IKB31103 – BUSINESS CONTINUITY PLANNING

MINI PROJECT: BUSINESS CONTINUITY PLAN FOR MAJLIS AMANAH RAKYAT (MARA) – TERTIARY EDUCATION SPONSORSHIP PROGRAMME (TESP)

Academic Case Study

Prepared as part of a Team-Based Academic Project
Contributor: Nurin Nabeeha binti Azahari

This document is a curated academic Business Continuity Plan prepared for portfolio demonstration purposes.
Sensitive operational details have been generalized or omitted.

Table of Contents

1.0 Introduction

1.1 Background of the Company

Majlis Amanah Rakyat (MARA), also known as the Council of Trust for the People, is a Malaysian government agency under the Ministry of Regional and Rural Development. Established on March 1, 1966, following the first Bumiputera Economic Congress in 1965, to support the economic and industrial growth of Bumiputera individuals, including Malays and other indigenous Malaysians.

MARA is dedicated to promoting entrepreneurship, skill development, and economic growth in Bumiputra communities. It offers a range of services and products, including comprehensive business training programs, financial assistance through grants and loans, and industry guidance. MARA also manages various educational institutions, including colleges and vocational schools, to enhance the skills and knowledge of Bumiputra individuals, thereby facilitating business success and economic empowerment within these communities.

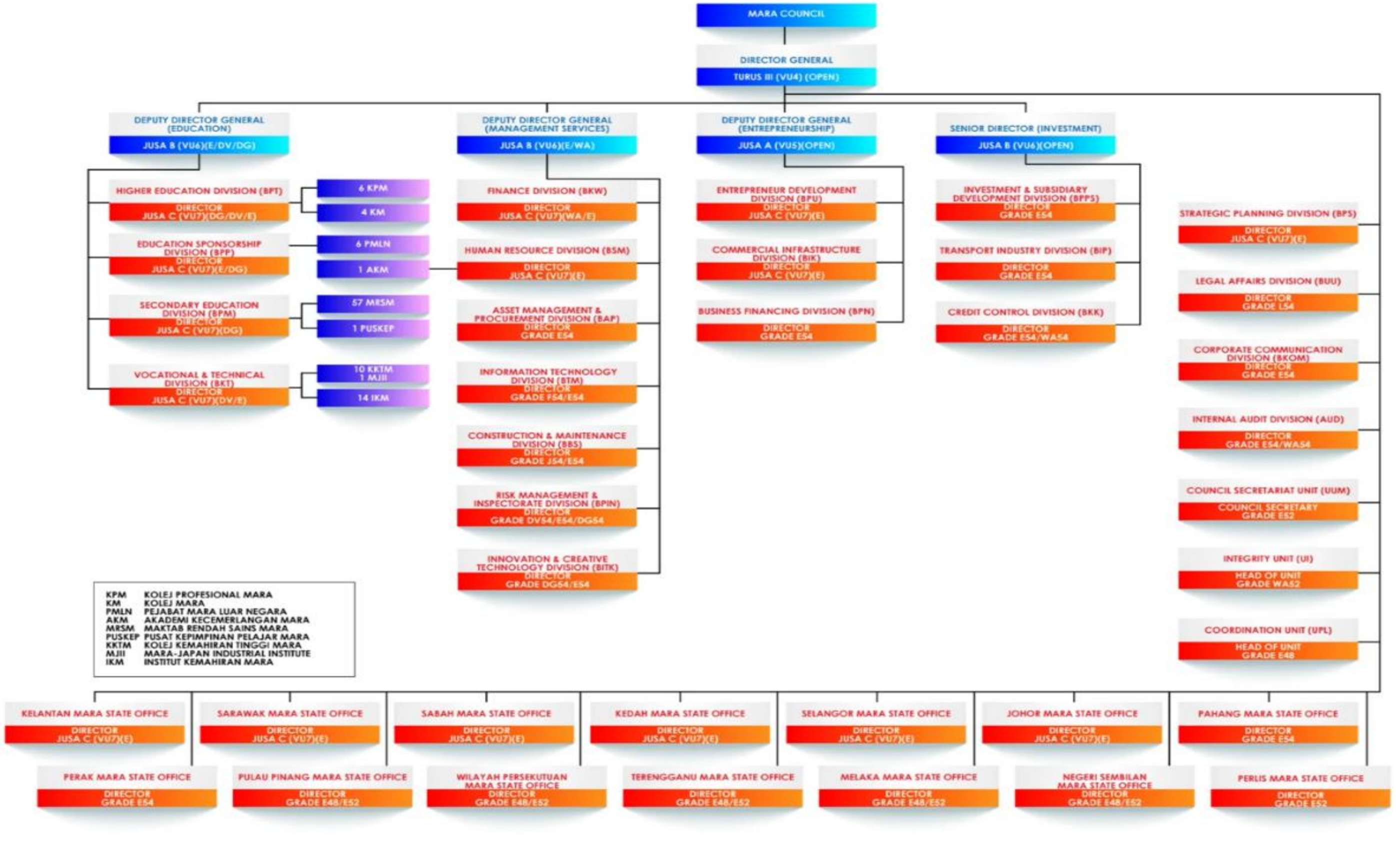
The scope of this Business Continuity Plan (BCP) covers the Tertiary Education Sponsorship Programme (TESP), a critical service provided by MARA to support Bumiputra individuals pursuing diploma and degree-level education. The TESP service relies on two key websites: the MyEduloan Portal for loan applications and e-Baki MARA for balance inquiries, loan statements, and loan repayments. Ensuring the constant availability and performance of these websites is crucial for seamless service delivery to Bumiputra students.

