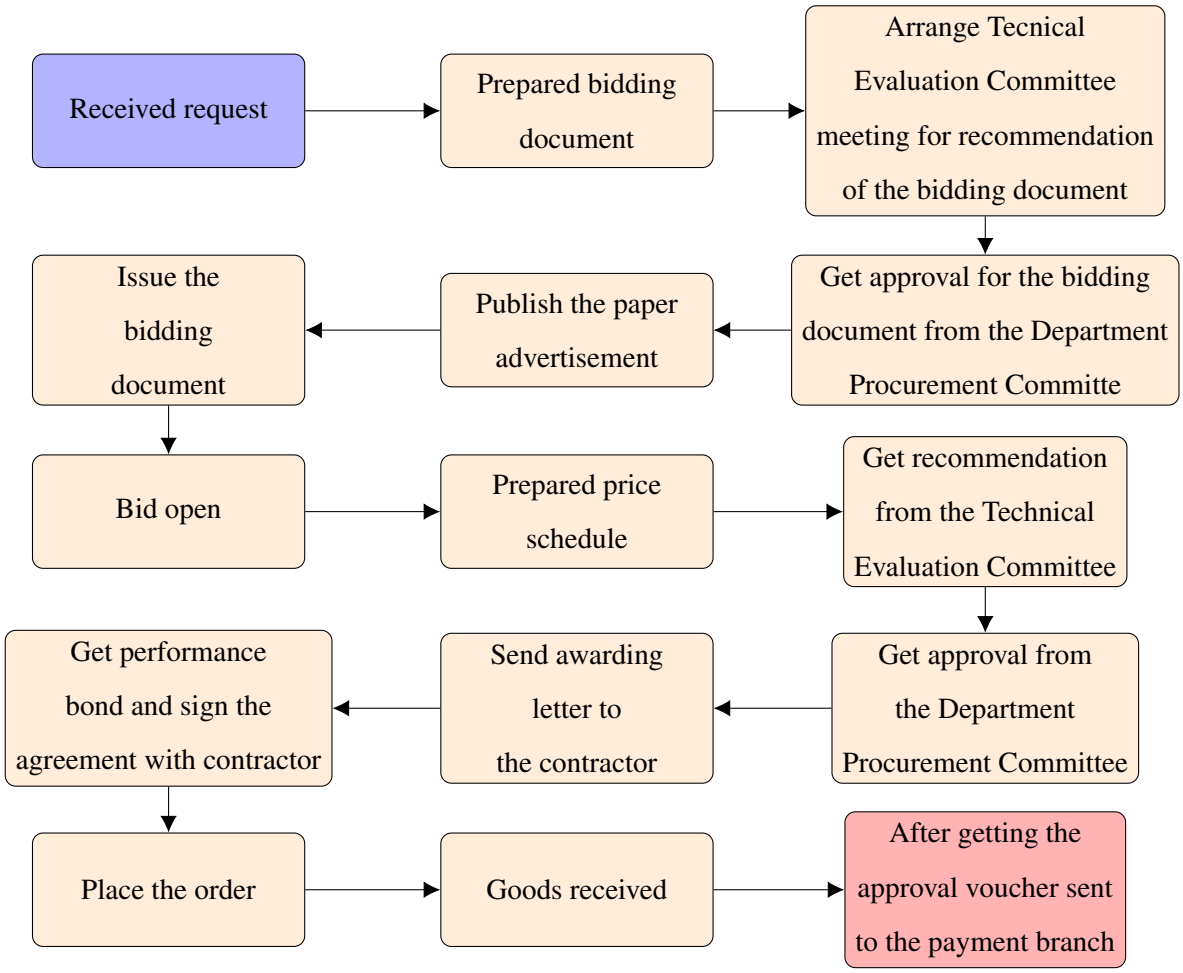
- Process of the purchase of Goods / Services



- Department Procurement Committee Meetings

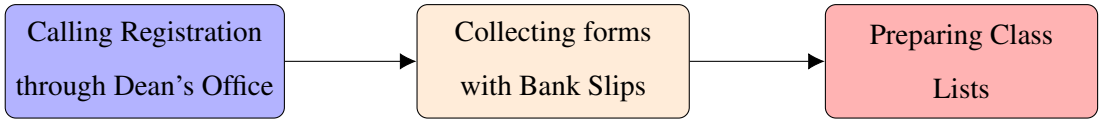


- National Competitive Bidding Procedures

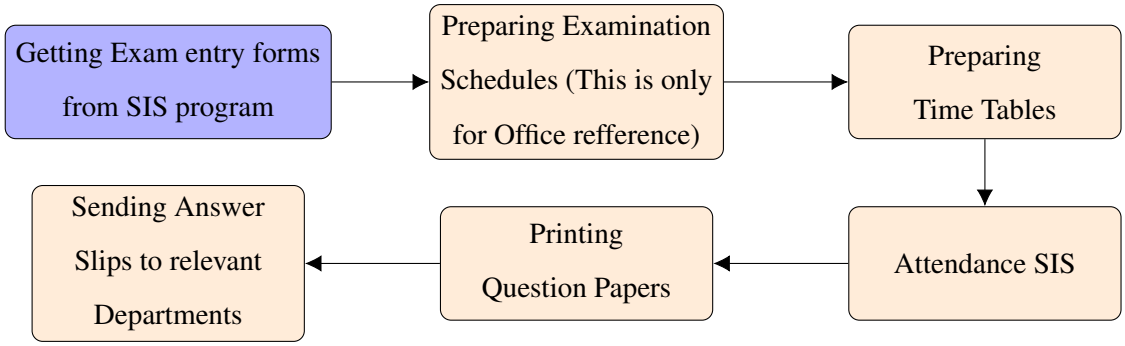


Exam Branch

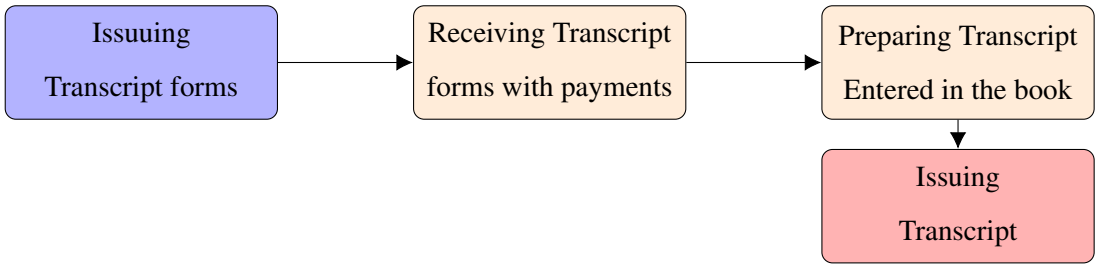
- Student Registration



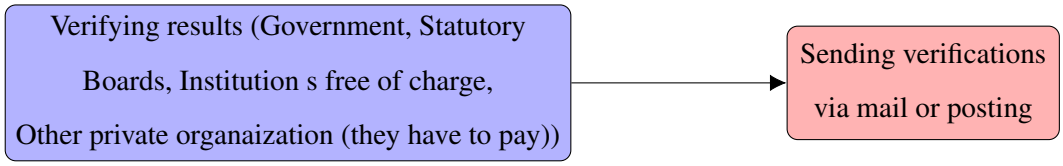
- Conducting Examinations



- Issuing Transcripts



- Verifications



- Convocation

  Preparing Convocation Schedules

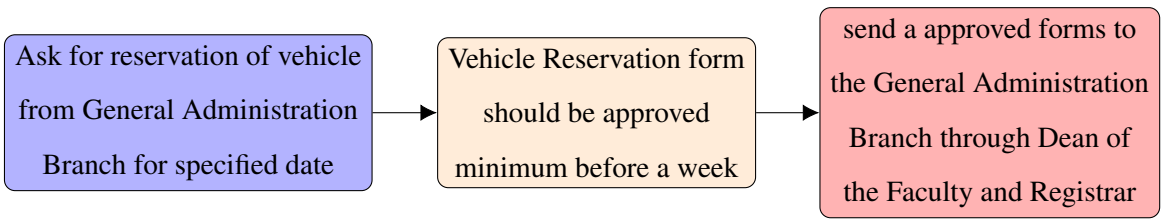
  - Cloak Schedule to General Administration to issue cloak and garlands
  - Printing Schedule to prepare certificates (Sinhala, English and Tamil)
  - Certificate Schedule to get Registrars and SAR Exams approval also to issue certificates to students.

General Administration Branch

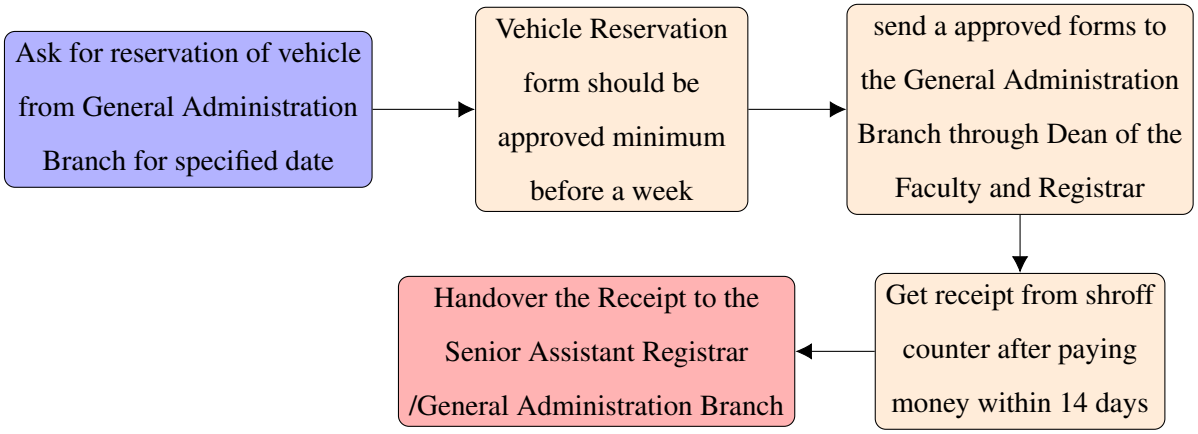
- Reservation of Vehicle

  For daily official activities

  - Vehicle reservation for should be submitted minimum before a day For travel

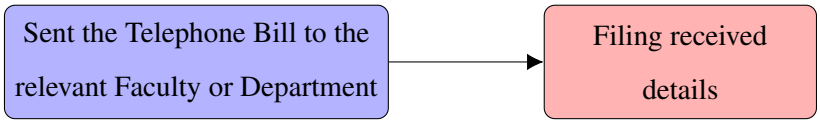


– Reservation of vehicle for rent basis

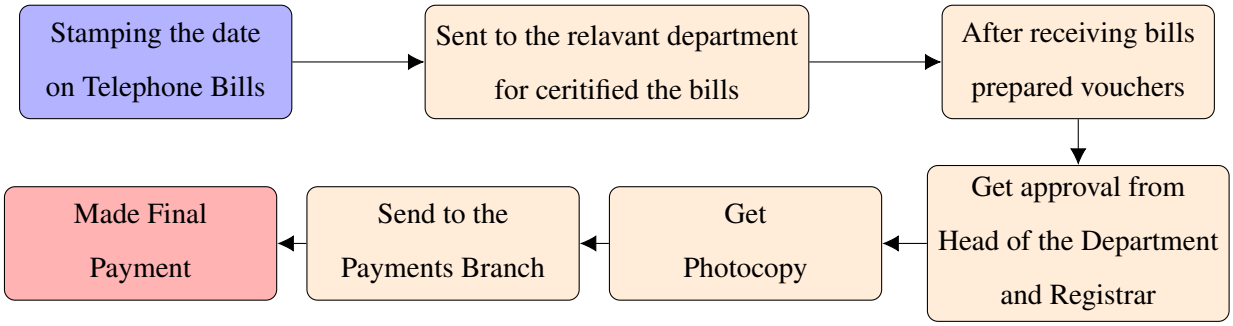


- Telephone Bills

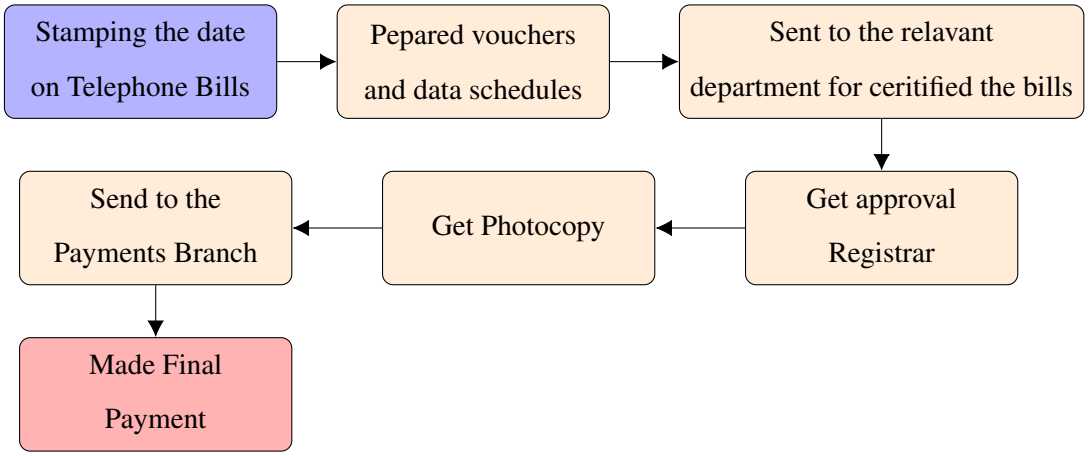
1. Bills relevant to the Faculties and Department



