The National Law Institute University, Bhopal

Offers Programme

Master

of

Cyber Law and Information Security

Project On

"Risk Management of an Academic Institution using ISO 31000:2018"

Subject

"Information Security and Risk Management"

SUBMITTED TO:

Mr. Mayank Tiwari

SUBMITTED BY:

Isha Gaur

(2019MCLIS58)

Table of Contents

ABSTRACT

Risk management is a process the organizations deals with the risks associated with the various activities taking place in their organization, because of which the probability of failure decreases and that of success increases and the level of uncertainty associated with the objectives of the organization. Risk management must be integrated into the culture of the organization and this will include mandate, leadership and commitment from the Board supporting accountability, performance measurement and reward, thus promoting operational efficiency at all levels. Organizations have to bear losses in terms of its reputation, economic losses and societal outcomes, if they do not manage or mitigate the risk associated.

In this paper, we will deal with Risk Management standard 31000:2018 in an academic institute. The study undertaken analyses the framework, principles and processes of the RM policy. Risk identification, analysis and evaluation are done and risk treatment plan is also studied. The documents are attached which includes the asset inventory and checklist drawn by the implementer.

KEYWORDS: ISO 31000:2018, University, Policy, Integration, Framework, Principles, Process, Risk Criteria, Implementation.

1. INTRODUCTION

Risk management is recognized as a prominent aspect of the good governance of a successful academic institution. The need for effective risk management framework is widely recognized by academic and industry to manage all type of risks encountered by an organization. However, managing risk practices in the not for profit arena, including public higher education institutions, appear to be significantly less developed as compared to that of business world. For implementing ISO 31000:2018 it is necessary to identify that an organization contain information asset or not. While identifying the risk the profit of an organization should not be affected. The organizations follow some internal rules and principles, however, by implementing ISO 31000:2018 the organizations adhere the standard and abide by the principles and processes defined under the standard and help organizations to manage a risk in a better way. ISO 31000:2018 can be implemented over an entire organization as well as to specific projects or activities.

2. ACADEMIC ISNTITUTE

In this paper, we are performing risk management of an academic institute XYZ University. The XZY University is recognized for pioneering and leading trends, exploring new knowledge, promoting new ideas, and transforming innovation that can be turned successfully. The institution has some assets and the critical assets that need to be protected. Keeping in mind the needs and expectations of the students, professors and employees, the XYZ University wants to implement the standard. However, the institute is far behind from business and industry, but it requires to implement risk management to minimize the consequences of unfavourable events.

3. RESEARCH IMPLEMENTATIONS

3.1 LITERATURE REVIEW

For writing this paper we have gone through various books, case studies, and articles related work done on the research of standard for risk management. The paper **The risk management in higher education institutions by Ljiljana Ruzic and Jelena Dakic**, the authors tried to connect and apply their knowledge in risk management in other areas, as well as the knowledge gained by their experience in managing the higher education institution. The example of one higher education institution is used in analysing the risk, and initial model was developed further with corrections in accordance to specifics and conditions is made. The risk was classified based on the process and activity noticed by the authors within their own institution. They described an entire spectrum of the measures for preventing or minimizing all the risks they noticed. Another paper **Risk management in higher education: An open distance learning perspective by Elmarie Sadler and Jacobus Stephanus Wessels**, discussed the continuing scholarly discourse on risk and risk management within the context of higher education institutions by reporting on a qualitative assessment of the appropriateness of the risk management framework of a selected open distance learning institution. The assessment is based on a single instrumental case study of an open distance learning institution. The assessment was undertaken by conducting a qualitative content analysis of the institution's enterprise risk management framework document. In paper **A Framework for Risk Management Practices and Organizational Performance in Higher Education,** we analysed a framework of risk management practices and organizational performance in the

Malaysia's public universities was established. this framework is expected to produce a risk management practices that will stimulates innovative idea of managing risk in higher education, specifically in the autonomous public universities setting, and offers transformative research idea in the area of risk management for non-profit organizations. The case study **The Case – HETS by Jelena Dakic**, the Higher Education Technical School of Professional Studies in Novi Sad (HETS) created a team of experts consisting of teachers from different vocations. The school created a document about the risk assessment in the OHS area from hundreds of companies. Risk management in the workplace, and in the work environment in relation to people's health and safety was considered by all of the companies. The companies varied, as well as the workplaces and environments, so various vocational education teachers were involved. By observing and analysing work conditions in various companies, the teachers obtained experience and routine in their risk assessment for certain workplaces. They gained a deeper understanding and greater confidence in decision-making

3.2 STATEMENT OF PROBLEM

Academic institutions need to minimize the risk associated with the processes and stakeholders. Risk management is necessary for business institutions as well as academic institutions to manage the risks.