MARA is committed to fulfilling its responsibility to Bumiputra students by proactively identifying potential risks and implementing mitigation strategies. Through thorough planning and proactive measures, MARA aims to protect the credibility and dependability of the TESP service, ensuring that students will always have access to vital financing options for their education, even in the event of unforeseen challenges.

1.2 Company Organizational Structure

MARA operates under Ministry of Regional and Rural Development, with several main departments including Education, Management Services, Entrepreneurship, and Investment. For this BCP, the primary focus is on the following departments:

- Secondary Education Division (BPM)
- Information Technology Division (BTM)
- Risk Management and Inspectorate Division (BPIN)


MARA COUNCIL
DIRECTOR GENERAL
TURUS III (VU4) (OPEN)
DEPUTY DIRECTOR GENERAL (EDUCATION)
JUSA B (VU6)(E/DV/DG)
DEPUTY DIRECTOR GENERAL (MANAGEMENT SERVICES)
JUSA B (VU6)(E/WA)
DEPUTY DIRECTOR GENERAL (ENTREPRENEURSHIP)
JUSA A (VU5)(OPEN)
SENIOR DIRECTOR (INVESTMENT)
JUSA B (VU6)(OPEN)
HIGHER EDUCATION DIVISION (BPT)
DIRECTOR
JUSA C (VU7)(DG/DV/E)
6 KPM
4 KM
EDUCATION SPONSORSHIP DIVISION (BPP)
DIRECTOR
JUSA C (VU7)(E/DG)
6 PMLN
1 AKM
SECONDARY EDUCATION DIVISION (BPM)
DIRECTOR
JUSA C (VU7)(DG)
57 MRSM
1 PUSKEP
VOCATIONAL & TECHNICAL DIVISION (BKT)
DIRECTOR
JUSA C (VU7)(DV/E)
10 KKTM
1 MJII
14 IKM
FINANCE DIVISION (BKW)
DIRECTOR
JUSA C (VU7)(WA/E)
HUMAN RESOURCE DIVISION (BSM)
DIRECTOR
JUSA C (VU7)(E)
ASSET MANAGEMENT & PROCUREMENT DIVISION (BAP)
DIRECTOR
GRADE E54
INFORMATION TECHNOLOGY DIVISION (BTM)
DIRECTOR
GRADE F54/E54
CONSTRUCTION & MAINTENANCE DIVISION (BBS)
DIRECTOR
GRADE J54/E54
RISK MANAGEMENT & INSPECTORATE DIVISION (BPIN)
DIRECTOR
GRADE DV54/E54/DG54
INNOVATION & CREATIVE TECHNOLOGY DIVISION (BITK)
DIRECTOR
GRADE DG54/E54
ENTREPRENEUR DEVELOPMENT DIVISION (BPU)
DIRECTOR
JUSA C (VU7)(E)
COMMERCIAL INFRASTRUCTURE DIVISION (BIK)
DIRECTOR
JUSA C (VU7)(E)
BUSINESS FINANCING DIVISION (BPN)
DIRECTOR
GRADE E54
INVESTMENT & SUBSIDIARY DEVELOPMENT DIVISION (BPPS)
DIRECTOR
GRADE E54
TRANSPORT INDUSTRY DIVISION (BIP)
DIRECTOR
GRADE E54
CREDIT CONTROL DIVISION (BKK)
DIRECTOR
GRADE E54/WA54
STRATEGIC PLANNING DIVISION (BPS)
DIRECTOR
JUSA C (VU7)(E)
LEGAL AFFAIRS DIVISION (BUU)
DIRECTOR
GRADE L54
CORPORATE COMMUNICATION DIVISION (BKOM)
DIRECTOR
GRADE E54
INTERNAL AUDIT DIVISION (AUD)
DIRECTOR
GRADE E54/WA54
COUNCIL SECRETARIAT UNIT (UUM)
COUNCIL SECRETARY
GRADE E52
INTEGRITY UNIT (UI)
HEAD OF UNIT
GRADE WA52
COORDINATION UNIT (UPL)
HEAD OF UNIT
GRADE E48
KPM KOLEJ PROFESIONAL MARA
KM KOLEJ MARA
PMLN PEJABAT MARA LUAR NEGARA
AKM AKADEMI KECEMERLANGAN MARA
MRSM MAKTAB RENDAH SAINS MARA
PUSKEP PUSAT KEPIMPINAN PELAJAR MARA
KKTM KOLEJ KEMAHIRAN TINGGI MARA
MJII MARA-JAPAN INDUSTRIAL INSTITUTE
