Commonwealth of Massachusetts

Massachusetts Office of Information Technology

# Enterprise Business Continuity for IT Management Standards

**Reference #: ITD-STD-SEC-15.1 Issue Date: June 5, 2013
Issue #: 1**

## Table of Contents

[Table of Contents 1](#_Toc438198121)

[Executive Summary 1](#_Toc438198122)

[Whom this Standard Applies To 2](#_Toc438198123)

[Requirements 2](#_Toc438198124)

[Roles and Responsibilities 9](#_Toc438198125)

[Related Documents 10](#_Toc438198126)

[Contact 11](#_Toc438198127)

[Appendix A: Terms 12](#_Toc438198128)

[Appendix B: Document History 17](#_Toc438198129)

## Executive Summary

These standards have been developed to establish the minimum requirements that must be met to be in compliance with the Enterprise Business Continuity of IT Management Policy.

In order to comply with these standards; Agencies must validate that their Business Continuity Plan (BCP) is consistent with and meets all sections of this document including:

* Risk Assessment and Business Impact Analysis
* BCP Documentation and Procedure Implementation

These standards have been developed to be read and used in conjunction with the overarching [Enterprise Business Continuity of IT Management Policy](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/it-policies-standards-and-procedures/ent-pols-and-stnds/enterprise-business-continuity-management-policy-and-standards/enterprise-business-continuity-policy.html)[[1]](#footnote-1) and supporting Enterprise IT Business Continuity Management Procedures templates and guidelines.

## Whom this Standard Applies To

All agencies and entities governed by the overarching Enterprise Business Continuity Management Policy are required to adhere to requirements of these, supporting standards.

Other Commonwealth entities are encouraged to adopt, at a minimum, requirements in accordance with this Enterprise Business Continuity Management Policy or a more stringent agency policy that addresses agency specific and business related directives, laws, and regulations.

## Requirements

Agencies are required to 1) have a policy including vision, mission statement, roles and responsibilities, and 2) develop, implement, test and maintain a Business Continuity Plan (BCP) including a Disaster Recovery (DR) Plan and Continuity of Operations Plan (COOP) for all Information Technology Resources (ITR) that deliver or support Critical Business Functions on behalf of the Commonwealth of Massachusetts, 3) the program shall include applicable authorities, legislation and regulations and 4) operational procedures to support the program.

In order to meet this requirement; the BCP must include and ensure:

* Thorough evaluation is conducted of how loss or disruption of functions will impact systems or services that support Critical Business Functions, and categorized according to the time frames required for recovery of each function.
* Data is protected in a manner commensurate with the agency’s data classification delineations to ensure that sensitive data is not compromised or disclosed during a system disruption or emergency.
* Copies of the plans and supporting materials to execute the plans are securely stored in a remote location; at a sufficient distance to escape any damage from a disaster at the agency’s main information processing facilities and be available (via remote connection, external e-mail location, etc.).
* Plans are documented, implemented and annually tested including the testing of all appropriate security provisions to minimize impact to systems or processes from the effects of major failures of IT Resources or disasters.
* Plans are maintained and accurate throughout the course of the year ensuring that changes are incorporated as business, security or other drivers occur.
* Continuous testing and monitoring of the plans including execution and simulation of outage or catastrophic event, and recovery at alternate site(s).
* Recovery procedures are published and individuals responsible for carrying out tasks within the documented procedures are appropriately trained to fulfill their responsibilities.

In order to achieve these goals, the following standards must be met:

### Risk Assessments and Business Impact Analysis Standards

Agencies are required to conduct risk assessments to identify, estimate, and prioritize risk to organizational operations and to produce a documented business impact analysis that identifies all Critical Business Functions of the agency, entity or business unit and their supporting information systems.

