Proceedings of the 5th Faculty of Industrial Technology
International Congress Bandung, Indonesia,
September 17-18, 2025
ISSN 2962 – 1798

Design of a Business Continuity Plan and Disaster Recovery Plan at UPT – TIK Based on the COBIT 2019 Assessment Result

Mira Musrini Barmawi [a], *Tri Rahayu Purwanti* [a], and *Asep Rizal Nurjaman* [a]

[a] Information System, Institut Teknologi Nasional Bandung 40124 West Java, Indonesia

Abstract. Information technology plays an important role in supporting academic and business operations in higher education institutions; however, its implementation also presents risks such as technical disruptions, natural disasters, and information security incidents that may affect finances, reputation, and business continuity. Therefore, it is necessary to evaluate IT governance to ensure alignment with organizational objectives. Data collection was carried out through literature review, interviews, direct observations, and questionnaires, which were analyzed using the COBIT 2019 Process Assessment Model (PAM) and Design Guide. The evaluation results show that the capability of domain DSS04 – Managed Continuity is at level 1 with an achievement of 51% (Largely Achieved) and a gap of two levels from the target, indicating the need for improvement in Managed Continuity. Based on these findings, a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) were designed with reference to ISO 22301:2012, with risk identification conducted using the OCTAVE and FMEA methods. The analysis identified 17 risks with 37 business impact assessments, as well as the determination of MTD, RPO, and RTO along with strategies to mitigate the risks.

1 Introduction

Information technology plays an important role in supporting academic and business operations in Higher Education as well as enhancing the effectiveness and efficiency of decision-making[1]. However, its implementation faces challenges such as disruptions and security issues[2]. Higher Education institutions are also vulnerable to risks since most of their business processes depend on IT, making assets and resources susceptible[3]. Errors in IT implementation can cause financial losses, decrease user trust, and damage reputation [4]. These risks may arise from technical factors or natural disasters such as floods, earthquakes, fires, and information security incidents[5]. Such disruptions have the potential to cause financial harm, damage reputation, and create problems in the supply chain that affect customers, partners, and stakeholders[6], and may even hinder or halt business processes[7]. Therefore, evaluation is needed to ensure IT alignment with organizational goals so that its implementation truly supports the achievement of objectives [8].

One of the approaches used in the evaluation is COBIT (Control Objectives for Information and Related Technology), a framework for the governance and management of information and technology that is intended for use by the entire enterprise[9]. The COBIT framework clearly distinguishes between governance and management. Governance ensures that stakeholder needs, conditions, and options are evaluated to determine balanced and agreed-upon enterprise objectives. Direction is set through prioritization and decision-making [10].

A Business Continuity Plan is a plan for ensuring business continuity, allowing business processes within an organization or company to be maintained during both normal and critical situations. A Business Continuity Plan is used to sustain business operations continuously before, during, and after disruptive events [11]. In addition to BCP, a Disaster Recovery Plan is also necessary for recovery planning and to ensure the achievement of a restored condition within a specified timeframe, enabling the organization or company to resume its functions with minimal losses[12].

ISO 22301:2012 is an international standard for the implementation of a Business Continuity Management System (BCMS). This standard helps organizations prepare for, prevent, respond to, and recover from disruptive incidents such as natural disasters and unforeseen events. It covers risk identification, mitigation strategies, and business continuity, and applies the Plan-Do-Check-Act (PDCA) cycle. ISO 22301 consists of 10 clauses. Clauses 1 to 3 include

[1] Corresponding author: aseprizal@itenas.ac.id

ISSN 2962 – 1798

the scope, normative references, and terms and definitions, while the core BCMS requirements are addressed in clauses 4 through 10 [13].

According to Albert, the OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation–Small) procedure is a framework for assessing security risks. Its approach is designed based on criteria that outline the key components of data security risk assessment. [14]. The OCTAVE method uses three phases to examine technology-related issues. For the assessment within OCTAVE, researchers use FMEA (Failure Mode and Effect Analysis). FMEA is a technique for identifying and understanding potential failures. It involves four evaluation criteria: severity, occurrence, and detection. To determine the level of risk, the Risk Priority Number (RPN) is used [15].

