Program Definition 3

Mission 3

Vision 3

Structure/Scope 3

Business Continuity Management Governance 3

Business Continuity Management within the University 3

Business Continuity Management Steering Committee 4

Business Continuity Management Strategy Overview 4

First Line 4

Second Line 5

Third Line 5

Business Continuity Management Scope of Activities 6

Business Impact Analysis 6

Risk Management 6

Business Continuity Planning 6

Disaster Recovery 6

Emergency Management 6

Training, Exercise and Awareness Program 6

Program Driving Influence 7

Objectives 8

Business Continuity Management Objectives 8

Program Improvement and Maturity 9

Policies and Standards 9

Overview and Structure 9

Organizational Factors: 10

Regulatory Factors: 10

Review and Approval 10

Policy Exceptions / Deferrals 10

Distribution 10

Control Activities 10

Roles and Responsibilities 10

Reporting Structure 10

Interdepartmental Responsibilities 10

Appendices 12

Appendix 1: List of Divisions 12

Appendix 2: RACI Chart 13

Appendix 3: Revision History 14

Appendix 4: Contact Information 14

Program Definition

Mission

The mission of the Business Continuity Management Program (BCMP) at the University of Rochester (UR) is to build a culture of resiliency by ensuring strategies and plans are in place to prevent and counteract interruptions to business activities and protect critical business functions from the effects of major failures of internal or external disasters and to ensure their timely resumption of services.

Vision

The University will create and sustain a culture of organizational resiliency through a comprehensive and collaborative program composed of professional, knowledgeable staff who advocate minimizing risk and building efficiency and proficiency in responding to disruptive events.

Structure/Scope

The BCMP is charged with the business continuity activities for the organization. For this document and subsequent BCMP policies and standards, ‘organization’ is defined as the University of Rochester, the University of Rochester Medical Center and all the departments within each division. Specific areas of focus for the BCMP include but not limited to:

- Governance
- Disaster Recovery
- Business Impact Analysis
- Training, Exercises and Awareness
- Business Continuity
- Crisis Management
- Risk Management

A list of all divisions is provided in Appendix A.

Business Continuity Management Governance

The University of Rochester Business Continuity Management Program’s primary oversight body is the University Business Continuity Management Governance Committee. The University of Rochester (UR) Business Continuity Management Governance Committee is the guiding body to review risks and mitigation strategies associated with patient care, research, administration, and academics, set priorities for BCM Program implementation and risk mitigation, and is accountable for mitigating business continuity and disaster recovery risk levels acceptable to the University. This group defines the BCM overview and strategy, conducts final approval of, and changes to, BCM policies prior to going to the University Policy Committee for approval and adoption, and approves standards and guidelines necessary to ensure commonly acceptable practices are being employed across the organization.

The UR Business Continuity Management Governance Committee also ensures compliance with all necessary legal, regulatory and accreditation requirements are met by incorporating these requirements into policies and standards prior to going to the University Policy Committee. The Business Continuity Management Governance Committee will escalate problems to the Senior Leadership Group (SLG) and/or President’s Cabinet when necessary.

Business Continuity Management within the University

The Business Continuity Management Governance Committee is chaired by the University Senior Vice President (SVP) of Administration and Finance, Chief Financial Officer and Treasurer (CFO). Members of the committee include key business leaders across all major groups at the University, including but not limited to:

