Journal of Information Systems and Informatics

Vol. 4, No. 4, December 2022 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

http://journal-isi.org/index.php/isi Published By DRPM-UBD

Information Technology Risk Control of University in a Work from Home Situations

Iqbal Santosa[1], Rahmat Mulyana[2]

[1]Prodi S1 Sistem Informasi, Fakultas Rekayasa Industri, Universitas Telkom, Jl. Telekomunikasi Terusan Buah Batu 40257, Bandung
[2]Department of Computer and Systems Sciences, Stockholm University, Borgarfjordsgatan 12, Kista, 16455, Sweden
Email: [1]iqbals@telkomuniversity.ac.id, [2] rahmat@dsv.su.se

Abstract

The University is one of the educational institutions affected by the COVID-19 pandemic. Most of its activities, which are academic management, human resource management, information technology services, and so on were changed into WFH (Work from Home) supported by information technology. Utilization of information technology in supporting WFH can create various risks and needs to be controlled either preventive, detective, or corrective to minimize the impact. This research will focus on planning for university information technology risk control in working from home conditions by referring to the ISO 31000:2018 standard for risk management processes, COBIT 5 Generic Risk Scenario for defining risk scenarios, and DoD Instruction 8500.2 and NIST SP 800-53 in the identification of risk controls. The resulting solution is in the form of a risk treatment plan. This solution is expected to assist universities in identifying risks related to information technology and planning controls related to the implementation of work-from-home in their environment.

Keywords: Information Technology, Risk Management, Work from Home

1. INTRODUCTION

Information Technology (IT) has become essential to various human activities. The use of IT usually poses risks that can impact the organization or company. Risk is the effect of uncertainty on objectives; an effect is a deviation from the expected —positive, negative, or both; objectives can have different aspects and categories, and can be applied at different levels [1]. Failures experienced by organizations in managing risk can be caused by a lack of understanding of the risks that occur and failure to identify appropriate risk response activities. In addition, failure to establish a risk management strategy and communicate the strategy may result in inadequate risk management. Risk management is a systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring the risk [2]. The consequences of failing to manage risk can lead to ineffective and inefficient activities, projects that are not completed on time, and strategy is not delivered.

Since the COVID-19 pandemic, many large technology companies have implemented work-from-home (WFH) policies to prevent the spread of the virus. Companies that implement WFH, such as Google, Facebook, and Twitter, set WFH permanently. They believe that the company will continue to do well with WFH. That is in line with a survey conducted by Fundera, where 86 percent of workers said that they are more productive if they work alone [3]. In these big companies and universities, most of their activities have also shifted to Work from Home (WFH) from the original Work from Office (WFO). That applies to both its main activities, namely academic management, and support activities such as human resource management and information technology services. The implementation of work-from-home activities is made possible using information technology, whether in the form of websites, cloud apps, mobile apps, remote access tools, etc.

Currently, Indonesia is hit by the Covid-19 pandemic, all levels of Indonesian society work together in handling Covid-19 from the central government level to the lowest level, namely in the family sphere. The Covid-19 outbreak has had a systemic impact on every level of society. The work sector, both formal and informal, such as education, and tourism, must work hard to adapt to the development of the Covid-19 infection. Therefore, Indonesia has adopted the employment sector policy by implementing the Work from Home (WFH) method [4]. In general, WFH means how employees work outside the office, it can be at home, at a cafe, at a villa, or anywhere it depends on the comfort of an employee when he is not in the office. WFH is usually used by employees when they are bored with the office atmosphere and want to feel a different atmosphere, more flexible and able to unify the work atmosphere and real life to increase productivity more [5]. With the WFH method, there are many risks faced by various parties, one of which is an organization or company such as data security issues, so it is advisable to send essential work data not using a regular network, disturbances in the environment around the house at work, difficulty in monitoring employees at work, etc.

During the Covid-19 pandemic, most of the activities at Telkom University, both teaching and learning activities, and organizational activities were carried out on a WFH (Work from Home) basis. That also applies to the School of Industrial and System Engineering (FRI) and the Directorate of Information Technology Center (PuTI), which mainly carry out their activities from home. Bring work activities to home can cause various risks to FRI, especially those related to the Academic Sector, Student Affairs, Finance and Human Resources (HR), and Laboratory Affairs, as well as PuTI in the Information Technology Infrastructure Section (IsTI) and Information Technology Product Development (DevTI).

