Contents

Scope

For the purposes of this policy document all references to "organization" or "organizations" shall refer to both the University of Rochester as well as the University of Rochester Medical Center and Affiliates (URMC). This policy applies to the entire organization.

12.0 Business Continuity Management

12.01 Information Security Aspects of Business Continuity Management

12.a Including Information Security in the Business Continuity Management Process

This section is designed to address information security considerations in the Business Continuity Management Program. See Sections 12.02 Business Impact Analysis and 12.05 Incident Management for detailed requirements.

Level 1 Requirements

The Business Continuity Management Program (BCMP) and processes shall bring together the following key elements of business continuity management:

1. identifying all the assets involved in critical business processes (see 12.02);

2. considering the purchase of suitable insurance, which may form part of the overall business continuity process, as well as being part of operational risk management;

3. ensuring the safety of personnel and the protection of information assets and organizational property; and (see 12.05)

4. formulating and documenting business continuity plans addressing information security requirements in line with the agreed business continuity strategy (see 12.c).

Level 2 Requirements

Level 1 plus:

The Business Continuity Management Program and processes shall bring together the following key elements of business continuity management:

1. identifying critical information system assets supporting organizational missions and functions (see 12.03);
2. understanding the risk(s) the organization is facing in terms of likelihood and impact in time, including an identification and prioritization of critical business processes;
3. understanding the impact which interruptions caused by information security incidents are likely to have on the business (it is important that solutions are found that will handle incidents causing smaller impact, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information assets (see 12.02);
4. implementing additional preventive detective controls for the critical assets identified to mitigate risks to the greatest extent possible;
5. identifying financial, organizational, technical, and environmental resources to address the identified information security requirements (see 12.03);

6. testing and updating, at a minimum, a section of the plans and processes put in place at least annually (see 12.06);
7. ensuring that the management of business continuity is incorporated in the organization's processes and structure; and
8. assigning responsibility for the business continuity management process at an appropriate level within the organization.

Level 1 Industry Control Mapping

1 TAC § 390.2(a)(4)(A)(xi)
AICPA A1.3
AICPA CC3.1
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-2(8) (HIGH)
CMSRs 2013v2 PM-9 (HIGH)
CRR V2016 EDM:G3.Q1
CRR V2016 SCM:G1.Q1
CRR V2016 SCM:MIL2.Q1
CRR V2016 SCM:MIL2.Q2
CRR V2016 SCM:MIL2.Q4
CSA CCM v3.0.1 BCR-09
FedRAMP CP-2
FedRAMP CP-2(8)
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.308(a)(7)(ii)(D)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.312(a)(2)(ii)
IRS Pub 1075 v2014 9.3.6.2
ISO/IEC 27002:2005 14.1.1
ISO/IEC 27002:2013 17.1.2
MARS-E v2 CP-2
MARS-E v2 PM-9
NIST Cybersecurity Framework ID.AM-5
NIST Cybersecurity Framework PR.IP-11
NIST Cybersecurity Framework PR.IP-9
NIST SP 800-53 R4 CP-1
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-2(8)

Level 2 Industry Control Mapping

1 TAC § 390.2(a)(4)(A)(xi)
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-2(8) (HIGH)
CRR V2016 AM:G2.Q1
CRR V2016 CCM:G1.Q2
CRR V2016 EDM:G3.Q1
CRR V2016 SCM:G1.Q1
CRR V2016 SCM:G3.Q1
CRR V2016 SCM:G3.Q3
CRR V2016 SCM:MIL3.Q4
CSA CCM v3.0.1 BCR-09
FedRAMP CP-2
FedRAMP CP-2(8)
FFIEC IS v2016 A.6.35(a)
FFIEC IS v2016 A.6.35(c)
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.308(a)(7)(ii)(D)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.312(a)(2)(ii)
IRS Pub 1075 v2014 9.3.6.2
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.1
ISO/IEC 27002:2013 17.1.2
MARS-E v2 CP-2
NIST Cybersecurity Framework DE.AE-4
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.BE-5
NIST Cybersecurity Framework PR.IP-9
NIST SP 800-53 R4 CP-1
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-2(8)
NIST SP 800-53 R4 PM-9

12.b Business Continuity and Risk Assessment

This section is designed to address information security considerations in the Business Continuity Management Program. See Sections 12.02 Business Impact Analysis and 12.0 Business and IT Recovery for detailed requirements.

Level 1 Requirements

This process shall identify the critical business processes. Information security aspects of business continuity shall be based on identifying events (or sequence of events) that can cause interruptions to the organization's critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters and acts of terrorism). This shall be followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period. Based on the results of the risk assessment, a business continuity strategy shall be developed to identify the overall approach to business continuity. Once this strategy has been created, endorsement shall be provided by management, and a plan created and endorsed to implement this strategy.

Level 2 Requirements

Level 1 plus: This process shall identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as

operations, staffing, materials, transport and facilities. The consequences of disasters, security failures, loss of service, and service availability shall be subject to a business impact analysis. Business continuity risk assessments shall be carried out annually with full involvement from owners of business resources and processes. This assessment shall consider all business processes and shall not be limited to the information assets, but shall include the results specific to information security. It is important to link the different risk aspects together to obtain a complete picture of the business continuity requirements of the organization. The assessment shall identify, quantify, and prioritize risks against key business objectives and criteria relevant to the organization, including critical resources, impacts of disruptions, allowable outage times, and recovery priorities.

