Managing Computer Security, Risk Analysis and Threat Using ISO 31000:2009: Case Study at Seiyun Community College, Yemen

Abdullah A. Al-khatib[1] and Mohammed A. Hassan[2]
(Corresponding author: Abdullah A. Al-khatib)
Faculty of Computer Science, Landshut University of Applied Science[1]
Am Lurzenhof 1, 84036, Landshut, Germany
Department of Information Systems, Seiyun Community College[2]
Seiyun, Yemen
(Email: S-aalkha@haw-Landshut.de)
(Received Jan. 13, 2018; Revised and Accepted June 18, 2018; First Online Mar. 17, 2019)

Abstract

In modern digital era, all organizations are completely dependent on Computers and related devices. For that reason, it is mandatory for the organization to manage computer security in order to run smoothly. This paper discusses a case study of Seiyun Community College (SYNCC) for managing computer security, analyzing the risk and threat to the organization's computer system. This case study is performed using the data collection method from the archives. The findings show that SYNCC is lacking in computer system security behind ISO 31000:2009 standard which leads to failure in running the organisation. Finally, from the analysis, it is recommended that SYNCC develop a security plan to cover all the aspects of the information and communication technology. Educating the users is also needed in order to implement the security policy.

Keywords: Analyzing Risk; Analyzing Threat; Enterprise Risk; ISO 31000:2009; Risk management

1 Introduction

Higher educational Institutes are currently faced with a great demand for human, technological, and environmental resources, among others, that must be harmoniously related so that they can provide and optimise the different services. These services include communication over long distances, thereby reducing geographical limits, the storage of vital and large amounts of user information, the provision of support to users and a number of functions that can be provided with the interrelation of these resources. Also the growth of educational Institutes has increased the risks that are implicitly due to changes or updates that are generated by this growth. For this reason, those Institutes must be prepared to face these risks and to generate a support guide for Institutes to use.

An increasing number of higher educational Institutes are beginning to worry about this issue and they are asking how this can be implemented it and what costs can be incurred. Companies that are now entering the world of business are the ones that are most exposed since their ignorance of the subject leads to greater vulnerability. Before starting to function in an orderly manner, companies may have absorbed losses generated by some risk not taken into account or not controlled, so the guide will be based on the standard ISO 31000 that is fully defined for Risk management [12].

Seiyun Community College (SYNCC) is a governmental College in Yemen that is established in 2003. Presently, the College has five departments that are located in geographically separated buildings. Communication between these buildings is based entirely on Internet Protocol (IP) network. National and International communications, on the other hand, are heavily dependent on Internet services. The Information and Communication Technology (ICT) center provides services to the College. Prominent among the services it provides access to the Internet, Email services, staff and student information systems, and ICT Capacity Building Training (CBT). ICT center also operates wireless and fibre networks for intra campus connectivity. ICT vision of the College is to have Information Technology equipment for the entire community of the SYNCC and electronic classrooms and other equipment for educational delivery. The ICT mission of the College is to provide access to information and knowledge to the SYNCC community and beyond as a way to improve Teaching, Learning, Research and Community Services for its stakeholders.

There are a number of risk management standards and frameworks have been developed by countries and na-

tional standards bodies. Some of such standards and frameworks are: CoCo (Criteria of Control) standard which was developed by the Canadian Institute of Chartered Accountants in 1995, IRM (Institute of Risk Management) is one of the best-established and most widely used risk management standards was produced by the IRM in 2002 in co-operation with AIRMIC and Alarm, BS 31100 is published by British Standards Institution in 2008, COSO ERM is framework produced by the Committee of Sponsoring Organizations of the Treadway Committee in 2004. COSO ERM framework (2004) contains all of the elements of the earlier Internal Control version COSO (1992), Turnbull is framework produced by the UK's Financial Reporting Council in 2005. The standard that had the widest recognition was the Australian Standard AS 4360 (2004). AS 4360 was withdrawn in 2009 in favour of ISO 31000. The latest addition to the available standards is the international standard ISO 31000:2009 which was published in 2009. Although some standards are better recognized than others, organizations should select the approach that is most relevant to their particular circumstances. [7].

