THE UNIVERSITY OF TEXAS
MD Anderson Cancer Center
Making Cancer History®

Business Continuity Planning

Audit Control No. 2021-108
March 18, 2022

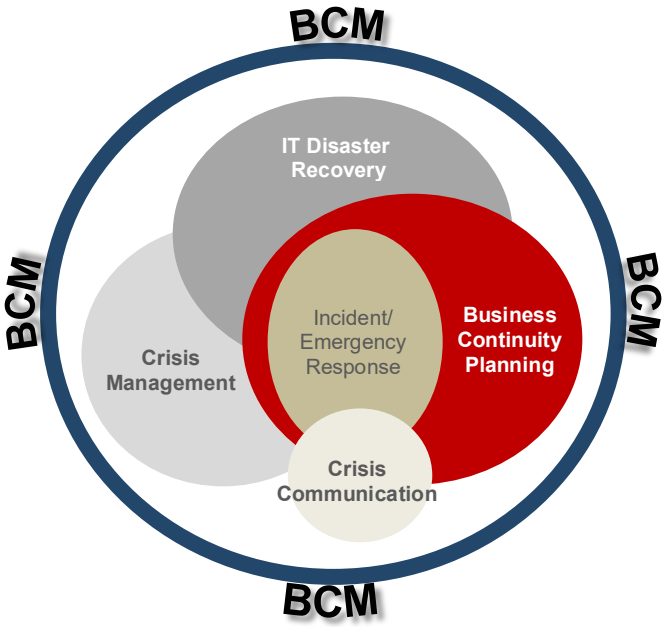
Audit Team:
Ann Lovelady
Randy Ray
Melissa Prompuntagorn
Anthony Buancore

MDA21-108 Business Continuity Planning

EXECUTIVE SUMMARY

Business Continuity Planning (BCP) is a **key** component of the Business Continuity Management (BCM) framework. It is a set of documented strategies and processes that helps the Institution ***plan,*** respond, manage and successfully resume critical operations in the event of a business disruption. This continuous process of planning, preparing and addressing identified institutional vulnerabilities decreases the level of risk and cost to the Institution while minimizing the impact to patients, employees and suppliers.

A well-designed BCM Program consists of BCP, Information Technology (IT) Recovery, Incident and Emergency Response, Crisis Management and Communication as depicted in the graph. All these components are integrated and collectively provide a framework that supports the Institution's continual commitment to organizational resiliency. Stakeholders, business partners, our community and regulators expect the Institution to be prepared to respond and adapt quickly and effectively to a threat or disruption. These expectations are further increased as we strive to become a High-Reliability Organization[1].



A 2019 assessment, performed by an external vendor, confirmed that the Institution's Incident/ Emergency Response and Crisis Management practices are consistent with industry standards. For example:

- The Institution utilizes an Incident Command System framework during real crisis events,
- An Emergency Management Strategic Advisory Council provides oversight and monitors critical resources,
- Information Technology Disaster Recovery (ITDR) management conducts annual resiliency testing (tabletops and technical recovery) for Tier 1 applications, and conducts Tier 2 & 3 testing every two years,
- EHSSEM conducts regular exercises of its Emergency Operations Plan and has a defined, well-documented process for tracking real crises, and
- The Institution utilizes a web-based training application to provide Emergency Management Preparedness and BCM awareness training to employees.

[1] *High-reliability organizations operate under challenging conditions yet experience fewer problems than would be anticipated as they have developed ways of "managing the unexpected" better than most organizations.*
(Source: Managing the Unexpected: Sustained Performance in a Complex World, K.E. Weick and K.M. Sutcliffe)

The prior assessment also recommended that management develop and implement a Business Impact Analysis (BIA). A BIA is management's analysis of critical resources, systems, facilities, and interdependencies that are required for the continuity of operations, along with the related risks, downtime and financial impact in the event of a business disruption. Environmental Health and Safety Sustainability and Emergency Management leadership planned to start facilitating this process in the Spring of 2020, but these plans were placed on hold due to the COVID-19 pandemic. Without a formal BIA in place, management could have a challenge prioritizing which critical areas and related interdependencies should be addressed initially in the event of a disruption.