Level 1 Industry Control Mapping

1 TAC § 390.2(a)(4)(A)(xi)
AICPA CC3.1
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-2(8) (HIGH)
CRR V2016 AM:G1.Q2
CRR V2016 EDM:G3.Q1
CRR V2016 SCM:G1.Q2
De-ID Framework v1 Physical and Environmental Security: General
FedRAMP CP-2
FedRAMP CP-2(8)
HIPAA § 164.308(a)(7)(ii)(A)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(E)
IRS Pub 1075 v2014 9.3.6.2
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.1
ISO/IEC 27002:2005 14.1.2
ISO/IEC 27002:2013 17.1.1
ISO/IEC 27002:2013 17.1.2
MARS-E v2 CP-2
NIST Cybersecurity Framework DE.AE-4
NIST Cybersecurity Framework ID.BE-2
NIST Cybersecurity Framework ID.BE-5
NIST Cybersecurity Framework ID.RA-1
NIST Cybersecurity Framework ID.RA-3
NIST Cybersecurity Framework ID.RA-4
NIST Cybersecurity Framework ID.RA-5
NIST Cybersecurity Framework ID.RM-3
NIST Cybersecurity Framework PR.IP-9
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-2(8)

Level 2 Industry Control Mapping

CMSR s 2013v2 PM-8(High)
CRR V2016 AM:G3.Q1
CRR V2016 AM:G7.Q1
CRR V2016 RM:G2.Q2
CRR V2016 SCM:G1.Q4
CRR V2016 SCM:MIL2.Q4
CRR V2016 SCM:MIL3.Q4
CSA CCM v3.0.1 BCR-09
HIPAA § 164.308(a)(7)(ii)(A)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(E)
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.2
ISO/IEC 27002:2013 17.1.1
MARS-E v2 PM-8
NIST Cybersecurity Framework ID.BE-2
NIST Cybersecurity Framework ID.BE-4
NIST Cybersecurity Framework ID.RA-3
NIST Cybersecurity Framework ID.RA-4
NIST Cybersecurity Framework ID.RA-5
NIST Cybersecurity Framework ID.RM-3
NIST SP 800-53 R4 PM-8
NIST SP 800-53 R4 RA-3

12.c Developing and Implementing Continuity Plans Including Information Security

This section is designed to address information security considerations in the Business Continuity Management Program. See Sections 12.03 Business and IT Recovery for detailed requirements.

Level 1 Requirements

A formal, documented contingency planning policy (addressing purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance); and formal, documented procedures (to facilitate the implementation of the contingency planning policy and associated contingency planning controls) shall be developed, disseminated, and reviewed annually.

The business continuity planning process shall include the following:

1. implementation of the procedures to allow recovery and restoration of business operations and availability of information in required timescales;

2. particular attention shall be given to the assessment of internal and external business dependencies and the contracts in place;

3. documentation of agreed procedures and processes; and

4. testing and updating of at least a section of the plans.

The planning process shall focus on the required business objectives (e.g., restoring of specific communication services to customers in an acceptable amount of time). The procedures for obtaining necessary electronic covered information during an emergency shall be defined. The services and resources facilitating this shall be identified, including staffing, non-information processing resources, as well as fallback arrangements for information processing facilities. Such fallback arrangements may include arrangements with third parties in the form of reciprocal agreements, or commercial subscription services. The organization shall coordinate contingency planning activities with incident handling activities.

Developed business continuity plans shall:

1. identify essential missions and business functions and associated contingency requirements;

2. provide recovery objectives, restoration priorities, and metrics;

3. address contingency roles, responsibilities, assigned individuals with contact information;

4. address maintaining essential missions and business functions despite an information system disruption, compromise, or failure;

5. address eventual, full information system restoration without deterioration of the security measures originally planned and implemented;

6. be reviewed and approved by designated officials within the organization; and

7. be protected from unauthorized disclosure and modification.

Continuity and recovery plans shall be developed and documented to deal with system interruptions and failures caused by malicious code. Business continuity plans shall include recovering from malicious code attacks, including all necessary data and software back-up and recovery arrangements.

Copies of the business continuity plans shall be distributed to the Information System Security Officer, System Owner, Contingency Plan Coordinator, System Administrator, and Database Administrator (or the organization's functional equivalents).

If alternative temporary locations are used, the level of implemented security controls at these locations shall have logical and physical access controls that are equivalent to the primary site, consistent with the HITRUST CSF.

The information system implements transaction recovery for systems that are transaction-based.

Level 2 Requirements

Level 1 plus:

The business continuity planning process shall include the following:

1. identification and agreement of all responsibilities and business continuity procedures;

2. identification of the acceptable loss of information and services(see 12.02);

3. operational procedures to follow pending completion of response, recovery and restoration including:

i. alternative storage and processing site possibilities; and

ii. emergency power and back-up telecommunications to the primary site.

4. appropriate education of staff in the agreed procedures and processes, including crisis management (see 12.06).

Business continuity plans shall address organizational vulnerabilities and therefore may contain covered information that needs to be appropriately protected. Copies of business continuity plans shall be stored in a remote location, at a sufficient distance to escape any damage from a disaster at the main site. Management shall ensure copies of the business continuity plans are up to date and protected with the same level of physical and logical security as applied at the main site. Other material necessary to execute the continuity plans shall also be stored at the remote location.