ISO 31000:2009 [10] is an international standard published in 2009 that provides a generic approach to risk management, establishes minimum principles required for effective management, proposing an integrated framework from the definition of strategies, planning, administration, information and communication, policies, values and culture. In this way, risk management is systematic, transparent and credible in any scope and context. Although it is a standard, it is not the objective of the standard to establish a uniform implementation scheme in organizations, their design and implementation will vary according to the particularities (objective, context, structure, operations, functions, processes, products, services, assets, *etc.*) of each entity.

ISO 31000:2009 is used as a methodology to harmonize the risk management process, and in the current or future models that the organization has, it is necessary to consider that this standard is not used as a basis for certification. Its implementation is established with a systematic application of policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analyzing, evaluating, treating, monitoring and reviewing the risks [5]. The success of the model depends on the adequate structuring of the framework providing the foundations and criteria that will be embedded in the different levels of the organization. The framework allows management of risks to be aligned with a process adjusted to the context of the organization, and allows the assurance of timely communication that is used for decision-making and the allocation of responsibilities. Figure 1 shows the interrelation of the different components of the framework in an iterative way. It should be noted that this framework does not prescribe the management system of an organization but facilitates the integration of risk management with the entire administrative system, emphasizing that the process must be initiated

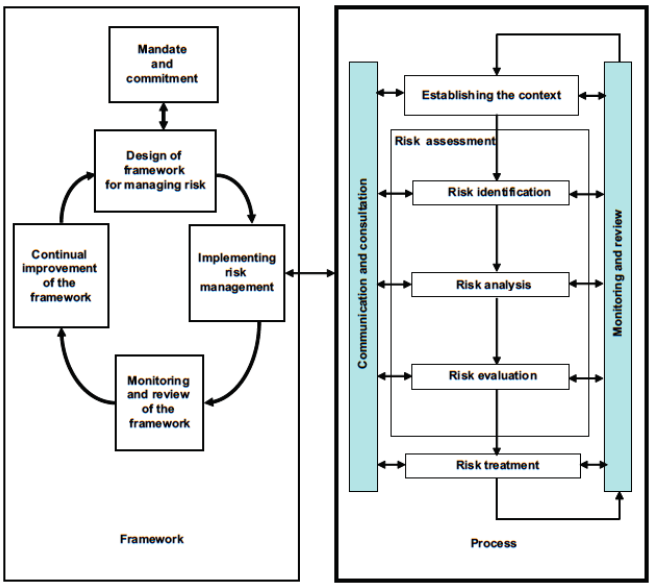

Figure 1: ISO 31000:2009 risk management framework and process [10]

in the top management of the company, showing its commitment and issuing Guidelines for risk management [8]. Once the principles are known, its framework to be followed by the organization in this risk management model shows the third pillar of the "Risk Management Process", which is shown in greater detail in ISO 31010: 2009 [9].

This study relies heavily on the literature and research in the context of risk management. Since ISO 31000 was initially published in November 2009 only a few academic research articles about standards have been published. Purdy [21], Shortreed [23], Leitch [15] and Aven [1] were among the first to examine the new research framework. While Purdy and Shortreed examined different aspects of the new standard in a positive tone, Leitch and Aven were very critical of the terminological and functional defects of the new standard. Health emergency management in mass gatherings and the applicability of ISO 31000 was examined by Hills [17] and examples of real-life mass gatherings with the Asia Pacific region were examined in the context of ISO 31000 which is of little value in the present study.

With the exception of study publications by professional organizations, such as PwC or Aon, risk management has been the focus of very little academic research thus far. Review of risk management related articles in academic journals and working papers has indicated that academic research on risk management is largely descriptive. In addition, findings of previous studies have been inconsistent. In [11] risk management consultancies and professional organizations have developed risk maturity models to investigate the performance of risk management. Models generally include a series of performance criteria which intend to measure how well the audited organization is performing in its risk management.

The contribution of this case study is that no scien-

tific studies on ISO 31000:2009 have been yet published in Yemen. Therefore, this present study is the first one to venture into that area. In addition, educational Institutes save time and find a clear and precise document and students will be able to obtain information more easily on the norms. This does not suggest that further research be discontinued, since as mentioned above, technology is an area that remains constantly changing and not being updated is considered as risk.

The remainder of this paper is organized as follows. Section 2 presents the Analysis and Discussion. The Recommendations and Critical Reviews are given in Section 3. Finally, Section 4 draws the Conclusions.