[16] Research on Business Continuity Plans has been conducted by several researchers. One such study focused on designing a BCP to ensure business continuity during disruptions in information technology, referring to the ISO 22301 standard. The evaluation results indicated that the company had not fully implemented a BCP, thus highlighting the need for BCP development in accordance with the ISO 22301 guidelines.

2 Methods

This study designs a Business Continuity Plan based on the results of measurements using COBIT 2019.

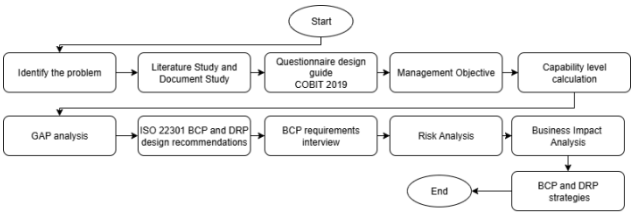

Fig. 1. Methods

3 Result and Discussion

This study identified three highest design factors: ED01, BAI06, and DSS04. This study uses the DSS04 domain because it is relevant to maintenance processes, business planning, and incident handling in IT services, in accordance with the background and issues raised. Measurements were conducted by distributing questionnaires to roles mapped based on the DSS04 domain.

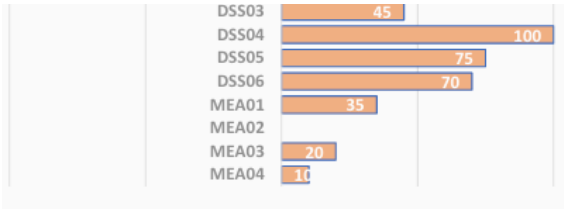

Fig. 2. All Design Factor

The respondents' answers were then converted and calculated to obtain the average score.

3.1 Management Objective

Based on the theory in DSS04, the focus is on managing the continuity of IT services, which includes planning, preparedness for disruptions, and system recovery to ensure that services continue to operate in accordance with needs and issues, as outlined in the introduction. The table below presents the average scores of the processes within the DSS04 domain. The results for DSS04.01 are (0.79), DSS04.02 (0.81), DSS04.03 (0.48), DSS04.04 (0.33), DSS04.05 (0.29), DSS04.06 (0.08), DSS04.07 (0.79), and DSS04.08 (0.50), resulting in an overall average of 0.51.

Table 1. Level Assesment

Level	Process	Assessment	Achieved
1	PA 1.1	L	Yes

3.3 Gap

Based on the calculation results, the assessment involved 4 respondents.

Table 2. Gap

Management Practice	Level		
	As - is	Target	Gap
DSS04	1	3	2

3.4 Spider Chart

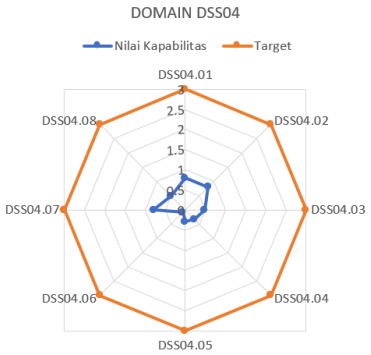

Fig. 3. Spider Chart DSS04

The entire DSS04 process has not yet reached Level 3, thus management improvements are needed to enhance capability.

3.5 Rekomendation

UnTo achieve level 3, the researcher recommends the measures presented in the table below.

Table 3. Recommendation Level 1 - 3

Level 1 Performed	
Purpose	**Rekomendation**
PA 1.1 The implemented process achieves its process purpose.	Organizations need to establish clear policies regarding the availability of critical information, conduct risk assessments, and regularly test the Business Continuity Plan (BCP). The BCP document must also be updated annually, and relevant staff should receive training to ensure readiness in emergency situations.
Level 2 Performed	
Purpose	**Rekomendation**
PA 2.1 Performance Management - A measure of the extent to which the performance of the process is managed.	Organizations need to comprehensively plan and monitor BCP activities, establish clear RTO (Recovery Time Objective) and RPO (Recovery Point Objective), develop a well-defined RACI matrix, and build KPI evaluations. In addition, it is essential to identify needs and strengthen interdepartmental communication to support the effectiveness of the BCP.
PA 2.2 Work Product Management - A measure of the extent to which the work products produced by the process are appropriately managed. The work products (or outputs from the process) are defined and controlled.	Organizations need to manage BCP documents in a structured manner through the identification of work products, implementation of document controls, use of standard templates, and regular scheduling of reviews and change tracking.