3.3 OBJECTIVES

- To review the risks associated with an academic institution.
- To implement ISO 31000:2018 in XYZ University.
- To identify and understand risk management.
- To analyse the framework and processes of Risk Management using ISO 31000:2018.
- To find out the practices need to follow to manage the risks in an academic institution.

3.4 HYPOTHESIS

Academic institute can reduce unfavourable events by Risk Management using ISO 31000:2018.

3.5 RESEARCH QUESTIONS

- What are the risks associated with XYZ University?
- How can ISO 31000:2018 be used for managing risk in XYZ University?
- What are the framework and processes of ISO 31000:2018 used in risk management?
- How to implement ISO 31000:2018 in an academic institution?
- What is the process of risk assessment and risk treatment in Iso 31000:2018?

3.6 RESEARCH METHODLOGY

The research methodology adopted for this paper is Doctrinal.

4. SCOPE

The XYZ University has some assets and the critical assets that need to be protected. Keeping in mind the needs and expectations of the students, professors and employees, the scope of ISO 31000:2018 in XYZ University is to develop rules and policies for information security to protect informational assets. The Risk management standard takes into consideration the context of the university, the roles, responsibilities, authorities and accountability of the stakeholders. Apart from design, the standard also takes in account the implementation of risk assessment, risk treatment plans, monitoring and continuous improvement in the university.

5. TERMS AND DEFINITIONS

For implementing ISO 31000:2018 in an academic institution, we need to understand some terms and definitions. Some of the terminologies that are required to understand are as follows:

1. **Risk**: Risk is the effect of uncertainty on objectives. Risk is usually expressed in terms of risk sources[1], potential events[2], their consequences[3] and their likelihood.
2. **Risk Management**: Risk management is the set of activities to direct and control an organization with regard to risk. Risk Assessment and Risk Evaluation will together constitute to risk management.
3. **Stakeholder**: Stakeholders are the individuals or organizations or any interested parties that can be affected by the decision or activity of an organization. The term "interested party" can be used as an alternative to "stakeholder".
4. **Impact**: Uncertainty of something will lead to impact.
5. **Likelihood**: Likelihood is change of something happening whether defined, measured or determined subjectively or objectively.
6. **Asset**: Any resource can be an asset depending upon its value to the organization/ individual. It may vary from individual to individual.
7. **Confidentiality**: It means only the authorized user should access the information unauthorized user should not access the information.
8. Integrity: Integrity is the proof of originality of the information that should be preserved and only authorized user can do the modifications.
9. **Availability**: It means Information should be available whenever it is required to the authorized user.
10. **Risk Assessment**: Risk identification[4], risk analysis and risk evaluation will together constitute risk assessment.
11. **Risk Evaluation**: Depending upon the value of likelihood and its impact the priority is set if it is to be treated or tolerated.

[1] Risk source is the element which alone or in combination has the potential to give rise to risk.
[2] Potential events are the occurrence or change of a particular set of circumstances. An event can have one or more occurrences and can have several causes and several consequences. An event can also be something that is expected which does not happen, or something that is not expected which does happen. An event can be a risk source.
[3] Consequence is an outcome of an event affecting objectives. A consequence can be certain or uncertain and can have positive or negative direct or indirect effects on objectives. Consequences can be expressed qualitatively or quantitatively. Any consequence can escalate through cascading and cumulative effects.
4 Process of finding and recognizing risk.

12. **Risk Treatment**: Risk Treatment is the process of selecting and implementing of measures to modify risk. Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.
13. **Monitoring and Review**: It refers to continually monitoring and checking if any changes takes place and also understanding the effectiveness of the subject matter.

