Deanship of Information Technology

Al-Imam Muhammad Ibn Saud Islamic University Riyadh

BCMS Manual

DIT-BCM-MAN-001-01

Document Control

Version History

Version	Description of Amendment	Reason for Amendment	New Revision No and Effective Date	Amendment done by	Approved by
V0.1	Ahmad Khalil	Initial draft 1.0	AK	MA	V0.1
V1.0	Mansour Ahmad	Version 01	1.0	MA	MA

Approval

Approved by	Position	Date	Signature
ABDULMAJEED M. ALOUMI	Quality assurance administration manager	18/10/2016	
DR. WALEED AL JANDAL	Dean of IT deanship	18/10/2016	

Table of Contents

1. Introduction

Al-Imam Muhammad Ibn Saud University recognizes and acknowledges that the protection of its assets, business operations, and services is a major responsibility to safeguard the interests of its stakeholders. As part of a national initiative to automate and provide accessible services to its students, faculty, and employees, the University seeks to establish a viable plan for the recovery and continuity of its electronic services (e-services) in case of disasters.

Al-Imam Muhammad Ibn Saud University is committed to supporting resumption and recovery efforts at alternate facilities, if required. The University and its management are responsible for developing and maintaining a viable continuity & recovery plan that conforms to acceptable insurance and ethical practices, and is consistent with the provisions and direction of the University's strategic and tactical plans. The plan will also support the philosophy of providing and maintaining the highest quality of services to its students, faculty, and staff.

The Deanship of Information Technology has been established in 1430 to manage the technology and e-services at the university.

The vision of the Deanship of IT is "to enable Al Imam University to be the pioneer in the field of electronic services through the creation of a distinct integrated environment for information technology"

The mission statement is "Improving the services offered by the University and provide an environment of high-quality electronic services that are based on information and communication technology in line with the Kingdom of Saudi Arabia strategies to operationalize the concept of e-government in all public universities deanships"

The main objectives of the Deanship of information technology:

- Hire the best global practices and information systems and IT tools to increase efficiency and effectiveness in the administration and regulation, as well as alignment with the e-government.
- Promote the use of information technology solutions to support the policies, processes and procedures that increase the accountability, transparency and responsibility in all functions within the university.
- Enhance the Infrastructure and IT tools that support the faculty for excellence in teaching and research development.
- Enhance the Infrastructure and IT tools that support students to develop academic success.

2. Purpose

The purpose of this document is to define and develop the Business Continuity Management Framework and Business Continuity structure in order to improve organizational resilience in alignment with business strategy by managing, operating and controlling the Business Continuity Management Systems (BCMS) of Al-Imam Muhammad Ibn Saud University Riyadh – Deanship of Information Technology (IMSIU IT), aligned with international ISO 22301 standard requirements.

3. Scope

This document applies to all components and phases of the Business Continuity Management System.

IMSIU IT's Business Continuity Management System covers the following scope and boundaries:

- All employees (permanent and contractual employees).
- All divisions / sections under the Deanship of IT
- Critical business processes for the above business units/divisions.
- Infrastructure and facilities at IMSIU IT Riyadh offices

4. Context of the Organization

The Deanship of Information Technology has been established in 1430 to manage the technology and e-services at the university.

The vision of the Deanship of IT is "to enable Al Imam University to be the pioneer in the field of electronic services through the creation of a distinct integrated environment for information technology"

The mission statement is "Improving the services offered by the University and provide an environment of high-quality electronic services that are based on information and communication technology in line with the Kingdom of Saudi Arabia strategies to operationalize the concept of e-government in all public universities deanships"

4.1. Understanding the Needs and Expectations of Interested Parties

4.1.1. General

For more details refer to "Context of Organization" Document.

4.1.2. Legal and Regulatory Requirements

IMSIU IT has identified key legal and regulatory requirements that impact the BCMS as documented below:

- Government regulations of KSA
- Contractual requirements
- ISO 27001 requirements and guidelines

4.2. Determining the Scope of the Business Continuity Management Systems

4.2.1. Scope of the BCM

For detailed scope of the BCM refer to the section 3 of this BCM Manual document.

4.2.2. Scope Exclusion

None

5. Leadership and Commitment

5.1 Leadership

IMSIU IT senior management demonstrate their commitment to the BCM system by encouraging the resources to participate in the activities needed to design, implement, operate, assess and improve the BCM. Senior Management of IMSIU IT and other relevant management roles throughout the organization shall demonstrate leadership with respect to the BCM. This includes

- **Dean** who is the Sponsor of IMSIU IT's Business Continuity Management Systems. The Dean will be the approver for all decisions taken pertaining to implementation of BCM at IMSIU IT.
- **IMSIU IT Undersecretaries and Departments Heads** – Understand and validate critical products and services of each sector. As part of decision making team, provide inputs to the Dean/ Deputy Dean during crisis.

5.2 Management Commitment

Senior management of IMSIU IT demonstrates leadership and commitment for BCM by:

- Ensuring that IMSIU IT BCM policies and objectives are established and are aligned with the strategic direction and business objectives of IMSIU IT.
- Ensuring the integration of IMSIU IT BCM into its business processes.
- Ensuring that the resources needed for the business continuity management system are available.
- Communicating the importance of effective business continuity management and conforming to the BCM requirements.
- Communicate the BCM policy widely throughout the organization.
- Ensuring that the BCM achieves its intended outcome(s).
- Directing and supporting persons to contribute to the effectiveness of the BCM.
- Promoting continual improvement.
- Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

To achieve its commitment establishment, implementation, operation, monitoring, review, maintenance, and improvement of the BCM, IMSIU IT senior management is planning to undertake the following initiatives:

- Establishment of the BCM Steering Committee at IMSIU IT.
- Definition of the roles and responsibilities of Business Continuity Manager and the BCM Core Team.
- Appointing a functional recovery coordinator at each Department/ unit of IMSIU IT. The roles and responsibilities of the Functional Recovery Coordinators have been defined in the IMSIU IT's Business Continuity Plan Document.
- Implementing the IMSIU IT's Business Continuity Plan (BCP) comprising Incident Response Plan (IRP), Crisis Management Plan (CMP), Functional Recovery Plan (FRP) and the supporting procedures.
- Implementing the identified Key Performance Indicators for IMSIU IT to determine whether BCM goals have been achieved.