Risks that occur at the School of Industrial and System Engineering (FRI), among others, are in the Academic Field. There are problems with the internet network while the exam is in progress. That causes students to be unable to take the exam, so they must take a follow-up exam. In student affairs, student data redundancies occur due to online forms which cannot detect data redundancies. In matters of Finance and Human Resources (HR), there are problems with the employee daily presence system, which cannot save data automatically, so when the internet network is in trouble or if there is a power outage, the data that has been inputted is not stored, and employees need to input it again. In laboratory matters, internet network disturbances occur during practicum activities which interfere with the practicum activities [6].

Risks that occur at the Directorate of Information Technology Center (PuTI), among others, are the Information Technology Infrastructure Section (IsTI) there are obstacles related to the Virtual Private Network (VPN), namely the VPN application has not been updated by employees so that authentication fails so it cannot do remote access to devices in the office, as well as servers can experience problems due to increased user activity. In the Information Technology Product Development Section (DevTI), there are visual and functional bugs in the iGracias application, causing delays in all user activities involving the application.

The researcher uses the risk management process method ISO 31000:2018, COBIT 5 Generic Risk Scenario, NIST SP 800-53, and DoD Instruction 8500.2. ISO 31000:2018 is a revision of ISO 31000:2009 as a risk management standard. The risk management framework aims to assist organizations in integrating risk management into significant activities or activities and functions. The framework covers the integration, design, implementation, assessment, and improvement of risk management across all organizations. The organization should evaluate its risk management practices and processes evaluate and address gaps in the framework. In addition, the organization must also adjust the components of the framework that it will run to the needs of the organization [1].

The risk approach with COBIT 5 Generic Risk Scenario is used to input IT risk analysis activities related to key business impacts. The COBIT Generic Risk Scenario consists of (a) Risk scenario categories, providing a high-level description of the scenario categories with a total of 20 categories; (b) The risk scenario component, providing details about the type of threat, actor, event, asset/resource, and timing of each scenario category; (c) type of risk, there are three types of risk including the risk of benefit/value of IT empowerment, risk of IT programs and projects, and risk of IT operations and services; and (d) Example scenarios, given one or several small examples of scenarios from each scenario category with a total of 111 examples of risk scenarios, both positive and negative risks [7].

The first control recommendation in this study uses NIST SP 800-53, which aims to determine preventive measures against information systems or organizations designed to protect confidentiality and integrity and meet various security requirements that have been determined [8]. NIST SP 800-53 can help organizations create secure information systems and more effective risk management systems. NIST SP 800-53 provides 20 control families, as shown in Table 1.

Table 1. Security and Privacy Control Families

ID	Family	ID	Family
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

The second control recommendation used by the researcher is DoD Instruction 8500.2, which aims to implement policies, assign responsibilities, and establish procedures to implement an integrated layered network and information system protection [9]. DoD Instruction 8500.2 assists in implementing Information Assurance by defining controls that are divided into eight subject areas, as shown in Table 2.

Table 2. Information Assurance Control Subject Areas

Abbreviation	Subject Area Name	Number of Controls
DC	Security Design & Configuration	31
IA	Identification and Authentication	9
EC	Enclave and Computing Environment	48
EB	Enclave Boundary Defense	8
PE	Physical and Environmental	27
PR	Personnel	7
CO	Continuity	24
VI	Vulnerability and Incident Management	3

By focusing on the problems above, it can be concluded that the risk is vulnerable to occur at Telkom University and the School of Industrial and System Engineering (FRI). Hence, it is necessary to conduct research focusing on risk analysis and process control at the School of Industrial and System Engineering

(FRI) and the Directorate of Information Technology Center (PuTI) Telkom University in the Work from Home (WFH) situation. Several studies related to IT risk management in Indonesian universities have been carried out in [10], but so far have not been associated with the context of working from home, so this is an opportunity for us to start this research.

