Deanship of Information Technology

Al-Imam Muhammad Ibn Saud Islamic University Riyadh

Business Continuity Management

System Strategy & Plans

Document Control

Version History

Version	Description of Amendment	Reason for Amendment	New Revision No and Effective Date	Amendment done by	Approved by
V0.1					

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. Business Continuity Strategy

2.1. Prioritize and Categorize

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
Operational disruption	Identify work around to avoid bottle necks in impacted processes.

This table below prioritizes the various outage scenarios, as identified in the previous table, based on

- The total number of risk associated with each risk category and
- The distribution of critical / prioritized risks across different risk priority levels.

The identified priority of an outage scenario will determine the appropriate timeframe for initiating the selected mitigation strategy for that scenario

Risk Category

		People	Premises	Operations	Technology
Risk Priority	Immediate action required	1	4	-	3
	Urgent action required	2	4	1	-
	Quick action is advisable	1	3	1	3
	Total	**4**	**11**	**2**	**6**
Outage Scenarios		**Unavailability of employees**	**Unavailability of the work facility**	**Operational disruption**	**IT services outage**
Scenario Priority		**(3)**	**(1)**	**(4)**	**(2)**

2.2. Key Assumptions & Considerations

General

The report covers the strategy for continuity of the prioritized business process of IMSIU IT i.e. processes with their identified RTO ranging 0 hours – 6 Days as per the Business Impact Analysis (BIA) report. In the event of an extended business operations disruption exceeding 6 days, IMSIU IT is required to explore and take further actions to ensure the resilience of its operations including non-prioritized processes. Such action may include leasing and setting up a full functional work facility.

People Requirements

- It was assumed that the minimum number of human resources required for resumption and recovery process are already present in IMSIU IT.
- Each IMSIU IT division/ section will nominate a functional recovery coordinator who will assist BC manager in resumption and recovery activities.
- Each functional recovery coordinators is responsible for ensuring that the requisite people are available at the recovery site identified.
- Each functional recovery coordinators coordinator with support from IT, Facilities will ensure that the requisite equipment are available at the recovery site identified.
- Each functional recovery coordinator with support from IT will ensure that the vital records for each divisions / units are identified and provisions for backup or recovery at the backup site:
  - Ensure data is backed-up and it is kept off site
  - Essential documentation is stored securely (e.g. fire proof safe)
  - Copies of essential documentation are kept elsewhere in different medium so that they can

easily be reproduced.

IT & Technology Requirements

IMSIU IT Disaster recovery plan will be incorporated and linked with the corporate Business continuity plan. As of this date, IT DR site is operational from IMSIU IT office. However, no separate IT DR site is established for IT operations.

Critical Equipment

- It was assumed that the number of required workstations at the alternate recovery sites is equal to the number of laptop or desktop identified.
- It was assumed that the number of laptops/ desktops at the alternate recovery sites is equal to the minimum number of people working for the related division/ section during outages.
- Internet connectivity is equal to the number of facilities determined in the Business Continuity Strategy as alternate recovery sites and not based on the minimum number of workstations.
- Printer/ scanner/ fax, Filing cabinets, Vaults and Shredder are determined based on number of alternate locations as part of BCM strategy.

Vital records

Vita records needed for the recovery of each prioritized business process are documented in the individual Functional Recovery procedures for divisions and sections.

2.3. Protection & Mitigation Roadmap

For identified risks requiring treatment, IMSIU IT should develop proactive measures that (1) Reduce the likelihood of disruption, (2) Shorten the period of disruption and (3) Limit the impact of disruption on its key services. The table below explains the high level recommended action course to achieve the above:

Outage Scenarios	Selected Strategy Options	Recommended Protection and Mitigation Actions	Recommended Initiation Timeframe
General	NA	• Raising awareness of threats and disaster scenarios for IMSIU IT staff, students, visitors 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 to command center	Immediate action required: mitigation is recommended to be initiated ASAP
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 • Developing alternate recovery facilities. (other sites) • Transfer risk through purchase of insurance policy	Immediate action required: mitigation is recommended to be initiated ASAP

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.	Immediate action required: mitigation is recommended to be initiated ASAP
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 Deanship of IT Communication framework • Moving IT and Communications operations to Disaster recovery site	Immediate action required: mitigation is recommended to be initiated ASAP
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	Urgent action required: mitigation is recommended to be initiated within 100 days