6. PRINCIPLES

The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives. The risk management processes and procedures are designed on the basis of following principles:

1. Risk management is an integral part of all organizational activities.
2. A structured and comprehensive approach to risk management contributes to consistent and comparable results.
3. The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.
4. Involvement of stakeholders enables their knowledge, views and perceptions to be considered.
5. Risks can emerge, change or disappear as an organization's external and internal context changes.
6. Information should be timely, clear and available to relevant stakeholders.
7. Human behaviour and culture significantly influence all aspects of risk management at each level and stage.
8. Risk management is continually improved through learning and experience.

7. FRAMEWORK

7.1 GENERAL

The risk management framework helps the organization to integrate all the risk management related activities and processes. At all levels of organization use these processes for accountability and effective decision making. The aim of the framework is to achieve the objective of the organization with the help of stakeholders especially top management.

7.2 LEADERSHIP AND COMMITMENT

In XYZ University, Top management includes the following:

1. Chancellor
2. Vice Chancellor
3. Director
4. Registrar

The top management should ensure the risk management framework should be integrated in all the activities of the institution. They also describe the leadership and commitment by implementing the framework in the activities and components. Top management should issue the policy or statement regarding the establishment of risk management in the institute. The management plays a critical role in decision making strategic and rigorous planning. The head of the department can draft what is necessary and policy is designed to ensure organization

culture and align with the objectives. The legal and regulatory compliance[5] are drafted with the strategies of the organization and keeping in mind the risk management objective. The policies that are predefined in an institution should not conflict and should be compatible with each other. The security policies that are internally defined by the institution shall be compatible with the policies under ISO: 31000. Integration of the institutional process with the ISO: 31000 policies is required. It is necessary that the intention behind implementing the standard shall be achieved by assigning the authorities and accountabilities at all the levels of the institution.

7.3 INTEGRATION

This step includes every part of the institution's structure. It relies on the understanding of the context and structure of the institution. The governance guides everyone in the institution about the course of institute, the internal and external relationships, processes, rules and responsibilities to achieve the objective of the institution. The management people then make sure the directions of the governance should flow with all the processes within the institution at all levels. It is not a one-time process, it requires continuous improvement according to the circumstances and need of the institutions and its stakeholders.

7.4 DESIGN

7.4.1 UNDERSTANDING THE ORGANIZATION AND ITS CONTEXT

The XYZ University first need to understand and examine its internal and external context in the process of designing the risk management process.

The internal context of the XYZ University includes the following:

1. Chancellor
2. Vice Chancellor
3. Director
4. Registrar
5. Assistant Registrar
6. Dean Postgraduate (PG)
7. Dean Undergraduate (UG)
8. Head of Department (HOD)
9. Faculties
10. Employees
11. Students

Chancellor, Vice Chancellor, Director and Registrar are the top management. Assistant Registrar, Dean PG, Dean UG, HOD and Faculties are the middle level management. At the lowest level of the institution Employees that can be Librarian, Laboratory In charge, Account Manager, Clerks and Security Guards and Students are the fine line management in the XYZ University.

[5] Regulatory compliance is making sure that an organization is following the rules and standards set for its industry. These rules are usually set by government legislation or by proxy via government agencies. Regulatory compliance has to do with a set of guidelines that an organization is required to follow in accordance with the law. A compliance definition in hiring practices, advertising, accounting, benefits, workplace environment and safety, discipline, and termination Available at https://elearning.scranton.edu/resource/business-leadership/definition-on-regulatory-compliance accessed on 14-06-2020.

The external context of the XYZ University includes the following:

1. Government
2. University Grants Commission (UGC)
3. Ministry of Human Resource Development (MHRD)

Policies of the XYZ University are:

1. Examination Policy: It directs the method of examination would be followed by the university.
2. Asset Management Policy: It provides both an overview of how Asset Management[6] operates in order to maintain accurate inventory records and describes the role of University departments in this process.
3. Information Security Policy: It elaborates the security policies and the procedures that have to be followed in the University. It should be reviewed and updated periodically.
4. Backup Policy: It makes sure that all the critical and important data is backed up regularly by the institution. In case of any disaster or ransomware attack, data could be recovered from the back up files.
5. User Access Management Policy: It ensures the access should be given according to their role.
6. Password Management Policy: It mention the password setting criteria for everyone to use the University portals and other online services.
7. Change Management Policy: It describes how to deal with the changes in the process.
8. Student Policy: It provides the guidelines to for the student. This policy is made for the university students.
9. Physical Security Policy: It provides how physical security will be maintained inside the university.