2. METHODS

2.1. Data Collection Methods

This study uses a qualitative approach [11]. The data collection technique used in this study was the interview method. This interview method targets the Head of Academic Affairs, Head of Student Affairs, Head of Finance and Human Resources (HR), and Head of Laboratory Affairs at the School of Industrial and System Engineering (FRI) as well as the Head of Information Technology Infrastructure (IsTI) and Information Technology Product Development (DevTI) at the Directorate of Information Technology Center (PuTI).

2.2. Research Methods

This research uses a risk management process based on ISO 31000:2018 that is currently adopted by the organization. The risk management process includes several stages: risk identification, risk analysis, risk evaluation, and risk treatment (see Figure 1). The risk treatment stage would not reach the preparation and implementation of the risk management plan because these stages and so on will be carried out by the organization. The risk identification stage will be based on the Generic Risk Scenario in COBIT 5 For Risk. The risk treatment stage will be based on NIST SP 800-53 and DoD Instruction 8500 standards.

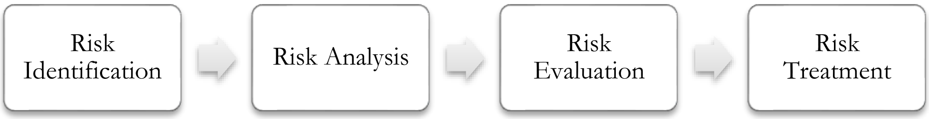

Figure 1. Research Methods

The first stage in this research is risk identification. The risk identification stage is carried out to determine the possibility of a threat risk with the impact on the company or organization [1]. Risk identification aims to identify and describe risks that can interfere with achieving its goals. Relevant, precise, and up-to-date information is essential in identifying risks. Several factors that need to be considered in identifying risks include the causes and occurrences of risks, threats and risk opportunities, the emergence of risk indicators, consequences and impacts on objectives, and tangible and intangible sources of risk.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

The second stage is risk analysis. The risk analysis process measures risk by looking at two aspects, namely the possibility of how significant the impact is and the likelihood of the risk occurring (likelihood)[1]. Risk analysis aims to understand the nature and characteristics of risk. Risk analysis involves risk sources, impacts, likelihood, scenarios, controls, and effectiveness. Risk analysis can be carried out with varying degrees of detail and complexity, depending on the purpose of the analysis, the availability and reliability of the information, and the available resources.

In measuring risk, this research uses the likelihood and impact level from the Telkom University Risk List Report [12]. There are 5 levels of possible risk or likelihood, including level 1, Highly Unlikely, level 2 Unlikely, level 3 Possible, level 4 Likely, and level 5 Very Likely. The impact is divided into five impact categories, namely operational category, compliance category, reputation category, financial category, and HR category. The impact level also has five levels of impact, including level 1 (no impact), level 2 (minor), level 3 (moderate), level 4 (major), and level 5 (extreme).

The third stage is risk evaluation. The purpose of evaluating risk is to support decisions. Risk evaluation involves comparing the risk analysis results and established risk criteria to determine the additional actions required. Based on the evaluation results, it is also determined that actions against these risks based on risk appetite/risk are acceptable with a minimum total risk of 4. These actions are determined to determine whether the related risks must be handled or not. Then the level is determined whether the risk is low (green), medium (yellow), or high (red) based on the risk matrix by looking at the level of occurrence with the total level of impact.

The last stage is risk treatment. Risk treatment aims to select and implement options for addressing risk. Risk treatment uses the results of the risk evaluation. Some risk treatments can be used to manage emerging risks, including avoiding the risk, taking the risk to pursue an opportunity, removing the risk source, changing the likelihood or consequences, sharing the risk, and retaining the risk.

3. RESULTS AND DISCUSSION

3.1. Risk Identification

The data used in this study is data obtained by researchers by conducting interviews with relevant stakeholders in FRI and the Directorate of PuTI. The following are the risk analysis results at FRI and the PuTI, as shown in Table 3. The risk codes shown are based on code from COBIT Generic Risk Scenario.