- Training of select BCM core team members to achieve the ISO 22301 Internal/ Lead Auditor certification.
- Further, periodic internal audit scope will cover operations of BCM across the IMSIU IT.

5.3 BCM Policy

IMSIU IT has defined and developed a Business Continuity Management Policy showing IMSIU IT management's intent.

The policy will be:

- Communicated within the organization,
- Stored on the IMSIU IT intranet and made available to interested parties, as appropriate,
- Reviewed annually for continuing suitability or when significant changes occur.

Refer to Document: IMSIU IT Business Continuity Management Policy for further details.

BCMS Policy

The Deanship of Information Technology at Al-Imam Muhammad Ibn Saud University Riyadh plays a fundamental role in providing Stakeholders and customers of the university as well as internal deanships and departments with the best-in-class information technology services and specialized solutions as well as managing available resources efficiently.

Being at this position, the Deanship of Information Technology recognizes, and is fully committed to provide a continuous service to its' customers and to protect the interests of stakeholders that collectively ensure the viability of the Deanship of Information Technology. Deanship of Information Technology is also committed to meeting all applicable legal and regulatory obligations, Federal requirements as well as directives from concerned official government bodies.

The Business Continuity Management System (BCMS) applies to all units, functions, processes or business elements that are considered critical, shall have a recovery plan for its operations within an agreed strategy.

Therefore, as an integral part of the business, Deanship of Information Technology adopts the following reactive and proactive approaches to minimize the effects of any major incident:

- Ensure that all prioritized processes and services of IMSIU IT departments have an updated business continuity plan/ functional recovery plan or processes in place to protect them

- Develop business recovery strategies and plans to mitigate major risks,

- Provide training in Business continuity for key resources (FRP coordinators, BCM core team)

- Prepare testing and audit plans, and conduct rehearsals to provide confidence that people are aware of their roles, and the processes to deliver their objectives,

- Continually improve the suitability, adequacy and effectiveness of the business continuity management system.

This policy is based on the "Business Continuity Management standard and guide" issued by the "International Organization for Standardization" ISO 22301 - Societal Security – Business Continuity Management System – Requirements.

This policy shall be communicated to all employees of the Deanship of Information Technology at Al-Imam Muhammad Ibn Saud University Riyadh. All individuals in the Deanship must comply with this policy as applicable to them. Each directorate/sector/department is responsible for its own BCM preparedness at all times.

This policy shall be reviewed for continuous suitability on an annual basis & when significant changes occur

5.4 Organizational Roles, Responsibilities and Authorities

IMSIU IT has established roles and responsibilities for BCM process and authorities. Relevant roles will be assigned and communicated within IMSIU IT through workshops and meetings.

Following are the high level roles and responsibilities of the different teams identified for the University's BCM Governance Model.

5.4.1. Crisis Management Team

The Crisis Management Team (CMT) is comprised of the University's Senior Leadership, with a primary role of directing recovery operations at time of disasters.

In case the incident is classified as a crisis/disaster, the CMT is in charge of formally declaring a disaster, invoking the continuity plans, and overseeing all recovery efforts during this disaster. The CMT will be supported by BCM Team for recovery co-ordination. The CMT would command the resources needed to recover the University's operations during a disaster.

5.4.2. Emergency Response and Damage Assessment Team

The Emergency Response and Damage Assessment team is responsible for evacuating the site in case required, assessing the tangible impact to the affected facility as a whole including any equipment in the building's computer and network rooms, issuing a preliminary report, and making recommendations to the Crisis Management Team. The team shall;

- Respond to disaster at Crisis Management Team direction;
- Evacuate the premises in case of fire, explosion and any other disaster that makes it unsafe for people to be within the premises;
- Take count of people evacuated and provide details to the Evacuation Team Leader;
- Contact and/or cooperate with local authorities and insurance agents as needed;
- Determine the nature and extent of damage, and an estimated time to repair, restore, or replace;
- Take measures to protect undamaged and salvageable equipment;
- Determine if affected area is safe for employees/students in conjunction with local authorities; and
- Produce damage report and deliver it to Crisis Management Team leader with recommendations.

5.4.3. Business Continuity Management Team

Al-Imam Muhammad Ibn Saud University will have a BCM team who will ensure proper coordination of Business Continuity activities within the University. The BCM Team shall:

- Facilitate BIA reviews with individual relevant Units/ Functions; and conduct risk assessment for the University in coordination with the concerned departments / functions (e.g. Information Technology, Services, Risk);
- Coordinate review of continuity plans and any related issues with the relevant Units / Functions; however, it is the responsibility of these individual Units to ensure that their plans are kept updated at all times, and that the continuity-related issues of their individual areas are highlighted and resolved in a timely manner;

- Co-ordinate, communicate and provide effective oversight of contingency matters within the University. They will review and conclude on the reasonableness of test plans, test results and publish the results to the senior management on an ongoing basis; and
- When continuity plans are invoked;
    - Receive notification when there is a contingency situation and initiates the process flow;
    - Utilize the continuity & recovery plan to establish priorities when assigning recovery resources once the plan is invoked; and
    - Coordinate, monitor, and report on recovery arrangements with support from Business and IT recovery teams.

