PROCEEDINGS OF THE 1st STEEEM 2019
Volume 1, Number 1, 2019, pp. 341-352
Universitas Ahmad Dahlan, Yogyakarta-Indonesia, December 30, 2019

Risk Management in Data Centers Using ISO 31000 Case Study: XYZ Agency

Asep Syihabuddin[1], Yohan Suryanto[2], Muhammad Salman[3]

[1,2.3]University of Indonesia

E-mail: [1]asep.syihabuddin@ui.ac.id, [2]yohan.suryanto@ui.ac.id, [3]muhammad.salman@ui.ac.id

Abstract. Data Center as the operational center of the entire application system and central data communication network system is required to fulfill all operational Information & Communication Technology (ICT) activities. The increase in the number of applications and ICT services at XYZ agency is causing problems at the existing Data Center. One of the problems is the emergence of disruptions/incidents of ICT applications and services. Recurring incidents cause problems that often require a long turnaround time and comprehensive root cause analysis (RCA) so that these incidents do not recur. With the existing problems in the Data Center, the XYZ agency will undertake a Data Center development project in which there are prerequisites for overcoming existing problems. In this Data Center development project activity, the risk management stage is needed as a process to identify the risks to be faced, risk control, and strategies for the existing risk mitigation process. ISO 31000: 2018 is used in the preparation of risk management in this Data Center.

1. Introduction

The development of information technology makes information the most valuable asset. Currently, private and government agencies are very dependent on information technology (IT) to achieve their business goals. IT is also used to drive the main and supporting business processes of the agency.

XYZ Agency is one of the government institutions that utilize information technology in fulfilling its duties as mandated by the law. Data processing and presentation of information is crucial for the XYZ agency. Due to the need for speed and accuracy in decision making, where data and information are presented in applications and other ICT services, the Data Center's role is vital. XYZ agency's commitment to the use of information technology is evidenced by the existence of the central infrastructure, the Data Center.

Considered as one of the most vital institutions in Indonesia, XYZ agency is well aware that the Data Center, which is the heart of ICT applications and services, has a vital role in protecting data and information. Without neglecting the integrity and confidentiality aspect, availability becomes a challenge in managing a Data Center.

In recent years there has been a significant increase in the number of ICT applications and services. This positively will affect Data Center management. Poor management will result in suboptimal information technology services. One of the applications of governance in managing the data center is to implement risk management. Risk management is one of the essential elements in measuring Data Center readiness to face all possibilities for failing information technology services.

For the data center operations to run as expected, a comprehensive risk assessment consisting of risk identification, risk analysis, and risk evaluation following the ISO 31000: 2018 framework on risk

management is needed. Risk assessment is expected to support Data Center readiness in dealing with various possible events or incidents failing information technology services.

2. Theoretical Basis

2.1 Data Center

A data center is a place that is used to place servers, storage, and other components related to data and information communication. These facilities usually include backup power supplies, data communication connections, environmental controls, fire prevention, and physical security devices [1]. Fig.1. shows the data center layout.

Fig. 1. Data Center Layout

In the construction of the data center, some aspects of philosophy should be considered carefully. These aspects include data center design that should be simple (simplicity), has a relative size (scalability), modular (modularity), and flexible (flexibility) and able to support the needs of long-term use so that workspace is required to be comfortable and safe (sanity) [2].

Following the TIA-942 standard, there are five essential processes required to build a data center, including site selection, evaluation of building infrastructure, room design, equipment management, and labeling [3]. Fig.2 shows the TIA-942 data center topology standard.

