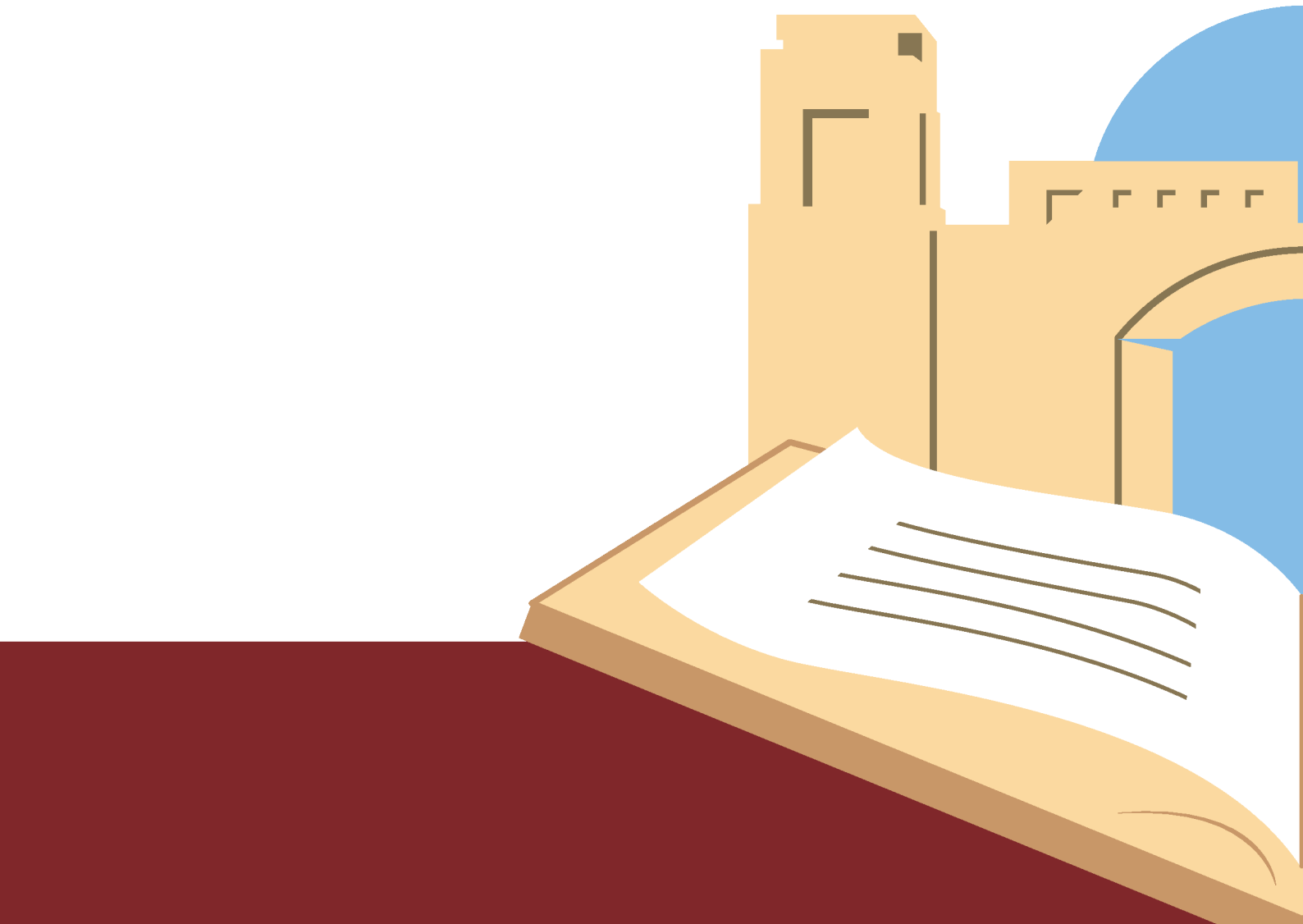
جامعة دار الحكمة
DAR AL-HEKMA UNIVERSITY

Information Technology Department
Business Continuity Management System

Manual

FA.IT.1.0.MN



DECUMENT CONTROL

VERSION HISTORY

Version	Description of Amendment	Reason for Amendment	New Revision No and Effective Date	Amendment done by	Approved by
V1.0	Ms. Jamila Mualim	Initial Draft	JM	RM	Ms. Huda Abdulraqib
V1.1	Ms. Rasha Almalik	Version 1	1.1	RM	Ms. Huda Abdulraqib