The organization shall identify alternative temporary locations for processing. The necessary third-party service agreements shall be established to allow for the transfer and resumption of information systems operations of critical business functions within a time-period (e.g., priority of service provisions) as defined by a risk assessment (see 12.b). The organization shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. The alternate location shall be at a sufficient distance to escape any damage from a disaster at the main site. The type of configuration for the alternate site shall be defined by the risk assessment (see 12.b). Acceptable solutions include:

1. cold sites - a facility with adequate space and infrastructure to support the system;

2. warm sites - partially equipped office spaces that contain some or all of the system hardware, software, telecommunications and power sources;

3. hot sites - office spaces configured with all of the necessary system hardware, supporting infrastructure and personnel; and/or

4. mobile sites - self-contained, transportable shells custom-fitted with IT and telecommunications equipment necessary to meet the system requirements.

The organization shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. The organization develops alternate processing site agreements that contain Priority-of-Service provisions in accordance with the organization's availability requirements, including recovery time objectives (RTOs). The organization shall ensure that the alternate processing site provides information security measures equivalent to that of the primary site.

Level 1 Industry Control Mapping

1 TAC § 390.2(a)(1)
1 TAC § 390.2(a)(4)(A)(xi)
AICPA A1.2
AICPA A1.3
AICPA CC3.1
AICPA CC3.2
CMSRs 2013v2 CP-1 (HIGH)
CMSRs 2013v2 CP-10(2) (HIGH)
CMSRs 2013v2 CP-10(4) (HIGH)
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-2(1) (HIGH)
CMSRs 2013v2 CP-2(2) (HIGH)
CMSRs 2013v2 CP-2(3) (HIGH)
CMSRs 2013v2 CP-2(4) (HIGH)
CMSRs 2013v2 CP-2(5) (HIGH)
CMSRs 2013v2 CP-7 (HIGH)
CRR V2016 AM:G7.Q2
CRR V2016 CCM:G1.Q2
CRR V2016 CCM:G1.Q3
CRR V2016 EDM:G3.Q2
CRR V2016 SCM:G1.Q4
CRR V2016 SCM:G1.Q5
CRR V2016 SCM:G1.Q6
CRR V2016 SCM:G2.Q1
CRR V2016 SCM:G3.Q3
CRR V2016 SCM:MIL2.Q1
CRR V2016 SCM:MIL2.Q3
CRR V2016 SCM:MIL2.Q4
CRR V2016 SCM:MIL3.Q1
CRR V2016 SCM:MIL3.Q2
CRR V2016 SCM:MIL4.Q3
CRR V2016 SCM:MIL5.Q1
CSA CCM v3.0.1 BCR-09

De-ID Framework v1 Physical and Environmental Security: General
FedRAMP CP-1
FedRAMP CP-2
FedRAMP CP-2(1)
FedRAMP CP-2(2)
FedRAMP CP-2(3)
FedRAMP CP-7
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(A)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.310(d)(2)(iv)
HIPAA § 164.312(a)(2)(ii)
HIPAA § 164.312(c)(1)
IRS Pub 1075 v2014 9.3.6.1
IRS Pub 1075 v2014 9.3.6.2
ISO/IEC 27002:2005 14.1.3
ISO/IEC 27002:2013 17.1.2
JCAHO IM.01.01.03, EP 2
JCAHO IM.01.01.03, EP 4
MARS-E v2 CP-1
MARS-E v2 CP-10(2)
MARS-E v2 CP-10(3)
MARS-E v2 CP-2
MARS-E v2 CP-2(1)
MARS-E v2 CP-2(2)
MARS-E v2 CP-7
NIST Cybersecurity Framework ID.AM-5
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.BE-4
NIST Cybersecurity Framework ID.BE-5
NIST Cybersecurity Framework PR.DS-1
NIST Cybersecurity Framework PR.DS-4
NIST Cybersecurity Framework PR.IP-7
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RC.CO-3
NIST Cybersecurity Framework RC.RP-1
NIST Cybersecurity Framework RS.CO-1
NIST Cybersecurity Framework RS.CO-4
NIST SP 800-53 R4 CP-1
NIST SP 800-53 R4 CP-10(2)
NIST SP 800-53 R4 CP-10(4)
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-2(1)
NIST SP 800-53 R4 CP-2(2)
NIST SP 800-53 R4 CP-2(3)
NIST SP 800-53 R4 CP-2(5)
NIST SP 800-53 R4 CP-7
NRS 603A.215.1
PCI DSS v3.2 12.10.1
Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3
Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3
PMI DSP Framework RC-1