5.4.4. Business Recovery Teams

This team comprises of the business/ functional owners of the continuity & recovery plans; and they must have the remit and authority to implement the following responsibilities:

- Conduct BIA for their areas at least once in two years or when any material changes occur in the business;
- Own the continuity & recovery plans related to their area and review them regularly to ensure they are up to date and fit for purpose;
- Embed BCM as an integral part of their day-to-day business operations, and ensure appropriate resource and funding is made available to run the process and to support business recovery requirements;
- Ensure appropriate provision is put in place to support recovery requirements or escalate via BCM team;
- Participate in BCM validation activities and provide sign-off on results and remedial actions and associated costs;
- Confirm that recovery capability supports business requirements or that there are plans in place to address the gaps;
- Ensure that all their employees are aware of their continuity/ recovery and incident management roles and responsibilities; and
- Coordinate recovery efforts for their areas with BCM team during an incident and report progress.

5.4.5. IT Recovery Teams

IT Disaster Recovery team will work under leadership of the University's IT Head and would be primarily responsible for recovering the IT systems during a disaster. The IT Disaster Recovery Team would consist of the following:

- IT DRP Team Leader/ DR Champion;
- Data Center Operators Team;
- Backup Recovery Team;
- Network & Communications Team;
- Software Team;
- Hardware Team; and
- Users & Support Recovery Team.

The IT DRP team leader/ DR Champion is responsible for the overall IT disaster recovery efforts, and acts as the point of contact and escalation for communication between the IT DRP teams and other business recovery teams. The responsibilities of the IT DRP Team Leader include:

- Providing immediate notification of disaster declaration to Recovery Team;
- Coordinating all Recovery Teams;
- Managing and monitoring the overall IT disaster recovery process;
- Reporting to BCM Team Leader on the status of recovery effort; and
- Continuing to provide support services to business users at the disaster recovery location.

6.0 Planning

6.1 Actions to Address Risk and Opportunities

When planning for the BCM, IMSIU IT has considered the risks referred to in IMSIU IT's Risk Assessment Report and IMSIU IT's Business Continuity Strategy documents that need to be addressed to:

- Ensure the management system can achieve its intended outcome(s),
- Prevent, or reduce, undesired effects,
- Achieve continual improvement.

Risk Assessment process establishes the risk context, identifies, analyzes and evaluates risks which affect the continuity of the organization.

On the basis of identified risks, IMSIU IT has developed and implemented actions to address these risks. These include controls across the organization's Policies and Procedures, Physical and logical controls, monitoring and reviews to minimize the risk to an acceptable level in the organization.

On basis of identified risks, risk treatment plans have been developed in accordance to the risk identified.

The outcomes of the risk treatment plans will be monitored and evaluated for its effectiveness of these controls.

6.2 Business Continuity Objectives and Plans to Achieve Them

IMSIU IT has developed business continuity objectives in the following area:

- Quality
- Capability
- Risk monitoring

Ref.	Area	Objective	Task	Measurement Method	Target	Timescale	Person responsible
1	Quality	Ensure that all prioritized processes and services of IMSIU IT departments have an updated business continuity plan/ functional recovery plan or processes in place to protect them	Hold workshop to define / review and update the Business continuity plan, crisis management plan, functional recovery plan and processes	Percentage of IMSIU IT processes and services with a plan and processes (BCP / CMP / FRP)	100%	12 months	Business Continuity Manager
2		Prepare testing and audit plans, and conduct rehearsals to provide confidence that people are aware of their roles, and the processes to deliver their objectives	Agreed test schedule with senior management and perform the tests. Results of the tests are communicated to BC Manager	Percentage of plans tested within 2 years	100%	24 months	Business Continuity Manager
3	Capability	Provide training in Business continuity for key resources (FRP coordinators, BCM core team)	Identify courses; secure budget	Number of trained people	20 people	12 months	Business Continuity Manager / HR Division
4	Risk monitoring	Develop business recovery strategies and plans to mitigate major risks	Hold workshop to review risk	Number of risk reviews done per year	4	12 months	Business Continuity Manager/Risk Management

Achievement against these objectives and the plan are tracked and evaluated as part of regular management reviews of BCM.

7.0 Support

7.1 Resources

IMSIU IT has identified and documented the resources needed for the establishment, implementation, maintenance and continual improvement of the BCM in section 5.4 Organizational Roles and Responsibilities of the IMSIU IT BCM Manual.

7.2 Competence

The below table provides the competency requirements for key BCM resources:

BCM roles	BCM awareness level required (High/ Medium/ Low)	BCM knowledge required	Method of achieving competency level	Competency evaluation	Maintenance of competency level
Business Continuity Sponsor: • **Dean (Incident Commander)** • **Deputy (Deputy Incident Commander)**	Medium	• General awareness and understanding of business continuity management and the BCM. • The aims and objectives and the need for top management support for the policy.	Internal awareness provided by the BC manager	Demonstrated through their ongoing support and input to the BCM via management reviews or attending key meetings	Periodical review of BC Policy and other BCM documentation – possible through management review meetings Involvement in BC exercise
Business Continuity Management Functional Coordinators	Medium	• General awareness of what a BCM contains. • Practical knowledge of how a Business Impact Analysis (BIA) is developed and what is required. The ability to assess the contents of a BIA and to know what is reasonable. • Good working knowledge of the	• Training from the BC Manager or from an external training provider • Work experience	• Review of BIA content • BC Manager tests the accuracy of the information provided and how it links with the plan. • Test assumptions made through exercising the plans	• Periodical review of BIA's Refresher BCM training as appropriate