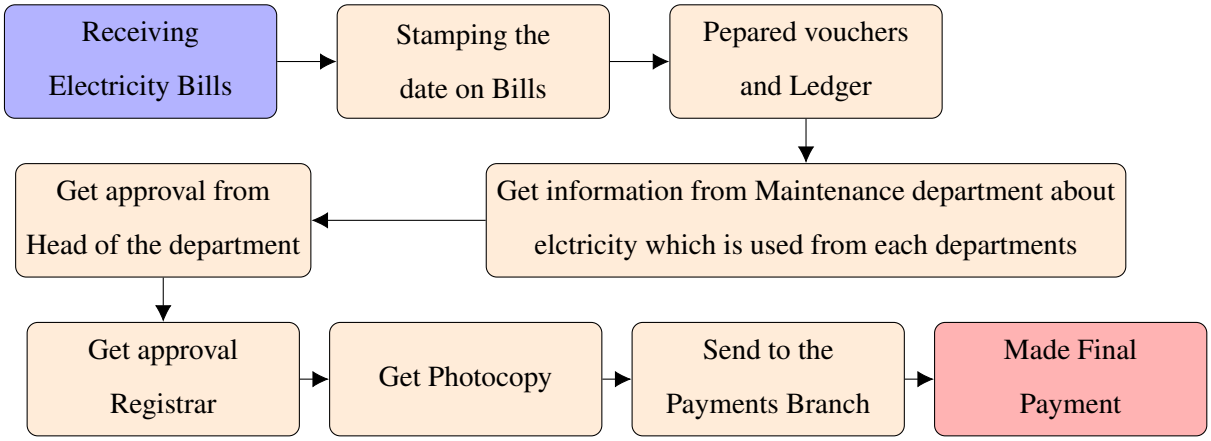
- Bills (Vice Chancellor / Registrars Office / Marshals)



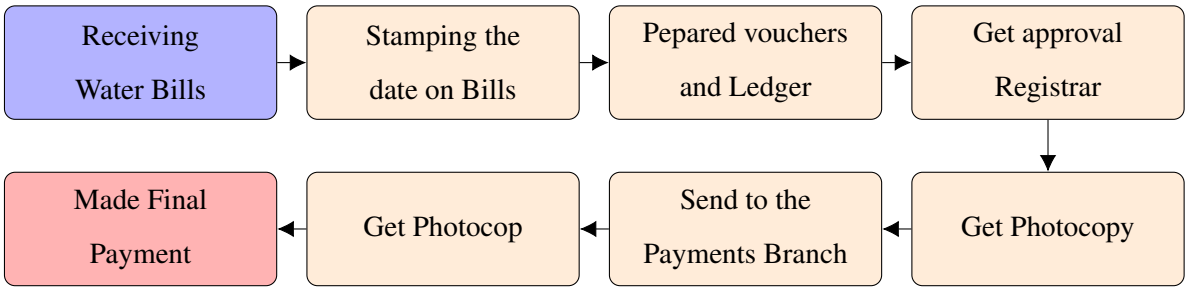
- Combined Telephone bill of College House



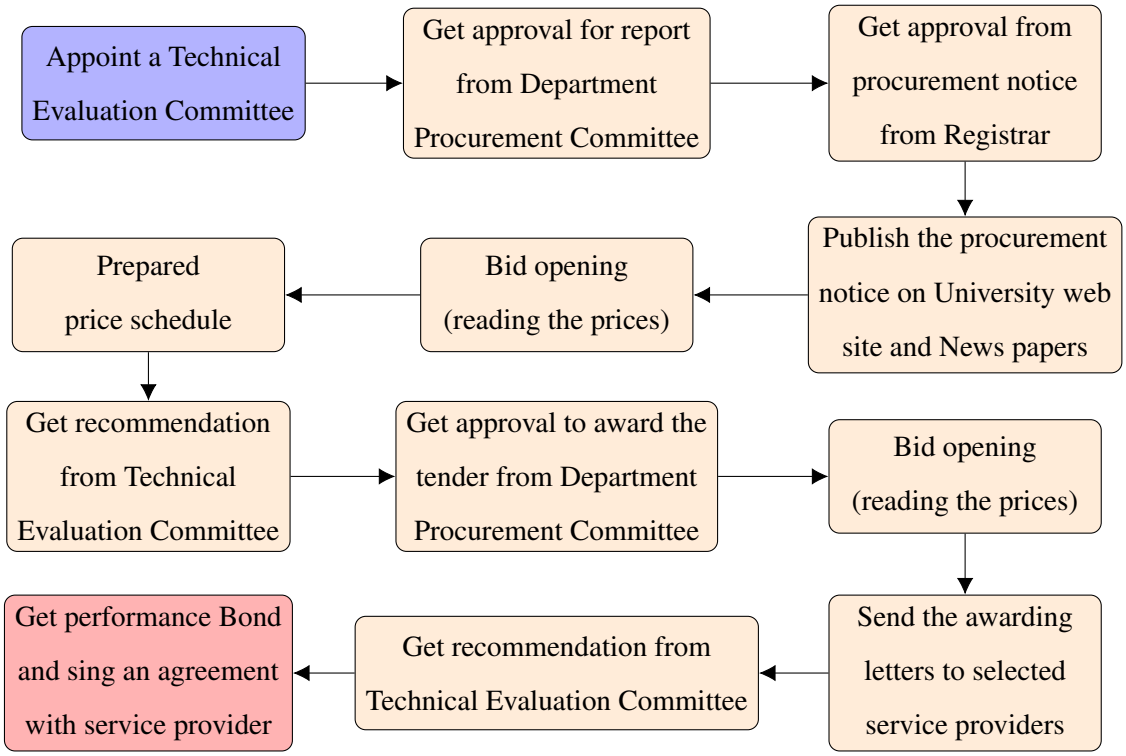
- Electricity Bills



- Water Bills

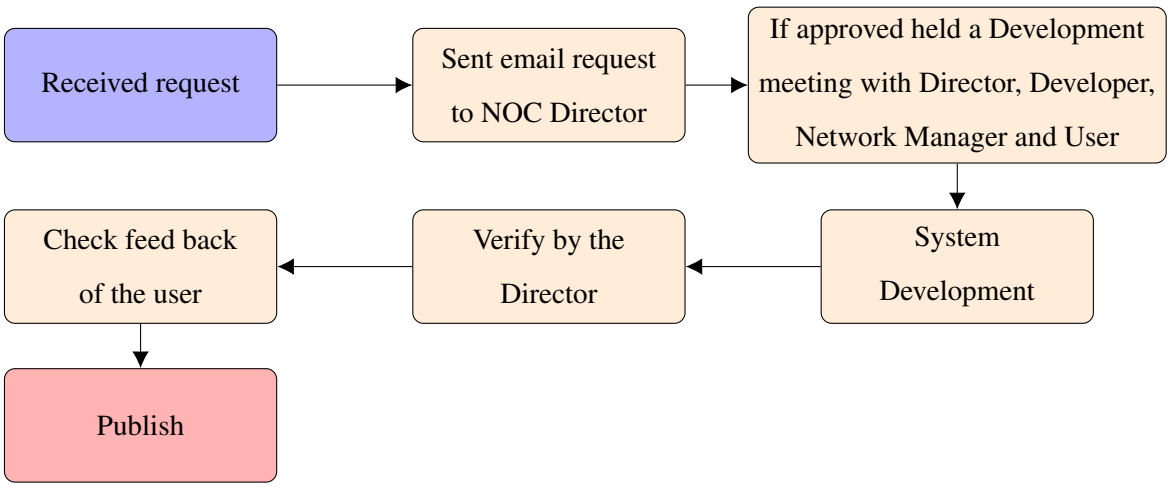


- Cleaning and Sanitary Services



Network Operation Centre

- New Web Development (Phase I)



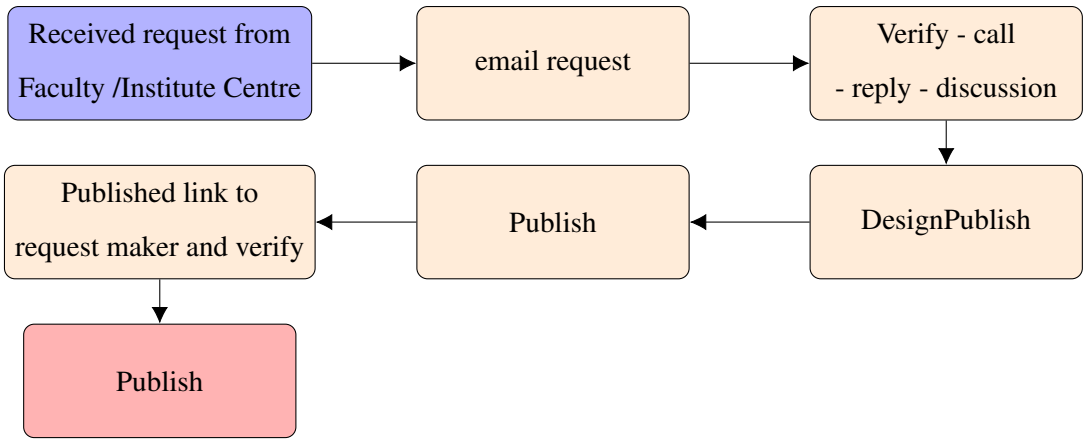
- Content Format Text, Videos, Photos
- Submission media email, pen drive etc.
- New Web Development (Phase II)

1. Hand over the system to Institute / Centre
2. Training Institute Web Developer / Programmer
3. Giving credentials to the developer

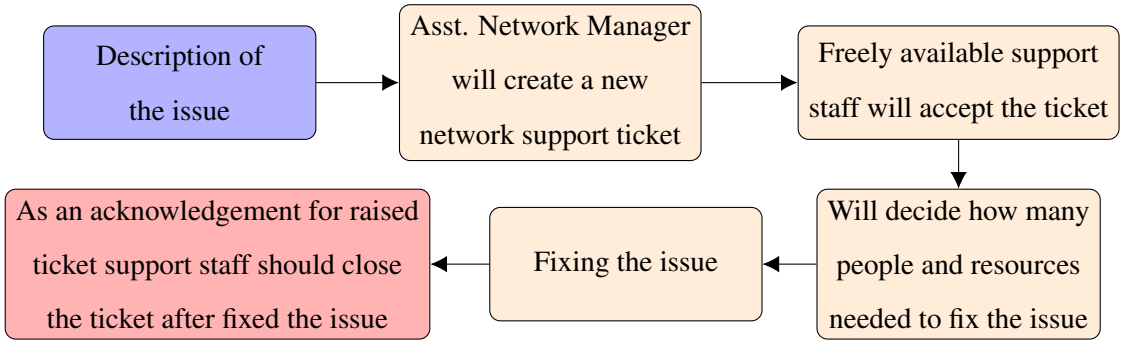
Daily Updates

Publishing
Updating
Modifying

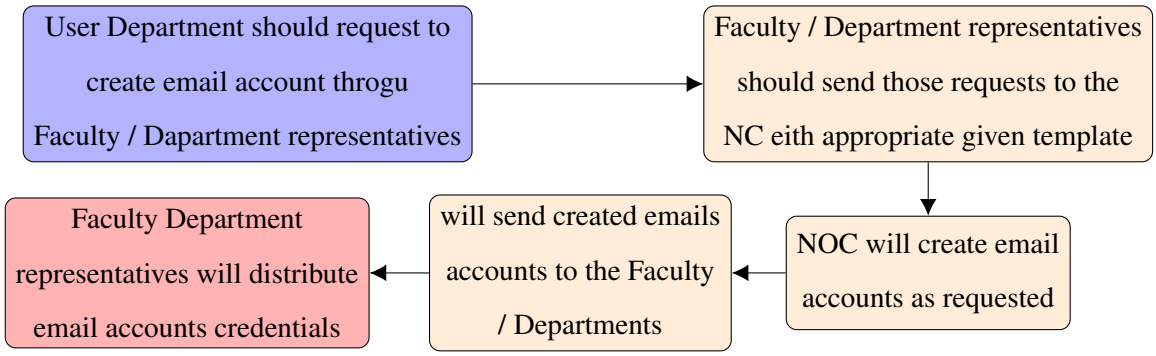
News / Article / Notice / Event etc.