IKM INSTITUT KEMAHIRAN MARA
KELANTAN MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
SARAWAK MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
SABAH MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
KEDAH MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
SELANGOR MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
JOHOR MARA STATE OFFICE
DIRECTOR
JUSA C (VU7)(E)
PAHANG MARA STATE OFFICE
DIRECTOR
GRADE E54
PERAK MARA STATE OFFICE
DIRECTOR
GRADE E54
PULAU PINANG MARA STATE OFFICE
DIRECTOR
GRADE E48/E52
WILAYAH PERSEKUTUAN MARA STATE OFFICE
DIRECTOR
GRADE E48/E52
TERENGGANU MARA STATE OFFICE
DIRECTOR
GRADE E48/E52
MELAKA MARA STATE OFFICE
DIRECTOR
GRADE E48/E52
NEGERI SEMBILAN MARA STATE OFFICE
DIRECTOR
GRADE E48/E52
PERLIS MARA STATE OFFICE
DIRECTOR
GRADE E52

Last Updated :13/5/2024

1.3 General Details of the Company

DETAILS	
Organization Name	Majlis Amanah Rakyat (MARA)
Headquarter Location	Jalan MARA, Kuala Lumpur
Plan Effective Date	Not publicly disclosed
Plan Revision Date	Subject to periodic review and updates
Plan Owner	Risk Management and Inspectorate Division (BPIN) • DRP Contributor: Not publicly disclosed

2.0 Risk Assessment / Disaster Definition

2.1 Threats Identification

The primary threats to MARA’s ICT operations for the MyEduloan Portal and e-Baki MARA systems include:

- Data center failure
- Backup system failure
- Cybersecurity threats
- Network failures
- Software failures
- Natural disasters

2.2 Threats Attributes

Threat	Description	Severity	Likelihood
Data center failure	The complete or partial shutdown of a data center due to power outages, hardware malfunctions, or other infrastructure issues. It can lead to loss of access to data and services hosted within the data center.	High	Likely
Backup system failure	If the backup system fails or isn't properly maintained, data recovery could be compromised during an outage or data loss event.	High	Likely
Cybersecurity threats	These include a wide range of malicious activities such as hacking, malware, phishing, and ransomware attacks aimed at stealing, disrupting, or compromising data and systems.	High	Almost certain
Network failures	Disrupt communication and data transfer between devices, servers, or locations.	Medium	Likely
Software failures	Software failures can occur due to bugs, coding errors, compatibility issues, or inadequate testing. These failures may cause applications to crash or behave unexpectedly, impacting productivity and data integrity.	High	Likely
Natural disasters	Events such as earthquakes, floods, hurricanes, fires, or tornadoes can physically damage data centers, servers, and infrastructure.	Very high	Rare

2.3 Risk Assessment

Based on the identified threats and their attributes, MARA assesses risks using severity and likelihood criteria to prioritize mitigation efforts and ensure preparedness.