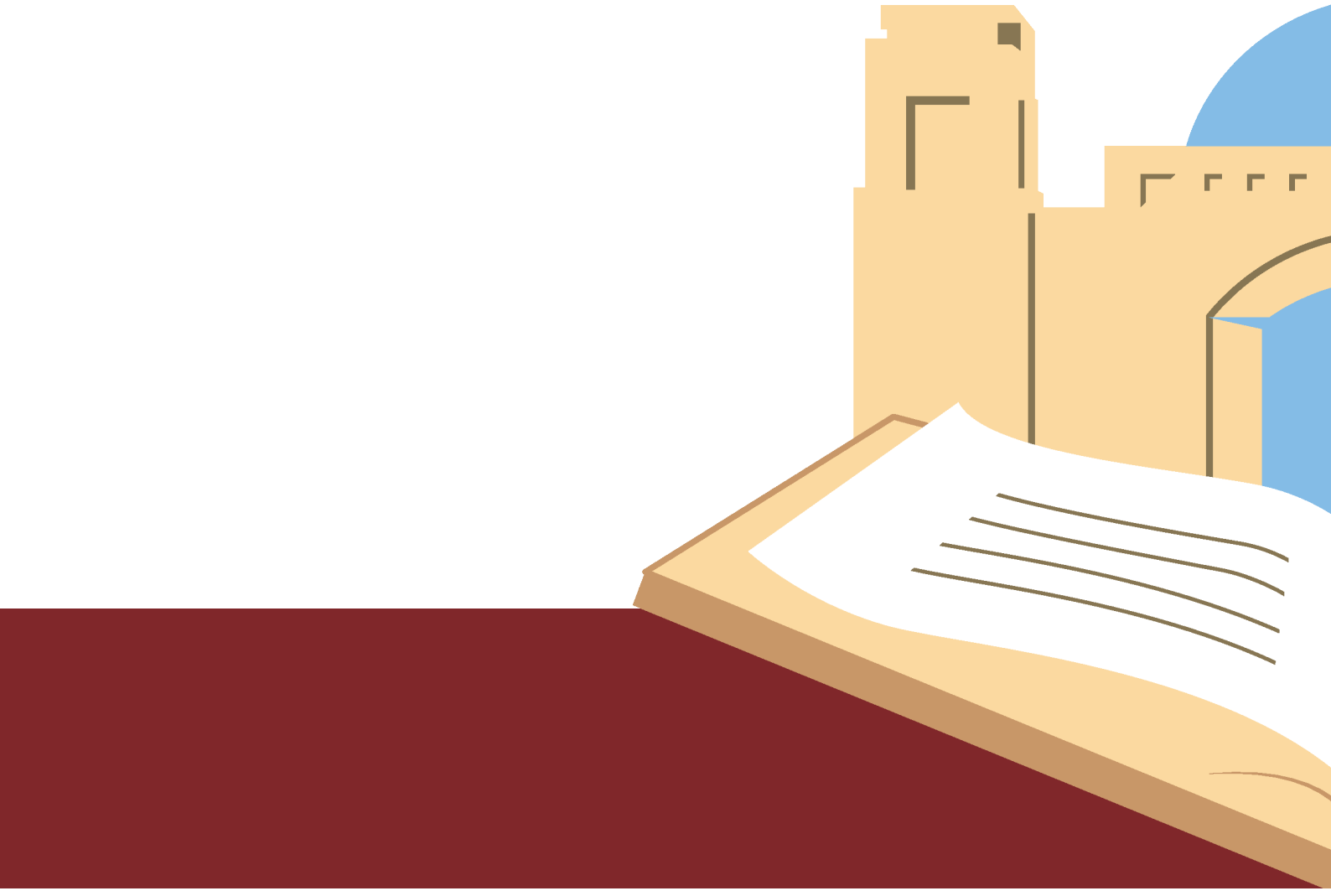
Approval

Submitted By: (signed)	**Ms. Rasha Almalik**	**Approved By: (signed)**	**Ms. Huda Abdulraqib**
Position:	**Director of Information Technology Department**	**Position:**	**Executive Director**

Contents

جامعة دار الحكمة
DAR AL-HEKMA UNIVERSITY

Information Technology Department Business Continuity Management System



1. INTRODUCTION

The Information Technology Department at Dar Al-Hekma University was established to lead the management, development, and security of the university's digital environment. It plays a pivotal role in advancing the university's mission through technology-driven solutions that support academic excellence, research, and administrative efficiency.

IT Mission:

> To enhance educational experience and operational efficiency by integrating cutting-edge technology, fostering digital literacy, and promoting a culture of continuous innovation and improvement.

2. Purpose

The purpose of this document is to define and establish the **Business Continuity Management (BCM) Framework** and structure for **Dar Al-Hekma University – IT Department**. This framework is designed to enhance organizational resilience by aligning business continuity practices with the university's strategic objectives and IT goals. It outlines the management, operation, and control of the **Business Continuity Management System (BCMS)** in accordance with the **ISO 22301 international standard** for business continuity.

3. Scope

All critical business processes within the Information Technology Department, including infrastructure, assets, and personnel, ensure the continuity and resilience of the University's digital infrastructure.

4. Context of the organization

Understanding the IT Department at Dar Al-Hekma University's internal and external contexts by identifying the external and internal factors that are relevant to the university's mission and impacting its ability to achieve the intended outcomes of its Business Continuity Management System (BCMS).

4.1. Understanding the Needs and Expectations of Interested Parties

4.1.1. General

For more details refer to context organization procedure

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

4.1.2. Legal and Regulatory Requirements

The IT Department at DAHU has identified the key legal, regulatory, and contractual requirements that impact the Business Continuity Management System (BCMS). These requirements include:

- Compliance with the Government regulations of the Kingdom of Saudi Arabia (KSA)
- Adherence to contractual obligations related to business continuity

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 section 3 of this BCM Manual document.

4.2.2. Scope Exclusion

None

5. Leadership and Commitment

5.1. Leadership

Dar Al-Hekma University (DAHU), top management demonstrates its commitment to the IT Business Continuity Management System (BCMS) through proactive leadership, oversight, and resource allocation. The **Finance and Administration Director**, as the top management for the IT Department, is responsible for ensuring that the BCMS is effectively implemented and aligned with the **strategic goals of the IT Department.** The **IT Director**, under her supervision, leads the operational implementation of the BCMS and ensures that business continuity practices are integrated into all IT services.

Senior management supports the BCMS by:

- Providing the necessary resources—HR, financial, and technological—to develop, maintain, and improve the BCMS.
- Ensuring that risk assessments and business impact analyses are conducted and reviewed regularly.
- Supporting the development, implementation, and testing of the IT Business Continuity Plan (BCP), which includes Incident Response, and Disaster recovery plans.