Table 3. Risk Identification

Risk Code	Risk Scenario	Threat	Risk owner
School of Industrial and System Engineering (FRI)			
1201	There is non-compliance with regulations	**T1** Students commit acts of cheating or cheating during exams	Head of Academic Affairs
0904	There is an operational interruption when the software is running	**T2** The delay in lecture activities was due to the application used to carry out the exam (LMS) down	Data Center
1602	There is a service interruption due to a DoS (Denial of Service) attack	**T3** There was a cyberattack on the server which caused the FRI website to go down	Head of Student Affairs
Directorate of Information Technology Center (PuTI)			
1601	There is an abuse of access trying to use computing devices in the office	**T4** Important files on the device can be lost or damaged	Head of IT Infrastructure
0601	The occurrence of damage to the data storage media	**T5** This causes data to be inaccessible in the data store	Head of IT Infrastructure
1901	There is an earthquake	**T6** Damage to infrastructure so that operations are hampered	Director of PuTI

3.2. Risk Analysis and Evaluation

When the risk identification process has been carried out, the next step is to carry out a risk analysis by measuring the low-high level of a risk that appears in FRI and PuTI during WFH by determining the level of risk events in Table 4.

Table 4. Risk Likelihood Score

Score	Possible Risk	Category
1	Highly Unlikely	1 event in 1 semester
2	Unlikely	>1 to 3 events in 1 semester
3	Possible	>3 to 5 events in 1 semester
4	Likely	>5 to 10 events in 1 semester
5	Very Likely	>10 events in 1 semester

Based on Table 4, the process of risk analysis that has been carried out on FRI and PuTI obtained several levels of risk impact, which are grouped into 5 levels as listed in Table 5.

Table 5. Impact Level

Impact Level	**Criteria**
No Impact	There is a small impact in the form of non-financial losses in the risk impact area, where the incident can still be handled through the applicable procedures and work processes
Minor	There is a small impact in the risk impact area where the incident can still be handled through the applicable procedures and work processes
Moderate	There is a significant impact on the risk impact area, but it can be handled through applicable procedures and work processes
Major	There is a significant and potentially systemic impact in the risk impact area that needs to be addressed quickly and appropriately
Extreme	There is a dangerous and systemic impact in the risk impact area that needs to be addressed quickly and appropriately

Based on Table 4 and Table 5, the risk analysis process is carried out using a risk matrix to help determine prioritized risk decision-making, as listed in Table 6.

Table 6. Risk Matrix

Scale	**1** **Highly Unlikely**	**2** **Unlikely**	**3** **Possible**	**4** **Likely**	**5** **Very Likely**
1 **No Impact**	Low	Low	Medium	Medium	Medium
2 **Minor**	Low	Medium	Medium	Medium	High
3 **Moderate**	Medium	Medium	Medium	High	Danger
4 **Major**	Medium	Medium	High	Danger	Danger
5 **Extreme**	Medium	High	Danger	Danger	Danger

Table 6 is used to support the risk decision-making process or risk evaluation. This process uses data from the risk analysis that has been prepared. The way to rank the risk is to multiply the likelihood score by the impact. The results of these calculations obtain the results shown in Table 7.

Table 7. Risk Analysis and Evaluation

Risk Code	**Threat**	**Likelihood**	**Impact**	**Risk Score**	**Level**
School of Industrial and System Engineering (FRI)					
1201	**T1**	3	1,6	4,8	Medium
0904	**T2**	2	1,2	2,4	Low
1602	**T3**	2	2,2	4,4	Medium
Directorate of Information Technology Center (PuTI)					

Risk Code	Threat	Likelihood	Impact	Risk Score	Level
1601	**T4**	2	2	4	Medium
0503	**T5**	2	1	2	Low
1901	**T6**	2	3	6	Medium

The risk calculation results shown in Table 7 show that there are several medium risks which are 1201, 1602, 1601, and 1901. There are also several low risks which are 0904 and 0503.

3.3. Risk Treatment

After finding the risk with the level of risk, then carry out risk treatment. In risk treatment, several treatment options are used in research, including accept, mitigate, and transfer. The treatment option is determined from the previous risk results based on risk appetite/acceptable risk, according to Table 8.