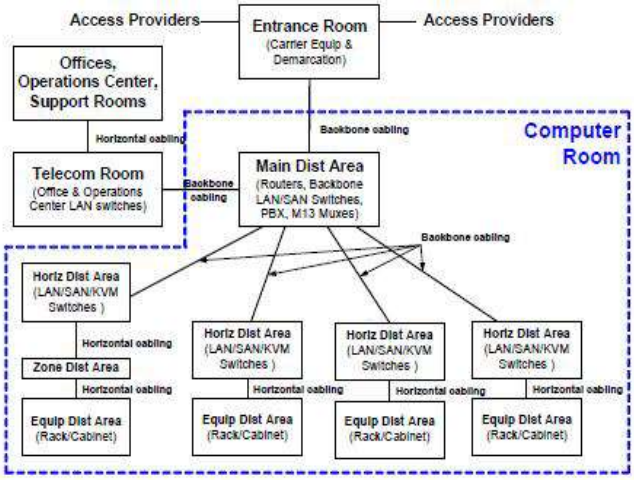

Fig. 2. TIA-942 Datacenter Topology Standard

2.2 Data Center Design

Other things to consider in building an ideal data center are as follows:

1. Requirements of network and telecommunications, power, and cooling equipment for the data center must be made at the maximum possible capacity. Besides, in designing a data center, possible additional needs that may occur with the appropriate ratio also need to be anticipated. In

this case, company policy can be integrated with the growing needs mentioned in the standard [4];
2. Determine the room requirements for each need in point 1;
3. Estimating aspects related to the primary needs in points 1 and 2, such as the safety of each device, grounding in the electrical system, electrical protection, and other facility requirements based on the architect and engineer. Provides the need for an operational center, loading dock, storage space, staging area, and other supporting areas [4];
4. The detailed process of data center design appears on the outset to be a purely mechanical process involving the layout of the area, computations to determine equipment capacities, and innumerable other engineering details. They are, of course, essential to the design and creation of a data center, however, the mechanics alone do not a data center make. The use of pure mechanics rarely creates anything that is useful, except perhaps by chance [5].

Based on these things, a guideline in designing the data center can be made in the form of the flow chart as follows. The a activity flow diagram in data center infrastructure design shows in Fig.3.

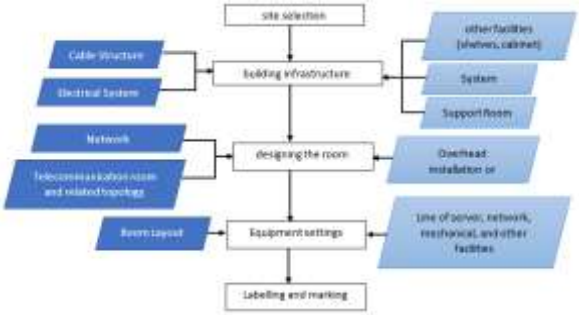

Fig. 3. Activity Flow Diagram in Data Center Infrastructure Design

2.3 Risk Management

2.3.1 Definition of Risk Management

According to ISO 31000: 2018 Risk management is a coordinated activity to direct and control an organization concerning risk [6].

Risk Management is a systematic approach to set the best actions under uncertainty by identifying, assessing, understanding, acting, and communicating on risk issues [7]. U.S. The Government Accountability Office (GAO) suggests that Risk Management is a continuous process of assessing risk, reducing that potential adverse activities will occur, and putting appropriate control to handle any events that do not occur. Risk management involves a continuous process of implementation - through a series of mitigation actions that absorb entity activities - the possibility of side effects and their negative impacts. Risk management shows risks before the organization carries out mitigation actions, such as residual risks, as well as after countermeasures have been taken [8].

2.3.2 ISO 31000:2018 Risk Management Framework

The risk management framework is a set of components that provides the basis and organizational arrangements for designing, implementing, monitoring, reviewing, and continuously improving risk management throughout the organization. The risk management framework is embedded in the overall strategic and operational policies and practices of the organization [9].

The risk management framework, according to ISO 31000:2018, is shown in the following Fig. 4.

Fig. 4. ISO 31000:2018 Risk Management Framework

Top management and oversight bodies, where applicable, should ensure that risk management is integrated into all organizational activities and should demonstrate leadership and commitment [6].