- Promoting awareness of business continuity responsibilities across all IT staff and relevant stakeholders.
- Establishing clearly defined roles for the Business Continuity Team and ensure members are trained and competent.
- Ensuring compliance with ISO 22301, SDAIA, NCA, and applicable legal, regulatory, and contractual requirements.
- Encouraging continual improvement through internal audits, corrective actions, and regular management reviews of the BCMS.

5.2. Management Commitment

Top Management ensures business resilience by committing to:

- Providing the necessary resources to uphold the IT business continuity management system.
- Ensuring thorough risk assessments and business impact analyses tailored to the operations, enabling the IT Department to manage risks effectively and implement control measures.
- Ensuring the development and regular review of the IT Business Continuity Plan to maintain the continuity and safety of the team, facilities, and operations.
- Ensuring that business continuity plans are effectively communicated throughout the IT Department.
- Ensuring the IT Department complies with customer specifications, international standards, and local regulatory and legal requirements.
- Ensuring the IT Department is knowledgeable about the Business Continuity Management System and is prepared to respond in the event of a disruption.
- Identifying the Business Continuity Team, clearly defining their roles, and providing them with appropriate training.
- Considering the sustainability requirements.
- Reviewing IT BCMS policy, objectives, plans, and impact analyses on a predefined cycle.

5.3. BCM Policy

The IT Department at Dar Al-Hekma University has established a Business Continuity Management (BCM) Policy that reflects the commitment of DAHU IT management to ensuring organizational resilience and continuity of critical services.

In alignment with the ISO 22301 standard, the policy will be:

- **Communicated** across the IT department and relevant stakeholders,
- **Published** on the DAHU IT intranet and made available to interested parties, as appropriate
- **Reviewed annually** to ensure its continued relevance, adequacy, and effectiveness, or sooner if significant changes occur.

BCMS Policy

The Information Technology Department at Dar AlHekma University plays a crucial role in delivering high-quality IT services to stakeholders. The department is dedicated to ensuring uninterrupted service and protecting stakeholder interests, both of which are key to the department's long-term sustainability.
The IT Business Continuity Management System (BCMS) covers critical units, functions, and processes that require a recovery plan. The IT Department utilizes both proactive and reactive strategies to minimize the impact of major incidents, including:

- Implementing a risk assessment and impact analysis plan aligned with the ISO 22301 requirements
- Developing recovery plans to mitigate significant risks.
- Integrating business continuity and disaster recovery (DR) planning into all operational requirements.
- Using third-party service providers to maintain appropriate and tested recovery strategies if necessary.
- Designing critical alternatives for continuous operation during system failures.
- Preparing, testing and auditing plans, as well as conducting drills to ensure readiness if needed.
- Improving the effectiveness of the business continuity management system continuously.

This policy is based on the "Business Continuity Management Standard and Guide" issued by the International Organization for Standardization (ISO 22301). It will be communicated to all employees of the Information Technology Department, and compliance is mandatory. Each unit is responsible for always maintaining its business continuity management preparedness. This policy will be reviewed to ensure its relevance and updated as necessary.

5.4. Organizational Roles, Responsibilities and Authorities

IT Department in Dar AlHekma University implements and maintains a structure, identifying one or more teams responsible for responding to disruptions. The roles and responsibilities of each team and the relationships between the teams are clearly stated. Collectively, the teams are competent to:

- Assess the nature and extent of a disruption and its potential impact.
- Assess the impact against pre-defined thresholds that justify initiation of a formal response.
- Activate an appropriate business continuity response.
- Plan actions that need to be undertaken.

- Establish priorities (using life safety as a first priority).
- Monitor the effects of the disruption and the organization's response.
- Activate business continuity solutions.
- Communicate with relevant interested parties, authorities, and the media

5.4.1. Incident Response Team

This team is responsible for coordinating and implementing business continuity plans during an emergency event. They are responsible for ensuring that employees are safe, that critical systems are restored, and that DAHU can continue to operate, this team will be responsible on the following:

- Contribute to risk assessments and BIAs.
- Ensure staff participate in incident response tests.
- Manage and contain the incident.
- Activate Incident Response Plan.
- Lead recovery efforts.
- Collaborate with HR and Support Services for safety

5.4.2. Disaster Recovery Team

IT Disaster Recovery team will work under the leadership of the University's IT Director and will be primarily responsible for recovering the IT systems during a disaster, the responsibility of the IT DRP team includes:

- Review and update disaster recovery plans.
- Regularly test recovery plans.
- Monitor IT systems for continuity readiness
- Activate disaster recovery plan.
- Deploy resources for recovery.
- Restore IT systems to operational state

5.4.3. Business Continuity Management Team

This team is responsible for ensuring that an organization can continue its critical operations during and after a disruption or crisis. This involves planning, implementing, testing, and maintaining Business Continuity Plans (BCPs), they have the authority to implement the following responsibilities:

- Support BCM program.
- Monitor BCMS resources and recommend improvements.
- Approve BCMS documentation changes.

- Assess incident impact.
- Coordinate internal communications and resources

5.4.4. Risk Assessment & Business Impact analysis Team/member

This team is responsible for identifying potential risks to the organization and assessing their potential impact. They work with business unit leaders to develop risk mitigation strategies and ensure that the organization is prepared to respond to potential disruptions, the team shall:

- Develop risk assessments and maintain risk register.
- Conduct BIAs and internal audits.
- Follow up on audit recommendations.
- Assess risks after the incident and update the risk register

6. Planning

6.1. Actions to Address Risk and Opportunities

The Dar Al-Hekma University IT Department has established a comprehensive risk assessment process as part of its Business Continuity Management (BCM) framework. This process involves defining the risk context and systematically identifying, analyzing, and evaluating risks that could impact the continuity of IT services critical to the university's operations.

