NFPA® 1600

Standard on Disaster/Emergency Management and Business Continuity Programs

2013 Edition

NFPA, 1 Batterymarch Park, Quincy, MA 02169-7471
An International Codes and Standards Organization

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® DOCUMENTS
NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF NFPA DOCUMENTS

NFPA® codes, standards, recommended practices, and guides ("NFPA Documents"), of which the document contained herein is one, are developed through a consensus standards development process approved by the American National Standards Institute. This process brings together volunteers representing varied viewpoints and interests to achieve consensus on fire and other safety issues. While the NFPA administers the process and establishes rules to promote fairness in the development of consensus, it does not independently test, evaluate, or verify the accuracy of any information or the soundness of any judgments contained in NFPA Documents.

The NFPA disclaims liability for any personal injury, property or other damages of any nature whatsoever, whether special, indirect, consequential or compensatory, directly or indirectly resulting from the publication, use of, or reliance on NFPA Documents. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Documents available, the NFPA is not undertaking to render professional or other services for or on behalf of any person or entity. Nor is the NFPA undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

The NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of NFPA Documents. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

REMINDER: UPDATING OF NFPA DOCUMENTS

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Documents") should be aware that NFPA Documents may be amended from time to time through the issuance of Tentative Interim Amendments or corrected by Errata. An official NFPA Document at any point in time consists of the current edition of the document together with any Tentative Interim Amendment and any Errata then in effect.

In order to determine whether an NFPA Document has been amended through the issuance of Tentative Interim Amendments or corrected by Errata, visit the Document Information Pages on NFPA's website. The Document Information Pages provide up-to-date, document specific information including any issued Tentative Interim Amendments and Errata.

To access the Document Information Page for a specific NFPA Document go to http://www.nfpa.org/document for a list of NFPA Documents, and click on the appropriate Document number (e.g., NFPA 101). In addition to posting all existing Tentative Interim Amendments and Errata, the Document Information Page also includes the option to sign-up for an "Alert" feature to receive an email notification when new updates and other information are posted regarding the document.

ISBN: 978-145590602-4 (Print)
ISBN: 978-145590648-2 (PDF)

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® DOCUMENTS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Documents

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Documents") should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of Tentative Interim Amendments. An official NFPA Document at any point in time consists of the current edition of the document together with any Tentative Interim Amendments and any Errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of Tentative Interim Amendments or corrected through the issuance of Errata, consult appropriate NFPA publications such as the National Fire Codes® Subscription Service, visit the NFPA website at www.nfpa.org, or contact the NFPA at the address listed below.

Interpretations of NFPA Documents

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing Committee Projects shall not be considered the official position of NFPA or any of its Committees and shall not be considered to be, nor be relied upon as, a Formal Interpretation.

Patents

The NFPA does not take any position with respect to the validity of any patent rights referenced in, related to, or asserted in connection with an NFPA Document. The users of NFPA Documents bear the sole responsibility for determining the validity of any such patent rights, as well as the risk of infringement of such rights, and the NFPA disclaims liability for the infringement of any patent resulting from the use of or reliance on NFPA Documents.

NFPA adheres to the policy of the American National Standards Institute (ANSI) regarding the inclusion of patents in American National Standards ("the ANSI Patent Policy"), and hereby gives the following notice pursuant to that policy:

NOTICE: The user's attention is called to the possibility that compliance with an NFPA Document may require use of an invention covered by patent rights. NFPA takes no position as to the validity of any such patent rights or as to whether such patent rights constitute or include essential patent claims under the ANSI Patent Policy. If, in connection with the ANSI Patent Policy, a patent holder has filed a statement of willingness to grant licenses under these rights on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license, copies of such filed statements can be obtained, on request, from NFPA. For further information, contact the NFPA at the address listed below.

Law and Regulations

Users of NFPA Documents should consult applicable federal, state, and local laws and regulations. NFPA does not, by the publication of its codes, standards, recommended practices, and guides, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

NFPA Documents are copyrighted. They are made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of safe practices and methods. By making these documents available for use and adoption by public authorities and private users, the NFPA does not waive any rights in copyright to these documents.