Integrating risk management relies on an understanding of organizational structures and context. Structures differ depending on the organization's purpose, goals, and complexity. Risk is managed in every part of the organization's structure. Everyone in an organization has the responsibility for managing risk [6]. When designing the framework for managing risk, the organization should [6]:

1. examine and understand its external and internal context,
2. demonstrate and articulate their continual commitment to risk management through policy, a statement or other forms that clearly convey an organization's objectives and commitment to risk management,
3. ensure that the authorities, responsibilities, and accountabilities for relevant roles concerning risk management are assigned and communicated at all levels of the organization.
4. ensure allocation of appropriate resources for risk management
5. establish an approved approach to communication and consultation in order to support the framework and facilitate the practical application of risk management.

Successful implementation of the framework requires the engagement and awareness of stakeholders in order to evaluate the effectiveness of the risk management framework [6].

The organization should continually monitor and adapt to the risk management framework to address external and internal changes. In doing so, the organization can improve its value. The organization should continually improve the suitability, adequacy, and effectiveness of the risk management framework and the way the risk management process is integrated [6].

2.3.3 Risk Management Process Based on ISO 31000:2018

The risk management process involves the systematic application of policies, procedures, and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording, and reporting risk. This process is illustrated in Figure 5 [6].

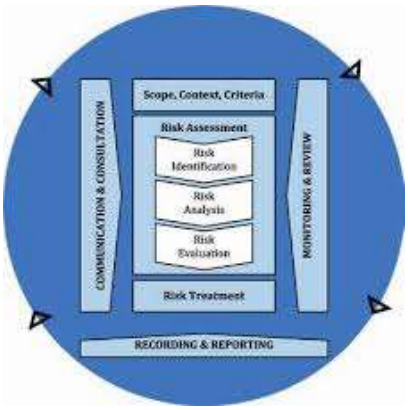

Fig. 5. Risk Management Process Based on ISO 31000:2018

The risk management process should be an integral part of management and decision-making and integrated into the structure, operations, and processes of the organization. It can be applied at strategic, operational, program, or project levels.

3. Research Methodology

The research methodology used in writing this paper is to conduct a literature study in the form of journals, white papers, reports, and writings related to risk management theory and experience in carrying out data center risk assessments.

From the collected information, an analysis is then carried out to make a risk analysis that pays attention to aspects of risk management. Moreover, doing interviews (The source used in the study were determined based on purposive sampling technique) [10], with the relevant person to collect data.

4. Discussion

4.1 Scope, Context & Criteria

The XYZ agency has guidelines for carrying out risk management as set out in the risk & control self-assessment (RCSA) guidelines. The guide is intended to facilitate the implementation of risk identification, monitoring, and summarizing risks, especially when reporting risks to the relevant Management [11].

Risk and Control Self Assessment (RCSA), is a tool/tool for risk management to identify and measure risks that are qualitative and predictive using the dimensions of impact (impact) and likelihood, by taking into account the controls/controls applied [11].

For that reason, the risk management process at the Data Center is scope & conducted following the RCSA guidelines. According to the RSCA, Risks are categorized into seven, namely: Reputation, Strategic, Operational, HR, Law, Integrity, and Security [12].

For the Context of Risk in the Data Center, we are focus on 2 (two) categories are Operational & Security. According to RCSA, risk criteria are a reference used in assigning likelihood and impact scores in measuring risk levels. Risk Rating / Level of Risk is obtained from the multiplication of likelihood and impact. The following are the risk criteria used as a reference in measuring risk [12]. Tha likelihood can shows in Table 1.

TABLE 1
LIKELIHOOD

Level	Description	Likelihood (Routine)	Likelihood (Non-Routine)
Rare (1)	Rarely happens	<50%	Max Occurs once in 2 years
Unlikely (2)	Could / May Happen	5% - <20%	Max Occurs once a year
Moderate (3)	Rarely happens	20% - <50%	Max Occurs once in 6 months
Likely (4)	Often happens	50% - 80%	Max Occurs once in 3 months
Almost Certain(5)	Almost certainly always happens	80% - <100%	Occurs more than three times a month

Annotation:
Routine or non-routine saw based on the event. Routine means that the risk event is related to daily operational issues. Non-routine means that the risk event is not related to daily operational issues, such as natural disasters.Tha impact can shows in Table 2.