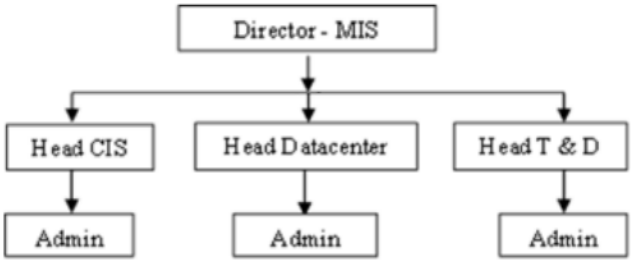

Figure 2: Security structure in SYNCC

2 Analysis and Discussion

For the development of the risk analysis within SYNCC, the standardization (ISO) 31000:2009 methodology was selected because it requires the participation of people who are directly involved in the operation of the critical information assets. Standardization is done in order to minimize risks and provide a higher quality service to its students by fully protecting its largest asset, which is the information on the aspects of reliability, integrity and availability, as each client makes strategic decisions [25].

The organizational, technological, and analysis aspects of an information security risk evaluation are complemented by ISO31000: 2009 risk management process. ISO 31000: 2009 is organized around these steps (illustrated in Figure 1), enabling organizational personnel to assemble a comprehensive picture of the information security needs.

SYNCC College's risk management process is consistent with the activities identified within the framework of IS0 31000:2009 method. To establish risk management process a reference was made to ISO 31000:2009. The process described below is based on ISO 31000:2009.

2.1 Communication and Consultation

The objectives at this step are to develop an effective communication process that serves as a basis for decision-making and for implementing the action plans required [10] in addition to identifying the College's Information and Communication Technology (ICT) assets such as information, hardware, human resources and the provision of policies and procedures to protect them.

2.1.1 Security Organization

This structured management framework directly monitors and controls the implementation of information security in SYNCC as shown in Figure 2. In this organization, the Director of Management Information Systems (Director-MIS) is the Chief information officer, followed by head of various units such as head of Datacenter, head of Corporate Information System (Head CIS) and head of Training and Development (Head T&D). Each individual unit has a number of staff called 'admin' that handles information system responsibility.

As can be seen from the diagram of Security Structure in SYNCC (Figure 2) each unit and admin handles some information system equipment and data that possesses security challenges. The College management is looking into the Director-MIS for the College information systems while head of units and admin are responsible for their individual units and services respectively. Reporting and implementation of security decisions starts from the admin to Director-MIS.

2.1.2 Human Resources

The SYNCC College has no centralized and well-documented security policy regarding employees, students, contractors, and part-time staff, but individual units have their own (Library and students affairs) registration/clearance policy where one will be asked to tender College belongings in his position before he is finally given clearance. In addition, the College has asked its new staff to sign or write an acceptance letter based on what has been stated in the appointment letter. The same thing applies to contractors, but here the College asked them to sign an agreement form that describes how the project will be executed, as well as penalties for failures. SYNCC does not conduct any security awareness training for its staff during and after recruitment. In addition, the College has no security policy for staff or contractors exiting SYNCC College to tender any access rights or equipment besides the one mentioned above.

2.1.3 Assets

Asset in information systems refers to anything from data, device, to other components of the environment that support information-related activities. In general, assets refer to hardware (*e.g.* servers, Desktop, laptops and switches), software (*e.g.* mission critical applications and support systems) and confidential information [19]. SYNCC have many assets (Network or systems) requiring protection as the following:

- *Desktops*: 208 PC (170 PC in student access rooms, 10 in the library, and 28 shared among staff in various

Table 1: Internal and external factors in SYNCC

Internal Factors	Description	External Factors	Description
Incident platform	Software designed for incident management.	Suppliers	Third parties that provide support services in the process and that allow the fulfilment of the objectives of the same.
Staff employees	They work in the help desk area in their different positions.	Customers	Are the people requesting the service.
Resources	Computer and communication equipment.	Economy	Influences the process due to the demand of potential customers and capital for investment in research and acquisition of new technologies.
Procedures	Refers to the procedures established in SYNCC area and which are endorsed by the quality area.	New technology	Refers to the hardware and software update.

offices).