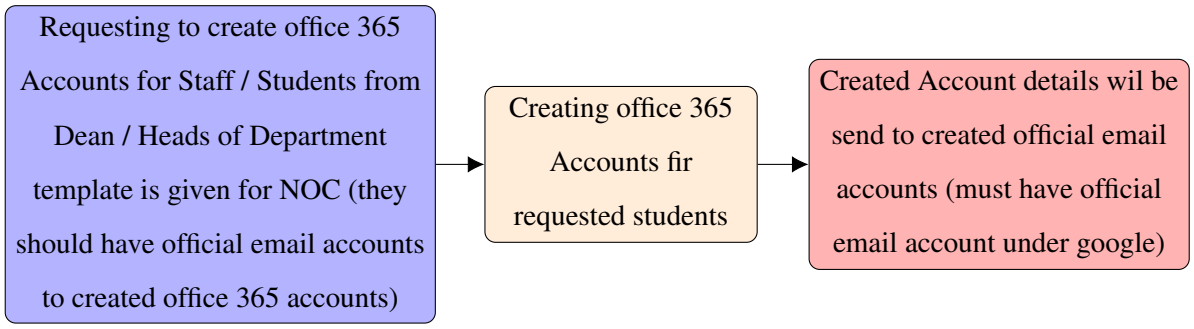
- Network breakdown and other IT related issues



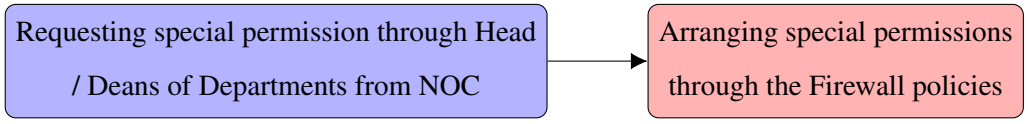
- Creation / Deletion / Password reset / User Name of email Accounts



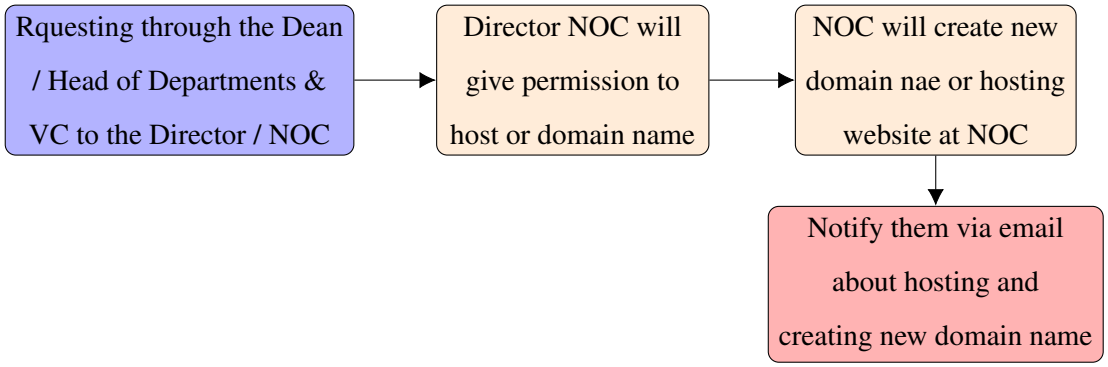
- Microsoft Office 365 Creation / Deletion / Password Reset