2.4. Determination & Selection

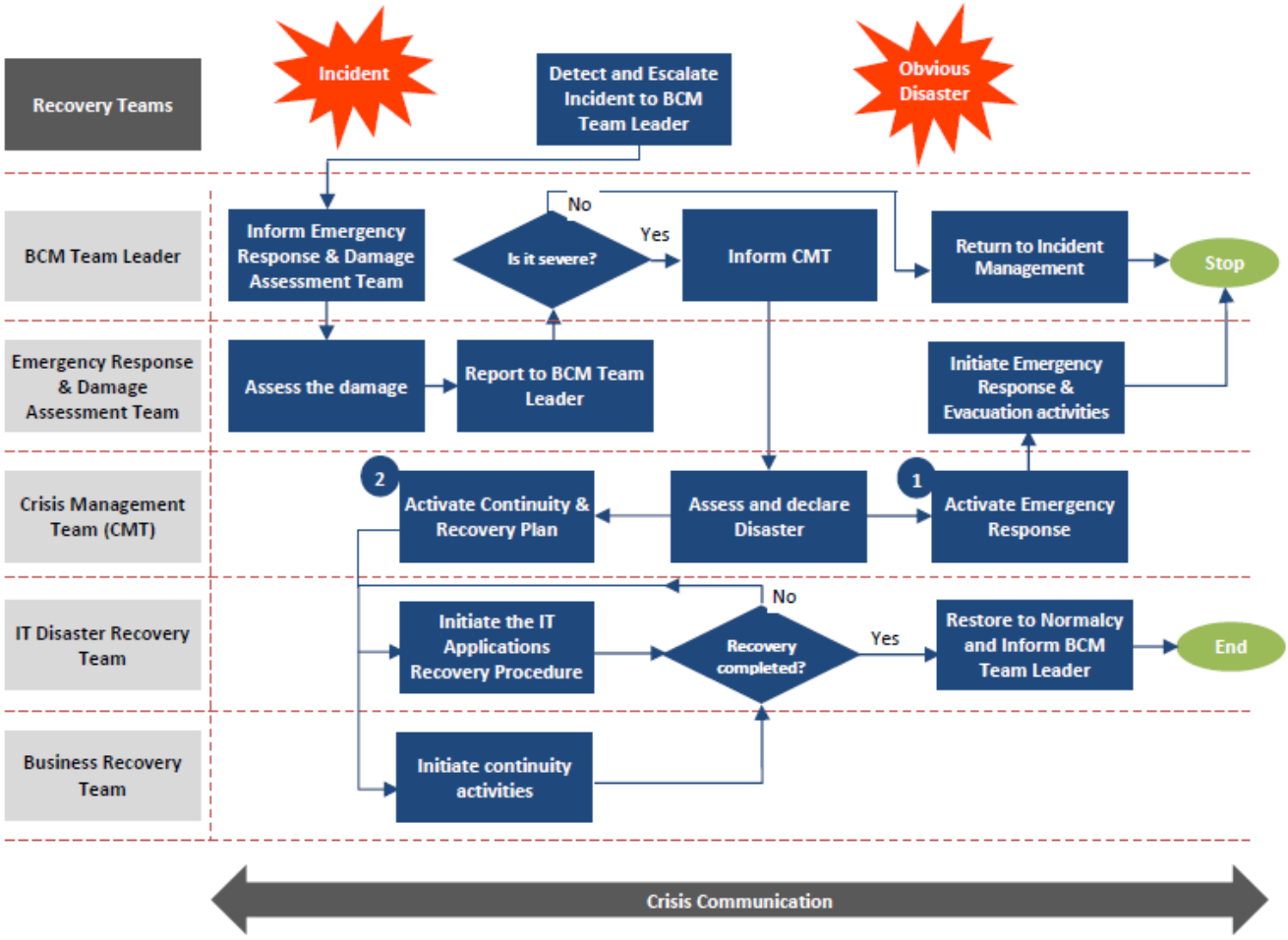
Selection and declaration of a specific strategy should be based on the disaster situation/ impact detailed above. The following table summarizes the various impacts that the University may face in a disaster and the corresponding strategy that should be declared by the Disaster Recovery Team Leader. The teams' actions and recovery activities are based on the declared strategy.

Description	Facility	Part Facility	Data Centre	Part Data Centre	People	Recovery Strategy
Business as usual	-	-	-	-	-	**N/A**
Primary facility unavailable	X	X	-	-	-	**Move to Alternate Facility:** Use alternate facility while using primary Data Center and people
Part primary facility unavailable	-	X	-	-	-	**Use Primary and Alternate Resources:** Use primary facility and part of alternate facility
Primary data center unavailable	-	-	X	X	-	**Use Alternate Resources:** Use primary facility while using alternate data center
Part primary data center unavailable	-	-	-	X	-	**Use Primary and Alternate Resources:** Use primary data center and part of alternate data center
Primary people unavailable	-	-	-	-	X	**Use Alternate Resources:** Use backup people
Primary facility and primary IT unavailable	X	X	X	X	-	**Move to Alternate Facility and Use Alternate Resources:** Use both strategies, to move to the alternate facility and use the alternate data center

Note: This Matrix is to be used as a guideline and reference only, real life situations at the time of a disaster may or may not be compatible with scenarios/ impacts recommended here, and the final decision to declare the disaster and the strategy to be followed solely rests with those in authority and having the responsibility to make such a decision.

2.5. Process Flow

In the event of disruption to e-services, a series of activities need to be conducted to report the incident and recover the services. The high level process flow diagram of the activities to be conducted and the corresponding team responsible for the activity is the Deanship of IT below. The activities to be performed are detailed in the subsequent sections. Throughout the process, crisis communication is key for the gathering, coordination and timely dissemination of crisis-related information to target audiences, in order to protect the university, its reputation and key stakeholders.



2.6. Detect, Assess and Declare Disaster

Disasters are disruptions that cause information resources supporting critical e-services to be inoperative for an extended period of time, which adversely impacts business operations. Disruption could last for a period ranging from several hours to several days, depending upon the criticality of the resource.