TABLE 2
IMPACT

Risk Category	Parameter/Attribute	Negligible (1)	Small (2)	Impact Moderate (3)	High (4)	Disaster (5)
Operational	Efficiency/ Effectivity	Decreased ability to achieve goals or individual work results	Decreased ability to achieve goals or work units / team / group / unit / section work results	Decreased ability to achieve the objectives or main work results of the Directorate / Bureau	Decreased ability to achieve the objectives or main work results of the Deputy / Secretary-General	Decreased ability to achieve the objectives or main work results of the organization
	Disruption of service	The activity stopped for <2 hours	Activity stops 2-4 hours	Activity stops >4 hours - 1 day	Activity stops for 1-3 days	The activity stopped for >3 days
	The performance	Failure to achieve one or more of the main results of individual work	Failure to achieve one or more main work results in Task unit/team/group/ unit/ section	Failure to achieve one or more of the main work results of the Directorate / Bureau	Failure to achieve one or more of the main works of the deputy/secretary-general	Failure to achieve one or more of the organization's primary work results in causing a significant impact on stakeholders
Security	Information	There is no information leak	There is a leak of sensitive information to unauthorized internal parties	Leakage of confidential information to unauthorized internal parties	There is a leak of sensitive information to external parties	There is a leak of confidential information to external parties

	Physical Asset	-	-	-	Assets are lost or damaged but do not interfere with the work unit or organization's activities	Lost or damaged assets that can disrupt the activities of work units or organizations

4.2 Risk Assessment

Risk assessment allows managers to prioritize risks by following perceived seriousness or other criteria set. In the risk assessment process, there are several activities, including identification, analysis, and evaluation [13].

4.2.1 Risk Identification

Risk identification includes determining the following:

1. Risk Source;
2. Risk Event;
3. Risk Cause;
4. Risk Impact.

Identification was done by looking at various factors which influence business processes, such as business profiles, applications, infrastructure, operation, and human resources. Therefore, the procedure results the list of risks which may be shown in the data center process [15]. The risk source comes from business processes related to the data center, namely the business processes of data center operational management. The top 10 (ten) list of risks that have been identified are as follows Table 3.

TABLE 3
TOP 10 LIST RISK IDENTIFICATION

Risk Number	Risk Event			Impact Category
	Description	**Risk Cause**	**Impact**	
R1	Occasional utility failures (telecommunications, electricity, PAC).	Interference in the third parties	The operation of the institution is disrupted	Operational
R2	Fire alarms on switches and routers do not work	1. The power cable is broken 2. Equipment and fire alarm sensor failure	Data Center Stopped functioning, and the institution's operations were disrupted	Operational
R3	PAC on switches and routers is broken	Damage to the Data Center room cooler	Data Center Stopped functioning, and the institution's operations were disrupted	Operational
R4	New (innovative) infrastructure is installed, and as a result, the system becomes unstable, causing operational incidents.	The new system has not been tested yet	The operation of the institution is disrupted	Operational
R5	Sensitive information is	IT Staf Negligence	Information Leakage	Security

	accidentally disclosed because it does not follow information handling guidelines. (password)			
R6	Leakage of sensitive information due to inefficient use / archiving / deletion of information.	IT staff negligence	Confidential information leakage	Security
R7	The hardware is not running correctly due to overheating.	1. The cooling system is not working correctly. 2. The wrong way to use by the user.	The operation of the institution is disrupted	Operational
R8	Destruction of the data center (sabotage or else.) by external parties	The security system is not optimal	Data Leakage	Security
R9	Malware interference on a critical operational server.	Antivirus devices are not running optimally	Institutional operational activities are not running	Operational
R10	ICT (Information & Communication Technology) infrastructure down	1. ICT hardware is damaged or has problems 2. Incomplete monitoring tools	1. Related operation is disrupted; 2. Data can not be accessed; 3. Routine activities that require resources from Directorate PINDA is interrupted; 4. Damaging credibility on public perception. 5. IT infrastructure can be damaged or lost data	Operational

4.2.2 Risk Analysis

Risk analysis considers the causes and sources of risk, the positive and negative consequences, and the possibility that consequences will occur. Factors that influence consequences and likelihood must be identified. Risks are analyzed by determining the consequences and their likelihood, as well as other risk attributes. The following are the results of a Data Center risk analysis formulated by determining the likelihood and impact of risks.