- Requesting to get special permissions from common Firewall restriction

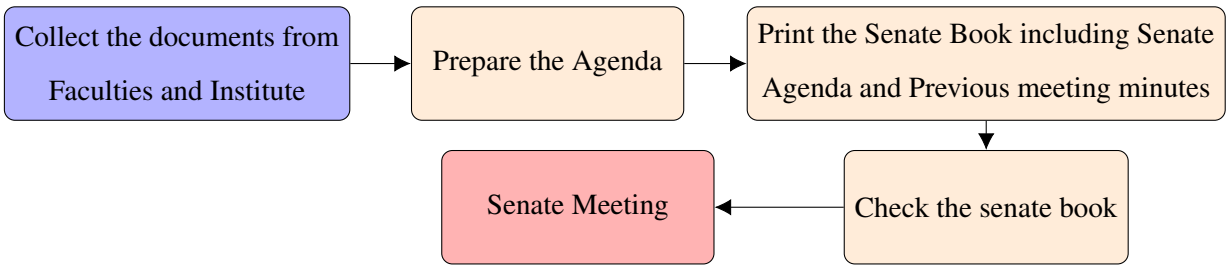


- Requesting to have a Domain Name or Hosting website at NOC

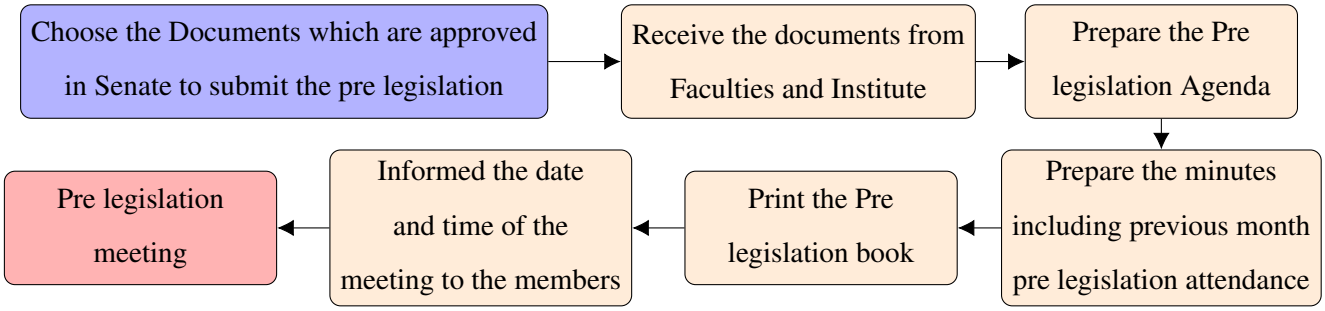


Academic & Publication Branch

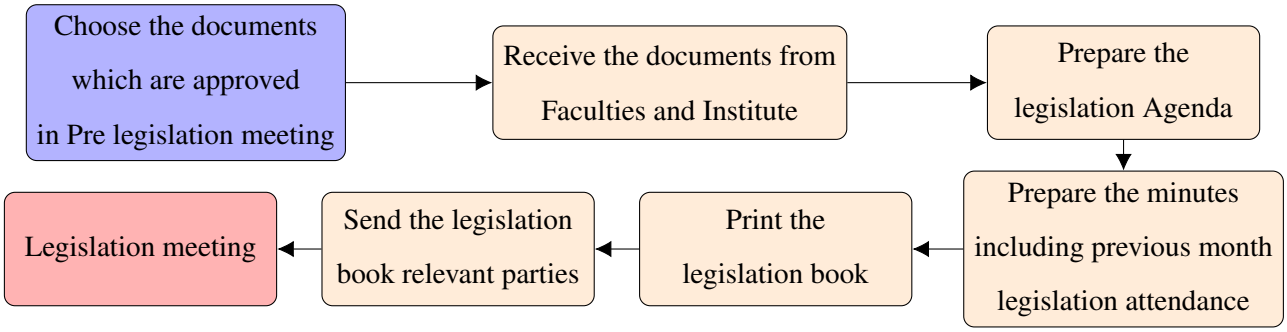
- Senate



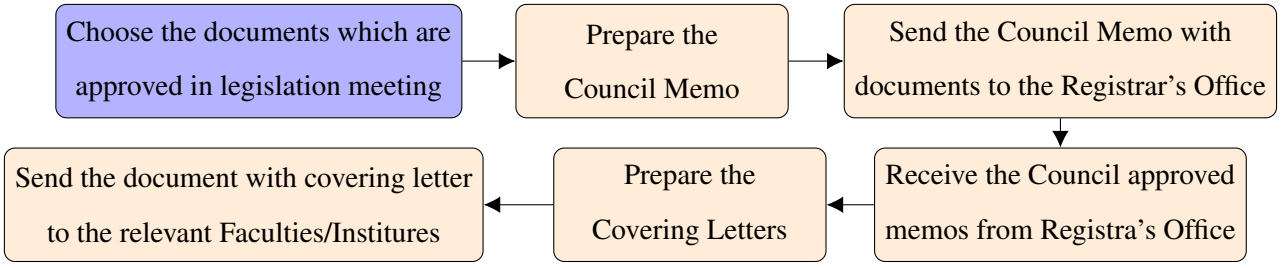
- Pre-Legislation



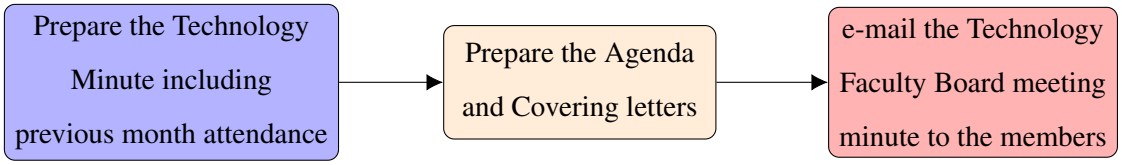
- Legislation



- Council

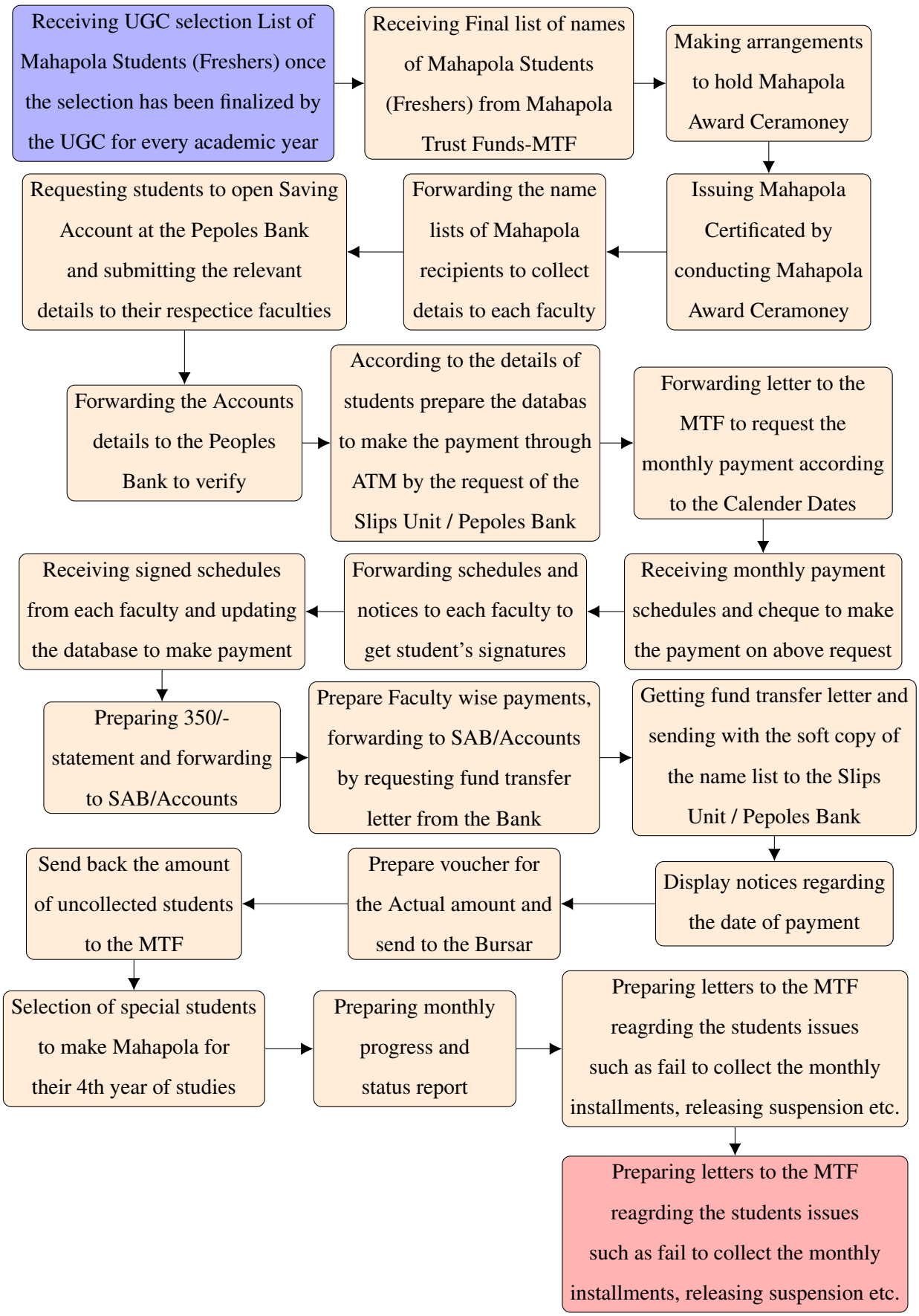


- Technology Faculty Board

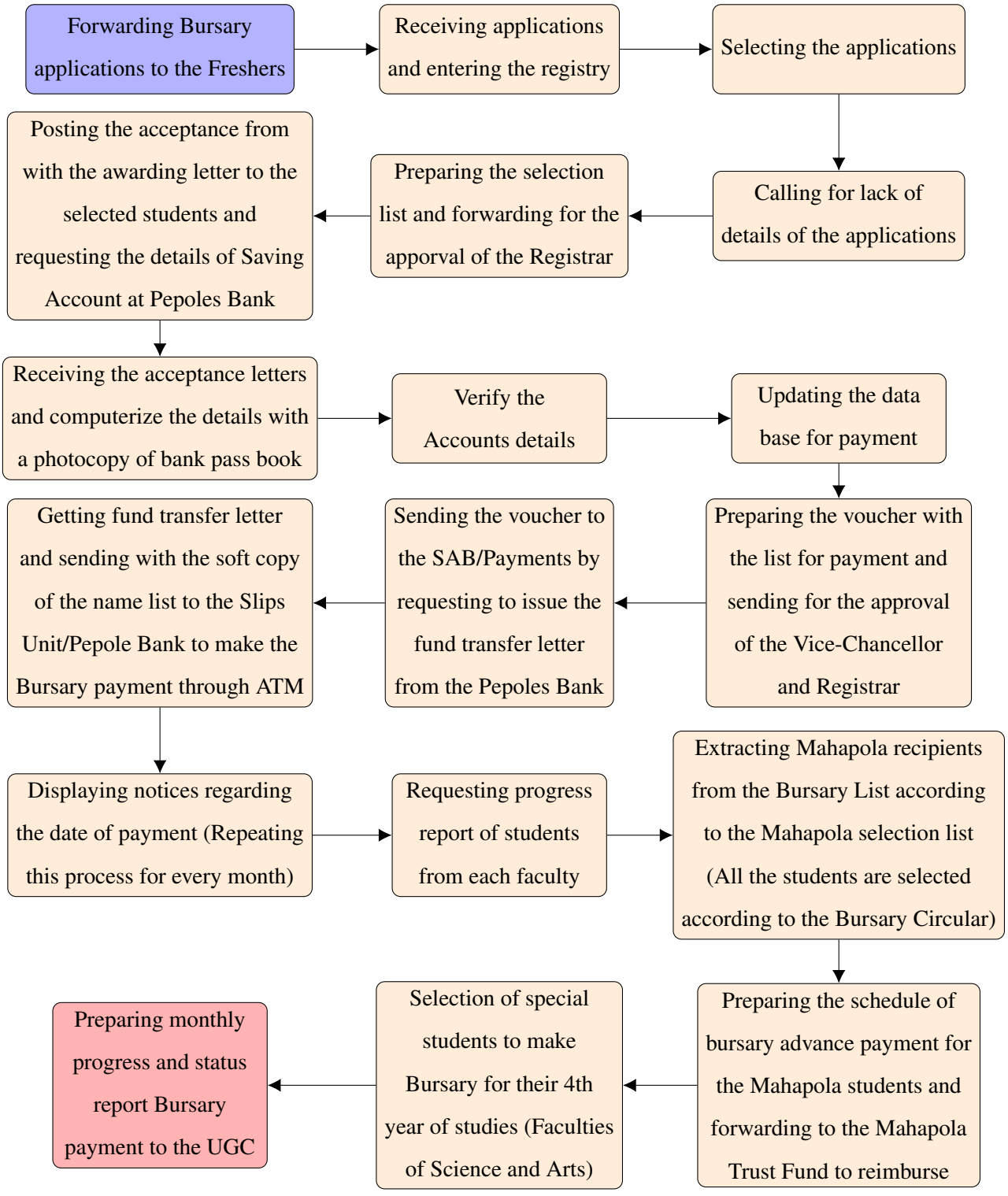


Student and Staff Affairs

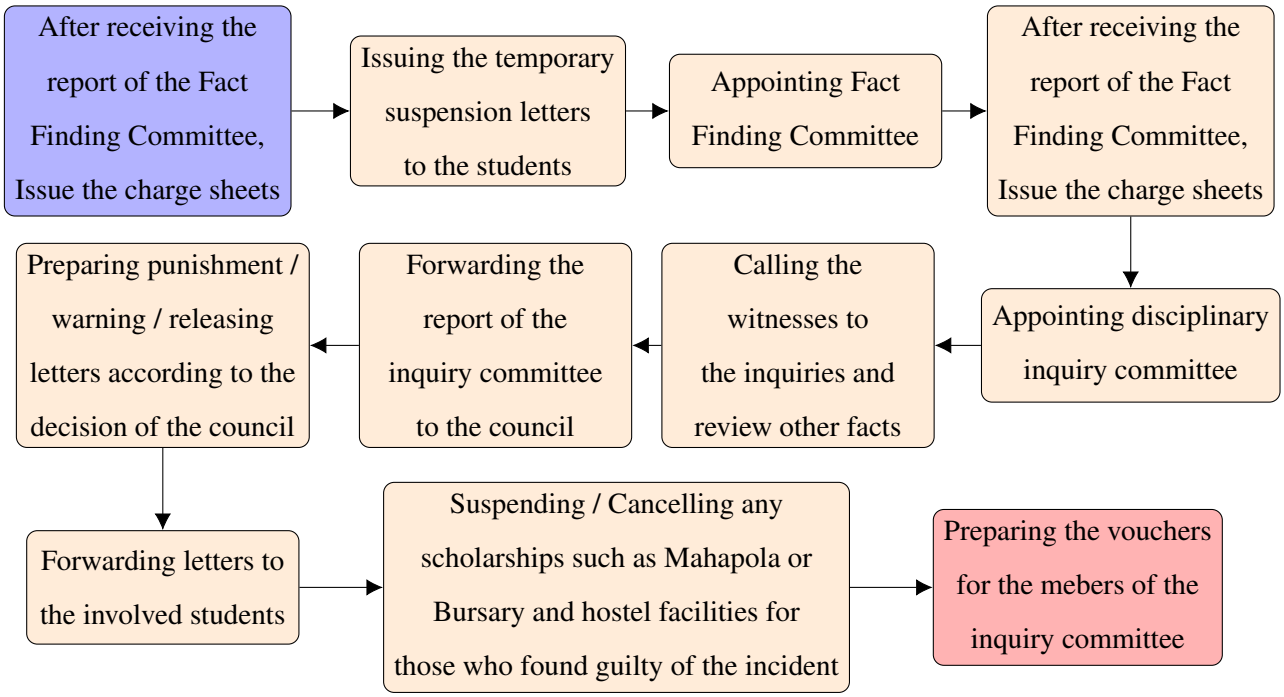
- Mahapola Payment Process



- Method of the payment of Bursary

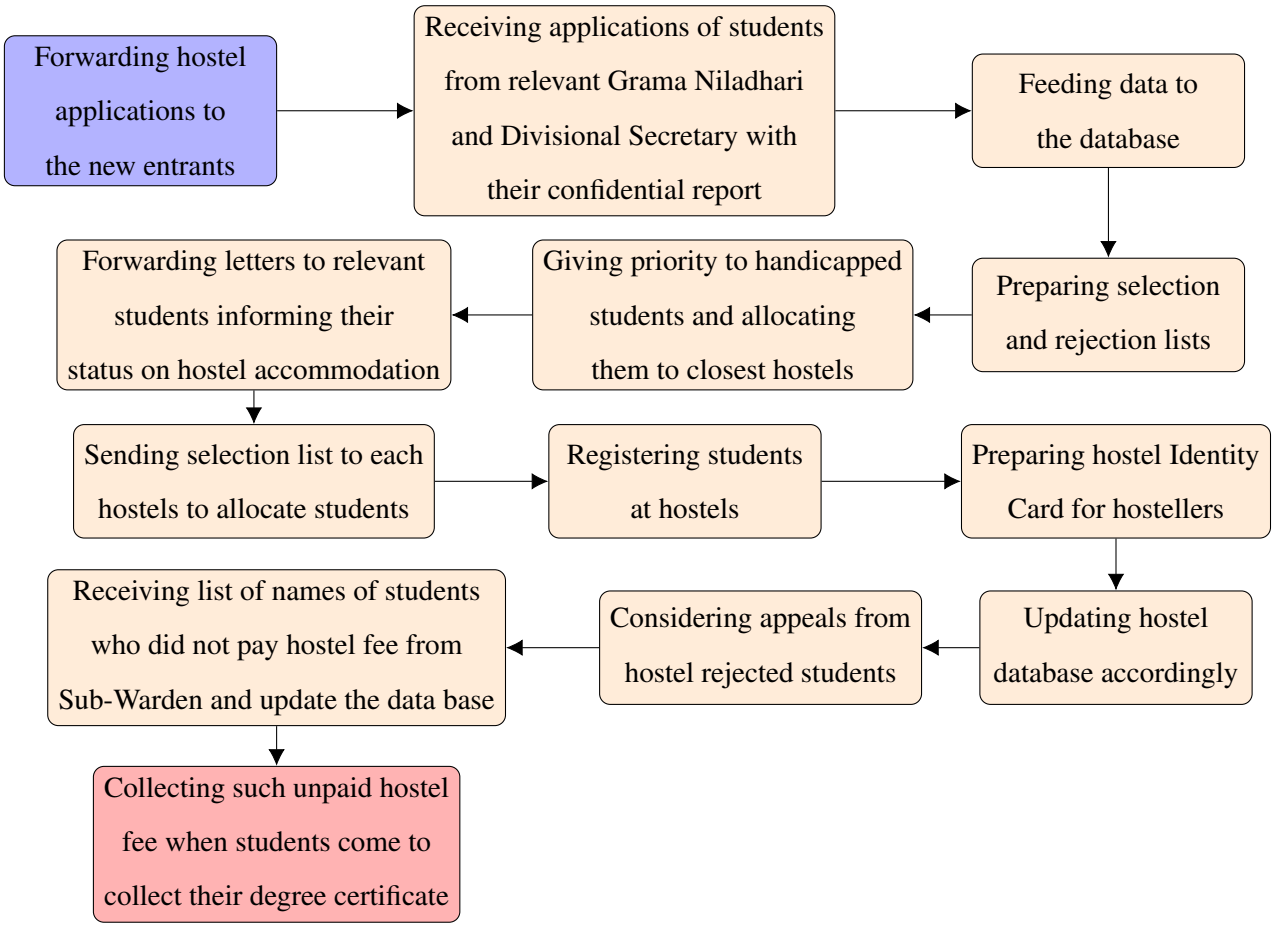


- Inquiries of Students

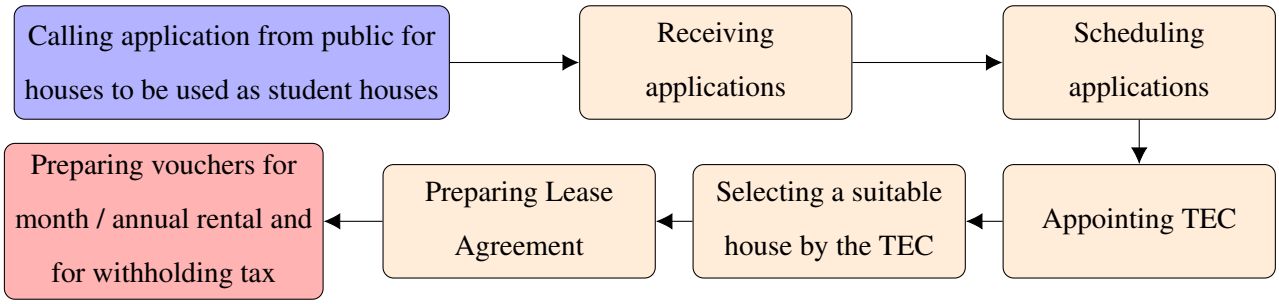


Hostels

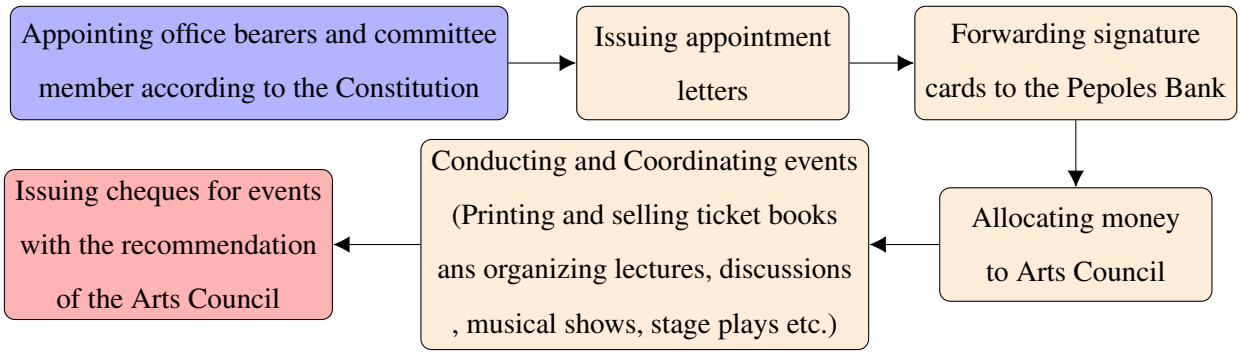
- Procedure for Hostel selection



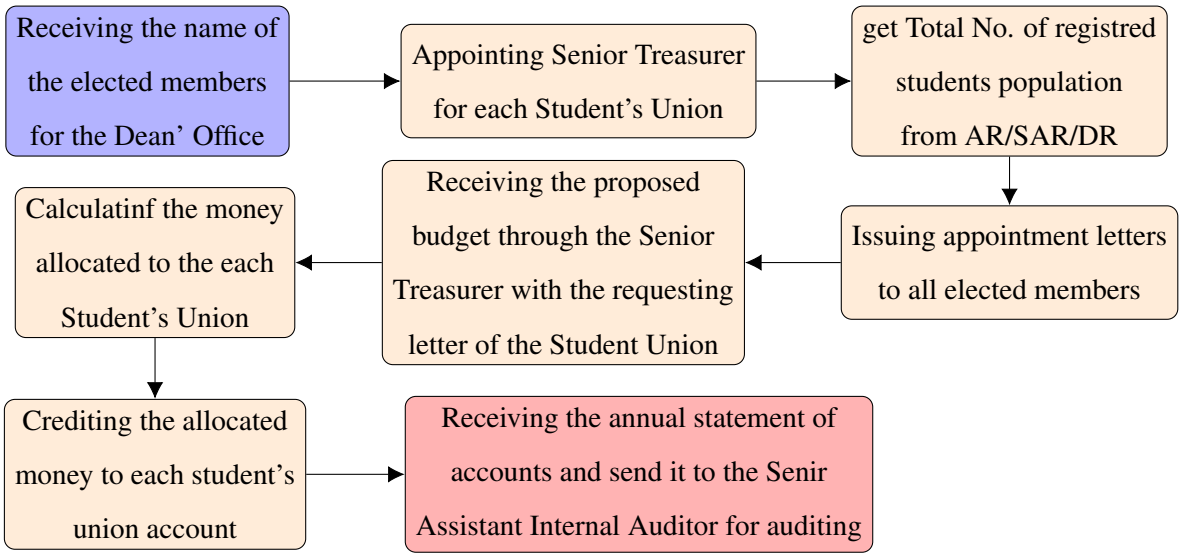
- Renting of Students Houses



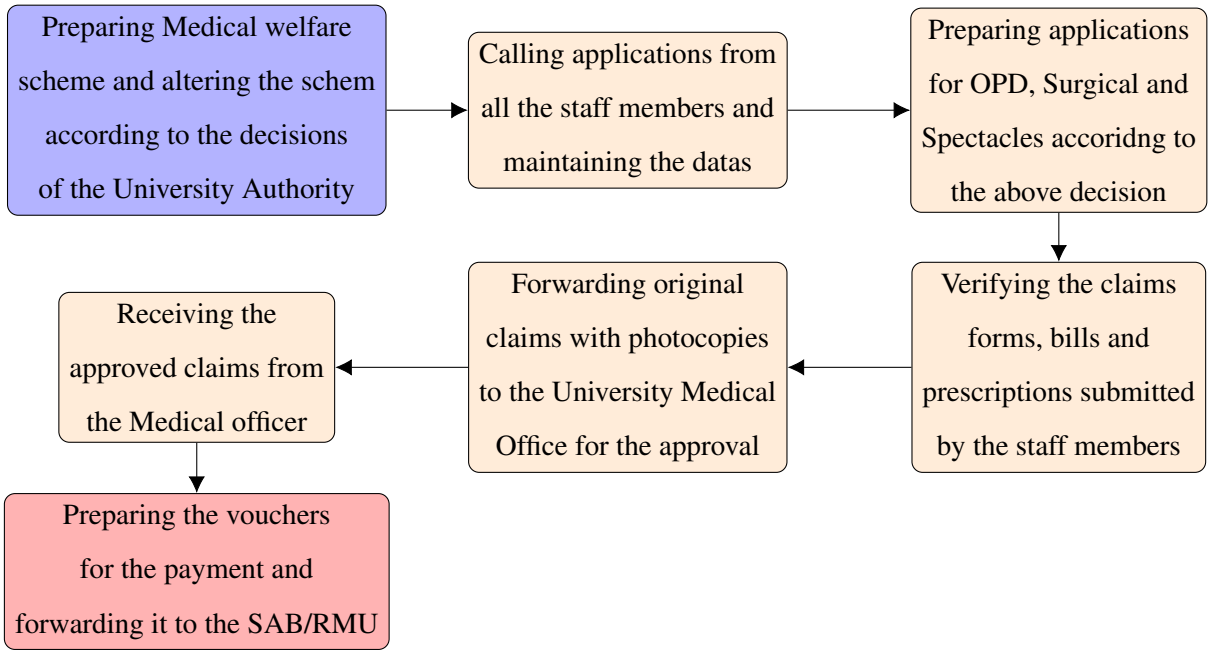
- Arts Council



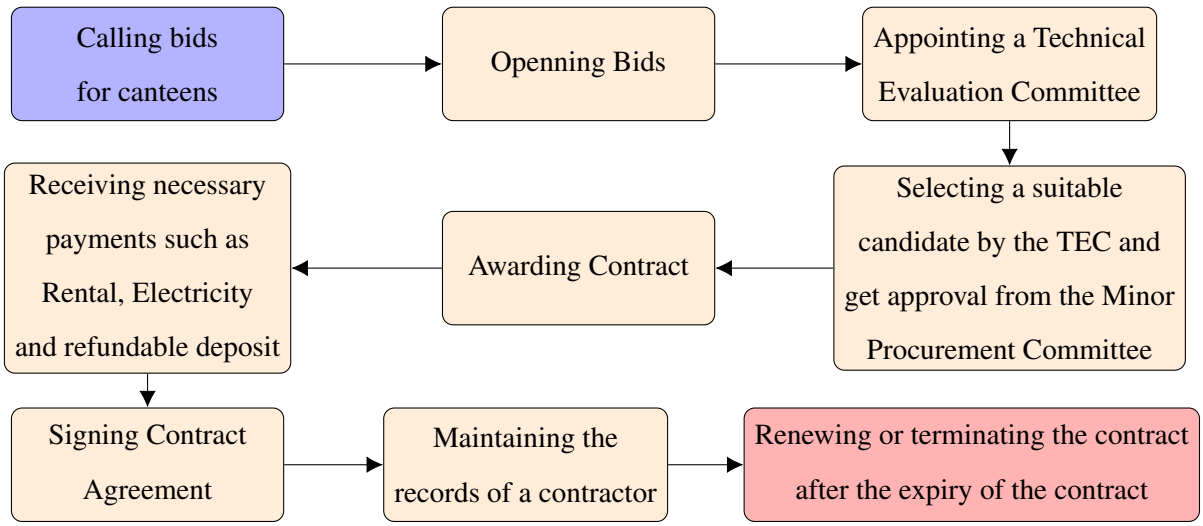
- Faculty Student Unions and the University Student Union



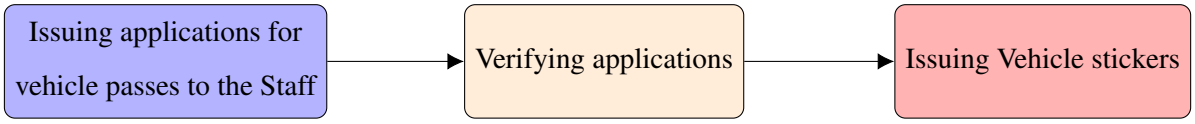
- Procedures of the Medical Welfare Scheme



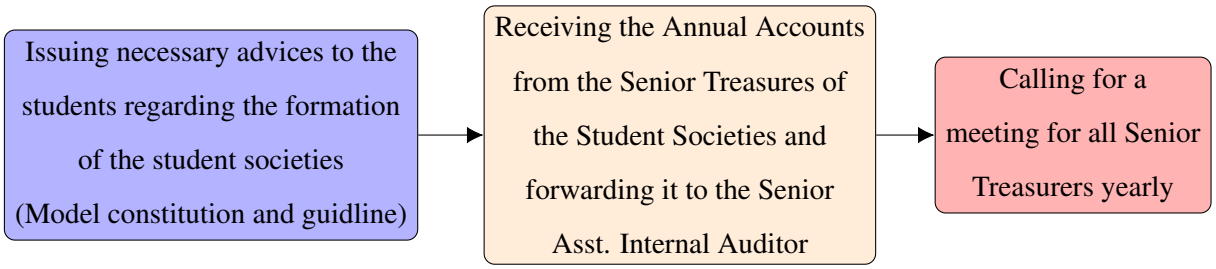
- Selection of Contractors for the Canteens



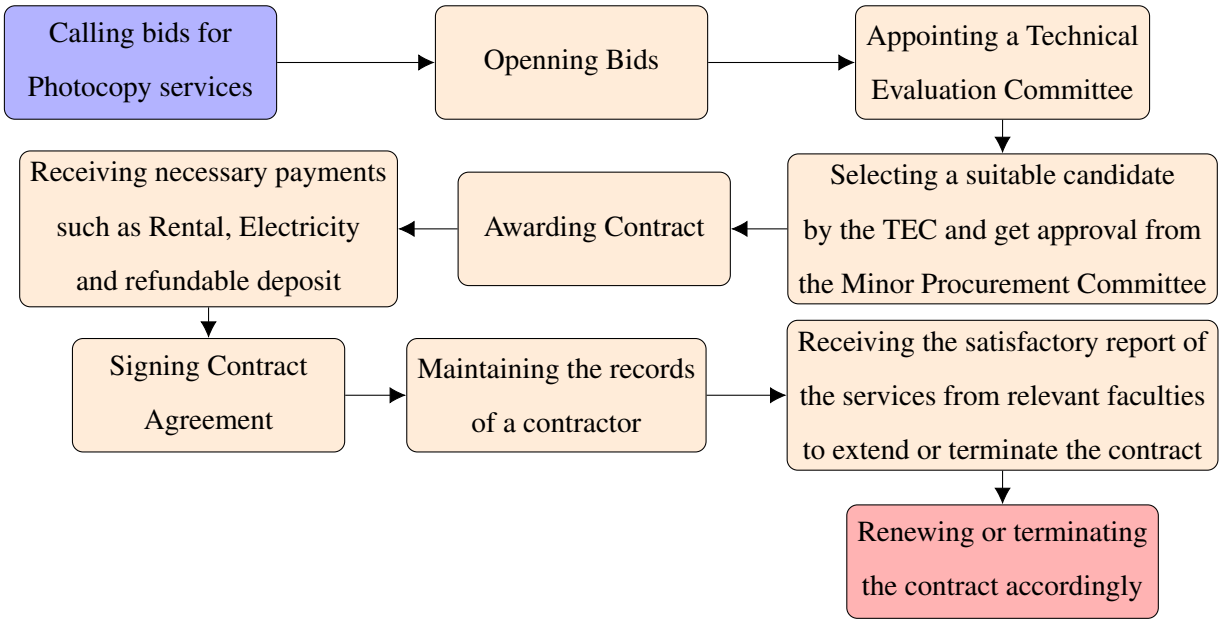
- Issuing Vehicle Passes



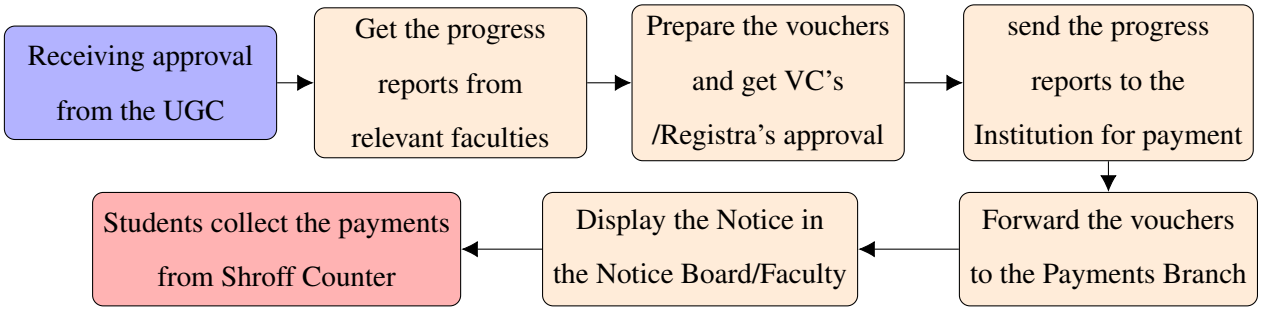
- Student Societies



- Procedure for selecting and maintaining



- Scholarships



4.6 Risk Assessment of the University of Colombo Administrative Departments

Departments

Examination Branch

Students Availability for new intake from Faculties

Observation

Observed that there is no proper way of calculating new student availability for each faculty.

Risk Rating	Low
Impact	High
Likelihood	Low

Description and risks

Risk of registering lesser number of students or exceeding the actual availability of the faculty.

Remediation and further information

Recommended to use and review student availability of the faculty annually, and should be proactively active system needed for calculation of the availability of the faculty intake.

Student Registration

Observation

Observed that lack of information given on the time of student registration, and lack of organizing to help and give services to students and parents.

Risk Rating	Low
Impact	Medium
Likelihood	Low

Description and risks

Risk of meeting difficulties at times when parents needed to relax after they have travelled long distance to come to student registration.

Remediation and further information

Recommended to have proactive organize the registration to facilitate everyone who are involving. Also, should provide all needed information regarding their future arrangements and

what facility do they have in the University of Colombo. Students motivation should start from their first day at the University. They should provide all given facilities such as google apps for business office 365, Microsoft imagine.

Examination time tables

Observation

Observed that examination time tables of faculties change due to various reasons like sports activities of students, natural disasters, etc.

Risk Rating	Medium
Impact	High
Likelihood	High

Description and risks

Risk of clashing examinations with their other activities of the University such as sports.

Remediation and further information

Recommended to consider all activities of the University before time tables are finalizing. Integration of required departments and to get required information from respective departments is a responsibility of examination branch.

Data Backup system

Observation

Observed that there is no proper way of storing data and to keep valuable data backups.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and risks