Effectively accomplishing this analysis and documentation will require that agencies meet the following standards:

* 1. All environments are evaluated as part of the Business Impact Analysis including but not limited to: desktop workstations and locally stored data; development, test, QA and production environments.
		1. Inventory and location of all deployed IT systems, environments and resources that support Critical Business Functions is identified and documented.
	2. Continuity planning sessions are conducted to identify, analyze, and prioritize mission critical functions based on: agency mission statement(s), criticality, scope and consequence of disruption, time-sensitivity, and coordination requirements with other agencies/entities including third parties, information processing facilities and IT support requirements. It is required that planning sessions:
		1. Are led by the individual(s) responsible for agency BCP
		2. Include line of business owners, subject matter experts, legal representation and executive representation
		3. Ensure that participants evaluate criticality of functions against the agency mission, scope of disruption, consequence of disruption, time-sensitivity, and coordination requirements with other agencies/entities including third parties, information processing facilities and IT support requirements.
		4. Validate documentation of for Critical Business Functions associated systems to help ensure that appropriate systems are addressed in the BCP.
		5. Ensure that analysis and prioritization and criticality align with the criticality and priority definitions for urgency and impact (P1-P5) that are being produced by the Commonwealth’s Information Technology Service Excellence Committee (ITSEC) for rating individual applications
	3. Impact assessment of disruption to systems that support Critical Business Functions is performed so that agencies can understand:
		1. Functional impact
		2. Financial impact
		3. Resource impact
		4. Public Perception or Confidence
	4. Tolerance Threshold for each identified IT system that supports Critical Business Functions is identified.
	5. Interdependency of IT Resource availability requirements is assessed and classified according to the criticality and priority status of the IT resources to the agency and business owner.
	6. Recovery prioritization for systems that support Critical Business Functions is articulated.
	7. Risk assessments are conducted to determine quantitative or qualitative value of possible or known threats
		1. Electronic (Hacking, Sniffing, Spoofing, Malicious Code, Viruses, Worms, Java, ActiveX, Trojans, etc.)
		2. Physical (Theft, Terminal hijack, etc.)
		3. Human (Social Engineering, Personnel, Sticky-note, etc.)
		4. Privacy (Employee, Constituent data, Customer data, Business Partner data, etc.)
		5. Down Time (DoS attacks, Bugs, Power, Natural Disasters, etc.)
	8. Documentation of the BIA is recorded and maintained to support of the development of the BCP.

### BCP Documentation & Procedure Implementation Standards

From a technology perspective; the BCP addresses the agency’s response to two primary issues: an event that causes an interruption to normal service delivery or “Incident”; and a major outage resulting from a catastrophic event or “Disaster”. Both areas must be accounted for and planned for in an effective BCP, but each may invoke very different procedures based on the classification of the interruption, severity of the impact and the criticality of the service.

Agencies are required to articulate specific information, including the details necessary to effectively respond, manage, and recover from either an incident or a catastrophic event. Further, protecting data and confidential information should be integrated into the BCP. At a minimum; agencies’ BCP must document the following:

* 1. Scope / Objectives
	2. Risk Evaluation and Required Security Controls
		1. Event Identification and Assessment
			1. Identify potential events that may impact the ability to deliver Critical Business Functions.
* Incidents that may impact 1 or more systems that support Critical Business Functions
* Major outages that impact critical networks or multiple critical systems
* Catastrophic event(s) having a broad impact on critical systems, critical networks or critical personnel requiring use of an alternate site or facility
	+ - 1. Identify severity of impact that would cause varying procedures to be enacted.
			2. Identify key personnel responsible for assessing impact and which procedures to follow during an event.
	1. Business Impact Analysis Outcomes
	2. Communications Procedures
		1. Address who is responsible for each type of communication that an agency will need to engage in including external organizations, e.g. call succession, e-mail exchange, escalation efforts, etc.
		2. Articulate how and when external entities are to be contacted as a result of a disruption of operations. Depending on the type of disruption that is occurring or has occurred, external organizations may need to be notified to provide targeted support or communications such as the Department of Public Safety, Department of Public Health or Law Enforcement Officials.
		3. Establish communication and notification procedures to inform and keep the entire organization aware of, and current on, the continuity plan, procedures and individual responsibilities relative to the plan.
		4. Communication Channels
			1. Identify the primary mechanism for facilitating communication during an Incident and a Disaster
			2. Establish communication and notification procedures to disseminate and respond to the media and the public, including special needs populations
			3. Identify alternate mechanisms for facilitating communication during an Incident and a Disaster taking into account the possibility that any number of contact mechanisms may not be available (e.g. where allowable, personal cell phone listings and/or personal email addresses, etc.)
			4. Maintain Primary and Alternate Contact Lists
	3. BCP Organization Structure
		1. Executive sponsorship: Individual that has overall responsibility for the team; communicates senior management's support and direction.
		2. Continuity Teams’ Structure & Roles: Identify the teams and positions within those teams that are required to facilitate tasks associated with the recovery of systems and services for incidents and events as well as emergency or disaster recovery efforts.
		3. The number and scope of teams will vary depending on an agency’s size, function and structure but are required to account for:
			1. Plan Coordination:
* Ensuring senior management alignment, support & approval
* Securing funding
* Articulating agency specific policies
* Coordinating development of agency procedures
* Implementing review, test and audit plan.
	+ - 1. Authority and Succession Planning:
* Identification of authority, succession of management and delegation of authority
* Command and control management including crisis, response, continuation and recovery management
	+ - 1. Vendor management:
* Verification that critical third party vendors are able and contractually obligated to meet relevant agency business continuity requirements.
* Identification of alternate third party vendors where possible and appropriate.
	+ - 1. Task Oriented Management:
* Incident Response
* Recovery Procedures
* Documentation
* Communication
* Disaster Response
* Recovery Procedures
* Documentation
* Damage assessment
* Finance and accounting
* Hazardous material handling
* Insurance and legal
* Contracting and procurement
* Crisis Communication Procedures
* Telecommunications
* Mechanical equipment usage
* Mainframe/midrange, LAN, hosting, networking, storage and backup usage
* COOP Response
	+ Alternate site use
	+ Transportation
	1. Damage Assessment
		1. Identify the cause of the emergency or disruption
		2. Measure the potential for additional disruptions or damage
		3. Identify area affected by the emergency
		4. Evaluate the status of physical infrastructure (for example, structural integrity of computer room, condition of electric power, telecommunications, and heating, ventilation, and air-conditioning)
		5. Review inventory and evaluate the functional status of IT equipment (for example, fully functional, partially functional, and nonfunctional).
		6. Evaluate type of damage to IT equipment or data (for example, water damage, fire and heat, physical impact, and electrical surge).
		7. Identify items to be replaced (for example, hardware, software, firmware, and supporting materials).
		8. Estimate time to restore normal services.
	2. Recovery Plans
		1. Critical Business Function System Recovery
			1. Prioritization of Recovery
			2. Interdependencies
			3. Resource requirements
			4. Security Controls
		2. Mobilizing Alternate Locations / Resources
		3. Managing Alternate Locations / Resources
		4. Critical Business Function System Support
			1. Short term
			2. Long term
			3. Local
			4. Regional
			5. Pandemic
		5. IT and Business Unit Recovery Procedures
			1. Procedures for recovery of each system that supports Critical Business Functions are required to be prioritized to ensure that time-sensitive, high importance business functions are recovered first.
			2. Recovery time for an IT resource should align with the recovery time objective for the business function or process that depends on the IT resource.
			3. Prioritization should take into consideration system interdependencies, system physical location and processing requirements including but not limited to:
* Computer room environment (secure computer room with climate control and backup power supply, etc.)
* Loss of general power source
* Hardware reliance (networks, servers, desktop and laptop computers, wireless devices and peripherals)
* Connectivity to a service provider (fiber, cable, wireless, etc.)
* Communication provider reliance
* Software application interdependence (electronic data interchange, electronic mail, enterprise resource management, office productivity, etc.)
* Data and restoration reliance
	+ 1. Leverage Enterprise Solutions to recover, replace or support business function requirements whenever possible, e.g. Second Data Center services, etc.
	1. Plan Implementation and Maintenance
		1. Plan Storage
			1. Securely store copies of plans and supporting materials in a remote location; at a sufficient distance to escape any damage from a disaster at the agency’s main information processing facilities and be available (via remote connection, external e-mail location, etc.).
		2. Plan Testing
			1. Scheduled annual testing of continuity plan and procedures including documented test results at a minimum annually or in the event of significant changes to IT Resource environment or agency organization.
			2. Analyze continuity plan test results and compare to test objectives, summarize results and communicate to management, with necessary adjustments made to the plan and objectives if needed.
		3. Plan Maintenance
			1. Agencies are required to identify appropriate mechanisms to ensure that plans remain current and updated between annual tests and reviews.
* Change management implications
* New/Major upgrades of system implementations
* New policy adoption
* New contract implementations
* New threat/risk identification
* Staff/resource/responsibility changes
	+ - 1. Update of continuity plan as part of an organization’s change management process to ensure that any changes to systems or environments are clearly understood from a continuity of operations perspective and documented as appropriate.
			2. Review continuity plan on a scheduled basis, at a minimum semi-annually or whenever there is a significant change to the agency’s essential functions or IT environment to ensure that all required updates to the plan have been performed and reflect the agency’s current IT Resource environment and associated Critical Business Functions.
		1. Plan Publication
			1. Agencies are required to publish plans and sufficiently train any and all individuals that are required or responsible for supporting any part of the BCP.