Level 3 Performed	
Purpose	**Rekomendation**
PA 3.1 Process Definition - A measure of the extent to which a standard process is maintained to support the deployment of the defined process.	Organizations need to develop SOP documents for BCP and DRP that include recovery workflows, timelines, emergency contacts, and manual procedures. A BCP process flow diagram should be created and linked to other processes such as IT services, security, and finance. In addition, it is necessary to prepare a personnel role matrix, an inventory list with readiness status, and success indicators through a regular audit schedule and BCP process evaluations.
PA 3.2 Process Deployment - A measure of the extent to which the standard process is effectively deployed as a defined process to achieve its process outcomes.	Organizations need to implement BCP SOP accompanied by training for all members and proper documentation. The BCP team structure and emergency response roles should be clearly communicated, and regular training should be conducted. Emergency contacts and manual forms must be prepared, infrastructure must be properly managed, and data from BCP drills should be collected to assess recovery time and the impact on services.

3.10 Mapping of Needs to the BCP

Table 4. Mapping BCP and ISO 22301:2012

Phase	Needs and Expectations	Status	BCP	Reference
PLAN	*The BCP must be useful for information technology*	Verified	Organizational profile	ISO 22301:2012
			Obejective	ISO 22301:2012
			Scope	ISO 22301:2012
			Roles and responsibilities	ISO 22301:2012
			Resources	ISO 22301:2012
			Communication flow	ISO 22301:2012
DO	*The BCP must help the organization face risks and disasters*	Verified	Risk analysis	ISO 22301:2012
			Business impact analysis	ISO 22301:2012
	The BCP must support information technology security	Verified	BCP strategy	ISO 22301:2012
			BCP procedure development	ISO 22301:2012
	The BCP must align with business operations	Verified	Training and testing	ISO 22301:2012
	The BCP must be useful for network systems	Verified		
CHECK	*The BCP should be updated periodically*	Recomendation	Internal audit	ISO 22301:2012
			Management review	ISO 22301:2012
ACT	*The BCP should be applicable for long-term use*	Recomendation	Continuous improvement	ISO 22301:2012

3.9 Plan

In the planning phase, the organization is expected to design a Business Continuity Plan (BCP) that aligns with the needs of the ICT Technical Implementation Unit (UPT – TIK).

ISSN 2962 – 1798

3.9.1 Objective

The purpose of developing this BCP is to formulate a business continuity plan that aligns with the needs and objectives of the ICT Technical Implementation Unit (UPT – TIK), to help reduce risks related to information technology that may disrupt operations, and to understand the impacts on the continuity of business processes.

3.9.2 Scope

In the development of a BCP, several functions and business processes are involved. These functions and processes are selected due to their strong association with the use of information technology.

3.9.3 Business Functionality

Table 5. Business Functionality

Business Functionality	Business Processes Related to the System
Information Systems	Provides web-based information systems and handles user complaints related to errors, interface issues, menu access, and system functions. Manages the monitoring system application, performs backups, and adds features when necessary.
Networking	Conducts maintenance and management of the network and its security, and optimizes the performance of information system applications.
Database	Enters student data into PDDIKTI and lecturer performance reports into the system..

3.9.4 Roles and Responsibilities

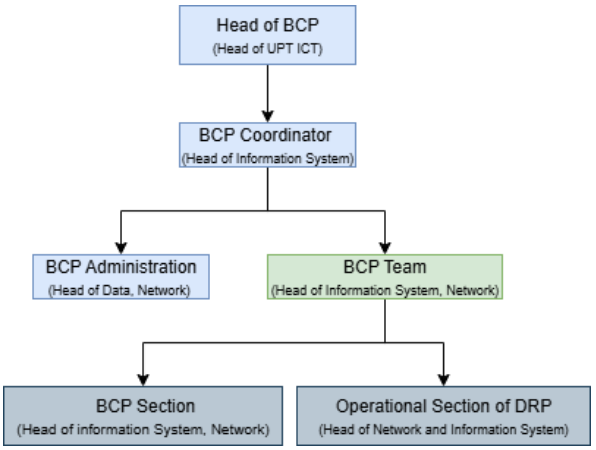

Fig. 4. Roles and Responsibilities

3.9.5 Rescources

In the implementation of the Business Continuity Plan, resource support is essential to ensure smooth operations. Therefore, the ICT Technical Implementation Unit (UPT – TIK) needs to identify equipment such as servers, generators, and communication tools. In addition, supporting software and documentation, such as emergency contact lists and IT service condition checklists, are also required

3.9.6 Communication Flow

The following is the communication pathway to ensure the implementation of the BCP is carried out according to plan.