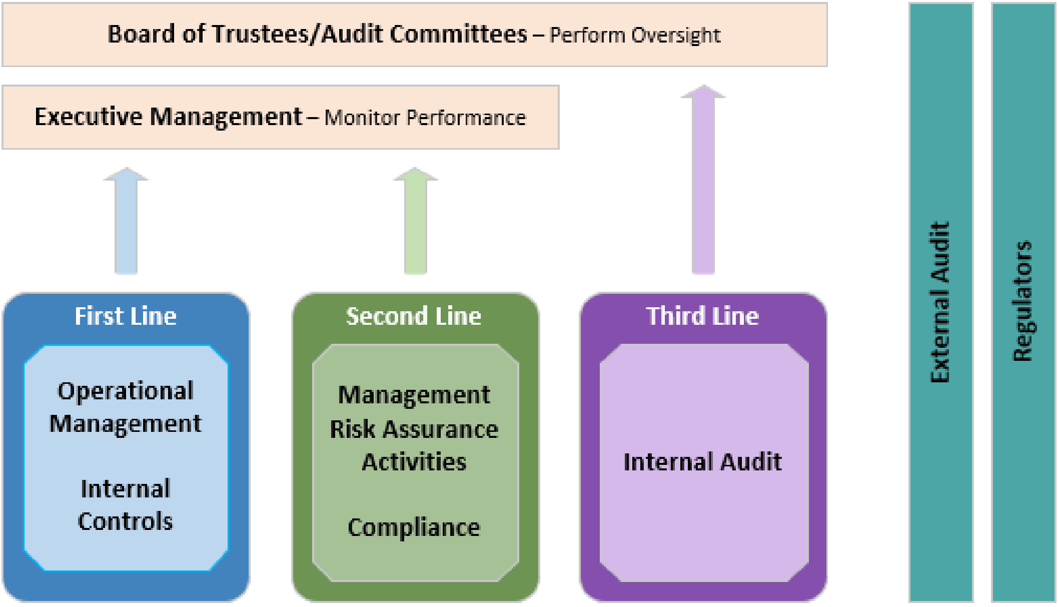
- Executive Vice President for Administration & Finance, & CFO
- Sr. VP & CFO, URMC
- Sr. VP & Chief Investment Officer
- Chief Audit Executive
- VP Info Technology & CIO
- Sr. Assoc. VP, University Facilities & Services
- Assoc. VP, URMC IT Technology & CTO
- VP & Chief Human Resources Officer
- Chief Info Security & Technology Officer
- Assoc. VP Risk Management
- Deputy to the Provost
- Assoc. VP Environmental Health & Safety
- Assoc. VP Research

Business Continuity Management Steering Committee

The BCM Steering Committee is composed of subject matter experts and other key stakeholders who provide recommendations and guidance to the Governance Committee regarding policies, standards, and implementation strategies across the enterprise (see Business Continuity Lines of Defense below). The BCM Steering Committee is chaired by the Business Continuity Management Program Manager.

Business Continuity Management Strategy Overview

As established through the Enterprise Risk Management (REM) Program, the University has adopted the Three Line Model to the operationalization and compliance of the BCMP.


Board of Trustees/Audit Committees – Perform Oversight
Executive Management – Monitor Performance
First Line
Operational Management
Internal Controls
Second Line
Management Risk Assurance Activities
Compliance
Third Line
Internal Audit
External Audit
Regulators

First Line

The first line is at the business level. This group is responsible for conducting and the documentation of all activities that meet the BCM policy and standard controls. As the most knowledgeable about the business, this group is responsible for business continuity plan development, updates, training and testing. Business areas shall assign business continuity liaisons who shall fulfill these activities and documentation for their business area.

Second Line

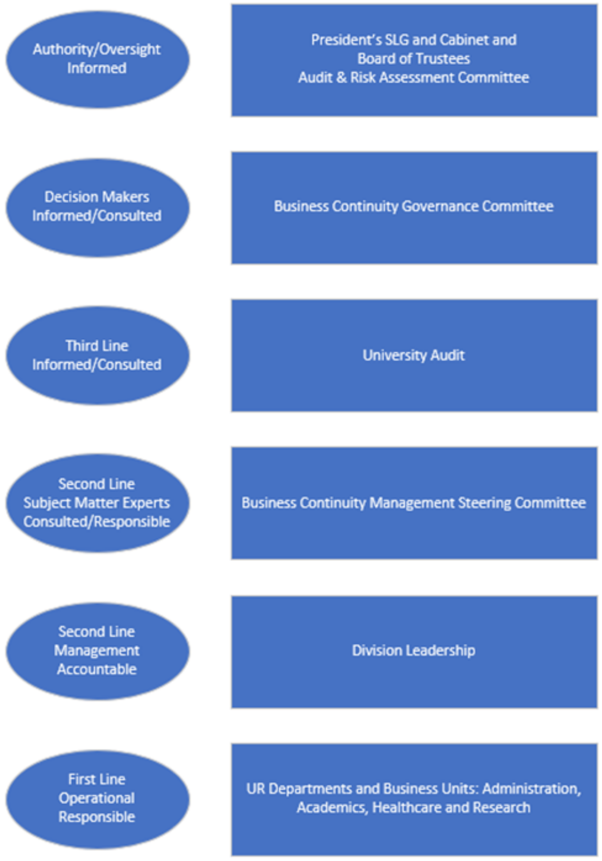
The second line is composed of the BCM Program staff and the BCM Steering Committee which is a group of subject matter experts in the various sub-specialties of BCM. The second line is charged with providing recommendations and subject matter expertise on control requirements, best practices and industry standards to the governance committee for policy and standard updates. Guidance and education to department-level staff responsible for business continuity management activities is also provided by this group and includes:

- Policy/standard changes
- Training, Exercise and Awareness Program
- Business Continuity plan development
- Disaster Recovery Program
- Coordination and collaboration with external partners
- Emergency Management
- Gap analysis
- Audit readiness
- Business Intelligence
- Program maturity level review
- Staff Readiness

Third Line

Internal Audit is the third line in the BCMP and audits compliance against, standards and plans.