## Roles and Responsibilities

All agencies and entities governed by the overarching Enterprise Information Security Policy are subject to the referenced roles and responsibilities in addition to those specifically stated within this supporting policy. The roles and responsibilities associated with implementation and compliance with this policy are detailed below:

### Assistant Secretary for Information Technology

* Develop mandatory standards and procedures for agencies to follow prior to entering into contracts that will provide third parties access to electronic highly sensitive information, including but not limited to, personal information or IT systems containing such information.
* Approval and adoption of the Enterprise Business Continuity Management Policy, supporting standards and their revisions.

### Secretariat Chief Information Officer (SCIO) and Agency Head

* Provide communication, training, implementation and enforcement of this policy.
* Provide proper third party oversight as applicable for any outsourced Business Continuity and Disaster Recovery services including IT Resources and alternate IT facilities.
* Review and approve Business Continuity and Disaster Recovery programs and plans submitted by the Secretariat or Agency.
* Continuous testing and monitoring of the plans including execution and simulation of outage or catastrophic event, and recovery at alternate site(s).

### Enterprise Security Board (ESB)

* Recommend revisions and updates to this policy and related standards.

### Massachusetts Office of Information Technology (MassIT)

* Maintain this policy and related standards including review of related recommendations of the Enterprise Security Board, issue policy revisions and updates.

### Third parties

* Required to comply with agency implementation of this policy at a minimum or a more stringent agency specific policy including:
	+ Conformance to agency Business Continuity Plan and supporting Disaster Recovery Plan and Continuity of Operations Plan.

## Related Documents

Related policies, standards, procedures, guidelines, etc.

## Contact

Standards@state.ma.us

## Appendix A: Terms

Key terms used in this policy have been provided below for your convenience. For a full list of terms please refer to the glossary of [Commonwealth Specific Terms](http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html)[[2]](#footnote-2) on the Massachusetts Office of Information Technology’s website.

**Alternate Site:** An alternate operating location to be used by business functions when the primary facilities are inaccessible. 1) Another location, computer center or work area designated for recovery. 2) Location, other than the main facility, that can be used to conduct business functions. 3) A location, other than the normal facility, used to process data and/or conduct critical business functions in the event of a disaster.

**Asset:** An item of property and/or component of a business activity/process owned by an organization. There are three types of assets: physical assets (e.g. buildings and equipment); financial assets (e.g. currency, bank deposits and shares) and non-tangible assets (e.g. goodwill, reputation).

**Business Continuity:** The ability of an organization to provide service and support for its customers and to maintain its viability before, during, and after a business continuity event.