Table 8. Risk Treatment

Threat	Treatment	Control	Control Description
School of Industrial and System Engineering (FRI)			
T1 Students commit acts of cheating or cheating during exams	Accept	-	-
T2 The delay in lecture activities was due to the application used to carry out the exam (LMS) down	Transfer	**MA-1** System Maintenance Policy and Procedures	There is a need for a consistent system maintenance schedule
T3 There was a cyberattack on the server which caused the FRI website to go down	Mitigate	**SC-5** Denial of Service Protection	Various technologies exist to limit, or in some cases, eliminate the effects of a Denial of Services (DoS) attack
Directorate of Information Technology Center (PuTI)			
T4 Important files on the device can be lost or damaged	Mitigate	**ECAT-1** Audit Trail, Monitoring, Analysis and Reporting	Records from the Audit trail containing all available sources are reviewed regularly for indications of inappropriate or unusual activity
T5 This causes data to be inaccessible in the data store	Mitigate	**SI-4** Information System Monitoring	Implement a system that can automatically monitor data storage media
T6 Damage to infrastructure so that operations are	Transfer	**CODP-1** Disaster and Recovery	There is a need for planning for the possibility of a disaster and post-disaster

hampered	Planning	recovery

4. CONCLUSION

Based on the research results above, it can be concluded that the results of risk identification related to risks that occur around the FRI and the PuTI found six threats grouped into six risk scenarios. The identified risks are then analyzed and evaluated, resulting in low and medium risk levels so that the accept, mitigate, and transfer handling options are selected according to the analysis, evaluation, and validation of the relevant stakeholders. Proposed risk management is categorized based on risk control in COBIT 5 For Risk, NIST SP 800-53, and DoD Instruction 8500.

This research impacts the FRI and PuTI as risk organizers who need to pay attention to the risks that occur and the proper risk management for risk mitigation according to the level of risk that has been analyzed. The implementation of risk management generated in this research is expected to detect, prevent, and resolve all risks in FRI and the PuTI.

This study is deficient, namely the condition of COVID-19, which has not decreased, causing researchers to be slightly hampered in validating related stakeholders. In further research, it is necessary to validate all possible risks that occur and adjust to the latest risk control standards used as well as other risk standards and prepare a roadmap for the implementation of risk management.

REFERENCES

[1] *ISO 31000:2018 Risk management — Guidelines*, ISO, 2018.

[2] *ISO 13485:2016 Medical devices — Quality management systems — Requirements for regulatory purposes*, ISO, 2016.

[3] M. Shepherd. "Surprising Working From Home Statistics." https://www.fundera.com/resources/working-from-home-statistics (accessed 28 September, 2022).

[4] R. W. Tuti, "Analisis implementasi kebijakan work from home pada kesejahteraan pengemudi transportasi online di Indonesia," *Jurnal Ilmiah Ilmu Administrasi,* vol. 3, pp. 73-85, 2020.

[5] U. T. A. Ahidin, Aris; Imbron; Khoiriah, Neneng, *COVID-19 dan Work from Home*. Desanta Muliavisitama, 2020.

[6] T. University. "Tel-U Kembali Jalani Audit Internal Secara Online." https://telkomuniversity.ac.id/tel-u-kembali-jalani-audit-internal-secara-online (accessed 9 November, 2022).

[7] ISACA, *COBIT 5 for Risk* (ISACA). 2013.

[8] *NIST Special Publication 800-53, Revision 5 — Security and Privacy Controls for Information Systems and Organizations*, NIST, 2020.

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

[9] *Department of Defense Instruction 8500.2 Information Assurance (IA) Implementation*, D. o. D. U. S. o. America, 2003.

[10] Y. Erlika, M. I. Herdiansyah, and A. H. Mirza, "Analisis IT Risk Management di Universitas Bina Darma Menggunakan ISO31000," *Jurnal Informatika Global,* vol. 11, no. 1, 2020.

[11] H. Hardani *et al.*, *Metode Penelitian Kualitatif & Kuantitatif*. Yogyakarta: CV. Pustaka Ilmu Group, 2020.

[12] T. University. "Laporan Daftar Risiko Universitas Telkom Periode Ganjil 2019-2020." https://audit.telkomuniversity.ac.id/risiko/ (accessed 28 September, 2022).