BCM roles	BCM awareness level required (High/ Medium/ Low)	BCM knowledge required	Method of achieving competency level	Competency evaluation	Maintenance of competency level
		business and its activities.			
BC Manager	High	• Comprehensive knowledge of ISO 22301 requirements and management systems in general • BCM technical knowledge	• Attend professional training courses addressing ISO 22301, BCM requirements • Dependent on previous work experience • Training or on the job learning	• Practical results of implementing BCM arrangements, through the results of the exercise, invocations etc. • Results of exercises and lessons learned	• Attend standard update events • Network with other BC managers across organizations • Practical work experience • Successful results of external audits
Internal Auditor	Medium	• Auditor qualification in BCM standard or other management systems with additional training for business continuity elements • Thorough knowledge of relevant BCM standard, requirements and examples of evidence. • Ability to know when a BCM system is effective	• Attend formal BCM training course (or use existing management systems qualification and attend transition course for BCM) • Undertake a number of internal BCM audits under supervision (if appropriate)	• Review of audit report to ascertain depth of knowledge, findings raised and general auditing skills	• Undertake refresher standard training as appropriate • Undertake periodic internal audits • Results of external audits do not identify many findings

7.3 Awareness

IMSIU IT has undertaken to develop appropriate BCM awareness program and material and a plan for building awareness within its organization. These cover information related to:

- Identifying and recognizing an incident.
- Understanding relevant business continuity plans.
- The business continuity policy.
- Contribution to the effectiveness of the BCM, including the benefits of improved business continuity management performance.
- The implications of not conforming with the BCM requirements, and
- Specific roles during disruptive incidents.

7.4 Communication

The IMSIU IT has determined the need for internal and external communications relevant to the BCM, which covers

- What it will communicate,
- When to communicate,
- With whom to communicate.
- How to communicate

These are documented as a part of the IMSIU IT's BCM Plan document.

Further, IMSIU IT has established, implemented, and maintained the following processes and procedures handling the internal and external communication during normal operations as well as during a crisis:

- **Management of Press Releases**

  This process describes the activities to be performed to manage the issue of a press release on behalf of The University. The process identifies the required activities which must be performed in order to ensure that Press Releases are clearly structured, serve to maintain The University's reputation and represent The University in the best possible light.

- **Management of Digital and Social Media**

  This process describes the activities which must be performed in order to post information on The University's website and/or on The University's social media sites. It is designed to ensure that the digital content which is published by The University meets branding standards and provide a consistent message and tone. The process involves obtaining information from the business unit and then ensuring that the information meets The University's standards before arranging for it to be made available in the relevant digital media. Effectively managing digital content will also serve to enhance The University's reputation and to help establish new business and customer relationships.

- **Management of Crisis Communication**

  This process describes the activities to be executed in the event of a crisis which affects The University's operations and image either directly or indirectly. Alternately, the process can be executed when a crisis affecting Riyadh city occurs and the University has an active role to play in managing the crisis

- **Management of Internal Communication**

  This process describes the activities to be performed in order for Communication's unit to issue Internal Communications on behalf of a specific business unit within The University to an audience within The University. This can include issuing The University's announcements or any division specific news which it wishes to share with a larger audience. The process involves receiving the necessary information and then determining the most appropriate medium to use to communicate this information within The University. This can include holding workshops or meetings, or preparing bulletins or emails as per The University's standards.

- **Management of Stakeholder Interactions**

  This process describes the activities to be performed in order for Communication's unit to manage Stakeholder Interactions.

7.5 Documented information

7.5.1. General

The Deanship of IT's BCMS shall include

- Documented information required by this International Standard, this include but not limited to, BCMS policy, manual, BIA, Risk registers, communication procedures…etc.
- Documented information determined by the organization as being necessary for the effectiveness of the BCMS such as Information security management system documents.

7.5.2. Creating and updating

When creating and updating documented information, The Deanship of IT shall ensure appropriate

- Identification and description (e.g. a title, date, author or reference number),
- Format (e.g. language, software version, graphics) and media (e.g. paper, electronic), and review and approval for suitability and adequacy.

7.5.3. Control of documented information

Documented information required by the BCMS and by this International Standard shall be controlled to ensure

- It is available and suitable for use, where and when it is needed,
- It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, The Deanship of IT shall address the following activities for all documents, as applicable

- Distribution, access, retrieval and use,
- Storage and preservation, including preservation of legibility,
- Control of changes (e.g. version control),
- Retention and disposition
- Retrieval and use,
- Preservation of legibility (i.e. clear enough to read), and
- Prevention of the unintended use of obsolete information.

7.5.4. Documents coding

Every document should be assigned a document code, the code system consists of 13-digits code as follows:

AAA-BBB-CCC-DDD-EE

AAA: Department/ Section Code

BBB: International Standard

CCC: Document Type

DDD: Serial No. starting from 01 for each section

EE: Revision No. like 01, 02, 03

For the Departments name, the Deanship of IT assigned the code DIT. The international standard is the business continuity management system BCM.

For the Document Type use the below list:

Document Type	**Code**	**Document Type**	**Code**
Manual	MAN	Report	ROT
Policy	POL	Key Performance Indicators	KPI
Procedure	PRE	Job Description	JDN
Guideline	GLN	Memo	MEM
Work Instructions	WOI	Letter	LTR
Strategy	STY	Brochure/ Pamphlet	BPT
Form	FOR	Drawing	DRW
Template	TEM	List	LST
Newsletter	NEL		

8.0 Operations

8.1 Business Impact Analysis and Risk Assessment

8.1.1. General

IMSIU IT has developed the IMSIU IT Business Impact Analysis and the Risk Assessment for the BCM. Additional details are available in the following sub-sections of this manual.