The purpose of this risk assessment is to:

- Ensure the Business Continuity Management System (BCMS) can achieve its intended outcomes,
- Prevent or minimize adverse effects that may disrupt IT services, and
- Support continual improvement of the BCMS.

Based on the risks identified, the IT Department has developed and implemented appropriate actions to address these risks. These measures include the application of organizational policies and procedures, deployment of physical and logical controls, and regular monitoring and review mechanisms to reduce risks to an acceptable level.

Furthermore, risk treatment plans have been formulated in response to the specific risks identified during the assessment. The effectiveness of these risk treatment plans, and associated controls will be continuously monitored and evaluated to ensure ongoing adequacy and efficiency in safeguarding IT service continuity.

6.2. Business Continuity Objectives and Plans to Achieve Them

DAHU IT has developed business continuity objectives in alignment with the IT Objectives:

- Improve Operational Efficiency
- Strengthening Cybersecurity.

No.	IT Goals	Area	Objective	Task	Measurement Method	Target	Timescale	Responsible
1	**Strengthening Cybersecurity**	Planning and Documentation	Make certain that 5 critical processes and services in the IT department have current business continuity plans or effective recovery processes in place.	Hold taskforce with IT BCMS team to define, review, and update the Business Continuity Plan	Percentage of IT processes and services with an active BCP	100%	12 months	Business Continuity Manager
2	**Improve Operational Efficiency**	Training and Awareness	Acquire yearly training or workshop sessions for key IT personnel to ensure they are familiar with their roles	Identify relevant courses and secure the necessary budget	Number of trained individuals.	5 staff	12 months	Business Continuity Manager / HR Division
3	**Strengthening Cybersecurity**	Risk and Impact Analysis	Complete annual risk assessments to identify and prioritize potential threats to business operations.	Conduct meeting to review and assess risks.	Number of risk reviews conducted annually.	1 review	12 months	Risk Assessment & Business Impact analysis Team

4	**Improve Operational Efficiency**	Testing and Continuous Improvement	Perform annual tests and drills of the business continuity plans to validate effectiveness and improve response strategies.	Agree on a test schedule with senior management and perform tests. Communicate results to the Business Continuity Manager.	Number of plans tested within a year.	1 test	12 months	Business Continuity Manager / Testing Team

Progress toward these objectives and the implementation of the plan are continuously monitored and assessed during regular BCM management reviews.

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

7. Support

7.1. Resources

Dar Al-Hekma University IT Department has identified and documented the necessary resources required for the establishment, implementation, maintenance, and continual improvement of the Business Continuity Management (BCM) system. This is detailed in Section 5.4, Organizational Roles and Responsibilities, of the DAHU IT BCM Manual

7.2. Competence

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

Role	BCM Awareness Level (High/Medium/Low)	BCM Knowledge Required	Method of Achieving Competency	Competency Evaluation	Maintenance of Competency
Business Continuity Team Manager	High	Comprehensive understanding of BCM principles, ISO 22301 requirements, and leadership in disruption management	Professional BCM training, on-the-job experience	Management reviews, exercise performance reviews	Periodic training, participation in exercises
Business Continuity Planner	High	Strong knowledge of BCM principles, ISO 22301 requirements, risk assessments, Business Impact Analysis (BIA), and recovery planning	Formal training, hands-on experience	Review of risk assessments/BIAs, exercise validation	Periodic training, periodic plan updates and exercises
Business Continuity	Medium	General BCM awareness and understanding of IT continuity requirements	Internal awareness sessions.	Contribution during drills	Ongoing training, participation in BCM exercises

Team Members			participation in BCM activities		
Incident Response Team	High	Detailed knowledge of incident response protocols and BCM principles	Incident response training, scenario-based drills	Incidents reports, exercise evaluations	Regular incident response exercises, Training courses
Risk Assessment & BIA Team	Medium	Knowledge of risk management, BIA techniques, and audit processes	Training in risk assessment and internal audit	Audit reports, risk register reviews	Ongoing audit training, periodic risk reviews
Disaster Recovery Team	High	Technical knowledge of IT systems recovery and disaster recovery planning	Technical training, participation in recovery tests	Testing results, post-incident recovery reports	Regular training, participation in DR exercises
Testing Team	Medium	Understanding of BCM testing methodologies and objectives	Internal training, on-the-job involvement in testing	Test exercise reports, feedback and lessons learned	Continuous involvement in test cycles, updates based on test outcomes

7.3. Awareness

Dar Al-Hekma University IT Department has created a Business Continuity Management (BCM) awareness program with clear materials and a plan to build awareness across the team. This program helps everyone understand:

- How to spot and recognize incidents that may disrupt work.
- The business continuity plans that apply to them.
- The business continuity policy.
- How their role helps make the BCM system work better and why it's important.
- What can happen if BCM requirements are not followed.
- What they need to do during a disruptive incident.

The program is regularly updated to keep it useful and relevant.