- *Laptops*: 23 (Dean, Deputy Deans, Head of Departments and Principal Officers).
- *Printers*: 34 (Dean, Head of Departments and Principal Officers).
- *Servers*: 5 (4 running Ubuntu Linux and 1 running Centos hosting services such as web applications, Drupal, Internet connection, e-mail, and student record databases).
- *Switches*: 36 (48 port Cisco & Juniper switches to provide connection on the campus).
- *Router*: 6 (50% from 3800 Cisco Router and 50% from 7200 Cisco router).
- *Firewall*: 2 (2 SRX650 Juniper firewall).
- *Power systems*: 128 KVA diesel generator and 250KVA inverter.

The servers within the Datacenter are linked using Cat6 cable, various buildings of the College are linked using fiber optic cable and the computers in access rooms are linked using Cat6 cables. The remainder are linked by an 802.11g wireless network with an access port.

Although SYNCC has firewall configured at border of the Internet to protect the publicly accessible servers, the security control mechanisms implemented at SYNCC are not sufficient. Below are some of the security vulnerabilities of SYNCC:

- *Virus protection*: Not present on any computer except the one that runs either free version or pirated, not up-to-date; generally, most users are aware of viruses but are a bit unsure about what they could do to prevent them.
- *Spam-filtering software*: Many users are complaining about spam, but no protection is in place.
- *Updates*: All Microsoft Windows systems including productivity tools are not up-to-date because they are pirated copies.
- *Laptop computers*: None of the laptop computers have security locks, stickers and engraving.
- *Wireless networking*: The wireless network is open to people who have wireless access capability to browse on the network.
- *Web browsing*: SYNCC does not have a policy on acceptable use, and no one is taking any security measures.
- *Backups*: SYNCC back up data on the server to an external USB hard disk drive; the backed-up data and the machines are located in same room which is unsatisfactory.

Besides the above-mentioned assets, SYNCC also have the following:

- Records of contracts with suppliers and vendors.
- E-mail database and archive of past e-mail messages.
- Request forms of various items.

- Documents of legal records stored in various filing cabinets.
- Financial records.
- Operations.

Operations refer to functions, procedures and methods of doing things within the College. In the College staff only follow the responsibilities and functions assigned to them by their officer. There is no authentic documented way of handling duties and responsibilities except that staff operate within the ambit of their functions and what they can do to assist the system. Contractors use the bill of quantities given to them when bidding for contract and later sign agreement document prepared by the College.

2.2 Establish Context

In this section, the organization articulates its objectives and defines internal and external criteria and evaluation factors to consider in risk management [6]. In other words, it is the set of circumstances that surround and condition risk management both internally and externally [24]. The internal context is the internal environment in which the College seeks to achieve its objectives and it establishes the mission, vision and objectives of SYNCC College, the policies that are implemented, the culture of the college, its structure, strategy, and everything that affects the internal operation of the same. The external context establishes the current rules that apply to the college according to its economic activity, public policies, demography, trade, technology, and everything that has a relationship with the college from an external environment and that affects its operation [3]. For this case study, the internal and external factors of SYNCC are shown in Table 1.

2.2.1 System Acquisition

This is basically IT driven and refers to the way the system is developed, its life circle, security assessment, and vulnerability tests [13]. Due to the lack of technical competency, not all of these were followed when deploying a system. SYNCC regularly updates Linux O/S and services such as nginx, mysql, and drupal, but does not have any documented plan for handling lost passwords and access rights.

2.2.2 Internal Standards and Regulation

These are sets of code of practice and rules for security in computing [20]. At SYNCC, although they follow some standards, they are not documented and binding. The following are some of the standards they use.

- *Password standard*: must be a minimum of six characters, which includes a combination of upper, lower and special characters.
- *E-mail user standard*: The user must be a member of the College community, recommended by his HOD and the user ID must include his/her name.
- *Operating systems standard*: They use Ubuntu Linux on the server side.
- *Application standard*: Mostly application that runs on Linux platform.
- *Non-access of porn materials*: As a standard, SYNCC have content filtering engine at the gateway.
- *Vendors*: a vendor must register in Yemen, pay taxes, and be certified by the College tender board.

2.2.3 Incident Management

This capacity is needed to respond to security incidents, including forensic investigations, remedial actions to mitigate, and escalate the incidents to the next level [20]. In the event of a security breach, a staff on duty will be contacted. The staff attending to user's requests such as hardware maintenance, software installation and connectivity issues. During serious incidents such as virus infections, equipment or Internet failure, staff on duty and another staff will help in solving the problem. Staff monitor the servers and firewall regularly to make sure that no breaches have occurred.