Business Continuity Organizational Structure



A full list of the sub-lines of business found in appendix A

A chart that defines who is responsible, accountable, consulted and informed (RACI) for program activities can be found in appendix B.

Business Continuity Management Scope of Activities

Business Impact Analysis

Business Impact Analysis determines the criticality of a business function to the organization and tolerable downtimes of the business functions which is key in the pre-planning phase. Business function is defined as any singular type of resource within the organization. Examples include a department or service. The business function is reviewed on the following objectives:

- Life safety (patient, student, staff, etc.)
- User impact
- Legal/regulatory/accreditation implications
- Reputational impact
- Educational impact
- Data Classification
- Patient care delivery
- Financial impact
- Backlog business functioning
- Service level agreement
- Research impact
- Employee productivity

Risk Management

Through a variety of risk assessments, BCMP monitors the University for risks that could impact business delivery, develops reports with findings, and delivers corrective action plan recommendations to risk owners. Trends in risk findings get reported to the Governance Committee.

Business Continuity Planning

Business Continuity Planning is the development of plans that address the life cycle of an incident including immediate response plans, continuity of operations plans and recovery plans. These plans focus on people, processes and buildings to ensure resiliency.

Disaster Recovery

Disaster Recovery focuses on the architecture design, development, maintenance and testing of information technology resources to ensure their availability meets the business needs as defined in the business impact analysis.

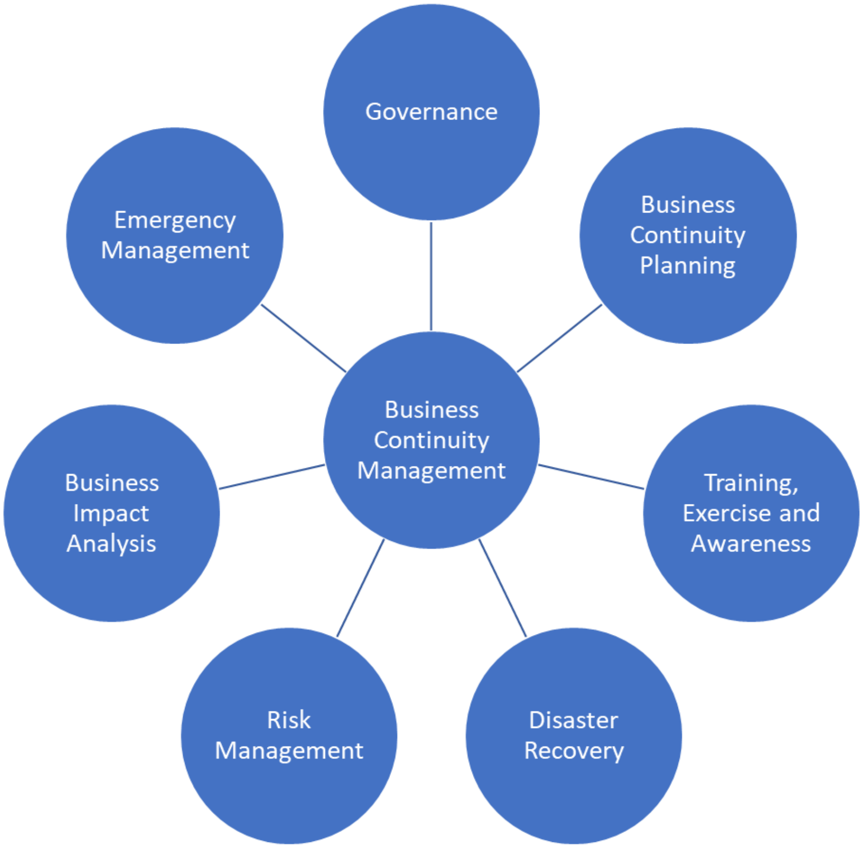
Emergency Management

Emergency Management is the defined methodology for how the organization manages an operational disruption or declared disaster and includes standard operating procedures for incident identification, evaluation, escalation, declaration, activation and deactivation with a significant focus on crisis communications.

Training, Exercise and Awareness Program

The development, execution and evaluation of business continuity related training awareness materials build organizational resiliency and validate the effectiveness of business continuity and disaster recovery plans. Training, exercise, and awareness program responsibility shall span across the first and second line of defense. The BCM Program office training and awareness program shall focus on educating the business continuity liaisons and increasing a culture of resiliency at the organization. Business continuity liaisons shall be responsible for training and awareness to staff in their business area and coordinating exercises to validate plans.