8.1.2. Business Impact Analysis

Business Impact Analysis (BIA) is the process of analyzing business activities and the impacts that a business disruption might have on them. It provides information from which relevant strategies for continuity are determined. Overall we executed the business impact analysis in three phases Initiate, Assess and Analyze. Details about activities undertaken in each phase are:

- **Initiate**
  - Define objectives
  - Identify divisions, sections, locations of IMSIU IT in scope
  - Identify Business Units (BU) in charge for each sections, divisions
- **Assess**
  - Conduct Interviews, Workshops with senior management and BU in charge
  - Identifying prioritized services, business processes, activities and support activities
  - Assess potential impacts to IMSIU IT services
- **Analyze**
  - Validation of information gathering in BIA process
  - Summarize process recovery priorities across BU's
  - Developing outcomes of BIA
  - Obtaining senior management's endorsement

8.1.3. Risk Assessment

Risk Assessment (RA) is a detailed and a comprehensive assessment of threats and vulnerabilities applicable to IMSIU IT. A Risk Assessment is required to identify a wide range of threats and the likelihood of their occurrence to gauge the risk level. RA process is the process in which risks is identified, analyzed and evaluated. The section below illustrates the steps of the RA Methodology:

- **Risk Identification**
  - Identify risks / threats that can disrupt performance of prioritized activities.

  - Perform risk identification based on outcomes of BIA through interviews, site visits, process reviews

- **Risk Analysis**
  - Analyze the identified risks based on their impact and likelihood to assess their severity to ensure that the most important risks are treated first.
- **Risk Evaluation**
  - Compare the results of the risk analysis with predefined risk criteria to determine whether a risk is acceptable or needs risk treatment.
  - Risk assessment criteria are determined on basis of business impact and likelihood and agreed with the management.
- **Risk Acceptance**
  - Risk value can range from catastrophic (Very high) to no action required (Very low).
  - Risk treatment plan to be developed to consider cost / benefit of implementation, practicable solutions for implementation, legal implications etc.

8.2 Business Continuity Strategy

8.2.1. Determination and Selection

Developing business continuity strategies is a process which involves, deriving the recovery methods out of the Business Impact Analysis (BIA) and Risk Assessment (RA) activities. Such a method will be consistent with the requirements of business and will tend to address the risks that can have an impact to the continuity of critical operations of IMSIU IT, and also will justify the investment that management is committing to the BCM System.

IMSIU IT has developed an appropriate business continuity strategy for

- Protecting prioritized business processes and underlying activities,
- Stabilizing, continuing, resuming and recovering prioritized business processes and underlying activities and their dependencies and supporting resources, and
- Mitigating, responding to and managing impacts.

IMSIU IT BC Manager with the support from procurement team conducts evaluations of the business continuity capabilities of suppliers.

The Outage Scenarios and recovery option based on the BIA and RA are mentioned below:

Outage Scenarios	**Recovery Options**
Unavailability of the work facility	Critical process staff / management work from alternate site. Remaining staff work from home.
Unavailability of employees	Cross train resources and distribute staff of critical divisions across multiple site
IT services outage	Use of the existing alternate DR site for IT data center and develop DR site for Call Center data center

Outage Scenarios	Recovery Options
Operational disruption	Identify work around to avoid bottle necks in impacted processes.

Additional details on developing the Strategy are documented in IMSIU IT's BC Strategy document.

8.2.2. Establishing Resource Requirements

IMSIU IT has determined the resource requirements to implement the strategies for various disaster scenarios. The types of resources considered include:

- People
- IT Applications, Systems and infrastructure
- Critical Non-IT Infrastructure such as Facilities, equipment and consumables
- Vital Records
- Transportation
- Finance
- suppliers

The IMSIU IT Business Continuity Strategy Report covers major outage scenario for IMSIU IT and the details of resource requirements to provide support at acceptable level.

8.2.3. Protection and Mitigation

For identified risks requiring treatment, IMSIU IT has developed proactive measures that aim to mitigate the impact of the identified outage scenarios. The table below shows the recommended proactive measures:

Outage Scenarios	Selected Strategy Options	Recommended Protection and Mitigation Actions
General	NA	● Raising awareness of threats and disaster scenarios for IMSIU IT staff and consultants ● Developing and updating key documents on a periodic basis – Business Continuity plans, procedures, recovery methods ● Periodic testing of the recovery plans ● Mobilizing decision making team (Crisis management team) at the command center
Unavailability of the work facility	Critical process staff / management work from alternate site. Remaining staff work from home.	● Implementing the fundamental safety and firefighting measures at the University's facilities ● Developing command center from which the Crisis Management Team can operate

Outage Scenarios	Selected Strategy Options	Recommended Protection and Mitigation Actions
		● Developing alternate recovery facilities. (other sites) ● Transfer risk through purchase of insurance policy
Unavailability of employees	Cross train resources and distribute staff of critical divisions across multiple site	● Identifying key human resources and their backups in each division / sections across IMSIU IT ● Conducting trainings across the critical divisions and their dependencies including suppliers ● Moving key resources and operations to alternate site.
IT services outage	Use of the existing alternate DR site for IT data center and develop DR site for Call Center data center	● Expediting the integration of the Call Center with Deanship of IT and initiating the development of the IT DR capability for the Call Center data center ● Developing redundancies across IT Communication framework ● Moving IT and Communications operations to Disaster recovery site
Operational disruption	Identify work around to avoid bottle necks in impacted processes.	● Revisiting the design of impacted business processes and developing a simplified processes to be followed during the time of emergency

The IMSIU IT Business Continuity Strategy Report covers the recommended protection and mitigation actions for IMSIU IT.

8.3 Business Continuity Plans

IMSIU IT has established and documented a detailed business continuity plan for responding to and managing any disruption due to an incident or crisis as well as the recovery of its activities within a predetermined timeframe.