2.2.4 Business Continuity Plan

The main objective of business continuity management is to neutralize interruptions to business activities, to safeguard critical business processes from the consequences of major failures of information systems, and to ensure their quick recovery [26]. In SYNCC the following measures have been implemented to allow ICT business activities to cope with failures:

- They keep a backup of important information on different media types.
- Installed and configured multiple servers as backup.
- Multiple environmental control devices.
- Power backup such as uninterruptible power supplies (UPS) and Diesel generator.
- Maintain and upgrade staff skill regularly as well as recruiting more staff to avoid losing key staff.

2.3 Risk Assessment

Risk assessment involves the identification of risks followed by their evaluation or ranking. It is important to have a template for recording appropriate information about each risk. The evaluation is subject to the results obtained in the execution of the management since all the companies have characteristics that make them different.

2.3.1 Identify Risks

The risk is the possibility that an event occurs that will have an impact on the achievement of the objectives. Risk is measured in terms of impact and likelihood [4]. Identification is the most important step for risk management since the risk that is not identified at this point will not be taken into account in the subsequent analysis and therefore will not be evaluated. According to Renn [22], to identify the risk it is necessary to have an adequate tool or technique defined by each entity or person according to its criteria. In addition, the people who execute this activity must have the appropriate knowledge about the process to be evaluated. All risks must be taken into account which means that both those with applied controls and those who do not have to be listed should be listed.

In SYCC, the potential risks are identified using two techniques. The first one is what-if analysis technique in which simple questions and scenarios are assumed to see if they can help to identify new risks and see what plans they need or already have in place to manage with these events. The second technique that is used to identify the potential risks is the automated scanning tools.

2.3.2 Risk Analysis and Evaluation

The objectives at this step are to separate the minor risks from major ones. This process includes identifying threats to information or information systems, determining the likelihood of occurrence of the threat, and identifying system vulnerabilities that could be exploited by the threat [16].

The potential risks encountered at SYNCC can break down into the following nine main categories:

- Epileptic nature of electricity supply.
- Harsh weather conditions. Very hot during the summer and cold winter.
- Possibility of prolonged downtime due to foreseen or unforeseen circumstances such as political issues and equipment failure.
- Continuous rise in software and support costs due to increase in both demand and complexities.
- Misuse of login details by staff and users.
- Lack of adequate skills to manage and implement systems.
- Lack of computer security policies.
- Experienced staff leaving for higher paying jobs.
- Threats against physical security for Crimes, Robberies, and Terrorism.

In SYNCC, they believe that these risk categories, and accordingly the risks included, can be rated as high, medium and low. Table 2 shows risk categories and their ranks.

Table 2: Risk assessment

Threat	Rate
Epileptic Power supply	2
Harsh weather	1
Equipment downtime	1
Rise of software and support	1
Cyber-criminal activities	2
Misuse of login details	2
Lack of adequate skills	2
Lack computer security policies	2
Experience staff leaving for high payment	2
Threats against physical security	2

2.3.3 Assets Management and Valuations

The definition of the risk profile allows comparing the results of its rating with the criteria defined to establish the degree of exposure of the process to risks [6]. In this way, it is possible to distinguish between acceptable, moderate or unacceptable risks and to set the priorities of the actions required for their treatment. Here, they manage the most important assets in the following ways:

Identification: They identify their hardware assets based on location and usage.

Location: Here they locate equipment based on usage *e.g.*, core network equipment, servers, and server software are in the datacenter; access devices located in the departments and units.

Responsible person: This depends on the location and usage *e.g.* Datacenter staff are responsible for datacenter holdings while personal/official access devices are to be the responsibility of the person using them. Network section staff are responsible for network access devices such as wired and wireless.

Protection: They deploy many measures to protect the assets such as power backup, physical security, access control, permissions.

In SYNCC, based on the value of the assets their corresponding importance: 5-critical, 4-very important, 3-important, and 2-good are given as shown in Table 3.

2.3.4 Treat the Risks

Once the risk has been fully identified, it is necessary to carry out its treatment [18]. Therefore, it is important to establish all the possible actions to mitigate the risk. These actions must be realizable and be effective in terms of mitigating the risk, and include:

- Defining new strategies.
- Plans for improvement.