The primary BCMP functions along with other BCM activities are designed to orchestrate business resiliency activity alignment with the organization's missions and reduce overall risk to the University.


Governance
Emergency Management
Business Continuity Planning
Business Continuity Management
Business Impact Analysis
Training, Exercise and Awareness
Risk Management
Disaster Recovery

Program Driving Influence

The BCMP follows the best practices designed for organizations including academic medical centers. The program framework is designed to overlay and provide alignment with industry standards and regulatory requirements where necessary. This includes, but not limited to:

- ISO 22301:2019 Security and Resilience – Business Continuity Management Systems Requirements
- BCI Good Practices Guidelines
- DRII Professional Practices 2017
- HiTrust CSF
- HIPAA 45 CRF 164.308
- CMS Emergency Preparedness Rule
- FEMA NIMS Standards
- NFPA 1600 2013

Objectives

The following objectives have been identified as the key areas where BCMP will focus its attention.

Business Continuity Management Objectives

Focus Area	Objective
Business Continuity Management Governance	• Maintain policies and procedures that meet legal, regulatory and accrediting standards • Provide strategic direction and priorities for the BCMP • Establish KPIs and KRIs for the program to be measured to • Provide reporting of program progress, successes and challenges to Senior Leadership Group
Business Impact Analysis	• Identify critical services to the organization • Determine Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for all business functions • Identify dependencies within the organization
Risk Management	• Continuously monitor for and identify risks to operations • Identify mitigation strategies to address risk • Evaluate effectiveness of mitigation efforts on residual risk
Business Continuity Plans	• Create plans to address immediate response, continuity of operations and recovery from a disruptive event
Disaster Recovery	• Architecture review based on business needs to ensure appropriate IT resourcing • Recover critical information technology resources to meet the business RTO defined in the BIA • Minimize data loss to meet RPO defined in the BIA
Crisis Management	• Establish standardized procedures for an efficient and prompt response, analysis, documentation, ongoing management and reporting of incidents
Training, Exercises and Awareness	• Educate business continuity liaisons on best practice and requirements • Build a culture of resiliency in the organization • Increase proficiency of department staff on appropriate response, continuity and recovery actions for various scenarios • Validate existing plans and procedures

Program Improvement and Maturity

The BCMP uses the Plan-Do-Check-Act (PDCA) model for continuous process improvement. Examples of activities in each phase of this model are listed below.

Plan (establish)	Establish policies and standards (controls), procedures and goals related to business continuity management and that align with the University's mission
Do (implement and operate)	Implement and operationalize business continuity management policy, standards (controls) and procedures
Check (monitor and review)	Assess performance against policy and standards (controls) and goals; report progress to Governance for review and to determine and authorize plans for remediation and improvement
Act (maintain and improve)	Maintain and improve the BCMP through the use of corrective action based on management review and review of scope of BCMP policy, standards and goals.

*Credit to ISO 22301 for the table

In coordination with the PDCA model, BCMP uses the maturity model index designed by NIST to track overall program growth. This model scores overall maturity on a scale of zero to five. The model is as follows:

Maturity Level					
Non-Existent	Initial	Repeatable	Defined	Managed	Optimized
No policy, procedures, controls in documentation or practice	Many of the required controls are defined in a policy but are not implemented	Most, if not all, of the control specifications are defined in policy, many are supported by procedures, but few, if any are implemented.	Most, if not all, of the control specifications are defined in policy and supported by procedures, and many are implemented as required.	Most, if not all, of the control specifications are defined in policy, supported by procedures, implemented, and many are routinely tested to ensure they function as required.	Most, if not all, of the control specifications are defined in policy, supported by procedures, implemented, tested, and many are actively managed to ensure they function as required.
0	1	2	3	4	5

BCMP views level 3 as a minimum acceptable level of control and targets a score of 5 for an optimal business continuity environment. Based on the data collected, the BCMP will be responsible for assigning a score for each section area of the BCMP and an overall program score. The scores will be decided upon based on Business Continuity Governance Committee judgment.

Policies and Standards

Overview and Structure

The scope of policies and standards addressed within the UR BCMP encompasses key areas of several standards and may additionally include areas of focus that are unique to the UR environment. For every identified business continuity management policy, a supporting standards document will be created that gives more detailed instructions on how to achieve the goals outlined in the policy. At the discretion of the UR BCMP, additional "guidance" and template documentation may be created to help clarify and normalize expectations.

Organizational Factors: Considering the size, resources dedicated, operational capacity, employees, and financial impact.

Regulatory Factors: Considering the compliance and legal requirements the organization is subject to.