7.4.2 ARTICULATING RISK MANAGEMENT COMMITMENT

The top management should demonstrate and articulate their continual commitment to risk management through a policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management. Their risk management commitment are as following:

1. Institution's purpose for managing risk.
2. Policies and objectives of the university.
3. Necessary resources.
4. Performance indicator of the institution.
5. Authorities, responsibilities and accountabilities
6. Top management decisions and implementation processes.

[6] Asset management is the process of developing, operating, maintaining, and selling assets in a cost-effective manner. Asset management encompasses the identification and management of risks that arise from the utilization and ownership of certain assets. This means that a firm will always be prepared to counter any risk that comes its way. Available at https://corporatefinanceinstitute.com/resources/knowledge/finance/asset-management/ accessed on 15-06-2020.

7.4.3 ASSISGNING ORGANIZATIONAL ROLES, AUTHORITIES, RESPONSIBILITIES AND ACCOUNTABILITIES

A proper committee and managers are set which manage and maintain the risk management process and ensure adequacy, effectiveness and efficiency. The roles, responsibilities and accountabilities in the institution are as follows:

1. Asset owner: The person accountable for the information asset he is using, if any incident occurs.
2. Risk Manager: responsible for drafting and developing the risk management policies and updating it whenever any changes takes place.
3. System Manager: Accountable for managing the risk associated with the computer systems, laptops.
4. Network Administrator: Responsible for managing the risks associated with the network devices in the university.
5. Information Officer: The information officer is responsible for who can access the information, ensuring that the risk assessments are performed, and all the controls[7] are in place.
6. Institute Management: Managers are responsible for managing the roles assigned and are also responsible to address any changes that occur.
7. Unit Manager: responsible for addressing the changes if any.
8. Process Administrator: responsible for monitoring and reviewing the processes on a regular basis, also keep the record of documents.

7.4.4 ALLOCATING RESOURCES

Appropriate resources are allocated by the top management for risk management in the university. Some of the resources that are required for the Institution are:

1. People
2. Professional training
3. Skills
4. Tools
5. Methods and processes to manage risk

7.4.5 ESTABLISHING COMMUNICATION AND CONSULTATION

The things associated with the risk management that has been designed for internal and external stakeholders within the institution, needs to be properly communicated and consulted at regular intervals of time. It can be communicated via emails or via notices whenever there is any new policy, or any changes take place. Proper communication in respect to stakeholders for effective exchange of information is necessary. Feedback and reporting with proper communication and consultation.

[7] Information security controls are measures taken to reduce information security risks such as information systems breaches, data theft, and unauthorized changes to digital information or systems. These security controls are intended to help protect the availability, confidentiality, and integrity of data and networks, and are typically implemented after an information security risk assessment.
Types of information security controls include security policies, procedures, plans, devices and software intended to strengthen cybersecurity. Available at https://reciprocitylabs.com/resources/what-are-information-security-controls/ Accessed on 11-06-2020.

7.5 IMPLEMENTATION

The framework is designed to apply risk management policy complying with the organizational processes and legal, regulatory requirements. Communication with internal and external stakeholders is required and timely sessions of training can be given to them. Various objectives that the organization needs to meet at different levels is mitigated while implementing the risk management processes.

7.6 EVALUATION

Periodical review is necessary and the risk management plans also needs to be reviewed, analysed and evaluated by the Process Administrator on a regular basis. This improves the effectiveness of the standard.

7.7 IMPROVEMENT

7.7.1 ADAPTING

Continual monitoring is needed to address the external and internal chances and to adapt the risk management framework.

7.7.2 CONTINUALLY IMPROVING

There are several technologies coming up every day with different threats associated with them thus the plan after being reviewed, steps for risks being mitigated is also to be understood.

8. PROCESS

8.1 GENERAL

The risk management process forms an integral part of the organization which is a systematic approach and embedded with the culture, activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk and practices followed by the institution.