The Business Continuity plan covers the following interrelated plans that, together, cover the subsequent phases of crisis management:

- **Incident Response Plan**: This involves response to contain the emergency situation. A large part of the response activities occurs on the scene of the incident.
- **Crisis Management**: This involves response to address the crisis. The key in this phase is to identify the key stakeholders and the various communications media and communicate effectively to the stakeholders.
- **Functional Recovery Plan**: This phase involves recovery of the critical functions identified in the Business Impact Analysis; each function shall have a functional recovery plan that would be executed by the respective functions.

The detailed procedures for the abovementioned plans are documented in IMSIU IT’s Business Continuity Plan document.

8.4 Exercising and Testing

8.4.1. General

Tests and exercises are activities designed to assess the ability of IMSIU IT's personnel to respond, manage, communicate with stakeholders, continue to perform assigned duties and recover from various scenarios of business disruption. BC Manager with input from BCM Core Team design tests scenarios. The results of tests are documented in order to assess if the Business Continuity plans, processes and teams are effectively achieving the recovery objectives of the IMSIU IT.

Other events which may initiate the requirement for an exercise include significant changes in the IMSIU IT's:

- Location or facilities
- Operating environment
- Tools and technology
- Key personnel
- Critical Suppliers and service providers, Outsource partners
- Use or purchase of critical assets
- Business objectives
- Rules and Regulations

For the maintenance of BCM across the organization, IMSIU IT needs to regularly review the BCM Manual, perform the BIA and the RA exercises and perform periodic testing of BCM Plans and processes, so that it can be recovered as per agreed time frames during a disruptive incident.

The purpose of the testing is to facilitate test planning, test execution, test review, and corrective action to BCM plans developed for IMSIU IT.

Testing Steps	Key Activities
Pre-Testing	• Test planning • pre-test meeting
Testing Execution	• Testing Work Premises • Testing Outage Scenarios • Testing Call Tree
Post Testing	• Testing results documentation and communication • Recommendations for Improvement • Testing participants debriefing

8.4.2. Pre-Testing

Pre-test planning meeting(s) must be scheduled sufficiently in advance of the desired exercising date for the specific BC plans of interest.

The Dean with overall responsibility for the content of the BCM plans should chair the pre-test planning meeting(s).

Planners (e.g., the BCM Steering Committee Members, BCM Manager, Functional Recovery Coordinators, etc.) and any other parties deemed necessary for the construction of the desired type and scope of BCP test should attend pre-test planning meetings.

The meeting(s) may be conducted face-to-face, by teleconference, or by other electronic means (e.g., e-mail, net meeting).

8.4.3. Testing Execution

This step involves testing of the work premises of IMSIU IT, testing the response and management of an emergency incident based on the outage scenarios identified in the IMSIU IT BC Strategy document. Testing the effectiveness and viability of the Call Tree included in the IMSIU IT BCM Plan document is also covered in the process.

The BCM Manager will be responsible for facilitating the testing process. He / she will also be responsible for evaluating the test and preparing the post-testing report.

Various BCM Team including the BCM Steering Committee members (Crisis Management Team) and Functional Recovery Coordinators and Teams are required to actively participate in the testing exercise.

The types of testing and testing calendar are shown in the table below:

Plans to be Tested	Frequency	Dates
Incident Response Plan	Annual	In November
Crisis Management Plan	Annual	In November
Functional Recovery Plan	Annual	In November
Real Life Simulation Testing	Once in 2 Years	In November

8.4.4. Post-Testing

- **Test Debriefing**

  Following completion of the test, the BCM Manager reviews the test plan with the participants and answers questions.

  The purpose of the debriefing is:

  - To review and evaluate the test
  - To provide feedback
  - To review lessons learned from the test
- **Test Evaluations**

  Test participants should evaluate the perceived value of the test and their overall reaction to the experience. Evaluation involves:

  - Evaluation of the existing plan
  - Evaluation of the test
  - Validation that the BCM program is effective
  - Evaluation of awareness levels for emergency procedures
  - Identification of the need for further training and tests
  - suggestions for improvement

- **Testing Report**

  The BCM Manager should incorporate debriefing comments, evaluation observations into a concise report of the event including lessons learned, issues that need correction, next steps and additional training needed

8.4.5. Keys to a Successful Test

- Top level support and involvement
- Realistic test plan
- Thorough preparation and attention to detail
- Clear introduction and instructions
- Participant feedback at debriefing
- Follow-up

Refer to document: IMSIU IT Test Execution and Reporting Form

8.5 Annual Maintenance

BCM Manual maintenance is performed in accordance to a review schedule and should be performed annually. The purpose of the BCM scheduled maintenance is to determine whether a change is required to the contents of the Business Continuity Management Manual.

The scheduled review is carried out jointly by the senior leadership of IMSIU IT, BCM Steering Committee Members and BCM Manager. Inputs from other personnel may be sought as necessary.

The Dean of IMSIU IT or the designated individual is the chair-person for all the BCM Manual maintenance meetings.

The BC Manager is responsible for documenting and acting on the changes discussed / agreed upon in the meetings.

9.0 Performance Evaluation

9.1 Monitoring, Measurement, Analysis and Evaluation

9.1.1. General

IMSIU IT has determined

- What needs to be monitored and measured,
- The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results,
- When the monitoring and measuring shall be performed, and
- When the results from monitoring and measurement shall be analyzed and evaluated.

IMSIU IT retains appropriate documented information as evidence of the results. IMSIU IT evaluates the BCM performance and the effectiveness of the BCM.

Additionally, IMSIU IT should:

- Takes action when necessary to address adverse trends or results before a nonconformity occurs, and
- Retains relevant documented information as evidence of the results.

The Process for monitoring performance provides:

- The setting of performance metrics appropriate to the needs of IMSIU IT,
- Monitoring the extent to which IMSIU IT's business continuity policy, objectives and targets are met,
- Performance of the processes, procedures and functions that protect its prioritized activities,
- Monitoring compliance with ISO22301 International Standard and other local requirements as well as IMSIU IT's business continuity objectives,
- Monitoring historical evidence of deficient BCM' performance, and
- Recording data and results of monitoring and measurement to facilitate subsequent corrective actions.