ISSN 2962 – 1798

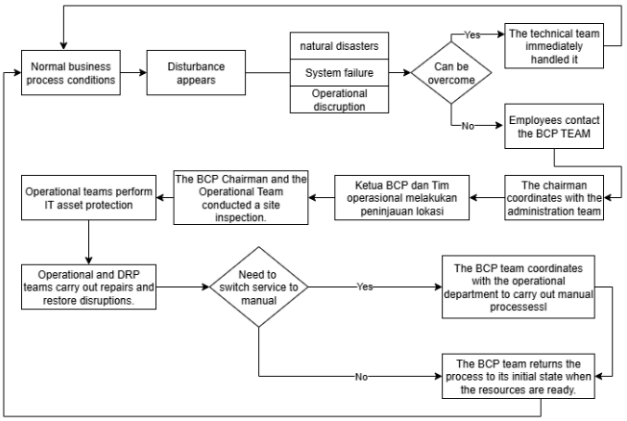

Fig. 5. Communication Flow

3.9.7 Emergency Communication Flow

Emergency communication devices are tools used to ensure communication channels remain available during a disaster, such as mobile phones.

3.10 Do

3.10.1 Risk Analysis

In the analysis phase, the goal is to help the organization understand the types of protection needed and the threats that may disrupt the continuity of services and critical assets. The risk analysis uses the OCTAVE method, which consists of three phases:

Phase 1: Building a Threat Profile Based on Assets

In this phase, critical assets are identified. The table 9 presents a list of critical assets along with their corresponding security requirements.

Table 6. Asset security needs

Asset catgory	Asset Name	Security Needs
Hardware	Server, PC	Servers must be accessible 24/7, PCs must have antivirus protection and function during the organization's working hours.
Software	Website	Must be accessible 24/7, with access rights restricted by user roles, and regular database backups in place.
Data	Student Data, Lecturer Data	Requires data backups and access control restrictions.
Network	Wi-Fi, Cables, Routers	Must be available during operational hours and controlled access must be ensured.

Table 7. Threat

Environmental Threats	Earthquake, lightning, flood, fire, building damage
Human Threats	Internet network sabotage, data theft, system breach
Infrastructure Threats	PC damage, server failure, theft of hardware equipment
	Virus attacks, software bugs
	Internet connection discruption, cable damage

Table 8. Security Practice

Responsibility	Security Practice
Network division	Performs maintenance on cables and networks CCTV is installed for monitoring
Information system divisio	Manages the information system and assigns different roles or access rights to each user, including lecturers, students, and other users.
Database division	Manages lecturer and student data
All UPT – TIK staff	Door access is granted only to those who have fingerprints and for guests there must be permission from inside the UPT - TIK building.

There is an organizational weakness due to the absence of Standard Operating Procedures (SOP), as well as the lack of a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP)

1) Phase 2: Identifying Infrastructure Vulnerabilities

Table 9. Potential Threats

Server	
Main Component	**Potential threats**
Generator, server room, hard disk, RAM, electricity	Generator failure during a power outage may cause the server to go down, Hard disk damage may result in data loss, ower outages can shut down the server, disrupting system availability.

2) Phase 3: Developing Security Strategies and Planning

For R-01, the total RPN is 147 (High), for R-09, it is 144 (High), R-15 has 135 (High), and R-16 has 252 (Very High). In this journal, there are four priority levels identified, as they obtained the highest scores. These scores were derived from the results of the questionnaire.

Table 10. Risk Analysis.