7.4. Communication

Dar Al-Hekma University (DAHU) promotes clear and effective communication related to the IT Business Continuity Management System (BCMS) and ensures participation and consultation among employees and contractors. This supports alignment, legal compliance, and continuous improvement across IT operations, which covers:

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

a. Communication between personnel of various units at IT Department in DAHU on matters relating to BCMS, significant aspects, and BCMS are carried out through internal memos, e-mail messages, IT helpdesk and meetings.
b. Additionally, IT instruction signs and posters are displayed across the facility (Classrooms and Labs) for the dissemination of BCMS information.
c. Any incoming communication on a BCMS-related issue (legal or contractual) including project-specific communication shall be forwarded to the DAHU Lawyer for review.
d. The IT Department shall review the communication, evaluate the requirement to respond to the external communication, and respond promptly. IT may discuss the response with the FA director before responding
e. For non-legal or non-contractual BCMS communication, the IT Department shall decide upon the type of response based upon its professional judgment.
f. The response to relevant external parties shall be documented and maintained by the IT.

g. IT maintains a list of significant aspects of its activities and shall communicate externally to relevant interested parties based upon request and approval by the top management.
h. The IT Department encourages the participation of its employees in the BCMS.
i. Employees have been trained and participated in the development of the risk register and in incident investigation. Relevant draft BCMS policy and procedures are discussed with the employees, and their feedback is sought before releasing the final draft.
j. In the event that there could be changes affecting the department contractors' (relating to BCMS matters), the IT Department shall hold consultations with them in this regard. The IT Department shall also be responsible for consultations with other relevant parties as required.

7.5. Documented information

7.5.1. General

The IT Department's Business Continuity Management System (BCMS) shall include:

- Documented information required by ISO 22301, including but not limited to the BCMS policy, manual, Business Impact Analysis (BIA), risk registers, communication procedures, and any other mandatory documents necessary to support the effective operation of the BCMS.
- Documented information determined by the IT Department is necessary to ensure the BCMS is effective, which may include related management system documents.
- All documented information shall be appropriately controlled to ensure it is available, protected against loss of confidentiality, improper use, or loss of integrity, and maintained up to date.

7.5.2. Creating and updating

- Documents must be authorized and listed in the Document Master List.
- Each document is coded by the standard coding structure and identified with its title, version number, and issue date.
- All documents must contain essential components including
- All documents must comply with the DAHU Visual Branding Guidelines regarding font and formatting.
- Revisions must be tracked using the "Track Changes" feature to ensure traceability.

7.5.3. Control of documented information

The documented information required by the BCMS and applicable standards shall be controlled by the IT Department at Dar Al-Hekma University to ensure that:

- It is available and suitable for use when and where needed,
- It is adequately protected against loss of confidentiality, improper use, or loss of integrity.

The IT Department will manage documented information through the following activities, as appropriate:

- Distribution, access, retrieval, and use.
- Secure storage and preservation, maintaining legibility.
- Control of changes, including version control.
- Retention and proper disposal of documents.

7.5.4. Documents coding

The IT Department adopts a standardized coding system to ensure clear identification, traceability, and categorization of all documents under the Business Continuity Management System (BCMS)

a. Document Types and Codes:

Document type	Code
Policy	PP
Process Procedure	PR
Document	DO
Manual	MN
Forms	FR
Flowchart	FC
Objective	OB
Plan	PL
Strategy	ST

b. Code Structure

Each document code is composed of four parts:

- Division Code
- Department Code
- Serial Number and Version

- Document Type Code

Example: FA.IT.3.0-PP

- FA = Finance and Administration Division
- IT = Information Technology Department
- 3.0 = Document serial number and version
- PP = Policy

c. Form Coding Extension

For forms related to a specific procedure, an additional code is appended to indicate the form number.
Examples:

- FA.IT.1.0-PR – Refers to Procedure Number 1.0
- FA.IT.1.0-PR.2.0-FR – Refers to Form Number 2.0 related to Procedure Number 1.0

8. Operations

8.1. Business Impact Analysis and Risk Assessment

8.1.1. General

The IT Department at Dar Al-Hekma University has developed both a Business Impact Analysis (BIA) and a Risk Assessment (RA) as essential components of the IT Department's Business Continuity Management (BCM) system. These processes help the university identify critical IT services, assess the potential impact of disruptions, and develop strategies to ensure business continuity. The following sections describe the BIA and RA methodologies, as well as how these processes are applied to support the university's IT services.

8.1.2. Business Impact Analysis

Business **Impact Analysis (BIA)** is a vital process for identifying and analyzing business activities and the consequences of disruptions. It helps prioritize essential IT services and forms the foundation for determining continuity strategies. The BIA process was carried out in three stages: **Initiate**, **Assess**, and **Analyze**, as detailed below:

a. Initiate Phase:

- **Define Objectives**: The goal of the BIA is to ensure the continuity of critical IT services and minimize disruptions to IT operations.

- **Identify IT units and scope**: The BIA scope includes all IT operations, including all units.

b. Assess Phase:

- **Identify Key Services and Activities**: The university's critical IT services, including Student Information System (SIS), Blackboard, university website, Shared folders and network infrastructure, are identified.
- **Assess Impact**: The potential impacts of service disruptions on financial, operational, reputational, and legal aspects are evaluated for each IT service.

c. Analyze Phase:

- **Validate Information**: The data collected is reviewed for accuracy and completeness.
- **Summarize Recovery Priorities**: The results are used to prioritize recovery activities across Business Units, focusing on the most critical services.
- **Develop BIA Outcomes**: Recovery strategies for each critical IT service are developed based on recovery time objectives (RTO) and recovery point objectives (RPO).
- **Obtain Senior Management Approval**: Senior management reviews and endorses the final BIA outcomes to ensure alignment with the university's business continuity goals.