9.1.2. KPI Measurement

The below KPIs shall be measured by the BC Manager, with inputs taken from various sections.

The method for monitoring shall include gathering evidence of the KPI in the form of records (test results, meeting notes, awareness attendance sheets, and internal audit reports).

The KPIs shall be monitored as per the specified frequency of the KPI and the results shall be analyzed and evaluated annually together with the BCM Steering Committee. The BCM Steering Committee shall identify any action to be taken to address adverse trends or results before a nonconformity occurs.

Senior Leadership – Governance				
#	**KPI**	**Purpose**	**Frequency of KPI activity**	**Suggested threshold achievement for activity** ***(minimum)***
1	% of BCM Documents reviewed and	Assess the review frequency of the	Annual	100%

Senior Leadership – Governance				
#	**KPI**	**Purpose**	**Frequency of KPI activity**	**Suggested threshold achievement for activity *(minimum)***
	approved by Senior Management on annual basis. *(* BCM Policy, BCM Manual, BIA, RA, BC Strategy, BC Plan, CMT Plans, Functional Recovery Plan, etc.)*	BCM Governance		
2	% of BCM Steering Committee meetings as per plan	Assess the monitoring and governance of BCMS across IMSIU IT by senior management.	Quarterly	100%

BCMS Review				
#	**KPI**	**Description**	**Frequency of KPI activity**	**Suggested threshold achievement for activity *(minimum)***
1	% of BCMS Internal Audits conducted	Assess the timely completion of the audit process	Annual	100%
2	% of BCMS Management Review conducted	Assess the involvement of management in the BCM processes	Annual	100%

BCMS Team / Crisis Management Team – Operational Level				
Sr. No.	**KPI**	**Purpose**	**Frequency of KPI activity**	**Suggested threshold achievement for activity *(minimum)***
1	% IT application and infrastructure recovered as per RTO	Assess the preparedness of its IT infrastructure environment against various forms of threat.	Semi Annually	95%
2	% of successful recovery of BCM testing vs. Number of Planned exercise completed in a year	Assess the preparedness of its BCM team to carry out essential operations in event of any disruption.	Annually	85%

IMSIU IT Staff Members, Vendors, Consultants – End User Level

Sr. No.	KPI	Description	Frequency of KPI activity	Suggested threshold achievement for activity *(minimum)*
1	% IMSIU IT personnel (staff and/or vendors) trained on BCP on annual basis	Assess the readiness of its employees to carry out essential operations in event of any disruption.	Quarterly	95%

9.2 Internal Audit

IMSIU IT conducts internal audits at yearly basis to provide information on whether the business continuity management system conforms to IMSIU IT's own requirements for its BCM and the requirements of ISO22301 Standard, and is effectively implemented and maintained.

- IMSIU IT plans, establishes, implements and maintains (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits
- Defines the audit criteria and scope for each audit
- Selects auditors and conduct audits to ensure objectivity and the impartiality of the audit process
- Ensures that the results of the audits are reported to relevant management and
- Retains documented information as evidence of the implementation of the audit programme and the audit results.

The audit programme, including any schedule, is based on the results of risk assessment of IMSIU IT's business processes and underlying activities, and the results of previous audits. The audit procedure covers the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results.

The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities include the verification of the actions taken and the reporting of verification results.

9.3 Management Review

Senior management reviews the IMSIU IT's BCM, at annual basis, to ensure its continuing suitability, adequacy and effectiveness.

The management review includes consideration of

- The status of actions from previous management reviews,
- Changes in external and internal issues that are relevant to the business continuity management system,
- Information on the business continuity performance, including trends in

  - Nonconformities and corrective actions,
  - Monitoring and measurement evaluation results, and
  - Audit results,
- Opportunities for continual improvement.

Management reviews considers the performance of IMSIU IT, including

- Follow-up actions from previous management reviews,
- The need for changes to the BCM, including the policy and objectives,
- Opportunities for improvement,
- Results of BCM audits and reviews, including those of key suppliers and partners where appropriate,
- Techniques, products or procedures, which could be used in IMSIU IT to improve the BCM' performance and effectiveness,
- Status of corrective actions,
- Results of exercising and testing,
- Risks or issues not adequately addressed in any previous risk assessment,
- Any changes that could affect the BCM, whether internal or external to the scope of the BCM,
- Adequacy of policy,
- Recommendations for improvement,
- Lessons learned and actions arising from disruptive incidents, and
- Emerging good practice and guidance.

The outputs of the management review include decisions related to continual improvement opportunities and the possible need for changes to the BCM system, and include the following:

- Variations to the scope of the BCM;
- Improvement of the effectiveness of the BCM;
- Update of the risk assessment, business impact analysis, business continuity plans and related procedures;
- Modification of procedures and controls to respond to internal or external events that may impact on the BCM, including changes to
  - Business and operational requirements,
  - Risk reduction and security requirements,
  - Operational conditions and processes,
  - Legal and regulatory requirements,
  - Contractual obligations,
  - Levels of risk and/or criteria for accepting risks,
  - Resource needs,
  - Funding and budget requirements; and
  - How the effectiveness of controls are changes to exercise program – type and frequency of exercises.

IMSIU IT retains documented information as evidence of the results of management reviews. IMSIU IT communicates the results of management review to relevant interested parties, and take appropriate action relating to those results.

10.0 Continual Improvement

IMSIU IT will, annually, perform a review of its BCM Program including the BIA, Risk Assessment, BC Strategy, and BC Plans.