Risk ID	Potential Failure	Potential impact of failure	Sev	Potential cause of discruption	Occ	Current control process	Det	RPN	Level
R- 01	Server damage	Business process disruption	7	Lighting	3	No lightning protection	7	147	High
R-09	Unauthorized website access	Data theft or damage	9	Weak security system	4	Access rights	4	144	High
R-15	Misuse of account data	Information leakage	9	Account sharing	5	No security training	3	135	High
R-16	Password sharing	Account misused by external parties	9	Lack of risk awareness	7	No security training	4	252	Very High

3.10.2 Business Impact Analysis

There are a total of 35 services, 7 at a very high level, 27 at a medium level, and 1 at a low level.

Table 11. Service Priority

IT Service	Critival level
SIKAD, SIKAD OLD, USM, PDPT Feeder, E-learning, Attendance, E-Journal	High
SIMSDM, SIKIDOS, Employee Performance Assessment System, SISTER, SIKAJUL, SIM SKK, ODT Online, Graduation Registration, SKPI, INFODATA, SIMKEU, SILOGIS, SIRKAT, SIMNAS, Student Activity System , CDC, Sistem Tracer Studi, KP/TA, SIMAT, Eprint Ver 3, SLIM, SETIADI, Library Website, E-Proceeding, SIKERMA, SIMPENMAS	Currently
Independent ASKER Information System	Low

Criticality Assessment and Recovery Time Analysis for Each Related Business Process.

Table 12. Recovery Time Analysis

Business Functionality	Related Business Process to the System	Level	MTD	RTO	RPO
Information System	Providing a web-based information system	High	Approximately 6 months	Less than 6 months	Approxymatel y 6 months
	Resolving complaints related to the information system reported by users, such as login errors, broken system interface, inaccessible menus, or malfunctioning features	High	<15 minutes	<15 minutes	<15 minutes
	Managing information system application	Medium	<15 minutes	<15 minutes	<15 minutes
Network	Conducting internet network maintenance	Medium	<15 minutes	<15 minutes	<15 minutes
	Optimizing the performance of information system applications	Medium	<15 minutes	<15 minutes	<15 minutes
	Performing hardware maintenance such as servers	High	<15 minutes	<15 minutes	<15 minutes
Data	Entering student data into PDDIKTI	High	Approximately 24 hours	Approximately 12 hours	Approximately 24 hours
	Entering lecture performace report	High	Approximately 24 hours	Approximately 12 hours	Approximately 24 hours

3.10.3 BCP Strategy

Table 13. Preventif Strategy, DRP, During discruption, Corrective, Testing and Training

Risk : Server Damage Cause : Lightning	
Preventive Strategy	**Description**
Install a Lightning Protection System (LPS)	LPS prevents direct lightning strikes to the server by directing the current safely to the ground, protecting hardware and installations from damage.
Install Surge Protective Device (SPD)	Server damage often results from power surges, not direct strikes. An SPD at the main panel absorbs surges before they reach sensitive equipment like servers.
Standard Grounding and Earthing System	Grounding drains lightning current to the ground to prevent damage, poor grounding can cause the current to spread to devices and damage the system.
Conduct Regular Inspections and Maintenance	All protection systems such as LPS, SPD, and grounding should be routinely inspected to ensure optimal function and to detect any faults or degradation.
Install a Lightning Monitoring System	Lightning sensors detect strikes in the surrounding area, enabling sensitive systems to be temporarily shut down to prevent potential damage.
DRP Strategy	

ISSN 2962 – 1798

The following are the steps to be taken in the event of server damage caused by lightning:

1. Temporarily disable data access to the main server.
2. Inspect the hardware for damage.
3. Coordinate with the team to replace damaged hardware.
4. Transfer service processes to manual systems (if needed) as a temporary alternative before the backup system is activated — for example, manual attendance or online record-keeping.
5. Verify the network system before resuming operations on the main server.
6. Activate the backup server.
7. Restore data from regularly stored backups.
8. Record all incidents and recovery times for future improvement.

Response Strategy During Disruption	Description
Identify the source of the disaster	Check and determine whether the damage was caused by lightning, a short circuit, or another factor.
Secure IT assets	During the disruption, IT assets must be protected. The storage room should ideally be designed to withstand earthquakes and fires to prevent further damage.
Activate the emergency team	A special team is assigned to handle the incident, assess the damage, and take immediate action.
Redirect services	Switch to a backup server if possible, to ensure services remain available.
Record the incident	All actions and events must be documented for future evaluation and improvement.