Risk of losing very important critical data of the University such as student information, results etc.

Remediation and further information

Recommended to use proper defined backup system for the examination branch. Highly recommended to use virtual backup system well as hard backup system reduce the risk of losing critical data. Google drive backup system is recommended where all users of the university granted unlimited storage.

Finance Division

Accessing the finance division

Observation

No Security Cameras available or no access log maintenance for the finance division section

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

We have observed that there is no adequate monitoring in the finance division which may lead to unauthorized activities inside the finance division where it carries most critical data of the University, such as loss of critical assets, vandalism, Data theft, eavesdropping etc.

Remediation and further information

Adequate monitoring should be established and monitored; CCTV cameras would be a good option to consider. Also, should have access log system for the finance division.

Suppliers interaction with employees of the finance division

Observation

Observed that the suppliers always coming to check whether their payments are ready and for some other reasons.

Risk Rating	Medium
Impact	Medium
Likelihood	Medium

Description and risks

It may lead to unauthorized access to critical data of the division and work latency of finance division employees.

Remediation and further information

Recommendation is not to allow them inside the finance division unless they have permitted by the heads of finance division branches.

Latency of confirmation the goods received by the user department

Observation

Observed that there is a confirmation latency on goods received by most user departments.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

It may cause supplier payments late. Damage the University of Colombo reputation.

Remediation and further information

Recommended to have proper monitoring system for the receiving good from suppliers. Such as sending a copy of delivery note to the supplies division too.

Submission of recommendations

Observation

Observed that there is some latency on specification and product recommendation from technical persons well as the user department.

Risk Rating	Medium
Impact	High
Likelihood	High

Description and risks

It may cause to latency on all future processes, of goods such as goods receiving, payments of the suppliers.

Remediation and further information

Recommended to have a proper reality kind of monitoring of those documents which are sent for recommendation.

Submission of department procurement committee documents

Observation

Observed that the department procurement committee documents not submitted on time by the faculties to prepare those documents to take up in the meeting.

Risk Rating	Low
Impact	Medium
Likelihood	High

Description and risks

There would be a risk of having invalid, wrong documents at the time of the meeting.

Remediation and further information

Recommended to submit those critical documentation few days before the meeting. Which helps all those DPC officers to go through the documents and do appropriate changes before the meeting.

Backup system

Observation

Observed that there is no proper way of storing data backups to use when an incident occurred.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Risk of losing very important data of the finance division, data only stored on the hard disk of the office computer devices.

Remediation and further information

Strongly advice to store data on Google cloud or any other different geographical area. (When all users of the UOC has given unlimited storage on Google cloud, therefore better of using it for free other than using any other costly method to store backups.