During Internal Audit's assessment, we reviewed the Institution's BCP process and determined that some key areas have current business continuity, emergency preparedness and disaster recovery plans, while others are outdated or have no plans at all. Additionally, we noted that the Institution could strengthen its ability to respond to a disruption by:

- Establishing executive sponsorship and accountability for the execution of BCP across critical areas
- Developing and implementing a formal BIA that has been vetted by Senior Leadership
- Aligning the IT disaster recovery plan to the BIA
- Performing consistent testing of plans and modifying them as appropriate
- Providing training and education to individuals responsible for developing and implementing the plans
- Implementing an IT solution to help organize, maintain and secure critical information

Management Summary Response:
Management agrees with the observations and recommendations and has developed action plans to be implemented on or before December 31, 2022.

Appendix A outlines the methodology for this project. **Appendix B** provides a glossary of terms.

The courtesy and cooperation extended by the personnel in Environmental Health and Safety, Sustainability and Emergency Management are sincerely appreciated.

Sherri Magnus
Sherri Magnus, CPA, CIA, CFE, CRMA, CHIAP
Vice President & Chief Audit Officer
March 18, 2022

Detailed Observations

Observation 1:
Establish Executive Sponsorship and Accountability **RANKING: *HIGH***

Governance and executive sponsorship have not been established to ensure comprehensive business continuity planning across critical operational areas. Currently, EHSSEM acts as the custodian for the program. Establishing a governance framework, as well as designating an executive sponsor, would elevate the program's importance and establish accountability.

Executive sponsorship ensures that all stakeholders remain aligned and the needs of the organization are addressed from an enterprise-wide perspective. Ownership at an executive level enables business continuity planning to be visible to decision-makers and influences enterprise-wide adoption.

Recommendation:
Management should develop a governance structure and designate an executive sponsor to oversee the business continuity planning activity. The governance structure should include, but not be limited to, rules, practices and processes by which the business continuity program is overseen, directed and controlled.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Matt Berkheiser
Owner: Devina Patel
Implementation Date: August 31, 2022

Joint sponsorship has been established at the executive level, as indicated above. Management has drafted a charter to include bylaws, governance structure and scope of the program. We will revisit the existing policy in order to incorporate changes necessary resulting from the proposed charter requirements.

Observation 2:
Develop and Implement a Business Impact Analysis (BIA) **RANKING: *HIGH***

The Institution does not have a current Business Impact Analysis (BIA) that has been vetted and approved by Executive Leadership. The primary objective of a BIA is to assist management in identifying the critical resources, systems, facilities, records and interdependencies that are required for the continuity of operations, along with the related risks, in the event of a business disruption. Additionally, the BIA estimates the financial impact and the time it would take to recover critical resources.

Without a well-documented BIA, management will not have a plan outlining appropriate recovery strategies and solutions to mitigate the risks associated with an operational disruption.

Recommendation:
Management should coordinate with subject matter experts to develop and implement a formal BIA. The BIA should:

1. Identify activities that support critical business operations within the institution
2. Determine the financial, customer, operational, legal and/or regulatory impacts of each activity
3. Establish the timeframes in which business and technology activities must be recovered (recovery time objective)
4. Determine the amount of time mission-critical activities can be disrupted without causing significant harm to the organization's mission (maximum tolerable downtime or recovery point objective)
5. Define key internal and external relationships and dependencies of each activity
6. Identify the necessary resources that are required for the recovery of each activity and their associated recovery timeframes

Once the BIA is developed, a risk assessment should be conducted, and formal strategies documented in a formal plan. The existing hazard vulnerability assessment (HVA), while not comprehensive, could be leveraged in the risk assessment process.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Matt Berkheiser
Owner: Devina Patel
Implementation Date: December 31, 2022

EHSSEM Management is currently in the process of identifying potential 3rd party vendors through the sourcing process to develop a BIA. The contract request has been submitted. Once the BIA has been developed, a risk assessment will be conducted, and formal strategies will be documented in Business Continuity Plan(s).