8.1.3. Risk Assessment

The Risk Assessment (RA) is a comprehensive evaluation aimed at identifying, analyzing, and assessing the risks and vulnerabilities that could affect DAHU IT services. The RA process helps assess the likelihood of threats, their potential impacts, and the steps needed to address those risks. The RA methodology consists of the following steps:

a. Risk Identification:

- Identify Risks/Threats: Potential risks that could disrupt IT services are identified, including both internal and external threats.
- Risk Identification Process: Risks are identified through interviews, site visits, and process reviews, informed by the BIA outcomes.

b. Risk Analysis:

- Analyze Risks: Identified risks are analyzed based on their likelihood of occurrence and the severity of their impact on university operations.
- Assess Severity: The severity of risks is determined based on the impact on business operations and IT services.

c. Risk Evaluation:

- Evaluate Against Risk Criteria: The risks are evaluated against predefined criteria, which consider the impact and likelihood of occurrence.

- Determine Acceptability: Risks are assessed to determine if they are acceptable or need to be addressed through mitigation plans.

d. Risk Treatment:

- Develop Treatment Plans: For unacceptable risks, treatment plans are developed. These plans evaluate the cost-benefit of mitigation strategies and ensure compliance with legal and regulatory requirements.
- Risk Acceptance: Risks are classified on a scale from Very High (Catastrophic) to Very Low (No Action Needed), based on their impact and likelihood.

8.2. Business Continuity Strategy

The recovery strategy selection is based on the nature of disruption and its potential impact on the IT services at **Dar Al-Hekma University**. The following table outlines the potential scenarios and the corresponding recovery strategies:

Description	Facility Data Center	People Recovery Strategy
Business as usual	N/A	N/A
Primary facility unavailable	SaaS and DR Systems	Remote working
Primary IT unavailable	Restore from Off-site backup, SaaS and DR Systems	N/A

8.2.1. Process Flow

In the event of a disruption to IT services, a series of activities will be carried out to report the incident and recover services. The high-level process flow diagram will guide the recovery activities, which are detailed in subsequent sections. Throughout the process, **crisis communication** is vital to ensure timely dissemination of information to all stakeholders and protect the university's reputation.

8.2.2. Detect, Assess, and Declare Disaster

Disasters are significant disruptions that cause critical IT services to be unavailable for an extended period, impacting university operations. The most common sources for identifying a disaster include:

- **IT Operations and Technical Support**
- **Information Security** (major breaches or attacks)
- **Network and Internet Services**
- **Building Management/Physical Security** (e.g., fire, flood, bomb threats)

- **External Observers** (e.g., staff, emergency services)

In the case of an incident, it can be reported through the following channels:

- Directly to the **BCM Manager**.
- Through the **Observer's Reporting Manager** or **Supervisor**.
- **Administration**, or HR
- Incident tracker System, Change management form
- **IT Helpdesk**.

Once the incident is reported, the **BCM Team Leader** will assess the severity and decide if a disaster declaration is needed. If a disaster is declared, the continuity and recovery procedures will be activated to restore normal operations as quickly as possible.

8.3. Business Continuity Plans

The IT Department has developed and documented comprehensive **Business Continuity Plans (BCPs)** designed to effectively respond to and manage any disruptions caused by incidents or crisis. This plan outlines recovery strategies to restore IT services within a predetermined timeframe, ensuring minimal impact on the university's operations.

The **Business Continuity Plan** encompasses the following interrelated phases:

a. **Incident Response Plan:** It defines immediate actions to contain and manage the incident, focusing on stabilizing IT systems and minimizing further damage. It ensures swift on-site responses to prevent escalation and protect critical IT infrastructure.
b. **Disaster Recovery Plan:** It focuses on restoring IT services and infrastructure after a major disruption, ensuring recovery of critical functions within established recovery time objectives (RTOs). It includes backup systems, data restoration, and access to alternate IT sites.

8.4. Exercising and Testing

8.4.1. General

The IT Department plans exercise by defining objectives, scheduling them, and preparing scenarios, then obtaining necessary approvals. Participants will be notified, and all logistics will be arranged before the exercise. The exercises will be executed while observations and actions are recorded. Afterward, the results will be evaluated. Improvements will be made by updating plans and assigning corrective actions. Finally, all documentation related to the exercises will be maintained for future reference.

8.4.2. Preparation and Planning of BCM Exercises

The IT Department shall schedule preparation meetings well ahead of the planned BCM exercise dates to ensure thorough readiness. These sessions will be led by the IT Department Director responsible for BCM oversight. Participants will include the BCM Planner, testing team, and relevant stakeholders essential to designing the exercise scope and objectives.

8.4.3. Conducting BCM Exercises

The IT Department will execute BCM exercises that simulate disruptions based on scenarios outlined in the Business Continuity Strategy. Exercises will test the functionality of IT critical functions, incident responses, communication procedure. The BCM Manager is responsible for overseeing the execution, monitoring performance, and documenting observations. All BCM team members and coordinators must actively engage in the exercises. The exercise schedule is as follows:

- Full-scale Simulation Exercises: Annually (July- August)

8.4.4. Review and Analysis Post-Exercise

Immediately after an exercise, a debriefing session will be conducted by the BCM Manager with all participants to discuss performance outcomes, challenges, and lessons learned. Feedback will be collected through formal Exercise and Test Form assessing the effectiveness of plans, participant awareness, and identifying further training or testing needs. The BCM Manager will consolidate all insights into recommendations for improvements and follow-up actions.

For detailed documentation and reporting, refer to the IT Department's BCM Exercise Execution and Reporting Form: "FA.IT.8.0-PR.4.0-FR- Exercise and Test Form"

8.5. Evaluation of Business Continuity Documentation and Capabilities

The IT Department will regularly review and assess all business continuity documentation, including policies, plans, procedures, and recovery strategies, to ensure they remain current, effective, and aligned with University and IT Department objectives. This evaluation includes verifying that the documents reflect any changes in business processes, technology, or risk environment.