Corrective Strategy	Description
Evaluate and document the incident results	Conduct a thorough evaluation of the damage and document the entire process
Corrective actions on the system and enhancement of the server room environment	Upgrade the system with a backup server and equip the server room with environmental protections to prevent recurring damage..
Record the incident	Every action and event is recorded for future assessment.

Overview of Business Continuity Training	
Training Topic	Server damaged due to lightning
Training Type	Socialization and simulation
Training Description: The training covers both theoretical and practical aspects of server damage risks caused by lightning, as well as the use of LPS (Lightning Protection System), SPD (Surge Protection Device), and grounding. The goal is to enhance the team's quick response to disruptions.	
General Materials	
Recording of incident	Incident logging, brief explanation of ISO 22301 and the PDCA cycle, risks of IT system damage due to lightning, functions and mechanisms of LPS, SPD, and grounding, server recovery and service redirection, utilization of backup servers and backup systems, reporting and documentation processes, and communication flow during BCP incidents.
BCP Testing Results	
Roles and responsibillities	1. The BCP Testing ResultsKoordinator BCP memimpin rapat sebelum melakukan simulasi 2. The BCP coordinator led the briefing session prior to the simulation. 3. The administrative staff documented all process stages. 4. The BCP team provided technical direction, while the Operations and DRP teams executed all technical procedures.
Proses	1. Temporary shutdown of data access to the main server. 2. Physical inspection of hardware components. 3. Coordination with the team for replacement of damaged equipment. 4. Service transition to manual systems (if required). 5. Network and connectivity verification prior to recovery. 6. Activation of the backup server. 7. Data recovery from backups all incident, recovery times, and encountered obstacles were documented.

The table 14 presents strategies for when the website becomes inaccessible due to high user traffic.

Table 14. Preventif Strategy, DRP, During discruption, Corrective, Testing and Training

Risk : Website accessed by unauthorized parties Cause : Weak security system	
Preventive Strategy	**Description**
Use of two-factor authentication	Even if the password is leaked, additional verification such as OTP is still required.
Regular system and security update	Closing security gaps in CMS, plugins, and servers
Implementation of Web Application Firewal	To detect and block injection attacks or illegal access before reaching the server.
Admin access restriction	Access is only allowed from specific IPS, and admin accounts are limited.
DRP Startegy	
1. Redirect the website to a temporary maintenance page to prevent further damage. 2. Restore from the latest backup. 3. Inspect all servers and databases to detect malicious scripts	
Strategy During Discruption	**Description**
Temporarily disable access	To prevent users from being exposed to harmful content or data theft
Isolate affected servers	To prevent the spread of attacks to other services.
Reset all admin account passwords	To stop unauthorized external access that may still be active.
Coordinate with the team	To ensure a faster and structured response
Corrective Strategy	**Description**
Improve security system configuration	Strengthening firewalls, applying patches, and configuring servers properly.
Enhance password policy	Enforce the use of complex passwords and require regular password changes.
Implement real-time monitoring	Install IDS/IPS for intrusion detection and automatic reporting
Incident evaluation and documentation	As a learning tool to prevent recurrence of similar incidents
Overview of Business Continuity Training	
Training Name	Website Disruption Handling and System Recovery Training
Training Type	Technical and simulation-based
Training description: Provides basic understanding and skills in handling website disruptions such as server overload or downtime	
Training Target Audience:	For the UPT - TIK team
General Materials:	
Administrator education on account security management, including strong password policy, multi-layer authentication, and activity log monitoring. User awareness improvement to avoid clicking suspicious links, downloading files from untrusted sources, and to report immediately when anomalies are detected in the system	
BCP Testing Results	
Participants and Role Distribution	1. The BCP leader supervised the entire testing process. 2. The BCP coordinator led the meeting prior to the simulation. 3. The administrative team recorded all process stages and documented the event. 4. The BCP team provided technical direction for operational execution, and the DRP

ISSN 2962 – 1798

	team carried out all technical processes, including service redirection and backup server activation.
Process	Participants were able to explain the handling steps in case of account misuse and understood which parties must be contacted immediately when such incidents occur