Observation 3:
Align ITDRP to Business Impact Analysis **RANKING: *HIGH***

A Business Impact Analysis (BIA) serves as the foundation for a Disaster Recovery Plan (ITDRP). In the absence of the BIA, a Criticality Assessment (CA) has been established to apply a scoring system to objectively rank the criticality of applications and level of impact based on information provided by Application Owners. While the criticality assessment is a good start to identify impact, it does not fully assess the key functions within the institution and relevant applications systems that might be disruptive to the institution in the event of unavailability during a disaster.

Recommendation:
Once the BIA has been performed, management should revisit how applications have been prioritized to ensure alignment between the ITDRP and the BIA.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Craig Owen/Matt Berkheiser/Less Stoltenberg
Owner: Craig Owen
Implementation Date: 8/31/2023 (*assumes BIA will be done 12/31/2022*)

We concur with the observation and once a formal Business Impact Analysis (BIA) is developed and implemented, IT leadership will reassess all key supporting systems and align them with the key activities noted in the BIA.

Observation 4:
Perform Consistent Testing of Business Continuity Plans **RANKING: *HIGH***

When reviewing existing department plans, we found that testing is not consistently being performed. We noted that institution-wide testing is performed situationally, such as for potential cyberattacks. Without consistent testing of critical plans, the risks are increased that the plans may not be current, effective or executed as intended.

Recommendation:
Management should implement and maintain a program of testing to validate the effectiveness of its business continuity strategies and solutions. Testing should be aligned to address various types of disruptions, both brief and sustained. Testing should be performed at planned intervals and when there are significant changes within the organization or the context in which it operates. Management should utilize the results of testing to implement changes and improvements to the program.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Matt Berkheiser
Owner: Devina Patel
Implementation Date**:** December 31, 2022

EHSSEM Management will formalize a testing plan and schedule for business continuity plans for in-scope departments as confirmed by the Business Impact Analysis. Management will also obtain agreement for cooperation in testing from the management of these in-scope departments. Testing of plans will be performed as new plans are implemented and will continue to be performed for existing plans.

Observation 5:
Provide BCP Training and Education to Responsible Employees **RANKING: *HIGH***

While the institution provides training on emergency management, it includes only limited content on business continuity planning. Per discussions with various departments, we noted that individuals responsible for preparing plans were not provided with formal training. EHSSEM indicated that they will provide guidance in preparing a business continuity plan upon request.

Recommendation:
Management should ensure that employees responsible for preparing, updating, testing and executing departmental business continuity plans are competent and trained. Management should consider making the training mandatory for responsible staff.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Matt Berkheiser
Owner: Devina Patel
Implementation Date**:** December 31, 2022

EHSSEM Management will coordinate with Human Resources to make training available and mandatory for those responsible for developing and maintaining business continuity plans. Training should be taken by both responsible leaders and their support staff. Training will be set up and available by the implementation date.

Observation 6:
Implement an IT Solution to Manage BCP Program **RANKING: *MEDIUM***

The Institution has several IT solutions to be considered when determining a repository to organize, maintain and secure critical information. Currently, there is no single IT solution used in the BC planning process. Some departments are using Sustainable Planner, while others are using Excel or some portions of Archer. In the event of a business disruption or threat, a centralized source for accessing critical information is necessary to quickly make informed decisions. When plans lack complete and accurate information, management actions may be delayed, resulting in financial, operational or reputational effects to the Institution.

Recommendation:
Management should consider implementing a single IT solution that would ensure consistency and centralization of information.

Management's Action Plan:
Executive Leadership Team Member: Omer Sultan, Shibu Varghese, Rosanna Morris, David Jaffray
Division/Department Executive: Craig Owen/Matt Berkheiser/Less Stoltenberg
Owner: Devina Patel
Implementation Date: August 31, 2022

EHSSEM Management has designated Sustainable Planner as the IT application to use for this business continuity planning program. Management will continue to communicate this to end users. Management will coordinate with IT Management to consider additional solutions.

Appendix A

Objective, Scope and Methodology:

The objective of the review is to provide a general assessment of the institution's business continuity planning for critical operations. Our scope included controls and processes in place during the period of April through October 2021.