Additionally, the IT Department will evaluate its business continuity capabilities by testing and exercising recovery plans, assessing resource availability, staff readiness, and effective

coordination. Feedback from exercises, audits, and real incidents will be used to identify gaps and drive continual improvement.

The results of these evaluations will be documented, communicated to relevant stakeholders, and integrated into management reviews to support decision-making and ensure ongoing resilience.

9. Performance Evaluation

9.1. Monitoring, Measurement, Analysis and Evaluation

9.1.1. General

Monitoring and measurement of BCMS management system implementation will include the following

- Monitoring and measurement of processes will be conducted by reviewing the achievement of objectives and satisfaction surveys, as necessary, during Management Review Meetings.
- Monitoring and measurement of supplier performance and evaluation.
- Monitoring and measurement of stakeholder requirements.
- The business continuity exercise program will be applied.
- Training plans will be implemented.
- Resources needed will be provided.
- All requested backups will be available and effective.

9.1.2. KPI Measurement

#	Objective Area	Target / Measure	Frequency	Responsible Party
1	Planning and Documentation	Ensure 100% of the five identified critical IT processes and services have up-to-date Business Continuity Plans and recovery procedures	Reviewed annually or upon major changes	BC Manager
2	Training and Awareness	Achieve 100% participation of the five designated key IT personnel in BC training/workshops	Annually	HR, IT Manager, BC Coordinator

3	Risk and Impact Analysis	Complete at least one comprehensive review of risk assessments and BIAs	Annually or post major change	Risk Manager, IT Security Lead
4	Testing and Continuous Improvement	Conduct at least one BC exercise/drill annually with 100% execution rate to validate recovery capabilities	Annually	BC/DR Coordinator, IT Ops

9.2. Internal Audit

Dar Al-Hekma University's IT Department is committed to maintaining an effective IT Business Continuity Management System (BCMS) through regular internal audits in accordance with ISO 22301:2019. These audits verify that the BCMS complies with both the IT Department's business continuity requirements and the ISO 22301 standard. They also assess whether the BCMS is properly implemented, maintained, and continually improved to support the achievement of its objectives. Internal audits are conducted annually, with the audit program developed based on risk assessments, process importance, and previous audit results. The program specifies audit frequency, scope, criteria, methods, and responsibilities to ensure comprehensive and objective evaluations. Auditors are selected to ensure impartiality and competence.

Audit findings are documented and reported to relevant management, who are responsible for addressing any identified nonconformities and their root causes without undue delay. Corrective actions taken are then verified through follow-up activities, with verification results reported accordingly. All audit plans, findings, and related corrective actions are maintained as documented evidence to demonstrate conformity and support continual improvement of the BCMS. This internal audit process reinforces Dar Al-Hekma University IT Department's commitment to a resilient and reliable business continuity framework.

9.3. Management Review

Dar Al-Hekma University (DAHU) ensures the ongoing effectiveness, adequacy, and suitability of its IT Business Continuity Management System (BCMS) through scheduled management reviews. These reviews provide a structured platform to evaluate performance, identify improvements, and make informed strategic decisions.

a. **Frequency and Participants**
   The BCMS management review is conducted annually and is chaired by the Finance and Administration Director. All heads of the Finance and Administration Department. Unscheduled or additional meetings may be convened, with approval from the Finance and Administration Director, to address urgent or emerging issues.

b. **Management Review Input**
The BC Planner is responsible for preparing the management review agenda and distributing it to all participants at least one week prior to the meeting.

c. **Agenda Topics**
The management review agenda covers the following key topics:

- Status of action from the previous management review meeting
- Changes in internal and external issues relevant to the BCMS
- Feedback on BCMS performance, including trends related to:
    - Nonconformities (NCR) and corrective actions
    - Monitoring and measurement results
    - Internal and external audit outcomes
    - Business Continuity Plan drills
    - Achievement of BCMS objectives
- Feedback from interested parties
- Results of risk assessments and the risk treatment plan
- Opportunities for continual improvement
- Resource adequacy and allocation

d. **Management Review Output**
The outputs of the management review include decisions and actions related to the continual improvement, effectiveness, and sustainability of the BCMS. The management review findings are documented in a formal report, which is retained as evidence of the review and its results.

10. Continual Improvement

Dar Al-Hekma University IT Department continually improves its Business Continuity Management System (BCMS) through an annual review process that includes the Business Impact Analysis (BIA), Risk Assessment, Business Continuity Strategy, and Business Continuity Plans.

The Business Continuity Manager, in collaboration with BC Planner leads these reviews to ensure all BCM documentation remains current, effective, and aligned with both the Department's objectives and ISO 22301:2019 requirements.

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

Findings and recommendations from the review are documented in a report submitted to top management, facilitating informed decision-making and resource allocation.

The BCMS is also updated proactively whenever there are significant changes in IT services, organizational structure, senior management, or regulatory requirements.

Any non-conformities or gaps identified through reviews or internal audits are promptly addressed with corrective actions, supporting the ongoing enhancement of the BCMS.

These practices ensure the Dar Al-Hekma University IT Department maintains robust business continuity capabilities and demonstrates compliance with ISO 22301 standards.

11. Records

- Dar Al-Hekma University IT Business Impact Analysis (BIA) Report
- Dar Al-Hekma University IT Risk Assessment Report
- Dar Al-Hekma University IT Business Continuity Strategy
- Dar Al-Hekma University IT Business Continuity Plans (BCP)
- Dar Al-Hekma University IT Continual Improvement Framework
- Dar Al-Hekma University IT Internal Audit Reports related to BCMS
- Dar Al-Hekma University IT Management Review Reports

12. References

ISO 22301:2012 Business Continuity Standard.