Training Name	Password Sharing and Account Risk
Training Type	Awareness and Simulation
Training description: This training aims to provide students with insights into the dangers of sharing passwords, as well as explain how accounts can be misused by external parties.	
Training Target Audience	All Itenas students
General Materials:	
What is an account and why it must be protected	Students are introduced to the concept that a campus account is a personal identity used to access campus systems and must not be used by others.
The dangers of sharing passwords with others	Explained that password sharing carries a high risk as it can lead to misuse, data damage, and identity theft.
How to prevent account hacking	Creating strong passwords and avoiding the use of a single password for all accounts
What to do if an account is misused	Participants are given steps such as immediately changing the password, logging out from all devices, and reporting to the IT department.
Explanation of campus rules and ethics in account usage	Communicating campus regulations regarding account usage and the consequences of violations.
BCP Testing Results	
Process	Participants were able to explain the handling steps if an account was misused and understood whom to contact immediately in the event of such an incident.

Training Name	Prevention of Lecturer Account Data Misuse
Training Type	Socialization
Training description: This training is intended for lecturers to raise awareness of the dangers of account sharing, especially related to academic and administrative data. Through this training, lecturers will learn how to protect their accounts, understand campus regulations, and know the steps to take in case of a data breach.	
Training Target Audience	All Itenas lecturers
General Materials:	
How to protect an account	Create strong and hard-to-guess passwords using a combination of uppercase letters, lowercase letters, numbers, and symbols to make them difficult to predict. Using the same password for multiple accounts is very risky and must be avoided. Lecturers are also advised to change their passwords regularly, especially after using public devices, and to enable two-factor

	authentication if available. In addition, passwords should not be stored carelessly or written down in places visible to others.
If the account is misused	If account misuse occurs, the first step is to immediately reset the password to stop external access. After that, lecturers must log out from all devices previously used. This incident must also be reported immediately to the IT unit/UPT TIK so that activity logs can be checked to identify who accessed the account.
How to protect an account	Strong passwords must be created with a combination of uppercase, lowercase, numbers, and symbols. Avoid using the same password for multiple accounts, change passwords regularly (especially after using shared/public devices), activate two-factor authentication when available, and never store or write down passwords in places easily seen by others.
BCP Testing Results	
Process	Participants were able to explain the risk handling steps if an account was misused and understood which parties must be contacted immediately when such an incident occurred.

3.11 Check

In this phase, an audit of the BCP impelementation and a management review of the BCP will be conducted.

3.12 Act

The action phase is carried out by UPT – TIK to improve BCP performance in addition, a reassessment is also conducted during this phase.

4 Conclusion

Based on measurements using COBIT 2019, the DSS04 domain (Managed Continuity) achieved 100%, with PA 1.1 at *Largely Achieved* status of 51% at level 1, resulting in a two-level gap from the targeted capability. The study recommends the design of a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) referring to ISO 22301:2012. The design of BCP and DRP is formulated from organizational needs with risk identification using the OCTAVE method, which produced 17 risks and 37 business impact analyses. The results show 7 IT services at high risk, 27 at medium, and 1 at low, along with the determination of MTD, RPO, and RTO values. From this analysis, 4 priority risks with high and very high levels were identified for further mitigation. The values for maximun tolarable downtime (MTD), recovery point objective (RPO), and recovery time objective (RTO) were succesfully determined. Four top-priority risk to be addressed in the strategy are server damage causes by ligthing and Unauthorized access to the website. In addition, the training programs include socialization on the risks of password sharing and socialization on the prevention of lecturer account data misuse.

References

[1] R. Fadhilah, “Rencana Audit Teknologi Informasi Menggunakan Cobit 2019 Pada Unit Isti Universitas Telkom,” *JIKO (Jurnal Inform. dan Komputer)*, vol. 4, no. 3, pp. 157–163, 2021, doi: 10.33387/jiko.v4i3.3325.

[2] L. Ernawati and H. B. Santoso, “Identifikasi dan Analisa Risiko Penerapan Teknologi Informasi di Lingkungan Perguruan Tinggi,” *Seri Pros. Semin. Nas. Din. Inform.*, vol. 1, no. 1, pp. 21–28, 2017.

[3] H. Handoko and E. Elly, “Perancangan Rencana Keberlangsungan Bisnis dalam Manajemen Risiko Layanan Teknologi Informasi,” *J. Tek. Inform. dan Sist. Inf.*, vol. 9, no. 3, pp. 351–359, 2024, doi: 10.28932/jutisi.v9i3.6539.