MARA's BPIN division utilizes two approaches: Asset-based Risk Assessment for ISO/IEC 27001:2022 certification and Operational Risk Management (handled by BPIN).

Asset-based Risk Assessment		
Threat	**Severity Attributes**	**Description**
Data center failure	High	Potential for significant disruption and impact.
Backup system failure	High	Potential for significant disruption and impact.
Cybersecurity threats	High	Potential for significant disruption and impact.
Network failures	Medium	Moderate disruption with manageable impact.
Software failures	High	Potential for significant disruption and impact.
Natural disasters	Very high	High potential for significant disruption and impact.

Operational Risk Assessment		
Threat	**Likelihood Attributes**	**Description**
Data center failure	Likely	Will probably occurs in most circumstances.
Backup system failure	Likely	Will probably occurs in most circumstances.
Cybersecurity threats	Almost certain	Is expected to occur in most circumstances.
Network failures	Likely	Will probably occurs in most circumstances.
Software failures	Likely	Will probably occurs in most circumstances.
Natural disasters	Rare	May occur only in exceptional circumstances.

3.0 Business Impact Analysis

3.1 Critical Processes Supported by TESP

The Tertiary Education Sponsorship Programme (TESP) relies on critical processes facilitated by the MyEduloan Portal and e-Baki MARA to ensure seamless educational funding for Bumiputra students pursuing diploma and degree-level education.

1) MyEduloan Portal
    - Loan application submission
    - Loan application review and approval
2) e-Baki MARA
    - Balance inquiries
    - Loan statement generation
    - Loan record management
    - Loan repayment processing

These processes include:

Business Process	Criticality	Comment	Recovery Time Objective (RTO)	Recovery Point Objective (RPO)	Work Recovery Time (WRT)	Maximum Tolerable Downtime (MTD)
Processing new loan applications	Mission-critical	Students cannot apply for loans if MyEduloan Portal is down	4 hours	1 hour	4 hours	8 hours
Reviewing and approving loan applications	Mission-critical	Applications cannot be reviewed or approved without portal access	6 hours	1 hour	6 hours	12 hours
Generating loan statements	Mission-critical	Students cannot access loan statements if e-Baki MARA is down	4 hours	1 hour	4 hours	8 hours
Managing loan repayments	Mission-critical	Repayments cannot be processed without e-Baki MARA access	6 hours	1 hour	6 hours	12 hours
Updating loan records	Mission-critical	Critical for maintaining accurate financial records	4 hours	1 hour	4 hours	8 hours
Handling inquiries and support requests	Important	Increased support workload during downtime	8 hours	2 hours	8 hours	16 hours
Communicating with stakeholders	Important	Impaired communication channels	8 hours	2 hours	8 hours	16 hours
Managing financial data and reporting	Important	Data management and reporting affected by downtime	6 hours	2 hours	6 hours	12 hours

Notes:

- **Criticality:** Indicates the importance of each process to the TESP operation.
- **Availability Requirements:** Ensures continuous availability to meet operational needs.
- **RTO:** The maximum acceptable downtime for each process before service restoration is achieved.
- **RPO:** The acceptable data loss window in case of disruption.
- **WRT:** The time required to complete the necessary work to restore normal operations after service restoration.
- **MTD:** The maximum tolerable duration of a disruption before significant impacts are encountered.

3.2 Availability Requirements

The availability requirements for each critical process are outlined based on their criticality:

- Mission-critical processes require near-real-time availability to ensure continuous service delivery and minimal disruption to students.
- Important processes have slightly more flexibility in terms of downtime but still require timely availability to maintain operational efficiency.