13. Terms and References

- **Pivotal**: Very important or central.
- **Fostering**: Encouraging or helping to develop.
- **International Standard (ISO 22301)**: A worldwide rule or guideline to follow for business continuity.
- **Control Measures**: actions to reduce or manage risks
- **Business Continuity Plan (BCP)**: a detailed plan to keep business running during disruptions
- **Disaster Recovery (DR)**: process to restore IT systems after a major failure
- **Incident Response Team (IRT)**: group that manages emergency events and immediate problems
- **Risk Register**: list or record of identified risks and how they are managed
- **BCMS**: Business Continuity Management System

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

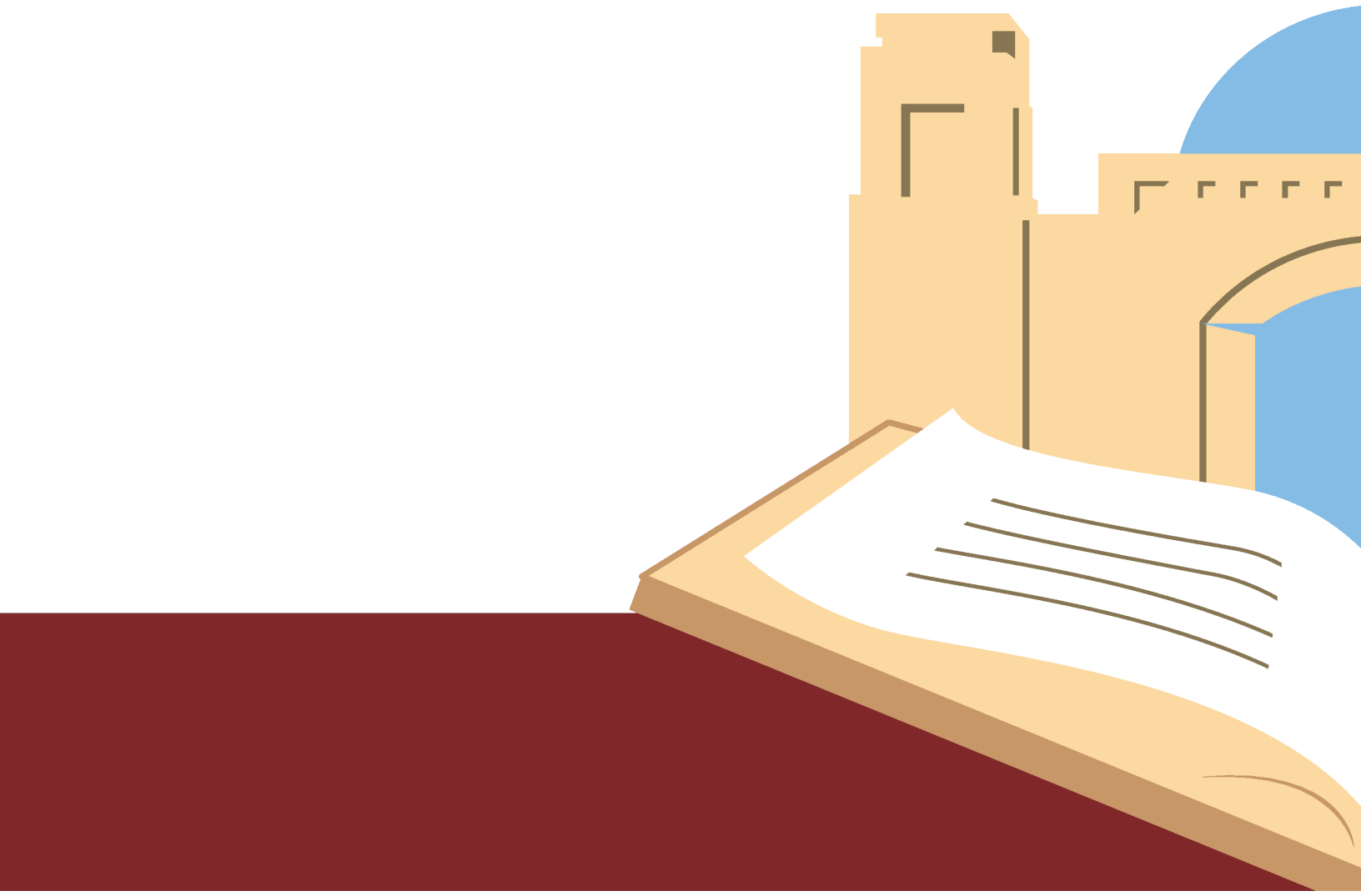
- **BCP**: Business Continuity Plan
- **BIA**: Business Impact Analysis
- **Ad-hoc**: A one-time or special action.
- **Contingency Plan**: A backup plan for emergencies.
- **KPIs (Key Performance Indicators)**: Metrics to measure the success of specific goals or actions.
- **Nonconformities (NCR)**: Issues or problems that don't meet standards.

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

Version/Modification Number 1/0	Release/modification date	Number of pages	Approved by
To be filled by QASP	To be filled by QASP	To be filled by QASP	To be filled by QASP

جامعة دار الحكمة
DAR AL-HEKMA UNIVERSITY

Information



xxxxxxxxxxxxxxxxxxxxxxxxxxxx

Purpose:

xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Membership:

- Xxxxx
- xxxxx

Chairperson: xxxxx

Terms of Appointment: xxxxxx

Frequency of Meetings: xxxxxxxxxxxxxx