The most likely sources of identifying a potential disaster are:

- IT Operations & Technical Support
- Information Security (Detection of major security breach or attack)
- Networks and Internet
- Electronic Gate
- Building Management / Physical Security (fire/ flood/ bomb threat, or information received from emergency services or local authority regarding incidents that may render the building or data center inaccessible or non-usable)
- A normal observer

In the event of an incident/ disruption reported by an observer, the observer can escalate the incident through the following ways:

- BCM Team Leader directly
- Observer's Reporting Manager/Supervisor
- Administration / Human Resources / Security
- Emergency helpdesk

In all cases, communication should be conveyed to the BCM Team Leader, whose first decision is to assess the severity of the event and decide if a Disaster should be declared. Once declared, the continuity and recovery procedures are activated, with the objective of restoring normal operations as quickly as possible.

It is important that individuals in the areas outlined above are aware of who should be contacted should a potential incident be identified. Contact details of relevant BCM Governance team members have been annexed to this plan.

External vendors and support agencies may need to be contacted in the event of disaster; and a contact list providing a list of relevant external contacts is annexed to this plan.

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.

3.1. INCIDENT RESPONSE PLAN

The Incident Response Plan is concerned with the immediate aftermath of an incident and is primarily concerned with keeping people safe.

3.1.1. Incident Response Team

The incident response team including:

- BCM Steering Committee / Crisis Management Team
- Incident Response Team
- Functional Recovery Team
- Internal Audit

During normal business operations and in the crisis time, all BCM teams will work together to ensure the resilience of the business operations of IMSIU IT. The roles and responsibilities of each team member across the various phases of the BCM framework is provided in the subsequent section.

3.1.2. Roles and Responsibilities

IMSIU IT will establish roles and responsibilities for BCMS process. Authorities for relevant roles will be assigned and communicated within IMSIU IT through workshops and meetings.

The key roles, responsibilities and authorities are defined in the table below:

Team Members	During Normal Operations	During Crisis		
		Incident Response	Crisis Management	Functional Recovery
The Dean (Incident Commander / Head of BCM Steering Committee)	• Key decision maker of BCM Steering Committee.	• Declare a Crisis / Activate of Business Continuity Plans.	• Approve decisions taken by BCM steering committee.	• Monitor the recovery process based on inputs from BCM Manager • Declare stand down of crisis and return of normalcy of operations.
Deputy Incident Commander	• Reviews progress and test results. • Update the Dean and BCM steering committee on the BCP preparedness.	• Act as Incident Commander in the absence of the Dean	• Act as decision maker in absence of the Dean • Update the Dean (Incident Commander) on Crisis management plan deployment	• Monitor the recovery process based on inputs from BCM Manager. • Provide guidance to BCM steering committee on steps for

			progress.	recovery process.
BCM Steering Committee / *Crisis Management Team (CMT)*	• Provide Sponsorship to the BCM Program. • Challenge and agree strategies and budgets. • Provide inputs during regulatory changes. • Agree recovery options and direction during crisis scenario as part of the planning activity. • Monitor the adequacy of resources to maintain and improve BCMS, and recommend to management the acquiring of additional resources where a risk is identified. • Approve important changes to BCMS documentation. • Review the results of measurement activities. • Perform management reviews. • Ensure that internal and external BCMS audits are conducted.	• Assist BC Manager in assessing the impact of the incident • Involve in informing team through the call tree mechanism • Assist Incident commander in decision making during evolving incident scenario	• Assess the need for activation of BCM plans. • Work with Incident Response Team, HR for human safety. • Work with General Service team and Civil defense for site recovery. • Work with IT team for IT Disaster Recovery Plan. • Work with the Communication team for media response	• Monitor the recovery progress based on inputs received from individual FRP coordinators. • Provide guidance to BC manager for recovery and resumption of operations.
Business Continuity Manager	• Manage the Business Continuity program. • Ensure all BCPs, IT DRP, FRPs are kept up-to-date, approved, and escalate issues to the BCM Steering Committee. • Conduct periodic Business Impact Analysis and Risk Assessment. • Ensure IT recovery and business priorities are aligned. • Schedule test cycles and document test	• Collect and track information on the incident from respective team • Inform BCM steering committee on the situation • Oversee the incident response team work • Convene BCM steering committee • Oversee measures for relocation of staffs to safer places. • Oversee relief and response to staff	• Work as a key member of the BCM Crisis Management Team • Facilitate Functional Recovery coordinators as per priority for functional / division recovery. • Records all events/ activities/ decision taken during the entire lifecycle of the crisis in the IMSIU IT Log of Events-Actions-Decision.	• Oversee and coordinate recovery and response activity with support from FRP team • Prepare log sheets and status report for informing BCM steering committee on recovery progress • Perform corrective measures in case of blockage to recovery procedures.