Level 2 Industry Control Mapping

1 TAC § 390.2(a)(4)(A)(xi)
AICPA A1.3
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-6 (HIGH)
CMSRs 2013v2 CP-6(1) (HIGH)
CMSRs 2013v2 CP-6(2) (HIGH)
CMSRs 2013v2 CP-6(3) (HIGH)
CMSRs 2013v2 CP-7 (HIGH)
CMSRs 2013v2 CP-7(1) (HIGH)
CMSRs 2013v2 CP-7(2) (HIGH)
CMSRs 2013v2 CP-7(3) (HIGH)
CMSRs 2013v2 CP-7(4) (HIGH)
CMSRs 2013v2 CP-9 (HIGH)
CMSRs 2013v2 CP-9(2) (HIGH)
CRR V2016 SCM:G1.Q5
CRR V2016 SCM:G1.Q6
CRR V2016 SCM:MIL3.Q1
CRR V2016 SCM:MIL3.Q2
De-ID Framework v1 Physical and Environmental Security: General
FedRAMP CP-2
FedRAMP CP-6
FedRAMP CP-6(1)
FedRAMP CP-6(3)
FedRAMP CP-7
FedRAMP CP-7(1)
FedRAMP CP-7(2)
FedRAMP CP-7(3)
FFIEC IS v2016 A.6.35(a)
FFIEC IS v2016 A.6.35(b)
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(c)
HIPAA § 164.310(a)(2)(i)
IRS Pub 1075 v2014 9.3.6.2
IRS Pub 1075 v2014 9.3.6.5
IRS Pub 1075 v2014 9.3.6.6
IRS Pub 1075 v2014 9.3.6.7
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.3
ISO/IEC 27002:2005 14.1.4
ISO/IEC 27002:2005 9.2.2
ISO/IEC 27002:2013 17.1.2
ISO/IEC 27002:2013 A.11.2.2
JCAHO IM.01.01.03, EP 1
JCAHO IM.01.01.03, EP 2
JCAHO IM.01.01.03, EP 3
MARS-E v2 CP-2
MARS-E v2 CP-6
MARS-E v2 CP-6(1)
MARS-E v2 CP-6(3)
MARS-E v2 CP-7
MARS-E v2 CP-7(1)
MARS-E v2 CP-7(2)
MARS-E v2 CP-7(3)
MARS-E v2 CP-7(5)
NIST Cybersecurity Framework ID.AM-5
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.BE-4
NIST Cybersecurity Framework ID.BE-5
NIST Cybersecurity Framework PR.AT-1
NIST Cybersecurity Framework PR.DS-1
NIST Cybersecurity Framework PR.DS-4
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RS.CO-1
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-6
NIST SP 800-53 R4 CP-6(1)
NIST SP 800-53 R4 CP-6(3)
NIST SP 800-53 R4 CP-7
NIST SP 800-53 R4 CP-7(1)
NIST SP 800-53 R4 CP-7(2)
NIST SP 800-53 R4 CP-7(3)
NIST SP 800-53 R4 CP-7(4)
NIST SP 800-53 R4 CP-9
NIST SP 800-53 R4 CP-9(2)

12.d Business Continuity Planning Framework

This section is designed to address information security considerations in the Business Continuity Management Program. See Sections 12.02 Business Impact Analysis, 12.03 Business and IT Recovery, 12.04 Problem Management, 12.05 Incident Management and 12.06 Exercises and Training for detailed requirements.

Level 1 Requirements

The organization shall create, at a minimum, one (1) business continuity plan. The business continuity plan shall describe the approach for continuity ensuring, at a minimum, the approach to maintain information or information asset availability and security. The plan shall also specify the escalation plan and the conditions for its activation, as

well as the individuals responsible for executing each component of the plan. When new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) shall be amended as appropriate.

The plan shall have a specific owner. Emergency procedures, manual "fallback" procedures, and resumption plans shall be within the responsibility of the owner of the business resources or processes involved. Fallback arrangements for alternative technical services, such as information processing and communications facilities, shall usually be the responsibility of the service providers.

The business continuity planning framework shall address the identified information security requirements, including the following:

1. the conditions for activating the plans which describe the process to be followed (e.g., how to assess the situation, who is to be involved) before each plan is activated;

2. emergency procedures which describe the actions to be taken following an incident that jeopardizes business operations;

3. fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time scales;

4. resumption procedures which describe the actions to be taken to return to normal business operations;

5. a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan;

6. awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective; and

7. the critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

Level 2 Requirements

Level 1 plus:

Each business unit shall create, at a minimum, one (1) business continuity plan. Procedures shall be included within the organization's change management program to ensure that business continuity matters are always addressed and timely as part of the change management process.

A business continuity planning framework shall address the identified information security requirements and the following:

1. temporary operational procedures to follow pending completion of recovery and restoration; and

2. the responsibilities of the individuals, describing who is responsible for executing which component of the plan. Alternatives should be nominated as required.

Level 1 Industry Control Mapping

1 TAC § 390.2(a)(1)
1 TAC § 390.2(a)(4)(A)(xi)
AICPA CC3.2
CMSRs 2013v2 CP-2 (HIGH)
CRR V2016 SCM:G1.Q3
CRR V2016 SCM:G3.Q2
CRR V2016 SCM:G4.Q1
CSA CCM v3.0.1 BCR-01
FedRAMP CP-2
FFIEC IS v2016 A.6.35(a)
FFIEC IS v2016 A.6.35(c)
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.312(a)(2)(ii)
IRS Pub 1075 v2014 9.3.6.2
ISO/IEC 27002:2005 14.1.4
ISO/IEC 27002:2013 17.1.2
JCAHO IM.01.01.03, EP 1
MARS-E v2 CP-2
NIST Cybersecurity Framework DE.AE-5
NIST Cybersecurity Framework ID.AM-5
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.BE-5
NIST Cybersecurity Framework PR.AT-1
NIST Cybersecurity Framework PR.IP-7
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RS.CO-1
NIST SP 800-53 R4 CP-2
Phase 1 CORE 102: Eligibility and Benefits Certification Policy v1.1.0 Subsection 3.3
Phase 2 CORE 202: Certification Policy v2.1.0 Subsection 3.3

Level 2 Industry Control Mapping

CRR V2016 SCM:G1.Q3
HIPAA § 164.308(a)(7)(i)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.312(a)(2)(ii)
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.4
ISO/IEC 27002:2013 17.1.2
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework PR.AT-1
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RS.CO-1

12.e Testing, Maintaining and Re-Assessing Business Continuity Plans

This section is designed to address information security considerations in business continuity plans. See sections 12.03 Business and IT Recovery and 12.06 Exercises and Training for detailed business continuity requirements

Level 1 Requirements

Business continuity plan tests shall ensure that all members of the recovery team and other relevant staff are aware of the plans and their responsibility for business continuity and information security and know their role when a plan is invoked.