Availability of the common financial data

Observation

There is no proper way of sharing common needful data within the finance division.

Risk Rating	Medium
Impact	High
Likelihood	Low

Description and risks

Difficult of accessing common needful data immediately when needed. Remediation and further information Recommended to use file sharing method between finance division authorized users.

Hard copy files storing

Observation

Observed that there is no proper mechanism to maintain and access hard copy files of financial division whenever needed.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Time and energy wasting of finding a hard copy files of finance division, it may cause permanently loss of important files too.

Remediation and further information

Recommended to maintain logs of file storing and it should be clearly share with authorized persons of the financial branch.

Working procedure

Observation

Observed that there is no defined working procedure at the finance division.

Risk Rating	Medium
Impact	Low
Likelihood	Medium

Description and risks

It may cause responsibility issues within the employees of the division, where no one has responsible of doing a work.

Remediation and further information

Recommended to have better defined working procedure to give responsibility for every employee of the finance division.

User trainings

Observation

Observed that there is no better way of sharing knowledge within the division

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

When a person not available, it is difficult to continue his or her work by another person of the division.

Remediation and further information

Recommended to use knowledge sharing method for the finance division or rotating working environment make all users knows each working capacity. Which helps to do work in more efficient and effective manner.

Cheque Payments

Observation

Preparing the cheques for voucher payments (write the check via Cash Book with using invoice selecting method)

Risk Rating	High
Impact	High
Likelihood	Medium

Description and Risks

Vendors outstanding balance is not updated when the cheque is preparing in SAGE. Vote balances are duplicated in the budget.

Recommendation and the further information

- When the user prepares the cheque to supplier, supplier should be select compulsory at Cash Book.
- Restrike to use the supply consumable and supply capital payment code in payment window at Cash Book.
- When the user prepares the cheque to supplier, supplier should be select compulsory at Cash Book.
- Restrike to use the supply consumable and supply capital payment code in payment window at Cash Book.

Update the account system

Observation

Should prepare the PAYEE tax schedule for deducted PAYEE tax by vouchers on daily basis.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and Risks

Couldnıt identify the correct amount separately from PAYEE tax General Ledger Account.

Recommendation and the further information

When the reconciliation of the PAYEE tax Payable Account, Faculty wise schedule refers from Research Management Unit.

Settle down account transfers

Observation

All the contribution and transfers from the Courses, Projects, and Development funds sometimes not settling down on end of the month.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and Risks

Risk of identifying transferred money in the future.

Recommendation and the further information

Recommended to settle down transferred money end of every month as a practice.

Payment Vouchers

Observation

There is no tracking system to check where the payment vouchers and status of the voucher.

Risk Rating	Medium
Impact	Medium
Likelihood	Medium

Description and Risks

Waste of time to find payment vouchers. Could lose the payment voucher due to various reasons.

Recommendation and the further information

Maintain a voucher register and a tracking system.

General Administration Branch

Vehicle arrangements

Observation

Vehicle arrangements are not up to standard, no proper mechanism to monitor drivers or vehicle arrangements.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Risk of using booked driver or vehicle for another job, especially like booked vehicles for examination duties are more critical.

Remediation and further information

Recommended to have proper monitoring and arrangement for university drivers and vehicles, it should be shared by faculties, so they would identify which vehicles are free. So, no need to call the General Administration branch to arrange.

Vehicle arrangement procedure

Observation

Observed that the vehicle arrangement system is a time-wasting procedure.

Risk Rating	Medium
Impact	High
Likelihood	High

Description and risks

It may cause late arrangements of vehicles and it will be a burden to drivers too.

Remediation and further information

Recommended to have online quick procedure to make vehicle arrangements with authorized parties.

Vehicle arrangements (When UOC vehicles not available)

Observation

Observed that there is no other way of getting vehicles to make up the unavailability of University vehicles due to high use of vehicles and drivers.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Unable to do the intended work due to unavailability of the University vehicles

Remediation and further information

Recommended to have private vehicles when needed, there should be an authorized process to use private vehicles when needful situations occurred.

Bill payments

Observation

Observed that there are late submission of bills to make payments. And late collection of bills from postal division of the General Administration branch.

Risk Rating	Medium
Impact	Medium
Likelihood	High

Description and risks

This may lead to disconnection of the utility supplying by service providers, and it may cost more when you are going to get the connection back again.

Remediation and further information

Recommended to use automated system or online tracking system for the bill payments of the University of Colombo administrative staff and branches, where you will be notifying when to send bills with recommendation and status of the bill payments. This should handle by the subject clerk of the General administration branch.

Attendance of cleaning service

Observation

Observed that cleaning services attendance not maintained well by the faculty representatives for the subject of cleaning.

Risk Rating	Medium
Impact	Medium
Likelihood	Medium

Description and risks

Risk of paying more or less to the cleaning service provider due to attendance issue, and late payments for the cleaning service department.

Remediation and further information

Recommended to use better attendance monitoring system for the cleaning service staff of the third-party cleaning service. And always sharing it with thee subject clerk of the General Administration branch to make the quick payment process. It will increase the confidentiality and well as integrity of the attendance monitoring system.

Billing process of cleaning service

Observation

Observed that the billing process is so slow and it will be a burden for both university and the third-party cleaning service.

Risk Rating	Low
Impact	Medium
Likelihood	High

Description and risks

Risk of getting late to pay cleaning service department and well as their innocent employees, who works for lesser amount of wages.

Remediation and further information

Recommended to use quick and better procedure and monitoring the procedure without any latency. Better to use online tracking system for the whole process with involvement from all parties.

Reservation of Board rooms

Observation

Observed that reservation of board rooms is very old system which uses a hard copy of form where departments have to fill and then General Administration subject clerk will note it down on his or her diary.

Risk Rating	Low
Impact	Medium
Likelihood	Medium

Description and risks

This system waste time of everyone who has involvement, and requesting party doesn't know whether the board room is free or not till asking the subject clerk of the General Administration branch.

Remediation and further information

Recommended to use online calendar system (recommendation is to use Google calendar as University of Colombo has their mail on the Google cloud) to make reservation of the board rooms of the University of Colombo administrative area. It will help all interested parties to check whether the board rooms are free or not through online. Also, reservation should allow through official email addresses of respective users who seeks to reserve board rooms.

Issuing Cloaks

Observation

Observed that cloaks issuing is very hard when the University convocation is taking place for all faculties.

Risk Rating	Low
Impact	Low
Likelihood	Medium

Description and risks

All students of the University must come to college house to collect their cloaks from General Administration Branch. Remediation and further information

Recommended to distribute those cloaks to the respective faculties of the University, where it will help both students and staff to distribute and collect without wasting much time.

Network Operations Centre

Monitoring Data Centre activities

Observation

No Security Cameras available.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and risks

We have observed that there is no adequate monitoring in the data Centre which may lead to unauthorized activities inside the data Centre such as loss of critical assets, vandalism, Data theft, etc.

Remediation and further information

Adequate monitoring should be established and monitored; CCTV cameras would be a good option to consider.

Location of the Data Centre

Observation

Observed that the location of the data Centre is not up to the world standard. Such as ISO 27k standard.

Risk Rating	Medium
Impact	High
Likelihood	Low

Description and risks

It would cause to natural disasters like flooding if the data Centre situated at the ground level of the building.

Remediation and further information

Recommendation is to move the data Centre in to the 1st floor or 2nd floor of the building if possible when the future expansions needed.

Proper door lock method

Observation

Observed that data room accessing door uses simple key lock method and it has access from two ends.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Unauthorized access to the server room, key locks can be break easily. Also having two access paths make it vulnerable twice as normal.

Remediation and further information

We recommend that to implement modern technologies such as, door locks requiring proximity card, code entry or magnetic card swipes. The access to the data Centre can be further controlled using biometrics authentication to have better level of security if business demand such level of security. Accessing the data Centre from only one side is recommended. If could permanently lock other access paths to the main server room of the University.

Accessing the University premises

Observation

We found that outside people can easily access the university

Risk Rating	High
Impact	High
Likelihood	Medium

Description and risks

We observed that there is no prevention method for outside people to access the university premises. Only have vehicle access prevention and detection at the University premises.

Remediation and further information

Highly recommended to implement an identification method and user accessing log file for the administrative buildings of the University specially finance division.

Securing the important assets

Observation

Observed that important backup media (such as external hard disks, pen drives, DVD/CD, etc.) are not securely maintain.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Anyone who could gain access to the premises would easily access to the physical devices, should not just keep backup files within the same geographical area, such as same premises.

Remediation and further information

Store those assets inside a locker room which are only accessed by high authorized users. Keep most important assets in offsite location. Also, should have better mechanism to store those backups on different geographical area, such as virtual environment like in the cloud storage.

Protecting physical assets of the University

Observation

Observed that there are no detective systems to detect suspicious activities within the university premises.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Risk of losing physical assets of the University, and to reduce suspicious activities.

Remediation and further information

There should be a proper detection system and log system to detect and prevent physical assets of the University. Recommended to have CCTV camera system and logs of physical assets going out and in to the University premises.

Power outage

Observation

No emergency lighting system for server room is found.

Risk Rating	Medium
Impact	Medium
Likelihood	Low

Description and risks

A power outage makes the data Centre in dark and the staff getting in or out of the data Centre can lead to accidental or deliberate damages to critical assets which include Data Centre staff.

Remediation and further information

Install emergency lighting system for the data Centre to avoid potential damages to critical assets.

Secure access to the data Centre location

Observation

Observed that there is no proper mechanism to detect or prevent unauthorized access to the data Centre premises. Also, not maintaining data Centre access logs of authorized persons.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Threat of unauthorized access by external party, and risk of authorized persons suspicious activities.

Remediation and further information

Recommended to maintain logs to detect authorized persons suspicious activities, and there should be a camera system to detect unauthorized access to the data Centre.

Data and power cable diagrams

Observation

There are lack of power cables and network cable diagrams available of the University.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Difficult to find damaged cables and to do the maintenance whenever it needed. Also, it could be difficult to do future expansions and maintenance of the University infrastructure.

Remediation and further information

Company should keep data and power cable diagrams for the university network. Servers Maintenance

Observation

No trained persons to handle immediate server maintenance when needed

Risk Rating	Medium
Impact	High
Likelihood	Low

Description and risks

Risk of major damages and availability of the critical servers

Remediation and further information

NOC support staff should have knowledge about the server rack system and servers to attend critical issues when needed.

Service level agreements

Observation

Observed that there are lack of service level agreements maintaining by the Network operations Centre.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Risk of not getting service level support from suppliers, or latency of getting the support when needed.

Remediation and further information

Recommended to maintain service level agreements with all their service providers and suppliers to get maximum support from them. Recommended to have online shared service level agreement monitoring system for the NOC.

Password policy

Observation

Observed that there is lack of password policy on servers and online portals.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and risks

Risk of accessing and tampering the most critical resources on servers and unauthorized activities on online portals. High risk of losing critical resources of the University.

Remediation and further information

Recommended to keep and maintain password policy for the servers and online portals access by NOC staff. This should be very critical and strongly recommended to have a complex password policy with better management.

IT and Email policy

Observation

Observed that there is no IT and email policy for the University of Colombo users.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

There will be an uncharacteristic use of IT and official email accounts. Such as using IT resources of the University to do their private works and doing inappropriate works. Using official email accounts to access materials which are not related to work environment or do things like criminal.

Remediation and further information

Strongly recommended to have IT and email policy to encourage them not to do such things unrelated to the working scope.

Network related inquiries

Observation

There is no method of log the inquiries made by users and monitoring those inquiries to better use. Also, should notify users when the work has been done.

Risk Rating	Medium
Impact	Medium
Likelihood	Medium

Description and risks

Risk of forgetting to do some of the due network related issues and it makes user satisfaction low too.

Remediation and further information

Recommended to have network related issues log system at the Network Operations Centre to keep record of past, present and future inquiries made by users of the University. It will help to increase user satisfaction.

Creating/Editing/Deleting of official email addresses

Observation

Observed that there is no defined mechanism to manage email accounts of the University staff and students. There are diverse ways of managing email accounts such as recommendation from facility representatives, users by their own coming to the network operations Centre, calling the NOC to manage accounts.

Risk Rating	High
Impact	High
Likelihood	Medium

Description and risks

Risk of misusing the email accounts and elevated risk of getting unauthorized access to someones official email account. Also email account managing administrators may misuse to do inappropriate and unrelated operations using their elevated level of privilege access.

Remediation and further information

There should be a super user access to the Administrative portal of Google domain to do top level operations whenever needed by the university. It should be with the Vice chancellor of the University of Colombo. Google domain administrators of the University should have a policy of managing user accounts.

Office 365 accounts Creating/Deleting/Editing and Subscription

Observation

There is no way of notifying whether the requested user have a valid official email address or not. Monitoring of office 365 accounts and late to get office 365 subscription.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Risk of creating office 365 accounts by using wrong official email accounts. Misuse of creating new office 365 accounts.

Remediation and further information

Recommended to validate email accounts before creating office 365 accounts for respective users. Also, should have better authorization procedure to create, edit and delete office 365 accounts.

Access permission (Firewall)

Observation

Observed that there is no proper permission procedure to create, edit and delete firewall access control lists.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Risk of getting unwanted permission access to resources and by passing those privileges to misuse the advantage his or her having. There could be a risk of having over-restrictions too.

Remediation and further information

Recommended to have clear authorized procedure to grant, edit and revoke firewall permissions. That should be come through Vice chancellor, registrar and the director NOC to the person who has administration rights to change such commands. It should just not let the administrator do change permissions, that kind of privileges should come through chain of top-level management process. Because all those who are authorizing such permissions have record of that and very much aware of the situation.