	results. • Collate and schedule training and awareness requirements. • Monitor, measure and analyze objectives and Key Performance Indicators (KPIs). • Report on the performance of the BCMS to senior management / BCM Steering Committee.	members. • Perform damage assessment and inform Incident Commander and BCM Steering Committee of the situation		
Support Team	• Assist BCM steering committee with information and support for managing BCMS. • Agree recovery options and direction during crisis scenario as part of the planning activity. • Assist in performing management reviews. • Assist in internal and external BCMS audits.	• Assist in assessing the impact of the incident • Involve in informing team through the call tree mechanism • Assist Incident commander in decision making during evolving incident scenario	• Work together as part of the BCM Crisis Management Team (CMT) along with support team and FRP coordinators under the overall command and control of the Incident Commander. • Work with Incident Response Team, HR for human safety.	• Assist in monitoring the recovery progress based on inputs received from individual FRP coordinators. • Assist BC manager for recovery and resumption of operations.
Functional Recovery Coordinators	• Provide inputs to the Business Impact and Risk Assessment including the vital records. • Agree recovery alternatives as described in the FRPs. • Attend awareness sessions and ensure that staff attend the awareness workshops. • Develop functional recovery plans and provide inputs to Business Continuity Manager for changes in business process and priorities. • Ensure participation of required staff in the functional tests.	• Coordinate evacuation of staff from premises • Coordinate mobilization of staff to alternate site • Coordinate occupation of alternate recovery site • Report status to Command Center	• Facilitate EHS/HR in roll call and human safety. • Update BC Manager of progress. • Communicate with Functional Recovery team members and their respective Sector / Division as per plan and Business Continuity Manager's instructions.	• Assist in monitoring the recovery progress based on inputs received from FRP team. • Facilitate Functional Recovery as per plan. • Assist BC manager for recovery and resumption of operations.

Fire Wardens	• Support BCM Manager in executing evacuation drills	• Evacuate staff from premises • Provide a count of staff at assembly point • Assist in relief and rescue operations and fire fighting in small scale.	• Not applicable	• Not applicable
Internal Auditor	• Perform internal audit for the scope area in accordance with NCEMA and ISO 22301 standards • Provide recommendations to the findings of the reviews • Perform follow ups on the recommendations of remediation activity	• Not applicable	• Not applicable	• Not applicable

3.1.3. Incident Response Procedures

The following procedures outline the steps to be followed in the event of a disaster

Step	No.	Key Activities	Responsibility
Respond to Disaster	1.1	• Evacuate staff from premises	• Fire Wardens
	1.2	• Assemble at Evacuation Assembly Point	• All Staff
	1.3	• Assess Damage of premises	• BCM Steering Committee

Step	No.	Key Activities	Responsibility
	1.4	• Activate Command Centre	• Incident Commander / Deputy Incident Commander
	1.5	• Activate Call Tree notification	• Incident Commander / Deputy Incident Commander
	1.6	• Activate Alternate IT DR site	• IT Team
	1.7	• Deactivate automated system measures for suspending non-compliant vehicles	• IT Team
	1.8	• Communicate the incident to external stakeholders (franchisees)	• Franchisee affairs team
	1.9	• Activate auto response emergency outage message at the Call Center	• Call Center team
	1.10	• Report status to Command Center	• Functional Recovery Coordinators
Mobilize to Alternate Locations	2.1	• Transport required staff to the alternate recovery site	• General Services team
	2.2	• Activate alternate recovery site	• BC Manager
	2.3	• Occupy alternate site	• Functional Recovery Coordinators
	2.4	• Report status to Command Center	• Functional Recovery Coordinators

3.1.4. Command Center

The Command Center is a physical or virtual facility located outside of the affected area used to gather, assess, and disseminate information and to make decisions to effect the recovery

The Command Center is the management focal point where implementations of tactical decisions are initiated during a disaster. The Command Center will have to be chaired by the Incident Commander (IC) or a designated alternate.

The activities that will be performed at the Command Center include:

- Identification and monitoring a crisis.

- Take quick tactical business decisions.
- Source and allocate resources to help recover from the disaster.
- Serve as a single point of communication for all entities internal or external to IMSIU IT.
- Management and reporting of incident response actions.

While setting up the Command Center the following should be made available in order to function effectively:

- General seating space for the CMT (Decision-making team) to function.
- Meeting room(s) with audio conferencing facility.
- Telephone lines in the seating space.
- Blueprint of the Head Office (HO) facility.
- Process manuals and documentation of IMSIU IT.
- Data lines, Internet connection with computers.
- Stationery for taking notes, logging actions etc.
- Arrangement for food, water and refreshments.
- Contact with a local doctor and hospital to handle medical emergencies that may arise due to stressful working requirements.

The functional recovery teams lead by their respective coordinators should carry out the following at the recovery site.

- The business process documentation made available for the respective recovery teams.
- Identify and occupy seating space for the recovery teams as planned by the BCP Manager.
- Ensure the computers / terminals provided in the seating space have all the required applications loaded and working.
- Ensure that the printers, fax, telephones etc. are working and adequate stationery is available for operations.
- Ensure that the Risk & Business continuity management sector coordinators have the log template to keep logging and recording all the activities performed during the recovery stages.

Once the recovery teams have carried out the above activities the respective coordinators should communicate to the CMT that the recovery teams are ready for operations and highlight any constraints.

3.1.5. Use of call tree for cascading information of incident

The Call Tree / Cascade is a structured mechanism of staff contact details, which help to ensure that all staff are contacted and informed that the business continuity / functional recovery plan, has been activated.

The purpose of the call tree / cascade mechanism is to have an efficient method to ensure that each staff member will be accounted for during a crisis or disaster.

Call trees / cascades also provides an effective mechanism for contacting business continuity / functional recovery teams during a crisis.

Business Continuity Manager should ensure update of the call trees / call cascades on a regular basis or as

and when the changes occur.

Incident Commander will begin the call tree / cascade by calling the next person on the tree or cascade. That person will then contact the next person on the tree or cascade and so on.