[4] I. Iskandar, “manajemen risiko teknologi informasi perusahaan menggunakan framework riskit (studi kasus : pembobolan pt . Bank permata , tbk),” *J. Sains, Teknol. dan Ind.*, vol. 9, no. 1, p. 104, 2011.

[5] Humdiana, “PERANCANGAN BUSINESS CONTINUITY PLAN : STUDI KASUS PADA PT.PAM,” pp. 1–9, 2020.

[6] J. Panda, S. Das, and D. Pattnaik, “Resilient IT Infrastructure: Strategies for Minimizing Downtime and

Ensuring Business Continuity," *J. Humanit. Soc. Sci. Res.*, vol. 6, no. S, pp. 76–86, 2024, doi: 10.37534/bp.jhssr.2024.v6.ns.id1255.p76.

[7] F. Yudhistira, "Kerangka Kerja Business Continuity Plan Sebagai Acuan Mitigasi Gangguan Teknologi Informasi di Perusahaan Sektor Perminyakan," *J. Ilm. Multidisiplin*, vol. 2, no. 1, pp. 136–141, 2023, doi: 10.59000/jim.v2i1.95.

[8] F. Susilowati, W. T. Saputro, and I. Y. Pasa, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja Cobit 5 di SMK XYZ," *INTEK J. Inform. dan Teknol. Inf.*, vol. 6, no. 2, pp. 64–72, 2023, doi: 10.37729/intek.v6i2.3870.

[9] ISACA, *COBIT 2019 Framework: Design and Guide*. 2019.

[10] M. Saleh, I. Yusuf, and H. Sujaini, "Penerapan Framework COBIT 2019 pada Audit Teknologi Informasi di Politeknik Sambas," *J. Edukasi dan Penelit. Inform.*, vol. 7, no. 2, p. 204, 2021, doi: 10.26418/jp.v7i2.48228.

[11] Y. Muflihah and A. P. Subriadi, "A basic element of it business continuity plan: systematic review," *J. Inform.*, vol. 12, no. 1, p. 17, 2019, doi: 10.26555/jifo.v12i1.a8370.

[12] B. Yuliad and A. Nugroho, "Rancangan Disaster Recovery Pada Instansi Pendidikan Studi Kasus Universitas Mercu Buana," *J. Tek. Inform.*, vol. 9, no. 1, pp. 30–39, 2016, doi: 10.15408/jti.v9i1.5575.

[13] E. H. Prakasita and R. V. H. Ginardi, "Tinjauan Kesiapan Terhadap Implementasi Business Continuity Management Systems (BCMS) Berbasis ISO 22301 dan ISO 27001 (Studi Kasus: PT. JPK)," *Inform. Mulawarman J. Ilm. Ilmu Komput.*, vol. 13, no. 2, p. 76, 2019, doi: 10.30872/jim.v13i2.902.

[14] D. R. Nurfadilah, W. N. H. Putra, and A. Rachmadi, "Analisis Manajemen Risiko Keamanan Sistem Informasi pada BKPSDM Kota Batu menggunakan Kerangka Kerja OCTAVE-S dan ISO 27001 : 2013 (Studi Kasus : Aplikasi E-Kinerja)," *J. Pengemb. Teknol. Inf. dan Ilmu Komputer, Univ. Brawijaya*, vol. 4, no. 9, pp. 3014–3020, 2020.

[15] L. Munaroh, Y. Amrozi, and R. A. Nurdian, "Pengukuran Risiko Keamanan Aset TI Menggunakan Metode FMEA dan Standar ISO/IEC 27001:2013," *Technomedia J.*, vol. 5, no. 2 Februari, pp. 167–181, 2020, doi: 10.33050/tmj.v5i2.1377.

[16] I. Setiawan, R. Waluyo, and W. A. Pambudi, "Perancangan Business Continuity Plan dan Disaster Recovery Plan Teknologi dan Sistem Informasi Menggunakan ISO 22301," *J. RESTI (Rekayasa Sist. dan Teknol. Informasi)*, vol. 3, no. 2, pp. 148–155, 2019, doi: 10.29207/resti.v3i2.911.