Table 3: Asset management and valuation

Asset	Category	Location	Owner	Rate
Student information system	Information	Datacenter	Datacenter	5
Web sites	Information	Datacenter	Datacenter	3
e-mail messages	Information	Datacenter	Datacenter	3
Backup data	Information	Datacenter	Datacenter	4
Bind DNS	Application	Datacenter	Datacenter	4
Nginx	Application	Datacenter	Datacenter	4
Apache	Application	Datacenter	Datacenter	4
Drupal	Application	Datacenter	Datacenter	4
Servers	Hardware	Datacenter	Datacenter	4
Border routers	Hardware	Datacenter	Datacenter	3
Firewall	Hardware	Datacenter	Datacenter	3

Table 4: Risk management

Asset	Value	Risk	Recovery cost	Priority	Mitigating risk
Student information system	5	High	High	High	Avoid or limit
Web sites	3	Low	Low	Low	Accept
e-mail messages	3	Medium	Low	Medium	Limit
Backup data	4	Medium	Low	Medium	Limit
Bind DNS	4	High	Low	High	Avoid or limit
Nginx	4	High	Low	High	Avoid or limit
Apache	4	High	Low	High	Avoid or limit
Zimbra	3	Medium	Medium	Medium	Limit
Drupal	4	High	Low	High	Limit
Server hardware	4	Low	Low	Low	Accept
Border routers	3	Medium	Low	Medium	Limit
Firewall	3	Low	Low	Low	Accept
Access switches	2	Low	Low	Low	Accept
Environmental conditions	3	Low	Low	Low	Accept
Power backup	3	Low	Low	Low	Accept
Developers	3	Medium	Medium	Medium	Limit
Sys/Network admin	3	Medium	Medium	Medium	Limit

- Physical readjustments.
- Process optimization.
- Others.

In addition, the objectives at this step are to develop and implement a management plan to mitigate identified risks. In addition, the process of taking actions to eliminate or reduce the probability of confidentiality, integrity, and availability of valued information assets being compromised to an acceptable limit [14].

There are three steps to risk mitigation: identify options, choose options, and implement options [2]. In SYNCC College, the risk is mitigated as follows:

- *Accept the risk*: When both the value of an asset and the risk are low, the risk is considered acceptable.
- *Limit the risk*: When the risk of an asset is high and can not be transferred, consider limiting it. This is done by updating systems, alternative power and restarting the system.
- *Avoid the risk*: Risk is avoided by either building an alternative system or by shutting down the system. Table 4 shows the summary of the risk mitigation process in SYNCC College.

2.4 Monitoring and Review

A regular process of review is performed to: identify new risks when they just arise, monitor existing risks and identify any changes that may influence the implemented risk controls, ensure that the existing risk controls are working effectively, and transfer the information on risks fully to appropriate parties. This allows the College to anticipate

and respond in advance to events that would otherwise cause damage to the College.

3 Recommendation and Critical Review

The overall discussion above analyzes how they manage computer security in SYNCC, Yemen. SYNCC started with assessing the ICT infrastructures and threats and finally identify risks and mitigate them. It is not clear whether the processes used by the College to categorize assets, threats and mitigation are correct since there are no formal documents that guides the staff in managing computer security. In addition, the staffs have no formal training in managing computer security as they depend only on residual knowledge. The methodology used in managing computer security does not conform to the minimum acceptable standard. The threats and risks identified were just very few and do not conform to each other. Many mitigations measures were not properly taken to contain risk posed by the threats. In general, SYNCC has to take into account the following recommendation in order to improve this security:

1) Develop computer security plan for SYNCC to cover all aspect of ICT and enforce the plan. The ICT staff can request the management to buy-in by making them believe in the benefits of securing the College information system. In addition, ICT staff can demonstrate the ROI (Return on Investment) when such policy is implemented.

2) Develop and implement acceptable policy such as password, email, internet access, backup and logins to secure server.

3) Risk assessment must not be based on assets values only, but on the likelihood of vulnerabilities and their impact to the system. Since all the assets have their inherent vulnerabilities, after the identification of vulnerabilities and their likelihood and impact, it is possible to identify the risk and suggest the adequate security controls to be implemented.

4) Educate users (i.e., employee and students) on computer security such as password, importance of security, safe browsing, virus prevention and updating operating systems.

5) SYNCC should use to secure data on IEEE 802.11 networks. For example, MAC address filter, WEP (Wireless Equivalent Privacy), WPA (Wi-Fi Protected Access), IEEE 802.11i (encapsulation of extensible authentication protocol) and IEEE 802.1X. In addition, they must apply function for protected from risks and threats as shown in Table 5.