Posting news on the University main website

Observation

Observed that there is no proper authorization process defined to post news on University of Colombo main website. Current system has only two parties which are user who sends news and Web administrator who handles the main website.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

This leads to posting of unwanted or unrelated news on the main website.

Remediation and further information

Recommended to have defined authorization process on posting news on main website. there should be a way of getting authorization over the content of the news posting on the main website.

Identification of the University of Colombo staff

Observation

Observed that the University staff do not use ID cards when they are at the University premises.

Risk Rating	High
Impact	High
Likelihood	High

Description and risks

Risk of unauthorized access to departments and branches of the University. Risk of theft where security guards of the University unable to identify persons of the University whether they are working at the University or not. Because thief easily get access to the University due to this security vulnerability of the University system.

Remediation and further information

Highly recommended to use ID cards which are given to the University staff by the University. University staff must wear their University identification cards when they are working in the University and when they travel within the University premises. This will help all security guards to identify visitors easily by looking at physically. It will reduce theft of the University which they are suffering time to time recent times within all university premises. Identification of temporary staff, trainees and visitors

Observation

Observed that there are no identification cards for the University of Colombo temporary staff, trainees and visitors.

Risk Rating	High
Impact	High
Likelihood	High

Description and risks

Risk of unauthorized access to the highly critical departments and data

Remediation and further information

Recommended to have identification cards for all temporary staff, trainees and the visitors who visiting the University premises and administrative departments.

Student and Staff Affairs Branch

Backup System

Observation

Observed that there is no defined backup procedure to protect sensitive data which are belongs to students of the University

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Loosing such kind of sensitive very important data, may not be able to recover again in for a long time. Because Student and Staff Affairs branch holds these sensitive data for so many years.

Remediation and further information

Recommended to use defined backup procedure to protect those invaluable sensitive data of the University of Colombo students. It is recommended to use Google drive backup system as cloud backup system to protect data from disasters. Highly recommended to backup most sensitive data periodically to the Google drive.

Password Complexity

Observation

Observed that the users of SSA branch doesnıt use complex passwords to protect their office computers and password uses to access student online systems.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

It will lead to unauthorized access to the computer through physically or virtually. Which make risk of getting sensitive information of students well as it could use to cheat and get benefit out of it.

Remediation and further information

Recommended to use complex passwords to access systems and their office computers to mitigate unauthorized accessing and altering sensitive data to gain benefit out of it.

Hostels bill payments

Observation

Observed that there is late submission of hostels bills to make payments.

Risk Rating	Low
Impact	High
Likelihood	Low

Description and risks

This may lead to disconnection of the utility supplying of Hostels, this is a high risk operation.

Remediation and further information

Recommended to use online recommendation from Hostel wardens and send those recommendation through an email to reduce the time and energy taking to proceed the payments.

Selection of Students (Bursary Payments)

Observation

Observed that there is no clean and obvious way of selecting bursary students, Selection criteria not well defined.

Risk Rating	High
Impact	High
Likelihood	Low

Description and risks

Risk of eliminating qualified students due to lack of selection criteria, Unsatisfactory of the University of Colombo.

Remediation and further information

Recommended to have well defined criteria and it should be openly distributed among students. Should not just wait till students come and ask from SSA division.

Document log system

Observation

Observed that there is no proper document log system for the SSA branch.

Risk Rating	Medium
Impact	High
Likelihood	Low

Description and risks

Risk of finding old documents due to lack of file log system, Loss of important documents due to physical damages and natural disasters.

Remediation and further information

Recommended to use proper document log system and keeping soft copies of important documents as a backup to overcome natural disasters like flooding. Should store those documents on cloud kind of storage.

Availability of hostels

Observation

Observed that availability of hostels always has issues, where sometimes hostel wardens doesnıt provide exact availability of hostels and sometimes more students allocated for a hostel without having enough availability.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Risk of having no hostels for students when hostel rooms are available, also having an issue of having number of allocated students than the availability of hostel rooms.

Remediation and further information

Recommended to have a proper tracking system for the Hostel room availability, like having flight seats booking availability of a flight. It will encourage everyone who involved to allocate students for the Hostels. This should be a responsibility of Sub-Wardens of the University of Colombo hostels and subject clerk of the SSA branch.

Selection of Students (Hostels)

Observation

Observed that the system which is used to select students is a very old system, students tend to get wrong recommendation from the grama sevaka niladaari about his or her family income.

Risk Rating	Medium
Impact	High
Likelihood	Medium

Description and risks

Risk of eliminating students which should be eligible for Hostels given by the University.

Remediation and further information

Recommended to use new adaptable system and should review annually for betterment of the University students and to make everyone happy about the system.

4.7 Criticality Level of Risk Assessment List

Problem Description	Criticality Level and Score
Student availability for new intake from faculties	16
Student registration	13
Examination time tables	27
Data backup system - Exam Branch	27
Accessing the Finance division	24

Suppliers interaction with employees of the Finance division	21
Latency of confirmation the goods received by the user department	24
Submission of recommendations	27
Submission of department procurement committee documents	20
Backup system - Finance division	23
Availability of the common financial data	20
Hard copy files storing	23
Working procedure - Finance division	17
User trainings - Finance division	24
Cheque Payments	27
Update the account system	27
Settle down account transfers	27
Payment Vouchers	21
Vehicle arrangements	24
Vehicle arrangement procedure	27
Vehicle arrangements (When UOC vehicles not available)	24
Bill payments	24
Attendance of cleaning service	21
Billing process of cleaning service	20
Reservation of Board rooms	17
Issuing Cloaks	13
Monitoring Data Centre activities	27
Location of the Data Centre	20
Proper door lock method	23
Accessing the University premises	27
Securing the important assets	24
Protecting physical assets of the University	23
Power outage	17

Secure access to the data Centre location	23
Data and power cable diagrams	24
Servers Maintenance	20
Service level agreements	24
Password policy	27
IT and Email policy	24
Network related inquiries	21
Creating/Editing/Deleting of official email addresses	27
Office 365 accounts Creating/Deleting/Editing and Subscription	23
Access permission (Firewall)	23
Posting news on the University main website	24
Identification of the University of Colombo staff	30
Identification of temporary staff, trainees and visitors	30
Backup system - Student and Staff Affairs Branch	23
Password Complexity	23
Hostels bill payments	16
Selection of Students (Bursary Payments)	23
Document log system - Student and Staff Affairs Branch	20
Availability of hostels	24
Selection of Students (Hostels)	24

Table 4.3: Risk assessment list

Chapter 5

FUTURE PLAN AND GOAL

Implementation of a proper local Information security management system for the University system and later local standardization for all public and private organizations in Sri Lanka.

ISMS Implementation Program

The Information Security Management System will implement the most appropriate way for the University of Colombo in the future.

- Implement the Risk Treatment Plan to achieve desired results with the identified security control methods, including cost and resources requires to control risks.
- Implement security controls to minimize the damage and check whether the security controls are up to date.
- Define how to measure the security control's effectiveness and efficiency of the proposed ISMS.
- Provide information security awareness and training for all stakeholders.

Chapter 6

CONCLUSION

The research and analysis detailed in this thesis attempts to answer many information security issues within the administrative departments of the University of Colombo. It is necessary to be proactive in addressing the issues associated with information security issues while we plan to go forward as a leading international University in the world. An Information Security Management System (ISMS) will help to implement necessary, appropriate and proportionate controls to protect critical information assets of the University and maximize the use of such critical assets to gain maximum benefits. The activities related to information security risk management will allow the University to a) consider the complete threat landscape, b) assess inherent risks within critical and sensitive processes, as well as c) select and implement suitable mitigation actions to reduce the risks to the University. A holistic information security environment is built around people, processes, and technology. Any security technology selected must have the necessary processes executed by competent and capable human resources. Establishing an effective Information Security Steering Committee (ISSC) will be crucial in prioritizing the response to security vulnerabilities found within the University and take ownership of protecting University of Colombo critical assets by applying adequate security controls.

Appendix A

Information Security Steering Committee Members of the University of Arizona:[8]

- Chief Information Security Officer
- Vice President, Information Strategy and University Libraries
- Vice President, Human Resources
- Senior Associate Vice President, University Relations
- Office of Responsible Conduct of Research
- Assistant Vice President, Financial Services
- Assistant Vice President, Risk Management
- Academic Leadership
- University Registrar
- University of Arizona Police Department
- Chief Auditor
- Health Sciences Associate Chief Knowledge Officer
- Faculty Senate Representative
- Office of General Counsel

Appendix B

List of Faculties, Institutes and Other Academic divisions of the University of Colombo

- **Faculties**
  - Arts
  - Education
  - Graduate Studies
  - Law
  - Management & Finance
  - Medicine
  - Science
  - Technology
- **Institutes**
  - Institute of Agro-Technology and Rural Sciences (IARS)
  - Institute of Biochemistry, Molecular Biology and Biotechnology (IBMBB)
  - Confucius Institute of University of Colombo (CIUC)
  - Institute of Human Resource Advancement (IHRA)
  - Institute of Indigenous Medicine (IIM)
  - National Institute of Library & Information Sciences (NILIS)

- **Centres**
  - Centre for Contemporary Indian Studies (CCIS)
  - Centre for the Study of Human Rights (CSHR)
  - National Education Research & Evaluation Centre (NEREC)
  - Staff Development Centre (SDC)
  - Social Policy Analysis & Research Centre (SPARC)
- **Units & Projects**
  - Career Guidance Unit (CGU)
  - Higher Education for the Twenty-first Century (HETC)
  - Improving Relevance and Quality of Undergraduate Education (IRQUE)
  - International Office University of Colombo (IOUC)
- **Schools & Campuses**
  - Sri Palee Campus (SPC)
  - University of Colombo School of Computing (UCSC)

Universities have several employee cadres in two main categories (Academic and Non-Academic). University of Colombo itself has around 2000 employees working at the University. But most of them dont know what their part of the system is and how they could engage to maximize the productivity of the University. It happens mainly due to lack of staff training when they joined or when they went to new departments.

Vice Chancellor is the overall administrative head of Academic and Non-Academic staff of the University. Registrar is the head of administrative and Non-Academic staff. Bursar is the head of financial departments of the University.

Everyone granted access to University information assets (e.g. email, teaching and learning materials, staff/student information, financial information, research information, and the systems used to process these) has a personal responsibility to ensure that they, and others who may be responsible to them, are aware of and comply with the Framework. Failure to adhere to the mandatory requirements of the Framework could result in disciplinary actions.

Appendix C

Signatures of Heads of The University of Colombo Administrative Departments

The undersigned have provided signed attestation below of the accuracy of the work procedures and processes of the University of Colombo administrative departments as described in section (3.5).

- Deputy Bursar, Supplies Division

- Senior Assistant Registrar, Examination Branch

- Senior Assistant Registrar, General Administration

- Senior Assistant Registrar, Non-Academic Branch

- Senior Assistant Registrar, Academic and Publication

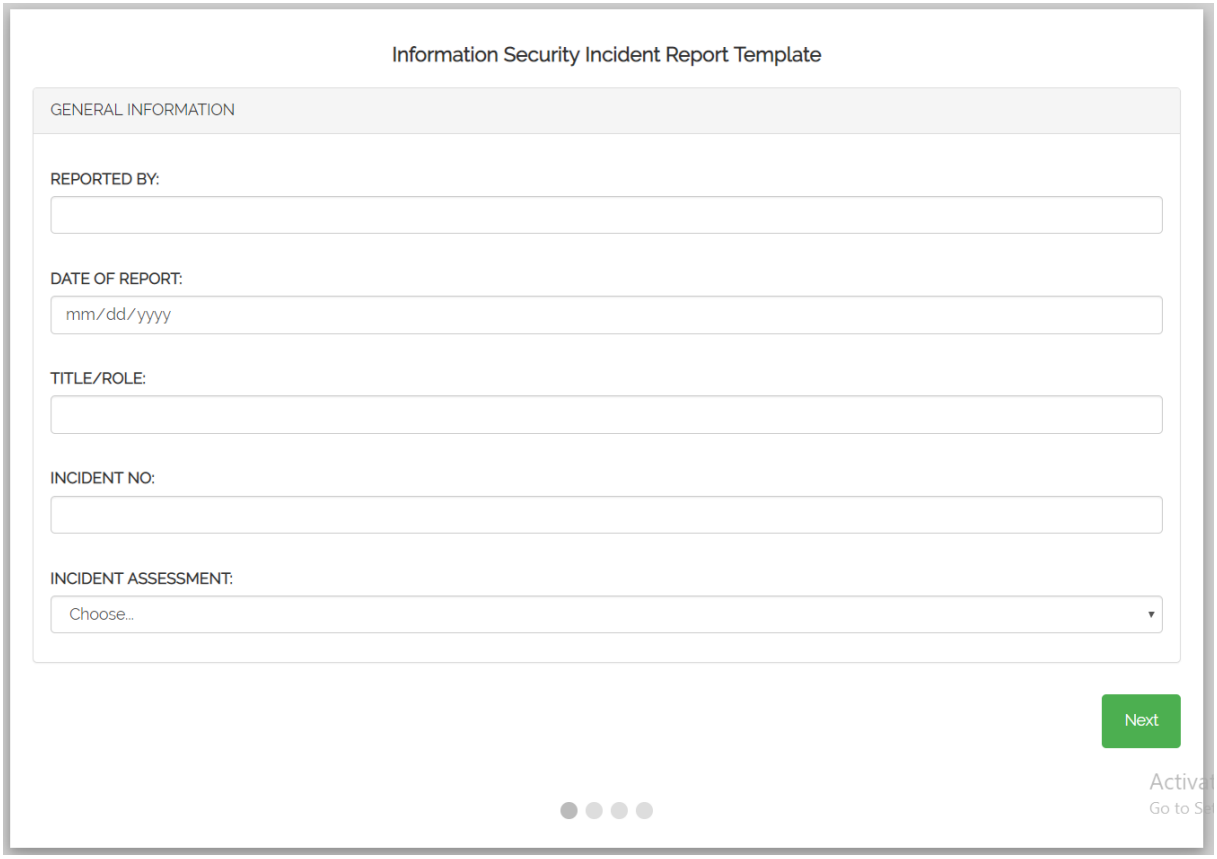
- Assistant Registrar, Student and Staff Affairs