4.2.3 Risk Evaluation

Based on risk identification and analysis, the following controls have been identified in Table 4.

TABLE 4
RISK ANALYSIS & CONTROL

Risk Number	Nilai (Skor) Inherent Risk			
	Likelihood	**Impact**	**Level of Risk**	**Existing Control**
R1	20% - < 50% or Max occurs once every 6 month (3)	High (4)	12	1. Study the flowchart of new infrastructure to be installed

				2. Conduct a trial before installing the new infrastructure
R2	5% - < 20% or Max Occurs once a year (2)	Disaster (5)	10	the existence of a password input prevention mechanism. (delay when input password error)
R3	5% - < 20% or Max Occurs once a year (2)	Disaster (5)	10	1. Report directly to BAS K4 Building team 2. Perform routine maintenance of the device and peripherals.
R4	20% - < 50% or Max occurs once every 6 month (3)	Moderate (3)	9	compensation from the staff who did the damage
R5	5% - < 20% or Max Occurs once a year (2)	High (4)	8	contact a third party to make repairs
R6	5% - < 20% or Max Occurs once a year (2)	High (4)	8	increase staff awareness of the confidentiality of work-related data
R7	5% - < 20% or Max Occurs once a year (2)	High (4)	8	informs that the device is not feasible
R8	5% - < 20% or Max Occurs once a year (2)	High (4)	8	1. Assistance for each external party that arrives 2. On the Notebook, encryption has been installed
R9	5% - < 20% or Max Occurs once a year (2)	High (4)	8	1. Check antivirus regularly 2. Update and upgrade of existing antivirus systems 3. Critical servers are backed up periodically
R10	5% - < 20% or Max Occurs once a year (2)	High (4)	8	1. Make ICT infrastructure maintenance plans more comprehensive; 2. Making an ICT infrastructure monitoring and evaluation plan; 3. Develop ICT infrastructure.

The purpose of risk evaluation is a consideration used in making decisions. Decisions are made based on the results of risk analysis regarding risk control and its priorities. Control is done by determining mechanisms that can be carried out on these risks.

4.3 Risk Treatment

In terms of risk treatment, several options are chosen, including: avoid, mitigate, or accept. But,

considering the list of risks in the Data Center, the mitigate option was chosen for high risks. Following is the mitigate plan for the risks chosen at XYZ Agency Data Center for risks number R9 & R10 can shows in Table 5.

TABLE 5
Risk Mitigation

Description of Mitigation Action Plan	Description of Mitigation Action	Risk Mitigation Plan for R9 *Output/Outcome*	*Evidence*
Anti-virus & spam	Anti-virus & spam Maintenance	Anti-virus & spam monitoring document	Anti-virus & spam monitoring document
Description of Mitigation Action Plan	**Description of Mitigation Action**	**Risk Mitigation Action for R10 *Output/Outcome***	***Evidence***
1. Establishing a plan to maintain comprehensive ICT infrastructure;	1. Maintenance of ELO; 2. Network maintenance; 3. Mail Maintenance; 4. Anti-spam Maintenance; 5. Server maintenance.	ICT infrastructure Maintenance Schedule	ICT Infrastructure Maintenance Schedule (Attached)
2. Making an ICT infrastructure monitoring and evaluation plan;	1. Server monitoring	Server Monitoring Schedule	Server Monitoring Schedule (Attached)
3. ICT Infrastructure Development	Server & storage procurement	Adding or replacing servers & storage	List inventory storage server (Attached)

1.2 Monitoring & Review

Monitoring and review are conducted to see the effectiveness of the risk mitigation plan, which has been made, the progress of the mitigation measures, and how much its influence in reducing the level of risk [14]. Based on the monitoring and review of the results of the two selected risk mitigation plans, there is a decrease in the level of risk. Reducing the level of risk proves that the risk mitigation plan has been active and declared to be successful in reducing the level of risk. This can be seen from the percentage of progress of mitigation actions as follows Table 6.