When contacting assigned staff, each person should communicate the following:

- His or her own status and the status of those before him or her
- Any damage or injury the staff person or those before him or her have experienced and / or what assistance they may need
- How the staff person can be reached if it has changed from what he or she originally provided prior to leaving the office. (i.e. if they changed locations, their cell phone is not working, or picked up by anybody other that the staff etc.)
    - **Calling procedure**

Initiate the call by saying “May I speak with (Individual name)?”

1. If available, provide the following information:

- Brief description of the problem;
- Location of the initial meeting place:
- Telephone number at the initial meeting place:
- Any immediate action requirements:
- Remind personnel to make NO public statements regarding the situation.
- Remind personnel not to call fellow employees and to advise their family NOT to call other employees.

2. If not available, say, “Where may I reach (Individual)?”

- If at any location other than work, obtain the number, make the call and provide the above information.
- If individual is at work, indicate you will reach the individual at work. (Do not discuss the situation with the person answering the phone)
- Record the information in the Result of Call column on the Personnel Alert Checklist and notify the Head of Communications immediately.

3.1.6. Call Tree Structure:

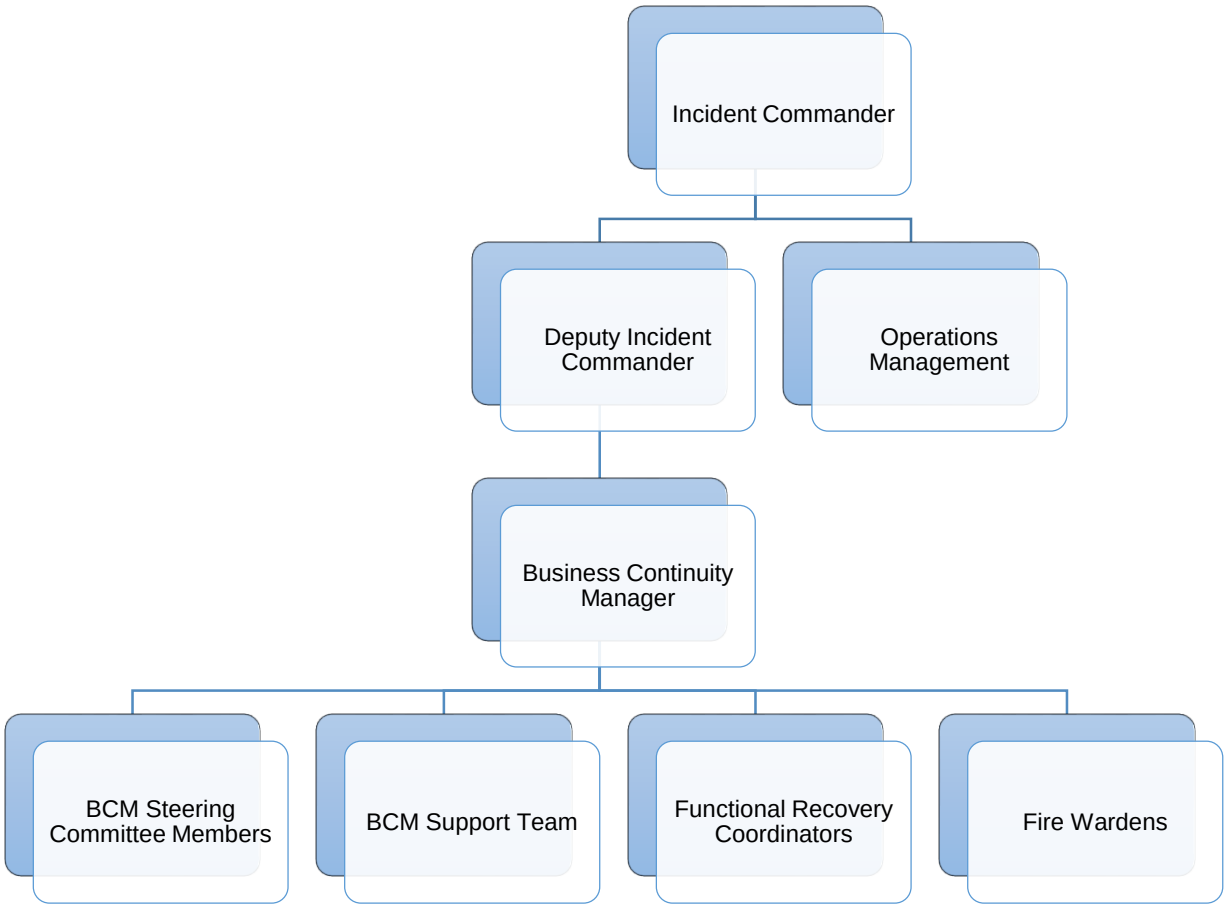


Figure 3: Call Tree Structure for IMSIU IT

3.1.7. Key Contacts:

#	Team	Team Member	Name	Division / Section	Work Contacts	Home Contacts
1	BCM SC	Incident Commander	*To be Identified*	*To be Identified*	*To be Identified*	*To be Identified*
2	BCM SC	Deputy Incident Commander	*To be Identified*	*To be Identified*	*To be Identified*	*To be Identified*
3	BCM SC	Operations Management	*To be Identified*	*To be Identified*	*To be Identified*	*To be Identified*
4	BCM SC	Business Continuity Manager	*To be Identified*	*To be Identified*	*To be Identified*	*To be Identified*
5	BCM SC	Departments Directors	*To be Identified*	All Divisions and Sections	*To be Identified*	*To be Identified*
6	Functional Recovery Team	Functional Recovery Coordinators	*To be Identified*	All Divisions and Sections	*To be Identified*	*To be Identified*
7	Functional Recovery Team	Fire Wardens	*To be Identified*	All Divisions and Sections	*To be Identified*	*To be Identified*