- Assistant Network Manager, Network Operations Centre

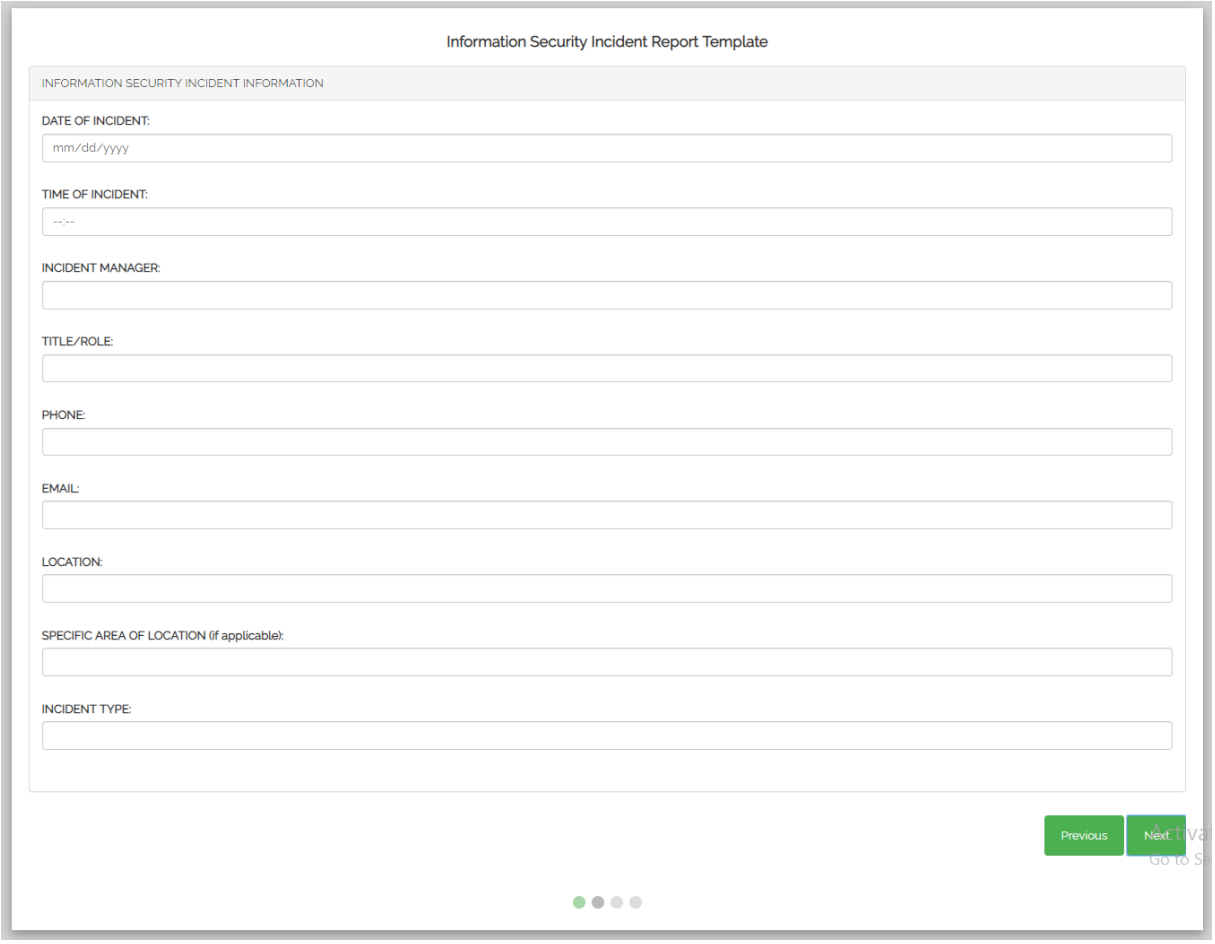
Appendix D

Information Security Incident Report Template

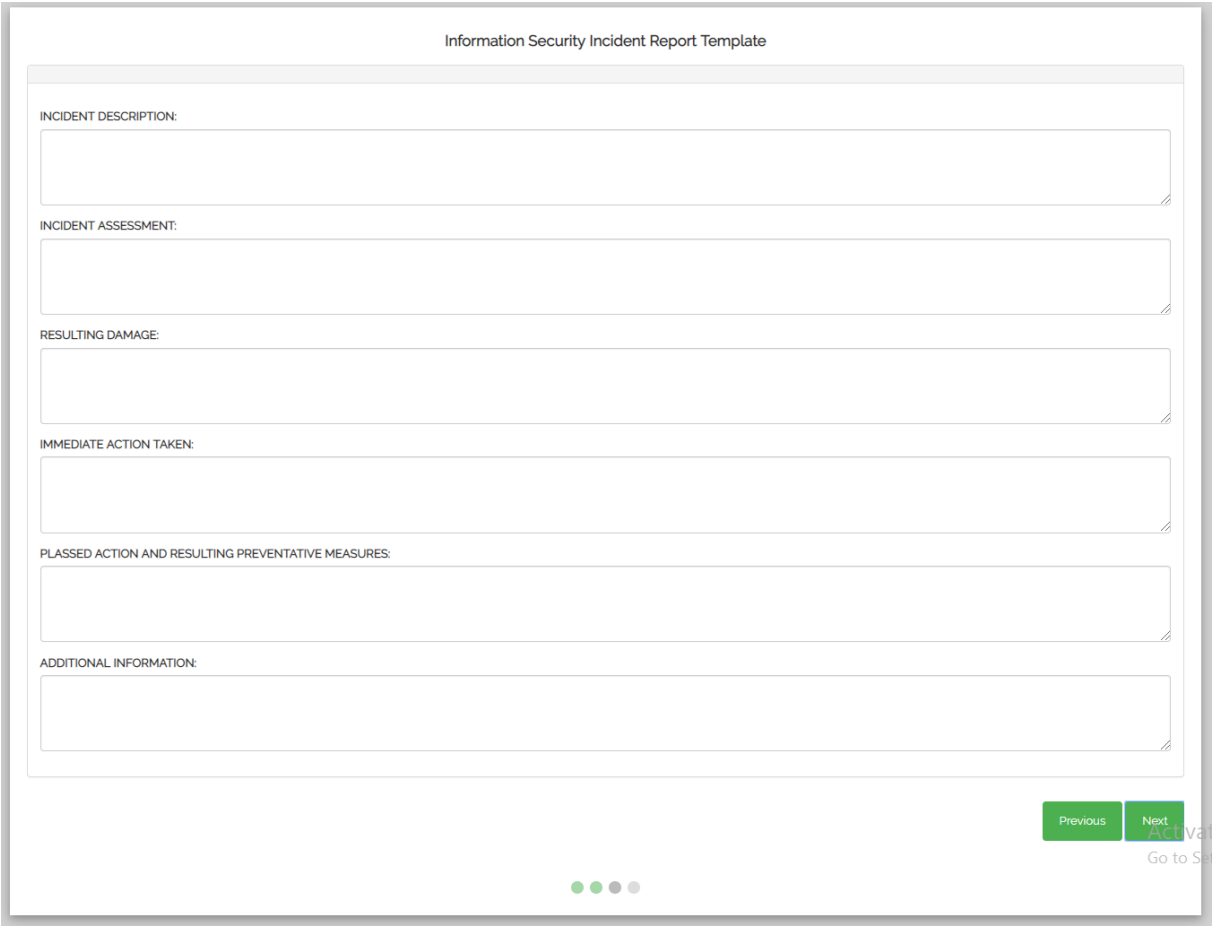
General Information



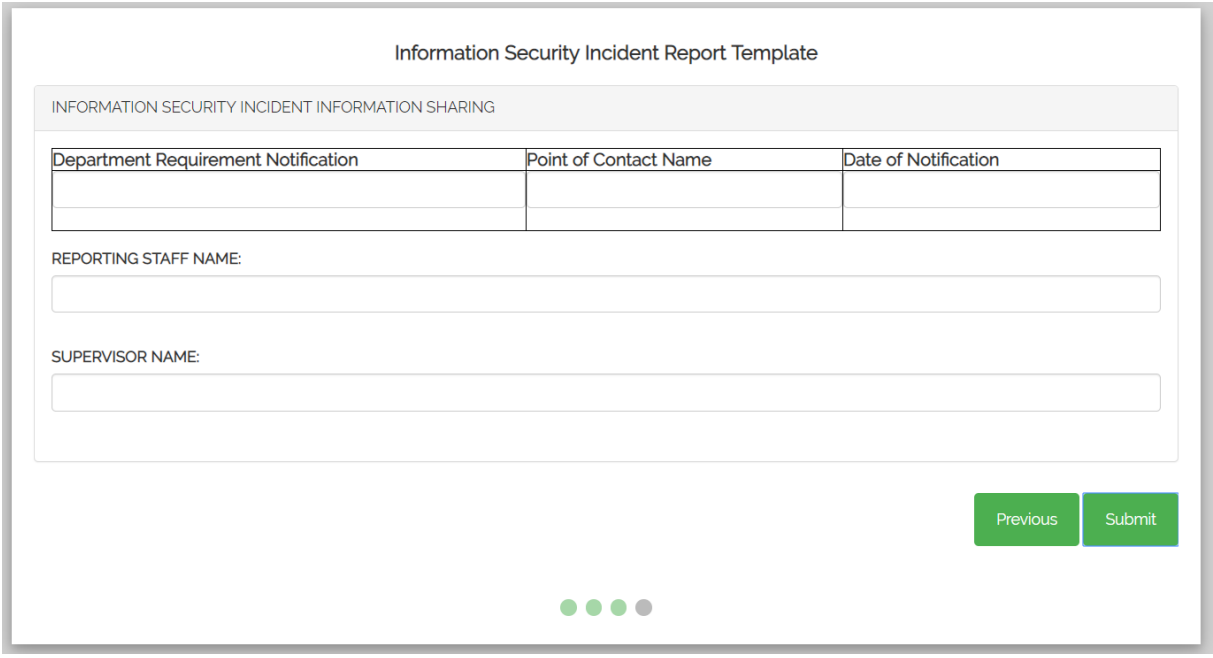
Security Incident Information



Security Incident Information Continue ...



Security Incident Information Sharing



Bibliography

[1] P. Ausick, "Ceos pick top 10 threats for 2019," Jan 2019. [Online]. Available: https://247wallst.com/economy/2019/01/22/ceos-pick-top-10-threats-for-2019/

[2] C. O. T. E. Communit, "Communication from the commission to the council, the european parliament, the european economic and social committee, and the committee of the regions: A mid-term assessment of implementing the ec biodiversity action plan," *Journal of International Wildlife Law & Policy*, vol. 12, no. 1-2, p. 108120, 2009.

[3] "Information security steering committee best practices - information security magazine." [Online]. Available: https://searchsecurity.techtarget.com/magazineContent/Information-security-steering-committee-best-practices

[4] "Iso/iec 27011:2008," Nov 2016. [Online]. Available: https://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43751

[5] "Iso/iec 27001 information security management," Nov 2018. [Online]. Available: https://www.iso.org/isoiec-27001-information-security.html

[6] "Iso 31000 and iso 27001 how are they related?" Dec 2016. [Online]. Available: https://advisera.com/27001academy/blog/2014/03/31/iso-31000-and-iso-27001-how-are-they-related/

[7] S. Harris, D. Mair, A. Evans, and M. Markose, "Information security standards framework," *Information Security Standards Framework*, Oct 2018. [Online]. Available: https://www.waikato.ac.nz/ict-self-help/guidelines/UOW-Framework-InformationSecurity-v1.4.pdf

[8] "Rcm implementation steering committee." [Online]. Available: http://rcm.arizona.edu/committee-members/steering-committee

[9] M. Karjalainen, “Developing an information security management system,” May 2014. [Online]. Available: https://core.ac.uk/download/pdf/38107661.pdf

[10] “Read ”the owner’s role in project risk management” at nap.edu,” *National Academies Press: OpenBook*. [Online]. Available: https://www.nap.edu/read/11183/chapter/7

[11] C. Joshi and U. K. Singh, “Information security risks management framework a step towards mitigating security risks in university network,” *Journal of Information Security and Applications*, vol. 35, p. 128137, 2017.

[12] “Information and data compliance.” [Online]. Available: https://warwick.ac.uk/services/idc/informationsecurity

[13] R.-E. Irimia and M. Gottschling, “Taxonomic revision of rochefortia sw. (ehretiaceae, boraginales),” *Biodiversity Data Journal*, vol. 4, p. e7720, 2016. [Online]. Available: https://doi.org/10.3897/BDJ.4.e7720

[14] L. Macdonald, “Monitoring telephone calls, email and internet use,” *Tolleys Managing Email & Internet Use*, p. 163185, 2004.

[15] C. C. for Occupational Health, “(none),” May 2019. [Online]. Available: https://www.ccohs.ca/oshanswers/hsprograms/hazard_control.html?=undefined&wbdisable=true

[16] “Annual global ceo survey,” *Choice Reviews Online*, vol. 51, no. 04, 2013.

[17] “Incident response (1/5): The 5 benefits of an incident response plan,” Jul 2018. [Online]. Available: https://www.hitachi-systems-security.com/blog/benefits-incident-response-plan/

[18] T. Kolomiyets and S. Vale, Jan 2017. [Online]. Available: https://statswiki.unece.org/display/GORM/GuidelinesonRiskManagement