8.2 COMMUNICATION AND CONSULTATION

For communicating with the external and internal stakeholders a Communication committee has been made which is responsible for properly communicating and consulting with internal and external stakeholders at regular intervals of time. This team so made will ensure the interests of internal and external stakeholders. Taking into account the interest of the stakeholders, each of the interested parties need their information or data to be secured. Privacy of data is expected regarding any information stored on or transmitted through Institute's information systems which can be monitored, accessed, inspected or disclosed at any time and without any prior notice. It is also important to identify how relevant their demands are. Therefore, for protecting their information the risks associated to it should be mitigated.

8.3 SCOPE, CONTEXT AND CRITERIA

8.3.1 GENERAL

The primary objective is to customize the risk management process, enabling effective risk assessment and appropriate risk treatment. It includes the scope of the processes and

understanding the internal and external context to deliver information services and meet the demands of stakeholders.

8.3.2 DEFINING THE SCOPE

The scope within the institution where risk management process has to be carried is identified and also the objectives of the institution behind implementing the standard is determined. The scope of the risk management is the complete educational institute including Classrooms, Library, Account Section, Examination Section, Labs, Administration section. The objectives should be updated as required.

Some of the objectives of the Institute for implementing the standard are as follows:

1. To achieve and hold appropriate protection of the institution assets.
2. To monitor if any incident takes place and how to address that incident.
3. Institution should not face any loss of information or data for example students profiles which may contain personal data like their phone numbers, address, etc.
4. The information that the institution holds should be safe and secure.
5. Backups[8] should be maintained of the records or any other information important to the organization.
6. Transmission of the information should be done in secure mode.
7. Maintain the CIA (confidentiality, integrity and availability) of information.
8. To secure the accessing or processing of students profiles.

8.3.3 EXTERNAL AND INTERNAL CONTEXT

The internal environment to the organization comes under this. The internal stakeholders include Chancellor, Vice Chancellor, Director, Registrar, Assistant Registrar, Dean PG, Dean UG, HOD, Faculties, Employees, Students and all the assets that are associated within the frame of the institution. The external environment to the organization is understood under this. The external stakeholders include- UGC Guidelines, MHRD Guidelines, policies that are outside the institution.

8.3.4 DEFINING RISK CRITERIA

Risk Acceptance Criteria is defined as-

RISK (L*I)	RANGE	CRITERIA
Likelihood*Impact	1 to 3	LOW
Likelihood*Impact	4 to 6	MEDIUM
Likelihood*Impact	7 to 9	HIGH

[8] The main purpose is to recover the lost data from an unpredictable event like deletion by mistake or file corruption which in many cases is caused by a virus. An example is **Ransomware**, which encrypts all your data when your computer gets infected and the second is to roll back the data at a specific time you want. This is a scenario that happens often in companies which have applications and databases and they want to test their applications with a specific version of data. Available at https://www.tutorialspoint.com/computer_security/computer_security_data_backup.htm Accessed on 12-06-2020.

8.4 **RISK ASSESSMENT**

8.4.1 GENERAL

The process of risk identification, risk analysis and risk evaluation are the part of risk assessment. It should be conducted systematically and iteratively with the use of best available information.

8.4.2 RISK IDENTIFICATION

For the asset present in the organization the risk is identified in the first step. The aim of identification is to generate a study of the risk and identified source is determined. Considering the values as: **High = 3, Medium = 2 and Low = 1**.

8.4.3 RISK ANALYSIS

Risk Analysis – After the risk identification the risk is analyzed in two ways –

1. Quantitative – Can be analyzed depending on the numbers and figures.
2. Qualitative – Can be analyzed depending upon the surveys

Risk Evaluation will be dependent upon **Likelihood * Impact**.