6) There are new features SYNCC should use to save college assets. Like Gateway with VPN, Cosign integration in gateway, Bluesocket gateway, 802.1x, Checkpoint gateway and Radius Server with Uniqname and Passwords.

Table 5: Security function

Function	Property
Firewall	Blocks or permits traffic from each user based on their role.
Redirection	Monitors web traffic from unregistered users and redirects them to the gateway's server.
Web Server	Presents user with login web page.
Authentication	Authenticates using servers such as Active Directory, LDAP or RADIUS.
Role Based Access Control	Registered users are assigned a role. Roles can control access based on IP address, network, protocol, time and location.
QOS Server	Bandwidth per user can be limited by role.
VPN Server	A Virtual Private Network protects the privacy of all traffic from a user with encryption.

7) Encrypted Access for Students, Faculty and Staff of SYNCC: All students, faculty, and staff will be required to encrypt their traffic on the wireless network by use of a VPN client on their computers.

8) Information is an asset of great value to the College and as such must be protected. That is why in the implementation of information security should be sought. Safeguarding the accuracy and completeness of stored or transmitted information, the content of which should remain unchanged unless modified by authorized personnel.

9) SYNCC has some security risks, Table 6 describes these risks and how to overcome them.

4 Conclusion

Information system in SYNCC College has over time been expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, many personnel were hired and no security policies were implemented. These changes meant that new risks will surface and risks previously mitigated by some means may again become a concern. Thus, the

Table 6: Security risks

Assets	How to Protect
Student information system, Web sites and e-mail messages system	Implementation of information security should be sought, Safeguarding the accuracy and completeness of stored or transmitted information, the content of which should remain unchanged unless modified by authorized personnel.
Backup data	Having saved in a remote location keeps it safe in case anything goes badly wrong with your computer.
Bind DNS	By ASA, PIX, and FWSM firewalls, Cisco Intrusion Prevention System (IPS) and Cisco IOS NetFlow feature.
Nginx	Having configuring SSL, restricting access by IP and performing a security audit
Apache	Having keep up to date, protect from Denial of Service (DoS) attacks , permissions on ServerRoot directories and Watching Your Logs
Zimbra	Firewall and use login username and password with htaccess.
Drupal	The Drupal has database abstraction layer provides placeholder mechanisms to prevent SQL Injection vulnerabilities.

need for well-organized computer security management is clear. To help keep the cost down, the risk assessment should occur whenever an information asset is classified, purchased or a new project is developed. A security review is often helpful. For SYNCC to derive the benefits of computer security management, it must first develop and implement security policy covering all aspects of Information and Communication Technology components. By studying risk management, SYNCC should develop a computer security plan, implement acceptable policy and educate users on computer security.

References

[1] T. Aven, "On some recent definitions and analysis frameworks for risk, vulnerability, and resilience," *Risk Analysis*, vol. 31, no. 4, pp. 515–522, 2011.

[2] T. Aven and E. Zio, "Some considerations on the treatment of uncertainties in risk assessment for practical decision making," *Reliability Engineering & System Safety*, vol. 96, no. 1, pp. 64–74, 2011.

[3] K. M. Brown, "The role of internal and external factors in the discontinuation of off-campus students," *Distance education*, vol. 17, no. 1, pp. 44–71, 1996.

[4] A. Ekelhart, S. Fenz, and T. Neubauer, "Aurum: A framework for information security risk management," in *42nd Hawaii International Conference on System Sciences (HICSS'09)*, pp. 1–10, 2009.

[5] T. Ernawati, D. R. Nugroho, *et al.*, "It risk management framework based on ISO 31000: 2009," in *International Conference on System Engineering and Technology (ICSET'12)*, pp. 1–8, 2012.

[6] S. Fenz and A. Ekelhart, "Verification, validation, and evaluation in information security risk management," *IEEE Security & Privacy*, vol. 9, no. 2, pp. 58–65, 2011.

[7] P. Hopkin, *Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management*, Kogan Page Publishers, 2017. ISBN-13: 978-0749483074.

[8] D. W. Hubbard, *The Failure of Risk Management: Why It's Broken and How to Fix It*, John Wiley & Sons, 2009. ISBN: 978-0-470-38795-5.