The test schedule for business continuity plan(s) shall indicate how and when each element of the plan is tested. These techniques shall be applied on a 'programmatic' basis such that the tests build upon one another, and in a way that is relevant to the specific response and recovery plan. The results of tests shall be recorded and actions taken to improve the plans, where necessary. Updates will also consider lessons learned from implementation of the business continuity plan(s).

Responsibility shall be assigned for regular reviews of at least a part of the business continuity plan, at a minimum, annually. The identification of changes in business arrangements not yet reflected in the business continuity plan shall be followed by an update of the plan.

Changes where updating of business continuity plans shall be made are acquisition of new equipment, upgrading of systems and changes in:

1. personnel;
2. 2. location, facilities, and resources;
3. 3. legislation;
4. 4. processes, or new or withdrawn ones;
5. 5. risk (operational and financial).

Level 2 Requirements

Level 1 plus:

Business Continuity Management exercises shall be conducted at least annually or more frequently as required. A variety of techniques shall be used in order to provide assurance that the plan(s) will operate in real life including:

1. table-top testing of various scenarios (discussing the business recovery arrangements using example interruptions);

2. simulations (particularly for training people in their post-incident/crisis management roles);
3. technical recovery testing (ensuring information systems can be restored effectively) including:
    i. system parameters are set to secure values;
    ii. security critical patches are reinstalled;
    iii. security configuration settings are reset;
    iv. system documentation and operating procedures are readily available;
    v. application system software is reinstalled and configured with secure settings; and
    vi. information from the most recent secure back-up(s) is loaded;
4. testing recovery at an alternate site (running business processes in parallel with recovery operations away from the main site);
5. tests of supplier facilities and services (ensuring externally provided services and products will meet the contracted commitment);
6. complete rehearsals (testing that the organization, personnel, equipment, facilities, and processes can cope with interruptions).

The organization shall review test results and initiate corrective actions to ensure the continued effectiveness of the plan.

Responsibility shall be assigned for regular formal reviews of each business continuity plan, which shall ensure that the updated plans are distributed and reinforced by yearly reviews of the complete plan.

The organization shall coordinate business continuity plan testing and/or exercises with organizational elements responsible for related plans.

Level 1 Industry Control Mapping

AICPA A1.3
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-4 (HIGH)
CRR V2016 SCM:G1.Q3
CRR V2016 SCM:G2.Q1
CRR V2016 SCM:G3.Q2
CRR V2016 SCM:G3.Q3
CRR V2016 SCM:G3.Q4
CRR V2016 SCM:G4.Q2
CRR V2016 SCM:G4.Q3
CRR V2016 SCM:MIL3.Q2
CRR V2016 SCM:MIL4.Q1
CRR V2016 SCM:MIL5.Q2
CSA CCM v3.0.1 BCR-02
FedRAMP CP-2
FedRAMP CP-4
FedRAMP CP-4(1)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(C)
HIPAA § 164.308(a)(7)(ii)(D)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.308(a)(8)
HIPAA § 164.310(a)(2)(i)
HIPAA § 164.312(a)(2)(ii)
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.5
ISO/IEC 27002:2013 17.1.3
JCAHO IM.01.01.03, EP 5
MARS-E v2 CP-2
MARS-E v2 CP-4
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.GV-3
NIST Cybersecurity Framework PR.IP-10
NIST Cybersecurity Framework PR.IP-7
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RC.IM-1
NIST Cybersecurity Framework RC.IM-2
NIST Cybersecurity Framework RS.CO-1
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-4
PMI DSP Framework RC-3

Level 2 Industry Control Mapping

1 TAC § 390.2(a)(4)(A)(xi)
CMSRs 2013v2 CP-2 (HIGH)
CMSRs 2013v2 CP-4 (HIGH)
CMSRs 2013v2 CP-4(1) (HIGH)
CMSRs 2013v2 CP-4(2) (HIGH)
CMSRs 2013v2 CP-4(4) (HIGH)
CRR V2016 SCM:G2.Q1
CRR V2016 SCM:G3.Q4
CRR V2016 SCM:G3.Q5
CRR V2016 SCM:MIL3.Q2
CRR V2016 SCM:MIL4.Q1
FedRAMP CP-2
FedRAMP CP-4
FFIEC IS v2016 A.6.35(c)
HIPAA § 164.308(a)(7)(ii)(B)
HIPAA § 164.308(a)(7)(ii)(D)
HIPAA § 164.308(a)(7)(ii)(E)
HIPAA § 164.310(a)(2)(i)
IRS Pub 1075 v2014 9.3.6.2
IRS Pub 1075 v2014 9.3.6.4
ISO 27799-2008 7.11
ISO/IEC 27002:2005 14.1.5
ISO/IEC 27002:2013 17.1.3
JCAHO IM.01.01.03, EP 5
MARS-E v2 CP-2
MARS-E v2 CP-4 (HIGH)
MARS-E v2 CP-4(1)
NIST Cybersecurity Framework ID.AM-6
NIST Cybersecurity Framework ID.GV-3
NIST Cybersecurity Framework PR.IP-10
NIST Cybersecurity Framework PR.IP-7
NIST Cybersecurity Framework PR.IP-9
NIST Cybersecurity Framework RC.IM-1
NIST Cybersecurity Framework RC.IM-2
NIST Cybersecurity Framework RC-IM-2
NIST Cybersecurity Framework RS.CO-1
NIST SP 800-53 R4 CP-2
NIST SP 800-53 R4 CP-4
NIST SP 800-53 R4 CP-4(1)