Our procedures included the following:

- Interviewed key EHSSEM personnel and responsible department staff
- Reviewed relevant institutional policies and procedures, including Institutional Policy ADM0929 "Business Continuity Planning"
- Reviewed relevant industry standards and white papers related to BCM and BCP, including ISO22301
- Obtained and reviewed available departmental business continuity plans
- Reviewed prior assessments and audits related to business continuity planning and disaster recovery

Our internal audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing*. The internal audit function at MD Anderson Cancer Center is independent per the *Generally Accepted Government Auditing Standards (GAGAS)* requirements for internal auditors.

Number of Priority Findings to be monitored by UT System: None
A Priority Finding is defined as "*an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.*

Appendix B Glossary of Terms

KEY TERM	DEFINITION
Business Continuity	The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.
	The capability of an organization to continue the delivery of products or services at acceptable predefined levels following a disruption.
Business Continuity Plan (BCP)	Documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes with be sustained during and after a significant disruption.
	One or more comprehensive written plans to maintain or resume business in the event or a disruption.
	Documented procedures that guide organizations to respond, recover, resume and restore to a predefined level of operation following disruption.
Business Continuity Management (BCM)	The process for management to oversee and implement resilience, continuity and response capabilities to safeguard employees, customers, and products and services
	A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and that provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Impact Analysis (BIA)	An analysis of an information system's requirements, functions and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.
	Management's analysis of an entity's requirements, functions and interdependencies used to characterize contingency needs and priorities in the event of a disruption.
	Process of analyzing activities and the effect that a business disruption might have on them.
Crisis Communications	As part of crisis management, crisis communication is the planning, development and delivery of all messaging utilized as part of a coordinated response to an event. Crisis communications should include audiences both internal and external to the organization and may include the use of phone, email, websites, social medial and mass notifications tools.
Crisis Management	The process of managing an entity's preparedness, mitigation response, continuity of recovery in the event of an unexpected significant disruption, incident or emergency.
Disaster Recovery (DR)	[One of the three core disciplines of BCM.] Also known a IT disaster recovery (ITDR), a set of processes, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications vital to an organization after a disaster or outage. Disaster recovery focuses on information or technology systems that support business functions, as opposed to business continuity, which involves planning for keeping all aspects of a business functioning amid disruptive events. Disaster recovery is a subset of business continuity.
Emergency Management/ Operations	See ***Crisis Management.***
Emergency Response	Actions taken in response to a disaster warning or alert to minimize or contain the eventual negative effects, and those taken to save and preserve lives and provide basic services in the immediate aftermath of a disaster impact, for as long as an emergency situation prevails.
Financial Risk	Economic and quantifiable impacts resulting from a disruption to normal business. This may include loss of revenue, unusual incurred expenses, market capitalization, sanctions or penalties due to legal or compliance concerns, etc.
Incident Response	The response of an organization to disaster or other significant event that may significantly impact the organization, its people or its ability to function productively. An incident response may include evacuation of a facility, initiating a disaster recovery plan, performing damage assessment, and any other measures necessary to bring an organization to a more stable status.
IT Disaster Recovery (ITDR)	See ***Disaster Recovery***.
Mission Critical	Any telecommunications or information system that is defined as a national security system (FISMA) or that processes any information the loss, misuse, disclosure or unauthorized access to or modification of would have a debilitating impact on the mission of an agency.
Operational Risk	The risk of loss resulting from inadequate or failed procedures and controls. This includes loss from events related to technology and infrastructure, failure, business interruptions and staff-related problems and from external events such as regulatory changes.

Resilience	Ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents or naturally occurring threats or incidents.
Reputation Risk	A type of risk that relates to unwanted or negative attention resulting from an event or disruption impacting normal business. Reputation risk can be realized due to negative social media activity (e.g., Glassdoor, Facebook or LinkedIn comments) intended to paint the organization in a negative light toward a broad audience.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
	The process of identifying the risks to an organization, assessing the critical functions necessary for an organization to continue business operations, defining the controls in place to reduce organization exposure and evaluating the cost of such controls.

Table property of Protiviti: A Guide to Business Continuity Management – Top 15 FAQs (pages 20 -24)