[9] IEC, "ISO 31010: 2009-11," *Risk Management–Risk Assessment Techniques*, 2009. (`https://www.iso.org/standard/51073.html`)

[10] ISO, "31000: 2009 risk management–principles and guidelines," *International Organization for Standardization, Geneva, Switzerland*, 2009.(`https://www.iso.org/iso-31000-risk-management.html`)

[11] S. R. Iyer, D. A. Rogers, B. J. Simkins, and J. Fraser, "Academic research on enterprise risk management," *Enterprise Risk Management*, pp. 419–439, 2010.

[12] C. Lalonde and O. Boiral, "Managing risks through ISO 31000: A critical analysis," *Risk Management*, vol. 14, no. 4, pp. 272–300, 2012.

[13] J. H. Lambert, Y. Y. Haimes, D. Li, R. M. Schooff, and V. Tulsiani, "Identification, ranking, and management of risks in a major system acquisition," *Reliability Engineering & System Safety*, vol. 72, no. 3, pp. 315–325, 2001.

[14] T. P. Layton, *Information Security: Design, Implementation, Measurement, and Compliance*, CRC Press, 2016. ISBN: 9781420013412 .

[15] M. Leitch, "ISO 31000: 2009—the new international standard on risk management," *Risk Analysis*, vol. 30, no. 6, pp. 887–892, 2010.

[16] S. S. Lim, T. Vos, A. D. Flaxman, G. Danaei, K. Shibuya, H. Adair-Rohani, M. A. AlMazroa, M. Amann, H. R. Anderson, K. G. Andrews, *et al.*, "A comparative risk assessment of burden of disease and injury attributable to 67 risk factors and risk factor clusters in 21 regions, 1990–2010: A systematic analysis for the global burden of disease study 2010," *The Lancet*, vol. 380, no. 9859, pp. 2224–2260, 2013.

[17] A. Liuksiala, *The Use of the Risk Management Standard ISO 31000 in Finnish Organizations*, 2012. (http://tampub.uta.fi/bitstream/handle/10024/84249/gradu06462.pdf;sequence=1)

[18] Microsoft, *Microsoft Esecurity Guide for Small Business*, 2004. (www.professorsteve.com/FACT_Sheets/MicrosofteSecurityGuideforSmallBusiness.pdf)

[19] T. R. Peltier, *Information Security Risk Analysis*, CRC press, 2005. (https://www.taylorfrancis.com/books/9781439839577)

[20] T. R. Peltier, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, CRC Press, 2016. (https://www.taylorfrancis.com/books/9780849390326)

[21] G. Purdy, "ISO 31000: 2009— setting a new standard for risk management," *Risk Analysis*, vol. 30, no. 6, pp. 881–886, 2010.

[22] O. Renn, "Three decades of risk research: Accomplishments and new challenges," *Journal of Risk Research*, vol. 1, no. 1, pp. 49–71, 1998.

[23] J. Shortreed, "Enterprise risk management and ISO 31000," *The Journal of Policy Engagement*, vol. 2, no. 3, p. 9, 2010.

[24] M, Sumner, "Risk factors in enterprise-wide/erp projects," *Journal of Information Technology*, vol. 15, no. 4, pp. 317–327, 2000.

[25] S. Q. Wang, M. F. Dulaimi, and M. Y. Aguria, "Risk management framework for construction projects in developing countries," *Construction Management and Economics*, vol. 22, no. 3, pp. 237–252, 2004.

[26] P. Woodman, "Business continuity management," *Chartered Management Institute, Savoy Court, Strand, London*, pp. 8–12, 2007.

Biography

Abdullah Abdulrahman graduated from Al-Ahgaff University Hathramout in 2009. He works in communtiy college from 2009. He enrolled to study Master in University Kebangsaan Malaysia (UKM) in Computer Sceince (Network Technology) in 2015. His research interests are in Software Defined Network (SDN) and IP Security (IPSec), Computer Security.

Dr. Mohammed A. Hassan is assistant Professor at Department of Information Systems, Seiyun Community College, Yemen. He received the B.S. degree in Mathematics and Computer Science from the University of Al-Ahgaff, Yemen, in 2002, the M.S. degree in Computer Science from The University of Hamdard, India, in 2008 and Ph.D. degree in Computer Science from The Central University of Hyderabad, India, in 2014. His research interests include human visual system models for solving image and video processing problems.