NIST SP 800-53 R4 CP-4(2) NIST SP 800-53 R4 CP-4(4)

12.02 Business Impact Analysis

12.f Business Impact Analysis

Level 1 Requirements

1. A Business Impact Analysis (BIA) shall be conducted on all business functions with representation from the business owners
2. The business function shall be reviewed by business owners for any critical functions with regard to, at minimum, the following aspects to determine the appropriate classification:
    i. Patient/Life Safety
    ii. Patient Quality of Care (Healthcare functions only)
    iii. User Impact
    iv. Financial Impact
    v. Legal/Regulatory/Accreditation Implications
    vi. Backlog Business Functioning
    vii. Reputational Impact
    viii. Education al Impact
    ix. Research Impact
    x. Data Classification
    xi. Service Level Agreements
3. Business functions shall be classified into the following categories based completion of the BIA process:
    i. Core
    ii. 24 Hour Critical
    iii. 3 Day Critical
    iv. 7 Day Critical
    v. 1 Month Critical
    vi. Non-Critical
4. Recovery Time Objectives (RTOs), Recovery Point Objectives (RPOs), key business processes and associated risks if the processes are not available shall be established as part of the BIA process.
5. All business functions dependent upon IT resources shall have a BIA completed that documents specific RTOs and RPOs for those IT resources.
6. All business functions that are nominated to Core or 24-hour critical status shall undergo approval by a governance body.
7. BIAs shall be reviewed and updated accordingly when the scope of the business function changes to ensure accurate classification.
8. A BIA template standard is available here.

Level 2 Requirements

Level 1 plus:

1. The Business Impact Analysis (BIA) shall be conducted with representation from the Business Continuity Management Program. It is the responsibility of the business owner to engage the BCMP to conduct an initial BIA or review.

Level 1 & 2 Industry Control Mapping

HIPAA 45CFR 164.308(a)(7)(ii)(e) NFPA 1600 5.2.2.2 NFPA 1600 5.3 (entirety)
NFPA 1600 5.1.3.5.1.4 NFPA 1600 5.2.3-5 PCI DSS 9.6.1

PCI DSS 12.2

12.03 Business and IT Recovery

12.g Business Continuity Plan

Level 1 Requirements
Business Continuity Plans (BCP) are documents that outline the processes and resources needed to recover a business function after a disruptive event.

1. BCPs shall be required for all business units at the organization.
2. BCP shall contain at a minimum but not limited to:
    i. Activation and Implementation requirements
    ii. Succession Plan
        i. Leadership
        ii. Delegation of Authority
        iii. Devolution
    iii. Mission Critical Functions/Processes
        i. Mission Critical Functions/Processes
        ii. Mission Critical Functions/Processes Priority Ranking
        iii. Mission Critical Functions/Processes Required Resources (equipment, staff etc.)
        iv. Mission Critical Functions/Processes Critical Files, Records and Databases
        v. Mission Critical Functions/Processes Vendors
    iv. Alternate Facilities Logistics
        i. Continuity Facilities
        ii. Continuity Communications
        iii. Alternate Facilities
    v. Restoration Plans
    vi. Test, Training and Exercise plans
3. Business continuity plans shall updated when there are changes in:
    i. Personnel
    ii. Location, facilities and resources
    iii. Legislation
    iv. Processes, or new or withdrawn ones
    v. Risk (operational and financial)
4. BCPs shall have an assigned owner responsible for leading the review process
5. BCPs shall be reviewed and approved by designated officials with the organization
6. BCPs shall be protected from unauthorized disclosure or modificaiton
7. A business continuity plan template standard is available here

Level 2 Requirements
1. Business continuity plans shall be reviewed and updated at least annually

12.h IT Disaster Recovery Procedures

Level 1 Requirements
IT Disaster Recovery Procedures (DRP) are documents that outline the processes and resources needed to recover an information technology system after a service disruption.

1. DRPs shall be required for any information technology system that is deemed 24 hour critical or higher criticality, as determined by the business impact analysis.
2. DRPs shall be created with representatives from all responsible resources needed to recover a business function.
3. DRP content, at minimum, shall include but not limited to:
    i. Procedure steps
    ii. Resources needed
    iii. Recovery sites
    iv. Hardware support
    v. Appendices as applicable
4. Recovery steps shall be listed in chronological sequence with language and detailed information so it can be executed in the absence of a primary subject matter expert (SME).
5. DRPs shall include steps for recovering IT resources from the primary production location to the DR location.
6. DRPs shall include steps for recovering data from backup sources.
7. DRPs shall include steps for reestablishing the IT resource back to the primary production location.
8. All information and documentation shall be included; links shall not be used.
9. DRPs shall be reviewed at least annually.
10. DRPs shall have an assigned owner responsible for leading the review process.
11. DRPs shall be kept in a location accessible to appropriate staff and available in the event of a network failure and available to the BCM Program
12. DRPs shall be reviewed and approved by designated officials within the organization
13. DRPs shall be protected from unauthorized disclosure or modification
14. A DRP template standard is available here.