8.4.4 RISK EVALUATION

Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine where additional action is required. The risk is identified depending upon the different levels such as high, medium or low so that they can be treated depending upon it in the risk treatment phase. Risk evaluation can be defines by the below diagram:

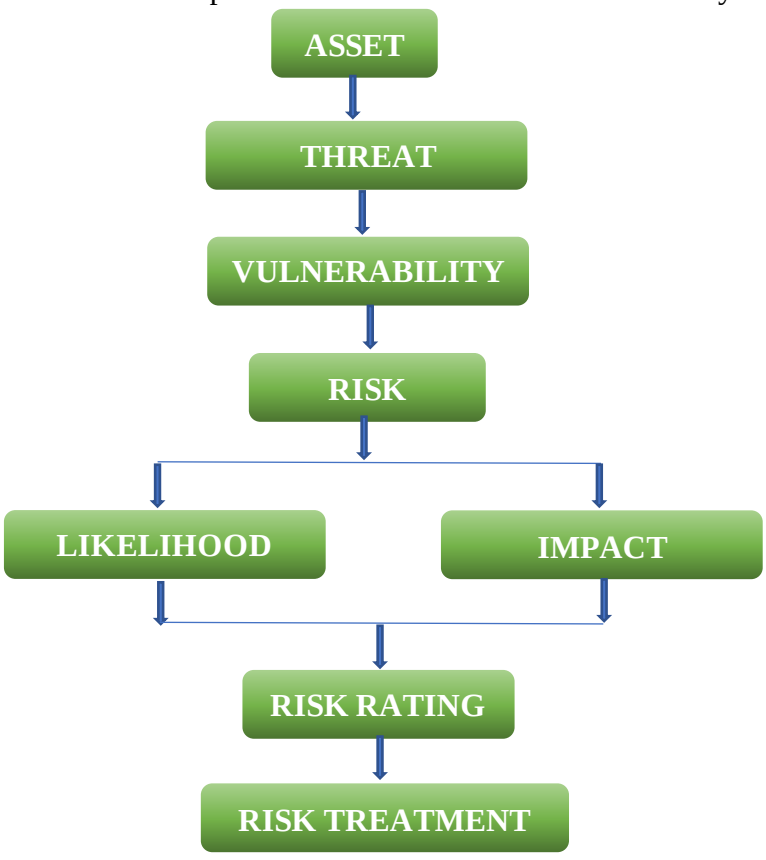

FIGURE 1: PROCESS FLOW OF RISK MANAGEMENT

8.5 RISK TREATMENT

The risks should be treated depending upon the risk levels decided in the risk evaluation phase. The priority should be set for their treatment. It involves balancing the potential benefits derived in relation to the achievement of the objectives against costs, effort or disadvantages of implementation. The selection of risk treatment options should be made in accordance with the organization's objectives, risk criteria and available resources.

8.6 MONITORING AND REVIEW

Monitoring and review must be clearly defined and once the treatment plan after analysis has been laid down monitoring must be done that whether the risk management plan that has been implemented is working properly or not.

8.7 RECORDING THE RISK MANAGEMENT PROCESS

The records provide the foundation for improvement in methods and tools as well as in the overall process.

Risk Assessment Sheet of XYZ University											
S. No.	ASSET NAME	CLASSIFICATION	CONFIDENTIALITY	INTEGRITY	AVAILABILITY	CIA Rating(C*I*A)	RISK IDENTIFICATION	LIKELIHOOD	IMPACT	RISK RATING	RISK TREATMENT
1	Desktops	Restricted	High	High	High	27	Damage, Data Theft, Hardware Theft, Loss of information, Financial Loss	High	High	9	Password,backup,firewall,Anti virus
2	Database	Critical	High	High	High	27	Loss of Information, Legal implication, Loss of reputation	High	High	9	Access control, Log managemnt, DLP
3	Policies	Public	Medium	Medium	High	12	Misuse of policies, Unauthorize access	Medium	High	6	Only Authories and governance can edit
4	Employees	Limited	High	High	High	27	Loss of education, loss of information, Loss of institution's objective,Loss of growth	High	High	9	Proper training, Backup resource, Background check, Contract and NDA, Awareness
5	Students	Limited	High	High	High	27	Loss of data, loss of reputation, loss of trust	High	High	9	Document verification, Proper classes, Awareness, Physical security
6	Personal Laptop	Limited	High	High	High	27	Damage, Data Theft, Hardware Theft, Loss of information, Financial Loss	High	High	9	Password,backup,firewall,Anti virus
7	Exam Papers	Critical	High	High	High	27	Loss of reputation, Unauthorize access	High	High	9	Physical security, access control
8	Modem	Restricted	High	High	High	27	Cyber attack, loss of information, Damage, physical theft	Medium	Medium	4	Repair, Physical Security, AntiVirus
9	Air Conditioner	Public	Low	Low	Medium	3	Damage,Physical theft,Fault, loss of property, work loss	Low	Low	1	Stablizers, Physical Security, Repair
10	Projector	Public	Low	Low	Medium	3	Damage,Physical theft,Fault, loss of property	Medium	Medium	4	Physical security,backup projector,alternatives
11	Router	Restricted	High	High	High	27	Cyber attack, loss of information, Damage, physical theft	High	High	9	Proper configuration, firewall,maintainance,physical security