IMPORTANT NOTE - BY USING THE ABOVE INSTRUCTIONS, YOU SHOULD NOT ALARM MEMBERS OF EMPLOYEE'S FAMILY UNNECESSARILY. DO NOT DISCUSS THE SITUATION WITH MEMBERS OF THE FAMILY. THIS IS MOST CRITICAL WHEN CALLING THE HOMES OF PERSONNEL BELIEVED TO HAVE BEEN PHYSICALLY AFFECTED BY THE DISASTER.

3.2. CRISIS MANAGEMENT PLAN

This section details out the Crisis Management Plan for IMSIU IT's personnel who may be required to respond to a crisis situation.

The Crisis Management Plan is a "live" document and requires regular updates to ensure that it is up-to-date and have realistic plans and procedures in place to deal with a crisis.

A crisis is typically a situation which will have a significant impact on the operation and / or reputation of IMSIU IT. A crisis situation requires immediate and coordinated action to minimize adverse impacts on reputation and operations of IMSIU IT.

3.2.1. Crisis Management Team

The Crisis Management Team (BCM Steering Committee) is constituted of senior members of IMSIU IT.

From a crisis perspective, the main functions of the Crisis Management Team (BCM Steering Committee) include:

- Update the Dean Office of the crisis and the progress to recovery.

- Establish the Command Center to become the single point of contact.
- Make tactical business decisions in the event of a crisis.
- Communicate appropriately with the employees and the media when required.
- Approve financial spends for recovery in the event of a crisis.
- Monitor recovery progress and remain available as a central point of contact in the event of a crisis.

3.2.2. Crisis Management Procedure

The following procedures outline the steps to be followed by the Crisis Management Team during this phase. Further detailed activities are included in the subsequent section – Functional Recovery Plan

Step	No.	Key Activities	Responsibility
Resume Operations	1.1	• Retrieve required items / resources required for operation from suppliers / vendors / contractors	• Functional Recovery Coordinators
	1.2	• Restore business function at alternate site and ensure site is fully functional	• BCM Steering Committee
	1.3	• Carry out Operations at alternate location	• Functional Recovery Coordinators
	1.4	• Report status to Command Center	• Functional Recovery Coordinators
Restore to primary facility and Resume normal operations	2.1	• Check and verify main building is operational	• BCM Steering Committee
	2.2	• Switch over to primary systems. Ensure data synchronization	• THE DEANSHIP OF IT Team
	2.3	• Report status to Command Center	• Functional Recovery Coordinators
	2.4	• Recommence normal mode of operations	• Functional Recovery Coordinators

3.2.3. Information Technology Disaster Recovery (IT DR) Plan

At the time of writing the current version of the plan, IMSIU IT has established a fully functional alternate IT DR site for its core IT operations managed by IMSIU IT. Moreover, IMSIU IT has approved the budget for developing and implementing a DR data center for its Call Center operations. The establishment of the new

DR site is planned to be competed in 2016.

The processes and procedures for recovering and restoring IMSIU IT data and systems are documented in the following documents which are in the custody of IMSIU IT's:

- IT Data Management
- IT Disaster Recovery
- Incident & Problem Management
- Data Restoration
- Veeam Backup & Replication document

3.2.4. Media Response Plan

This section of the document is define and document the Media response plan for IMSIU IT. The media response plan is developed to provide a controlled and well defined communication procedure to external entities – GSEC, AD government entities, media, social media, Franchisees and general public so that they are better equipped with correct information related to outage scenarios that affects IMSIU IT operations.

3.2.5. IMSIU IT's Media representative during crisis

In the event of a crisis, IMSIU IT should have:

- An official spokesperson whose responsibility will be to address, acknowledge and respond to media queries in a time bound professional manner.
- Address, acknowledge and respond to any queries related to IMSIU IT operations affected by the crisis
- Have established channels for official communication through email, fax, media briefs, social media accounts, IVR systems
- Issue early warnings or advance information of effects of IMSIU IT's service affected by disruption.

Any type of media queries or information related to the crisis should be directed only to the Head of PR and communication through the official channels and mediums as designated by IMSIU IT. This include:

- Official email ids
- Official social network accounts
- Official press note

IMSIU IT staff and non-staff should be trained as part of BCM awareness to direct any queries raised related to incident or outages to Head of PR & communication and not to respond to media queries.

3.2.6. Gathering, monitoring and disseminating emergency information

PR & communication section of IMSIU IT should monitor social media feeds, print and electronic media, telephone calls to understand the nature of queries raised by the general masses. A brief, concise response providing the information of crisis, present status and operational capabilities of affected services should be

provided by Head of PR & Communication on a periodic basis. IMSIU IT should ensure that information are factually correct to the maximum extent and can quell any speculations or rumors that may rise during the crisis scenario.