Level 2 Requirements

Level 1 plus:

1. DRPs shall be required for 3 day critical information technology systems
2. Architectural standards shall be defined for each criticality level
3. Information systems that house PHI shall be tested annually.
4. A DR test summary template standard is available here.

Level 1 & 2 Industry Control Mapping

JCAHO IM.01.01.03
HIPAA 45 CFR 164.308(a)(7)(ii)(A-D)
NFPA 1600 4.7.1
NFPA 1600 4.7.2 (2-4, 7)
NFPA 1600 9.6.2.1
NFPA 6.9.2.2 (1-10)
NFPA 1600 8.1.3
NFPA 1600 8.2.3

12.04 Problem Management

12.i Root Cause Analysis

Level 1 Requirements

To assist in process improvement and reduce overall risk to the organization a root cause analysis (RCA) process shall be implemented with the primary goals of identifying the underlying issue or initial event triggering an incident or service disruption and identifying any remediation actions to be taken. By implementing mitigation strategies to decrease probability and impact, risk of service interruptions and incidents will be reduced. The following considerations shall be made when preforming a RCA:

1. A primary responsible party shall be assigned to manage the RCA process.
2. RCA shall include representatives from all appropriate or affected departments within the organization.
3. Documentation of RCA shall be tracked in a location that is accessible by all appropriate staff and available to the BCM Program
4. RCA documentation, at minimum, shall include
    i. System with issue
    ii. Date of issue
    iii. Length of service disruption
    iv. Root cause
    v. Manager assigned to the RCA
5. Remediation and action items identified during a RCA shall be documented and tracked to ensure completion.
6. RCA findings shall be reviewed with organizational management
7. An RCA template standard is available here.

Level 2 Requirements

Level 1 plus:

1. RCA shall be conducted, at minimum, on any service disruption to critical business functions as determined by the Business Impact Analysis (see section 12.02)

12.j Post-Incident Debrief

Post-Incident Debriefings are conducted after a declared incident, as defined in section 12.05 of this document, to identify strengths and opportunities for improvement. The following guidelines shall be utilized for all Post-Incident Debriefs:

Level 1 Requirements

1. all participants (internal and external) with a relevant role to the incident shall be invited to the debrief
2. the debrief shall include at a minimum:
    i. review of incident events and decisions made by incident management team to identify strengths and opportunities for improvement
    ii. review of incident management procedures to identify strengths and opportunities for improvement
    iii. identification of action items and responsible parties
3. An after action report shall be created for all declared incidents that includes at minimum:
    i. Summary of events
    ii. Root cause summary (see section 12.i)
    iii. Action items
4. Open action items shall be tracked to completion to ensure appropriate and timely remediation has occurred
5. Business continuity management documentation shall be reviewed and updated as applicable after any incident.
6. After Action Reports and all other incident related documentation shall be tracked in a location that is accessible by all applicable staff and available to the BCM Program

Level 2 Requirements

Level 1 Plus:

1. Evidence of action item completion shall be located in a location that is accessible by all appropriate staff and available to the BCM Program.

Level 1 & 2 Industry Control Mapping

JCAHO PI.01.01.01
JCAHO PI.02.01.01
JCAHO PI.03.01.01
JCAHO EM.03.01.03
NIMS Element 7
NIMS Element 14
NFPA 1600 6.2.4
NFPA 1600 6.3.1-3
NFPA 1600 9.1.4-6
NFPA 1600 9.2.1-2
NFPA 1600 9.3
PCI DSS 10.8.1
PCI DSS 12.10.6

12.05 Incident Management

12.k Detection and Notification

Level 1 and 2 Requirements

For the purposes of Incident Management, an incident shall be defined as an occurrence or event, natural or human-caused that requires an emergency response to protect life or property. Incidents can, for example, include major disasters, emergencies, terrorist attacks, terrorist threats, wildland and urban fires, floods, hazardous materials spills, nuclear accidents, aircraft accidents, earthquakes, hurricanes, tornadoes, tropical storms, war-related disasters, public health and medical emergencies, and other occurrences requiring an emergency response.

The Organization shall adhere to the following for Incident Detection and Notification:

1. detection, reporting and escalation shall be defined for incidents and a responsible party shall be identified to own and manage these processes
2. all workforce members shall be trained on how to detect, report and escalate incidents
3. incident detection can occur at any level of the organization
4. notification method used to communicate an incident shall be reliable and redundant
5. notification of incidents shall include all essential resources needed for response

12.l Activation and Response

Level 1 Requirements

The Organization's activation and response actions shall include any actions to address immediate life safety concerns and scene stabilization. Response plans shall include:

1. declaration procedures that include
    i. activation levels
    ii. metrics for declaration
    iii. authority to declare
    iv. activation of resources
    v. additional notification procedures
2. communication procedures for
    i. key stakeholders (internal and external)
    ii. constituents
3. initial steps to ensure life safety, property preservation and scene stabilization
4. incident management organizational chart
5. job actions sheets too include key responsibilities for the incident management team
6. an incident commander and scribe shall be assigned for every event

Level 2 Requirements

Level 1 plus:

1. Manage all incidents with consistent application of the Incident Command System (ICS) as defined by the National Incident Management System (NIMS) organization structures, processes and procedures.