TABLE 6
RISK MITIGATION PROGRESS

% of Progress Mitigation Actions	Score (Target) *Residual Risk* R9		
	Likelihood	*Impact*	*Level of Risk*
100%	1	4	4
% of Progress Mitigation Actions	Score (Target) *Residual Risk* R10		
	Likelihood	*Impact*	*Level of Risk*
100%	1	4	4

Risk management is a continuous improvement process, we design the sustainable regularly improvement mechanism, the trigger improvement mechanism based on incidents, the comprehensive security audit mechanism to detect and reform the risk management issues, to ensure the continuous improvement of data center risk management [16].

5. Conclusion

Data Center must be able to provide full support as operational centers throughout the application system and data communication network. To be able to meet the SLA, a risk management study is needed at the Data Center. The study is needed to measure how much impact each incident or problem has had on the Data Center. To then be used as a consideration in determining controls that might be applied to overcome those events or risks. Besides, several risks were assessed as having a significant impact, and thus a mitigation plan was made for these risks. Mitigation plans are made by measuring the readiness of human resources and other resources needed. Finally, monitoring and review will be carried out on the mitigation plan.

Acknowledgment

This study was supported by Human Resources Research and Development Agency Ministry of Communication and Information of the Republic of Indonesia. The authors wish to thank to all Data Centers Staff at Directorate Communication Information and Data Management, CEC RI.

REFERENCES

[1] H.C. Kusuma „ "Implementation of Virtualization Machine in the Design of Cloud Data Center", 2017
[2] Lecturer Team, Data Center Design, "Mercu Buana University Lecture Module", Center for Learning & e-learning, 2016
[3] D.S. Dewandaru, "Designing Data Center Room Design Using TIA-942 Standard (Case Study of Road and Bridge Research and Development)", 2014
[4] D.E. Yulianti, "Best Practice in Designing Data Centers", http://opencontent.org/opl.shtml. 2008.
[5] S. Rob, "Enterprise Data Center Design and Methodology", 2001
[6] ISO-31000-2018-Risk-management-Guidelines, 2018
[7] Karen, Hardy, "Managing Risk in Government: An Introduction to Enterprise Risk Management", IBM Center for The Business of Government. 2010
[8] U.S. Government Accountability Office (GAO) Report, 2005
[9] J. Susilo, Leo, "Risk Management Based on ISO 31000 for Non-Sacrifice Industries.", PPM Management, 2011.
[10] Sugiyono, "Management Research Methods." Bandung, Alfabeta, 2014
[11] Risk & Control Self Assessment (RSCA) Guidelines, enterprise risk management, CEC-RI, 2015
[12] A. Syihabuddin, "Implementation of Risk Management in the Directorate Communication Information and Data Management", essay barchelor degree, STIA LAN Jakarta, 2017

[13] M.A. Fikri, "Risk Assessment Using NIST SP 800-30 Revision 1 and ISO 27005 Combination Technique in Profit-Based Organization: Case Study of ZZZ Information System Application in ABC Agency", The Fifth Information Systems International Conference, 2019

[14] "Risk Mitigation Planning, Implementation, and Progress Monitoring", https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk-mitigation-planning-implementation-and-progress-monitoring

[15] Arini, "Data Center Risks Analysis Through The Cobit Framework 4.1", Jurnal Online Informatika, 2019.

[16] Zheng Li, "Overview of Risk Management System of Commercial Bank Data Center", International Journal of Security and Its Applications, 2019.