The PR & Communication section should ensure all message that comes out from IMSIU IT official media outlets are reviewed and approved by Legal Affairs team and senior management of the organization.

3.2.7. Identification of audience of communication

Clear and precise communication is the key to successful management of a crisis. During a crisis, various stakeholders of IMSIU IT would require to be updated on the situation. It is therefore necessary to establish communication channels to the various stakeholders.

The following table describes the various communication types and the teams responsible for the same.

Communication Type	Responsible Team
Media Communication & External Stakeholders	Head of PR & Communication IMSIU IT Official Spokesman
Employee communication	Human Resources
Government emergency services like Police, municipality, fire brigade etc., Civil Defense	BCM Manager

3.2.8. Ongoing Users communication and safety briefing

PR & Communication section of IMSIU IT should develop IVR scripts for informing Users about the delay or disruption of services. Further, call center staff should be trained to address Users queries during crisis and direct them to PR & Communication section head, in case of further information requested.

3.2.9. Define the means and frequency with which the information is provided

The Head of PR & communication with support from BCM Manager and approval from senior management should develop a frequency for responding to media queries and social media queries. This should be based on the:

- Availability of resources such as media center, arrangement for access to social media etc.
- Availability of correct information from authorized people handling the crisis,
- Availability of information from HR and other internal resources.

At the minimum, at least one media briefing or news updates should occur within 24 hours period. Press briefing along with notes (orally or written) will be distributed to media after completion of the press briefing. In no instances, should people who are not trained to handle media queries or unauthorized person be allowed to face or respond the media.

3.3. FUNCTIONAL RECOVERY PLAN

The objective of this section is to define and document the Functional Recovery plan for IMSIU IT, in line with the requirements of ISO 22301 international standard.

The functional recovery plan is developed to provide a defined process for divisions and sections of IMSIU IT to recover from outage scenarios and resumption of services of its Prioritized Process at an acceptable level defined by IMSIU IT's management.

It also maps the outage scenarios and recovery strategy options that evolved from the BCM strategy document with available resources of Prioritized Processes for each divisions and sections.

Further, it lays down the process of resumption of normal operations after the crisis is over.

3.3.1. Prioritized Process

#	Prioritized Process	RTO	Responsible
1.	Management of Domain controller and Active Directory	< 4 hours	The Dean
2.	Management of MS Exchange Server	4 Hours – 2 Days	The Dean
3.	Management of Mobile Phones service	4 Hours – 2 Days	The Dean
4.	Management of File Server and Share Folders	4 Hours – 2 Days	The Dean
5.	Secure File Trasfer Protocol service	4 Hours – 2 Days	The Dean
6.	Management of all Deanship of IT Applications, Database, Appliances server infrastructure	4 Hours – 2 Days	The Dean
7.	Management of data storage	4 Hours – 2 Days	The Dean
8.	Management of IP Telephony	4 Hours – 2 Days	The Dean
9.	Management of Local Area Network	4 Hours – 2 Days	The Dean

#	Prioritized Process	RTO	Responsible
10.	Management of Internet service	4 Hours – 2 Days	The Dean
11.	Management of Wireless network	4 Hours – 2 Days	The Dean
12.	Management of RSA remote connectivity	4 Hours – 2 Days	The Dean
13.	Management of IT Helpdesk	4 Hours – 2 Days	The Dean
14.	Management of VMWare infrastructure	4 Hours – 2 Days	The Dean
15.	Virtual Desktop service	4 Hours – 2 Days	The Dean
16.	Management of CCTV infrastructure	4 Hours – 2 Days	The Dean
17.	Management of Deanship of IT Asset Management system	4 Hours – 2 Days	The Dean
18.	Management of data backup	4 Hours – 2 Days	The Dean
19.	Management of Deanship of IT archiving system and infrastructure	4 Hours – 2 Days	The Dean
20.	Management of Printer services	4 Hours – 2 Days	The Dean
21.	Management of Mcafee End Point systems (AV, IPS, DLP, Web & Mail Gateway)	4 Hours – 2 Days	The Dean
22.	Management of Data Center protection systems (Fire detection and suppression, Leakge system, AC/Humidity control system)	4 Hours – 2 Days	The Dean

3.3.2. Prioritized IT Systems / Applications

#	Prioritized IT Systems / Applications	RTO
1	BMC	< 4 hours
2	VEEAM	< 4 hours
3	NetApp	< 4 hours
4	MS SQL Server, .NET	< 4 hours
5	Intranet portal	< 4 hours

3.3.3. Employees Requirements

RTO ➔	0 – 4 Hrs.	4Hrs - 2 Days	3 – 4 Days	5 – 6 Days	14 - 7 Days
Director	2	2	2	4	4
Section Head	2	2	2	4	4
Employees	5	5	5	5	5

3.3.4. Vital Records

Vital Records
IT shared Folder, procedures and checklist

3.3.5. IT Infrastructure Requirements

IT Infrastructure	New Purchase
Laptops USB	7
Computer Desktops with USB	-
Hardened Data Card	-
Printer , scanner, fax, Copier	-
Internet Connectivity	-
Workstation	7
Wide Carriage Printer	-
Telephone	1
Filing Cabinet	-
Vault	-
Shredder	-

3.3.6. Non-IT Infrastructure Requirements

Non-IT Infrastructure	New Purchase
Letter Heads / Official Stationary	-
A4 Printer Paper	-
Stationery Set	4 Sets
Plastic folders	-
Box Files	-
Company Rubber Stamp (Min 2 in No.)	1
White Board	1

3.3.7. Key Suppliers

Supplier Name	Contact No.
Telecommunication Provider (Saudi Telecom Company)	800 124 1300 00966 55 177 8877
Microsoft	800-820-0135
HP	800-897-1444

4.1. Outage scenarios

IMSIU IT has identified 4 outage scenarios and developed recovery strategies accordingly.