Business Process	Availability Requirements
Processing new loan applications	24/7 availability with minimal downtime
Reviewing and approving loan applications	24/7 availability with minimal downtime
Generating loan statements	24/7 availability with minimal downtime
Managing loan repayments	24/7 availability with minimal downtime
Updating loan records	24/7 availability with minimal downtime
Handling inquiries and support requests	Monday to Friday, during business hours
Communicating with stakeholders	Monday to Friday, during business hours
Managing financial data and reporting	Monday to Friday, during business hours

3.3 Impact Analysis of Critical Processes

Financial Impact Analysis

The financial impact analysis is crucial for understanding the potential monetary consequences of disruptions to critical business processes within MARA's TESP:

Business Function	Business Process	Comment
Loan Processing	Processing new loan applications	Significant impact on students' access to funding, potentially delaying educational pursuits.
	Reviewing and approving loan applications	Delays in processing applications may lead to delayed disbursement of funds to students.
Loan Management	Generating loan statements	Delays in generating statements could hinder financial planning for students.
	Managing loan repayments	Inability to process repayments may result in penalties or interest accruals for students.
	Updating loan records	Critical for maintaining accurate financial records and ensuring compliance.
Communication and Support	Handling inquiries and support requests	Increased workload and potential complaints could strain operational resources.
	Communicating with stakeholders	Maintains stakeholder relations and ensures transparency in communication channels.
Data Management	Managing financial data and reporting	Risks of data loss or corruption could affect financial reporting accuracy and compliance.

<u>Operational Impact Analysis</u>

The operational impact analysis focuses on the broader operational consequences of disruptions:

Business Function	Business Process	Comment
Loan Processing	Processing new loan applications	Students cannot apply for loans, affecting service delivery and customer satisfaction.
	Reviewing and approving loan applications	Application processing halts, impacting workflow and service timelines.
Loan Management	Generating loan statements	Inability to access statements affects financial planning and customer service.
	Managing loan repayments	Delays or inability to process repayments affect financial operations and customer relations.
	Updating loan records	Critical for maintaining accurate financial records and ensuring compliance.
Communication and Support	Handling inquiries and support requests	Increased workload and potential complaints could strain operational resources.
	Communicating with stakeholders	Maintains stakeholder relations and ensures transparency in communication channels.
Data Management	Managing financial data and reporting	Data integrity issues affect reporting and compliance efforts.

4.0 Mitigation Strategy Development

4.1 Steps to Reduce Adverse Effects

The table below categorizes the steps taken by MARA to mitigate the impact of identified IT threats on the MyEduloan Portal and e-Baki MARA systems. It relates each step to specific threats and explains how these measures reduce adverse effects.

Threat Category	Identified Threat	Mitigation Step	Description	Mitigation Type
Hardware/Software Failure	Data Center Failures	Maintenance Contracts	Ensure maintenance contracts are in place to keep data center facilities operating reliably.	Risk Limitation
		Regular Maintenance Checks	Perform regular maintenance checks and updates to prevent failures and ensure continuous operation.	Risk Limitation
Data Loss	System Outages	Daily Backups	Conduct daily backups to minimize potential data loss.	Risk Limitation
		Differential Backups	Use differential backups to meet the Maximum Tolerable Downtime (MTD) at a lower cost.	Risk Limitation
Cyber Threats	Cybersecurity Breaches	Compliance with MARA Cyber Security Plan v3.0	Ensure compliance with the MARA Cyber Security Plan v3.0 to maintain robust security protocols.	Risk Avoidance
		Annual ISO/IEC 27001:2022 Certification	Maintain annual ISO/IEC 27001:2022 certification for the MyEduloan system to ensure organizational, human, physical, and technological controls.	Risk Avoidance
Network Disruptions	Network Failures	Redundancy in Network Connectivity	Ensure redundancy in network connectivity to limit the impact of network failures.	Risk Limitation
General IT Threats	System Vulnerabilities	Regular Security Audits and Updates	Conduct regular security audits and updates to mitigate vulnerabilities.	Risk Limitation
Service Disruptions	Incident Response	Develop and Regularly Update an Incident Response Plan	Develop and regularly update an incident response plan outlining procedures for addressing IT disruptions.	Risk Limitation
Operational Failures	Inadequate Support Systems	Regular Training and Simulations for Incident Response	Conduct tabletop exercises and simulations to test the effectiveness of the incident response plan.	Risk Limitation

5.0 Plan Development

5.1 Plan that use to response / activate the BCP.

The organization uses a Disaster Recovery Plan consisting of three phases:

- **Activation Phase**
  Aims to determine the level of damage and activate the plan.
- **Recovery Phase**
  Aims to restore critical application systems at alternative sites.
- **Reconstruction Phase**
  Aims to test and validate the application system critical can re-operate at the main site.