Review and Approval

Policies and standards will be reviewed and approved on at least an annual basis, or more frequently as needed. Changes to policy and standards are approved by the Business Continuity Governance Committee prior to going to the University Policy Committee for final approval, and maintained on the University's Policies and Procedures website.

Policy Exceptions / Deferrals

Exceptions and/or deferrals to business continuity management policies or standards may be put in writing to the Business Continuity Management Governance Committee. If requests are not approved and further analysis is desired, the requestor may bring it to the Business Continuity Management Program (BCMP) Manager for disposition. If further evaluation is needed, the BCMP Manager will bring the request to the Governance Committee.

Distribution

All business continuity management policies and standards are posted on the University's Policies and Procedures website to ensure all employees are kept up to date of changes. For major changes to policy and/or standard, the BCM steering committee will notify all applicable staff of the change through business continuity education and awareness email.

Control Activities

Based on the policies and standards defined within, a list of business continuity control activities will be defined. Control activities are defined as specific and measurable actions taken to maximize resiliency. These control activities are directly mapped to the specific sections defined in the corresponding standard, and serve as supplemental documentation to help ensure business functional area compliance with business continuity policy and standards. These controls will also serve as a basis for the BCM Steering Committee or Internal Audit to assess overall compliance with policies and standards. As these control activities are directly derived from the approved standard documents, they will not be separately reviewed or approved unless they differ from the approved documentation. The BCM Steering Committee will be responsible for creating and updating the control activity documents as procedures change.

Roles and Responsibilities

Reporting Structure

The UR BCM Steering Committee members reside in and report to leadership across the University.

Interdepartmental Responsibilities

Many roles and responsibilities related to or involving business continuity span multiple groups and departments. The following chart highlights critical areas of shared responsibility for business continuity management:

Activity	SME Department
Physical Security	Facilities, Public Safety
Training and Awareness	Facilities, Public Safety, Environmental Health & Safety, University IT, Information Systems Division, Public Relations, Department Business Continuity Liaisons
Crisis Communications	Public Relations
Risk Management	Facilities, Public Safety, Environmental Health & Safety, University IT, Information Systems Division

Crisis Management	Environmental Health & Safety
Disaster Recovery	University IT, Information Systems Division
Business Continuity	Environmental Health & Safety, Department Business Continuity Liaisons

Appendices

Appendix 1: List of Divisions

- Central Administration
- Eastman Institute of Oral Health
- Eastman School of Music
- Hajim School of Engineering
- Health Sciences
- Memorial Art Gallery
- River Campus Colleges
- School of Arts & Sciences
- School of Medicine & Dentistry
- School of Nursing
- Simon School of Business
- Strong Memorial Hospital
- UR Medical Faculty Group
- Warner School of Education

Appendix 2: RACI Chart

R = responsible
A = accountable
C = consulted

Activity	Business Area Leadership	Business Area Liaison	BCM Program Staff	BCM Steering Committee	BCM Governance Committee	University Audit
Develop Policy and Standards for the BCM Program	I	I	R	R	A/I/C	I
Update Policy and Standards to meet regulatory and accrediting requirements	I	I	R	R	A/I/C	I
Communicating changes in policy and standard to business area representatives	I	I	R	R	I	I
Documenting business continuity/disaster recovery plans	A	R	C/I	C/I	I	I
Updating business continuity/disaster recovery plans	A	R	C/I	C/I	I	I
Training staff on business continuity/disaster recovery plans	A	R	C/I	C/I	I	I
Testing business continuity/disaster recovery plans	A	R	C/I	C/I	I	I
Training Business area leadership and business continuity liaisons on BCM concepts	I	I	R	R	I/A	I
Documenting tests and live event After Action Reports	A	R	C/I	C/I	I	I
Determining continuity and recovery strategies for the business	A	R	C/I	C/I	I	I

I = informed

Appendix 3: Revision History

Modification(s) Made	Individual Making Modifications	Date of Modification	Reviewer	Review Date
Document Created	UR BCMP Program Director	1/29/2020		
Documented edited	UR BCMP Project Director	5/11/2021		
Document edited to include steering committee	UR BCMP Project Director	5/26/2021		
Document updated to align with ERM	UR BCMP Project Director	8/4/2021		
Document updated per Governance Committee review	UR BCMP Project Director	9/16/2021		
Document reviewed and approved; updated approval dates	UR BCMP Project Director	10/8/2021	UR BCM Governance Committee	10/1/2021

Appendix 4: Contact Information

Please address any questions or concerns with any policies set forth within this document to the Business Continuity Management Program office: (avincent@safety.rochester.edu).