12.m Incident Documentation

Level 1 Requirements

1. The Organization shall conduct real-time documentation with the purpose of capturing information used to make decisions or learn from an incident. All incident documentation shall include but not limited to:
   i. timeline of events
   ii. major decisions and supporting details
   iii. outcomes of major decisions
   iv. addition detail critical to the incident

2. Incident shall be subject to a post-incident debrief (refer to 0BCM10.1.d Problem Management Procedure).

Level 2 Requirements

Level 1 plus:

1. Document all incidents with consistent application of ICS processes and procedures

Level 1 & 2 Industry Control Mapping

JCAHO EM 02.02.07
PCI DSS 12.10
PCI DSS 12.10.1-2
NFPA 1600 5.15
NFPA 1600 6.4.1-2
NFPA 1600 6.5.1-5
NFPA 1600 6.7.1.1-3
NFPA 1600 6.7.2-8
NFPA 1600 6.8.1-4
NFPA 1600 7.4
Level 2 Industry Control Mapping
NIMS Element 2

12.06 Exercises and Training

12.n Exercises

Level 1 Requirements

The Organization shall perform exercises periodically to evaluate the capabilities and readiness of the BCMP. For any exercises performed the following shall be followed:

1. determine and document scope of the exercise
2. exercises shall be conducted on a 'programmatic' basis such that the exercises build upon one another, and in a way that is relevant to the specific response and recovery plan.
3. assemble applicable subject matter experts and business owners as part of the exercise planning team
4. review applicable BCMP documentation prior to the exercise to ensure information is up to date (e.g. emergency response plans, disaster recovery procedures, incident management procedures, etc.)
5. follow all applicable change management policies and procedures for approval of exercise
6. all exercises should have a post-exercise debrief conducted similar to an post-incident debrief (refer to section 12.j of this procedure)

7. an after action report shall be completed for all exercises that included that includes:
    i. summary of events
    ii. issues encountered
    iii. lessons learned
    iv. open action items
8. open action items shall be tracked to completion to ensure appropriate and timely remediation has occurred.
9. exercise related documentation shall be maintained in a centralized location that is accessible to appropriate staff within the organization.
10. a log of all exercises shall be maintained and shall indicate how and when each element of the plan is tested
11. Updates shall be made to BCM documentation from lessons learned in implementation of plans

Level 2 Requirements

1. Exercises its incident management plans at minimum, twice annually. If plans are activated in response to one or more actual emergencies, these emergencies can serve in place of emergency response exercises.
2. Exercises incorporate likely disaster scenarios that allow the organization to evaluate its handling of individuals served, communications, resources and assets, internal security and staff.
3. Representatives from administrative, support, and clinical services participate in the evaluation of all emergency response exercises and all responses to actual emergencies.
4. The evaluation of all emergency response exercises and all responses to actual emergencies includes the identification of deficiencies and opportunities for improvement. This evaluation is documented.
5. The organization modifies its Emergency Management Plan based on its evaluation of emergency response exercises and responses to actual emergencies.
   Note: When modifications requiring substantive resources cannot be accomplished by the next emergency response exercise, interim measures are put in place until final modifications can be made.
6. Subsequent emergency response exercises reflect modifications and interim measures as described in the modified Emergency Management Plan.

12.o Training

1. Training on Business Continuity Management plans shall be upon initial implementation of plans and upon changes to the plans
2. Additional Business Continuity Management plan training shall be conducted on an as needed basis as determined by organizational gap analysis or other methodology to determine needs.
3. Training shall address any opportunities of improvement when appropriate
4. A log of training offered annually and attendees shall be required for all trainings
5. The training log shall be kept in a centralized location that is accessible to appropriate staff within the organization and available to the BCM Program

Level 1 & 2 Industry Control Mapping

JCAHO EM.03.01.03
NIMS Element 7

Appendix 1: Revision History

Modification(s) Made	Modified by:	Date of Modification	Approver	Approval Date
Document Created	Lead Information Security Analyst	03/11/2013	Privacy & Security Executive Committee	6/6/2013
Made changes to sections consistent with HiTrust CSF V6 Summary of changes.	Lead Information Security Analyst	10/2015	Privacy & Security Executive Committee	12/3/2015
Added additional BCMP procedures	BCMP Project Director	6/2016	URMC Privacy & Security Executive Committee	7/7/2016
Document Updated to reflect adoption by University of Rochester	Lead Information Security Analyst	6/23/2016	URMC Privacy & Security Executive Committee	7/7/2016
Made changes to sections consistent with HiTrust CSF V9 and V8.1 Summary of changes. (No changes noted)	Clinical and Administrative Information Security Officer	12/3/2017		
Made changes to sections 12.02-12.06 to align with Level 1 & 2 tiers; added additional DR requirements based on Audit finding	BCMP Project Director	12/6/2017	URMC Privacy & Security Executive Committee	03/01/2018

Appendix 2: Contact Information

Please address any questions or concerns with any policies set forth within this document to the URMC Information Security Office <InformationSecurity@UR.Rochester.edu>.