**Business Continuity Plan (BCP):** Process of developing and documenting arrangements and procedures that enable an organization to respond to an event that lasts for an unacceptable period of time and return to performing its critical functions after an interruption.

**Business Impact Analysis:** A process designed to prioritize business functions by assessing the potential quantitative (financial) and qualitative (non-financial) impact that might result if an organization was to experience a business continuity event.

**Contact List:** A list of team members and/or key personnel to be contacted including their backups. The list will include the necessary contact information (i.e. home phone, pager, cell, etc.) and in many cases it is considered confidential.

**Contingency Plan:**  A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations.

**Contingency Planning:** Process of developing advanced arrangements and procedures that enable an organization to respond to an undesired event that negatively impacts the organization.

**Continuity Of Operations Plan (COOP):** Provides procedures and guidance to sustain an organization’s mission essential functions at an alternate site for up to 30 days. Information systems are addressed based only on their support of the mission essential functions.

**Critical Business Functions:** The critical operational and/or business support functions that could not be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing the organization. An example of a business function is a logical grouping of processes/activities that produce a product and/or service such as Accounting, Staffing, Customer Service, etc.

**Damage Assessment:** The process of assessing damage to computer hardware, vital records, office facilities, etc., and determining what can be salvaged or restored and what must be replaced following a disaster.

**Dependency:** The reliance or interaction of one activity or process upon another.

**Disaster:** A sudden, unplanned catastrophic event causing unacceptable damage or loss. 1) An event that compromises an organization's ability to provide critical functions, processes, or services for some unacceptable period of time 2) An event where an organization's management invokes their recovery plans.

**Disaster Recovery:** The ability of an organization to respond to a disaster or an interruption in services by implementing a disaster recovery plan to stabilize and restore the organization's critical functions.

**Disaster Recovery Plan:** The management approved document that defines the resources, actions, tasks and data required to manage the technology recovery effort. Usually refers to the technology recovery effort. This is a component of the Business Continuity Management Program.

**Escalation:** The process by which event related information is communicated upwards through an organization's established Chain of Command.

**Event:** Any occurrence that may lead to a business continuity incident.

**Exercise:** A people focused activity designed to execute business continuity plans and evaluate the individual and/or organization performance against approved standards or objectives. Exercises can be announced or unannounced, and are performed for the purpose of training and conditioning team members, and validating the business continuity plan. Exercise results identify plan gaps and limitations and are used to improve and revise the Business Continuity Plans. Types of exercises include: Table Top Exercise, Simulation Exercise, Operational Exercise, Mock Disaster, Desktop Exercise, Full Rehearsal.

**Hot site:** An alternate facility that already has in place the computer, telecommunications, and environmental infrastructure required to recover critical business functions or information systems.

**Impact:** The effect, acceptable or unacceptable, of an event on an organization. The types of business impact are usually described as financial and non-financial and are further divided into specific types of impact.

**Incident:** An event which is not part of a standard operating business which may impact or interrupt services and, in some cases, may lead to disaster.

**Incident Response:** The response of an organization to a 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.

**Information Security:** The securing or safeguarding of all sensitive information, electronic or otherwise, which is owned by an organization.

**Infrastructure:** The underlying foundation, basic framework, or interconnecting structural elements that support an organization.

**Internal Hot site:** A fully equipped alternate processing site owned and operated by the organization.

**ITSEC:** The objective of the IT Commonwealth Service Excellence Committee (ITSEC) is to better align IT with the business for the purpose of delivering the highest quality IT services at the most efficient cost. It fosters inter-agency communication and effective service delivery through the collaboration, sharing and adoption of best practices to achieve the collective goal of best serving the agencies and citizens of the Commonwealth.

**Loss:** Unrecoverable resources that are redirected or removed as a result of a Business Continuity event. Such losses may be loss of life, revenue, market share, competitive stature, public image, facilities, or operational capability.