Figure 2: Risk Assessment Sheet of XYZ University

9. CONCLUSION

Major risks like security breaches are one of the issues in today's world and hazardous to the organizations including Academic Institutions. They are spending hundreds of thousands of rupees every year for making their information secure and reducing the risk associated with the assets. The awareness is very important factor as if the institutions will be aware that they can reduce the risk by implementing the standard. The risk management plan undertaken by ISO 31000:2018 has been studied for XYZ University. Each risk that has been detected in the process needs to properly analysed and evaluated and hence proper treatment according with the Risk Management policy needs to be implemented. The top management plays a key role and the actions and policies they lay down are an integral part.

10. REFERENCES

1. A. Ahmad, N. Ishak and K. Ismail, "A Framework for Risk Management Practices and Organizational Performance in Higher Education", Available at

http://sibresearch.org/uploads/2/7/9/9/2799227/riber_b14-179_422-432.pdf Accessed on 08-06-2020.
2. A.Olechowski and J. Oehmen, "The professionalization of risk management: What role can the ISO 31000 risk management principles play?", Available at https://www.sciencedirect.com/science/article/abs/pii/S0263786316300631#! Accessed on 09-06-2020.
3. A. Lundquist, "Enterprise Risk Management (ERM) at U.S. Colleges and Universities: Administration Processes Regarding the Adoption, Implementation, and Integration of ERM", Available at https://scholarworks.wmich.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2183&context=dissertations Accessed on 07-06-2020.
4. A. Mas and B. Barafort, "ISO 31000-based integrated risk management process assessment model for IT organizations", Available at https://onlinelibrary.wiley.com/doi/epdf/10.1002/smr.1984 Accessed on 10-06-2020.
5. C. Lalonde and O. Boiral, "Managing risks through ISO 31000: A critical analysis" Available at https://www.researchgate.net/publication/270852873_Managing_risks_through_ISO_31000_A_critical_analysis Accessed on 12-06-2020.
6. D. Govender, "The use of the risk management model ISO 31000:2018", Available at https://link.springer.com/article/10.1057/s41284-018-0158-x Accessed on 09-06-2020.
7. E. Sadler and J. Wessels, "Risk management in higher education: An open distance learning perspective", Available at https://www.researchgate.net/publication/283256328_Risk_management_in_higher_education_An_open_distance_learning_perspective Accessed on 15-06-2020.
8. I. Akkiyat and N. Souissi, "Modelling Risk Management Process According to ISO Standard", Available at https://www.ijrte.org/wp-content/uploads/papers/v8i2/B3751078219.pdf Accessed on 16-06-2020.
9. J. Dakic, "The risk management in higher education institutions", Available at http://www.iiakm.org/ojakm/articles/2014/volume2_1/OJAKM_Volume2_1pp137-152.pdf Accessed on 15-06-2020.
10. T. Aven and M. Ylönenb, "The strong power of standards in the safety and risk fields: A threat to proper developments of these fields?", Available at https://www.sciencedirect.com/science/article/pii/S0951832018312250 Accessed on 21-06-2020.
11. U. Nugraha, "Implementation of ISO 31000 for Information Technology Risk Management in the Government Environment", Available at http://sersc.org/journals/index.php/IJAST/article/view/384 Accessed on 25-06-2020.
12. ISO 31000:2018 Risk Management Standard, Available at https://www.iso.org/standard/65694.html#:~:text=ISO%2031000%3A2018%20provides%20guidelines,any%20organization%20and%20its%20context.&text=ISO%2031000%3A2018%20can%20be,decision%2Dmaking%20at%20all%20levels.Accessed on 04-06-2020.