5.2 BC/DR teams

The BC/DR teams consist of every representative from listed group below:

- **Application Team**
- **Database Team**
- **Network Team**
- **MARA Data Center Team**
- **Cyber Security Governance Team**
- **Procurement Team**
- **Contract Admin**

Each representative supports the key personnel in executing their responsibilities during BCP activation and recovery operations.

5.3 Key Personnel

A designated coordinator leads the BC/DR teams and oversees plan activation, communication, and recovery activities.

6.0 Training and Testing

6.1 Training Method for the BCP

Effective training is essential; to ensure that all team members are prepared to execute the Business Continuity Plan (BCP) efficiently in the event of a disruption. MARA’s training program for the BCP includes the following components:

- **Regular Training Sessions**
    - ➢ The Disaster Recovery Planning (DRP) documentation is distributed to all relevant teams. Regular training sessions are conducted to ensure that team members are familiar with their roles and responsibilities during an incident or disaster. These sessions are designed to reinforce the procedures outlined in the BCP and to build confidence in executing the plan.
- **Workshops and Seminars**
    - ➢ Interactive workshops and seminars are organized to provide hands-on experience with the BCP. These sessions often include guest speakers or experts who can provide additional insights and best practices.

6.2 Testing Methods to Test the BCP

Testing the BCP is crucial to ensure its effectiveness and to identify areas for improvement. MARA employs several testing methods to validate the BCP:

- **Team Call Tree**
    - ➢ This is a communication strategy used during BCP activations. The team call tree ensures efficient dissemination of critical information to key staff members. It involves creating a hierarchical phone tree where each team member is responsible for notifying others in their designated group. This method is tested regularly to ensure quick and effective communication in case of a disruption.
- **Desktop Walkthrough**
    - ➢ A desktop walkthrough involves reviewing the BCP through a series of hypothetical scenarios. Scenarios are displayed one by one, and participants discuss the questions posed after reviewing the BCP. This method helps to familiarize team members with the BCP in a low-pressure setting and allows for discussion and feedback on the plan's effectiveness.
- **Scenario-Based Simulations**
    - ➢ These simulations create realistic threat scenarios to test the continuity plan's effectiveness. They introduce stress levels that challenge both the plan and participants in a robust and meaningful way. Scenario-based simulations help to identify weaknesses in the BCP and improve team coordination and response strategies.

7.0 Maintenance and Improvement

MARA ensures that the Business Continuity Plan (BCP) remains up to date with evolving IT threats and technologies by continuously reviewing and updating continuity procedures. This process involves regular revisions whenever there are changes in organizational structure, technology advancements, or regulatory requirements. By doing so, MARA ensures that their BCP is aligned with the latest developments and can effectively address any emerging challenges in the IT landscape.

MARA also engages in ongoing staff training and awareness programs to ensure that all employees are familiar with the latest protocols and procedures outlined in the BCP. By regularly conducting drills and simulations, MARA ensures that staff are well-prepared to respond effectively in the event of a disaster, thereby minimizing downtime and ensuring business continuity. This proactive approach helps to embed a culture of preparedness and resilience within the organization.

8.0 Conclusions

Majlis Amanah Rakyat (MARA) has developed a robust Business Continuity Plan (BCP) tailored to safeguard its critical operations, particularly focused on the Tertiary Education Sponsorship Programme (TESP). Recognizing the vital role of the MyEduloan Portal and e-Baki MARA systems in supporting Bumiputra students, MARA has meticulously identified potential risks such as data center failures, cybersecurity threats, and natural disasters.

Through a comprehensive risk assessment, MARA prioritizes mitigation strategies that include regular maintenance, backup protocols, cybersecurity compliance, and network redundancy. These measures aim to ensure near-real-time availability of mission-critical processes and minimize disruptions to student funding and administrative services.

Moreover, MARA emphasizes continuous improvement by regularly updating its BCP to align with evolving IT threats and technological advancements. Ongoing staff training and simulation exercises further reinforce readiness across the organization, fostering a culture of preparedness and resilience.

By implementing these proactive measures and maintaining a strategic focus on risk management, MARA demonstrates its commitment to ensuring uninterrupted support for Bumiputra students pursuing higher education, even amidst potential challenges.