**NIST:** The National Institute of Standards and Technology was founded in 1901 and is now part of the U.S. Department of Commerce. Today, NIST measurements support the smallest of technologies—nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair—to the largest and most complex of human-made creations, from earthquake-resistant skyscrapers to wide-body jetliners to global communication networks.

**Outage:** The interruption of automated processing systems, infrastructure, support services, or essential business operations, which may result, in the organizations inability to provide services for some period of time.

**Prioritization:** The ordering of critical activities and their dependencies are established during the BIA and Strategic-planning phase. The business continuity plans will be implemented in the order necessary at the time of the event.

**Quantitative Assessment:** The process for placing value on a business function for risk purposes. It is a systematic method that evaluates possible financial impact for losing the ability to perform a business function. It uses numeric values to allow for prioritizations. This is normally done during the BIA phase of planning.

**Recovery:** Implementing the prioritized actions required to return the processes and support functions to operational stability following an interruption or disaster.

**Recovery Management Team:** See: Business Continuity Management (BCM) Team.

**Recovery Teams:** A structured group of teams ready to take control of the recovery operations if a disaster should occur.

**Recovery Time Objective (RTO):** The period of time within which systems, applications, or functions must be recovered after an outage (e.g. one business day). RTO's are often used as the basis for the development of recovery strategies, and as a determinant as to whether or not to implement the recovery strategies during a disaster situation.

**Response:** The reaction to an incident or emergency to assess the damage or impact and to ascertain the level of containment and control activity required. In addition to addressing matters of life safety and evacuation, Response also addresses the policies, procedures and actions to be followed in the event of an emergency.

**Restoration:** Process of planning for and/or implementing procedures for the repair of hardware, relocation of the primary site and its contents, and returning to normal operations at the permanent operational location.

**Risk:** Potential for exposure to loss which can be determined by using either qualitative or quantitative measures.

**Risk Assessment / Analysis:** 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 for such controls. Risk analysis often involves an evaluation of the probabilities of a particular event.

**Simulation Exercise:** One method of exercising teams in which participants perform some or all of the actions they would take in the event of plan activation. Simulation exercises, which may involve one or more teams, are performed under conditions that at least partially simulate 'disaster mode'. They may or may not be performed at the designated alternate location, and typically use only a partial recovery configuration.

**System:** Set of related technology components that work together to support a business process or provide a service.

**System Recovery:** The procedures for rebuilding a computer system and network to the condition where it is ready to accept data and applications, and facilitate network communications.

**Test:** A pass/fail evaluation of infrastructure (example-computers, cabling, devices, hardware) and\or physical plant infrastructure (example-building systems, generators, utilities) to demonstrate the anticipated operation of the components and system. Tests are often performed as part of normal operations and maintenance. Tests are often included within exercises. (See Exercise).

**Threat:** A combination of the risk, the consequence of that risk, and the likelihood that the negative event will take place.

**Tolerance Threshold:** Maximum period which an enterprise can afford to be without a critical function or process.

**Uninterruptible Power Supply (UPS):**  A backup electrical power supply that provides continuous power to critical equipment in the event that commercial power is lost. The UPS (usually a bank of batteries) offers short-term protection against power surges and outages. The UPS usually only allows enough time for vital systems to be correctly powered down.

## Appendix B: Document History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Action | Effective Date | Next Review Date |
| 6/5/13 | Document Published | 6/5/13 | 1/30/14 |
| 2/10/14 | Reviewed | 2/10/14 | 2/11/15 |
| 2/20/15 | Reviewed | 2/20/15 | 2/21/16 |
| 12/16/2015 | Accessibility remediation – no content changes | 2/22/16 | 1/1/17 |

1. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/it-policies-standards-and-procedures/ent-pols-and-stnds/enterprise-business-continuity-management-policy-and-standards/enterprise-business-continuity-policy.html [↑](#footnote-ref-1)
2. http://www.mass.gov/anf/research-and-tech/policies-legal-and-technical-guidance/glossary-of-commonwealth.html [↑](#footnote-ref-2)