- Unavailability of the work facility
- Unavailability of employees
- IT services outage
- Operational disruption

3.3.8. Functional Recovery Procedure

Step	No.	Key Activities	Responsibility
Recovery of Work Facility	1.1	• Contact the Business Continuity Manager and indicate availability of team members and await instructions.	• Functional Recovery Coordinators
	1.2	• Contact the recovery team members to check and ensure their safety and availability.	• Functional Recovery Coordinators
	1.3	• Move to the designated alternate recovery site and occupy the seats allocated to the division / section.	• Functional recovery team
	1.4	• Coordinate the movement of the recovery team to the alternate recovery site	• Functional Recovery Coordinators
	1.5	• Check the accessibility of vital records, applications of the division / section	• Functional recovery team
	1.6	• Highlight any discrepancies with respect to applications, data accessibility or health and safety of the functional recovery team to the BC manager through the functional recovery coordinator.	• Functional recovery team
	1.7	• Confirm the relocation of the team to the BC Manager	• Functional Recovery Coordinators
	1.8	• Update the BC Manager periodically of the progress in recovery.	• Functional Recovery Coordinators
Recovery of people	2.1	• Review staff mapping for critical resources and their alternates. View staff availability during crisis and verify their current location.	• Functional Recovery Coordinators
	2.2	• Inform BC Manager on the availability of the team members and location of the team members.	• Functional Recovery Coordinators
	2.3	• Inform the BC Manager whether there are any requirements for staff movement to alternate locations and specify the number of people that required to be relocate to recovery sites.	• Functional Recovery Coordinators
	2.4	• Update the BC Manager periodically of the progress in recovery.	• Functional Recovery Coordinators
Recovery of IT Services	3.1	• Check the status of the IT/ Technology and data centre recovery with the Business Continuity (BC) Manager.	• Functional Recovery Coordinators

Step	No.	Key Activities	Responsibility
	3.2	• On receipt of confirmation of successful switch over of IT operations from the main data centre to the DR site, direct the recovery team to check the accessibility to the system.	• Functional Recovery Coordinators
	3.3	• In case of any concerns/ discrepancies, report the situation to the BC Manager.	• Functional Recovery Coordinators
	3.4	• In case the requisite system(s) are accessible, confirm recovery of the systems to the BC Manager	• Functional Recovery Coordinators
	3.5	• Based on confirmation received from the Functional Recovery Coordinator, check the access to the requisite system(s).	• Functional Recovery Coordinators
	3.6	• In case of any issues concerning the access, report the situation to the Functional Recovery Coordinator and await further instructions.	• Functional recovery team
	3.7	• In case of successful access to the system, inform the functional recovery coordinator	• Functional recovery team
	3.8	• Update the BC Manager periodically of the progress in recovery.	• Functional Recovery Coordinators
Recovery of Business Operations	4.1	• Seek the availability of manual work around for the affected process (es).	• Functional Recovery Coordinators
	4.2	• Review the identified work around along with the steps for security breaches, flaws or other potential risk to IMSIU IT.	• Functional Recovery Coordinators
	4.3	• Assist functional recovery coordinator in designing and implementing the work around	• Functional recovery team

Step	No.	Key Activities	Responsibility
	4.4	• Deploy the work around process upon approval from the BCM Steering Committee.	• Functional Recovery Coordinators
	4.5	• In case of any issues concerning the access, report the situation to the Functional Recovery Coordinator and await further instructions.	• Functional recovery team
	4.6	• Update the BC Manager on the recovery progress	• Functional Recovery Coordinators

3.3.9. Resumption to Normal Operations Procedure

Step	No.	Key Activities	Responsibility
Resumption to Normal Operations	1.1	• Review the safety of the work premises.	• Functional Recovery Coordinators (General Services Section)
	1.2	• Inform the BC Manager if the premises is safe to return	• Functional Recovery Coordinators (General Services Section)
	1.3	• Check if the IT facilities are available at the building	• The Deanship of IT Team
	1.4	• Inform the BC Manager IT facilities are available at the building	• The Deanship of IT Team
	1.5	• Inform the heads of divisions / sections on the readiness of: ▪ Office space for work ▪ IT facilities for work	• BCM Manager
	1.6	• Visit the primary site and test the office space and IT availability.	• Functional Recovery Coordinators
	1.7	• If satisfactory, inform the staff members to start mobilizing less Prioritized Processes of the division to the primary location and followed by Prioritized Processes.	• Functional Recovery Coordinators
	1.8	• Update the BC Manager on the progress of the business resumption.	• Functional Recovery Coordinators
	1.9	• Perform root cause analysis for the process and corrective actions after the recovery process.	• Functional Recovery Coordinators
	1.10	• Prepare a detailed incident report document and circulate to the team	• BCM Manager