This review is designed to ensure all BC capability documents are valid and consistent with IMSIU IT strategic objectives.

The review should be formally conducted by the BC Manager. The review should result in a report to Top Management. Review and update are necessary when a change occurs in the organization whether in terms of services or works or when a change occurs within Senior Management.

IMSIU IT will address the non-conformities and perform corrective actions that are applicable to the BCMS.

11.0 Records

- IMSIU IT Business Impact Analysis Report.
- IMSIU IT Risk Assessment Report.
- IMSIU IT Business Continuity Strategy Report.
- IMSIU IT Business Continuity Plan.
- IMSIU IT Continual Improvement framework.

12.0 Attachments

- IMSIU IT BCM BIA Template.
- IMSIU IT BCM RA Template.
- IMSIU IT Test Execution and Reporting Form.

13.0 References

- ISO 22301:2012 Business Continuity Standard.

14.0 Terms and References

- **Activity**

  A process, service, procedure, product, task, or combination of them that are managed by organization.

- **Audit**

  An organized, autonomous and documented form of activity of an organization conducted by an independent body in order to comply with the BCM Standard.

- **Awareness**

  Development of understanding of primary Business Continuity Management risks and issues. Awareness enables the workforce to identify threats and responding promptly and appropriately. Awareness is created among employees in the organization and it is less formalized as compared to training.

- **Business Continuity (BC)**

  The ability of the organization to continue its prioritized activities at predetermined levels after the occurrence of a disruptive incident.

- **Business Continuity Management (BCM)**

  A comprehensive management process, which highlights possible threats and impact of such threats on business operations of the organization. The identification of threats assists to develop organizational resilience, toward these threats, and an effective and suitable response that will protect the stakeholders' interest, brand name and reputation.

- **Business Continuity Management Program (BCM Program)**

  It is a component of overall organizational management system, which establishes, implements, operates, reviews, monitors, maintains and improves business continuity capability.

- **Business Continuity Plan (BCP)**

  Set of procedures in a documented form, which direct the organization to react, recover, restore and restart the predetermined level of operations after the interruption.

- **Business Continuity Policy**

  It is the major document that identifies the governance and scope of Business Continuity Plan along with BCM objectives and highlights the cause of its implementation

- **Business Continuity Strategy**

  The method of an organization to plan in order to recover and continue after a disruptive event.

- **Business Impact Analysis (BIA)**

  It is the process for analyzing business activities and the impacts that a disruptive incident might have on them.

- **Competence**

  Capacity to apply skills, resources and knowledge to accomplish desired goals.

- **Continual Improvement**

  Consistent activities to increase the performance level.

- **Compliance**

  Extent to which requirements are fulfilled.

- **Conformity**

  Extent to which mandatory requirements are fulfilled.

- **Corrective Action**

  Steps or measures that remove discrepancies.

- **Capability**

  Ability or capacity to perform a specific activity effectively.

- **Crisis**

  A crisis is a negative deviation in business operations of unusually large magnitude and/or develops exceptionally rapidly.

- **Disruption**

  An incident which disturbs routine operation, process or function of the business. These events could be anticipated or unanticipated.

- **Exercise**

  Activity in which the business continuity plans is rehearsed in a part or in whole to ensure that the plans contain the appropriate information and produce the desired results when put into effect.

- **External and internal issues**

  External or internal variables that can have impact over the business continuity capability of the organization.

- **Interested Party**

  Individual, group or an organization which can affect or be affected or consider to be influenced by an activity or decision.

- **Incident Response Plan**

  Set of procedure for immediate response after an accident, and it is focused upon the safety of personnel.

- **Internal Audit**

  A compliance review against BCM standard requirements. Therefore take corrective actions and suitable decisions accordingly.

- **IT Continuity**

  Capability of the organization to plan for and respond to incidents and disruptions in order to continue Information and Communication Technology (ICT) services at an acceptable predefined level.

- **Minimum Business Continuity Objective**

  Minimal level for product or service, which is considered as appropriate for the organization to accomplish business objectives after disruption.

- **Media Response Plan**

  Set of procedures that will enable an organization to communicate with media and interested parties through well-defined roles and responsibilities and use of available media channels to communicate and deliver the necessary information and instruction effectively during a disruption.

- **Maximum Acceptable Outage (MAO)**

  Time it would take for adverse impacts, which might arise as a result of not providing a product/service or performing an activity, to become unacceptable.

- **Non conformities**

  Mandatory requirements in the BCM standard not fulfilled.

- **BCM Objectives**

  The targets or goals that an organization wants to achieve throughout the BCM program.

- **Prioritized Activities**

  Activities that are critical and must be given priority when recovering from a disruptive incident in order to reduce the impacts

- **Resources**

  Resources include information, skills, people, technology, assets and premises, which are obtained and used by an organization to achieve its organizational goals and objectives.

- **Recovery**

  Retrieval or recapturing of normal or prior state.

- **Recovery Strategies**

  A strategy that is used by an organization to make sure it is regaining or continuing after an incident.

- **Risk Appetite**

  The extent to which an organization can afford to bear the risks and neutralize these risks to eliminate the threats.

- **Risk**

  The impacts of uncertainties on organizational goals.

- **Recovery Point Objective (RPO)**

  Point in time to which data have to be recovered in order to resume business processes.

- **Recovery Time Objective (RTO)**

  Time span after the occurrence of an incident in which an activity or product should be restarted or resources and assets should be restored.

- **IT Disaster Recovery (ITDR)**

  Activities and programmes that are invoked in response to a disruption and are intended to restore an organization's ICT services.

- **Risk Assessment (RA)**

  The process in which risks are identified, analyzed and evaluated.

- **Test**

  This is an activity or action that is undertaken to gauge the capabilities or effectiveness of a strategy or plan against a predetermined criteria or benchmark.