Use of NFPA Documents for regulatory purposes should be accomplished through adoption by reference. The term "adoption by reference" means the citing of title, edition, and publishing information only. Any deletions, additions, and changes desired by the adopting authority should be noted separately in the adopting instrument. In order to assist NFPA in following the uses made of its documents, adopting authorities are requested to notify the NFPA (Attention: Secretary, Standards Council) in writing of such use. For technical assistance and questions concerning adoption of NFPA Documents, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Documents and all requests for information on NFPA procedures governing its codes and standards development process, including information on the procedures for requesting Formal Interpretations, for proposing Tentative Interim Amendments, and for proposing revisions to NFPA documents during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101; email: stds_admin@nfpa.org

For more information about NFPA, visit the NFPA website at www.nfpa.org.

Copyright © 2013 National Fire Protection Association®. All Rights Reserved.

NFPA 1600®

Standard on

Disaster/Emergency Management and Business Continuity Programs

2013 Edition

This edition of *NFPA 1600, Standard on Disaster/Emergency Management and Business Continuity Programs*, was prepared by the Technical Committee on Emergency Management and Business Continuity. It was issued by the Standards Council on November 27, 2012, with an effective date of December 17, 2012, and supersedes all previous editions.

This edition of *NFPA 1600* was approved as an American National Standard on December 17, 2012.

Origin and Development of NFPA 1600

The NFPA Standards Council established the Disaster Management Committee in January 1991. The committee was given the responsibility for developing documents relating to preparedness for, response to, and recovery from disasters resulting from natural, human, or technological events.

The first document that the committee focused on was NFPA 1600, *Recommended Practice for Disaster Management.* NFPA 1600 was presented to the NFPA membership at the 1995 Annual Meeting in Denver, CO. That effort produced the 1995 edition of NFPA 1600.

For the 2000 edition, the committee incorporated a "total program approach" for disaster/emergency management and business continuity programs in its revision of the document from a recommended practice to a standard. They provided a standardized basis for disaster/emergency management planning and business continuity programs in private and public sectors by providing common program elements, techniques, and processes. The committee provided expanded provisions for enhanced capabilities for disaster/emergency management and business continuity programs so that the impacts of a disaster would be mitigated, while protecting life and property. The chapters were expanded to include additional material relating to disaster/emergency management and business continuity programs. The annex material was also expanded to include additional explanatory material.

For the 2004 edition, the committee updated terminology and editorially reformatted the document to follow the 2003 *Manual of Style for NFPA Technical Committee Documents*; however, the basic features of the standard remained unchanged. In addition, the committee added a table in Annex A that created a crosswalk among FEMA CAR, NFPA 1600, and BCI & DRII professional practices. The committee added significant informational resources to Annexes B, C, D, and E.

The document continues to be developed in cooperation and coordination with representatives from FEMA, NEMA, and IAEM. This coordinated effort was reflected in the expansion of the title of the standard for the 2000 edition to include both disaster and emergency management, as well as information on business continuity programs.

The 2007 edition incorporated changes to the 2004 edition, expanding the conceptual framework for disaster/emergency management and business continuity programs. Previous editions of the standard focused on the four aspects of mitigation, preparedness, response, and recovery. The 2007 edition identified prevention as a distinct aspect of the program, in addition to the other four. Doing so brought the standard into alignment with related disciplines and practices of risk management, security, and loss prevention.

The technical committee also expresses its appreciation to the U.S. Department of Homeland Security (DHS), IAEM, and NEMA for their continued support in the development of the standard, and for the use of their logos on the cover of the 2007 edition.

The 2010 edition of *NFPA 1600* was reordered and expanded. Chapter 4, Program Management, was expanded to emphasize the importance of leadership and commitment; included new requirements for defining performance objectives; and included new requirements for records

NFPA 1600, NFPA, and National Fire Protection Association are registered trademarks of the National Fire Protection Association, Quincy, Massachusetts 02169.

management. Finance and administration was also moved to the program management chapter. The most noticeable change from the 2007 edition was the rewriting of Chapter 5 into four chapters addressing planning, implementation, testing and exercises, and program improvement. The ordering of these chapters followed a typical program development process and is consistent with "plan, do, check, act" or continuous improvement processes. Requirements for business impact analysis, which had been previously been covered under the heading of "risk assessment," became a separate section within Chapter 5. Chapter 6, Implementation, included a new section on employee assistance and support. Testing and exercising was expanded within the new Chapter 7, and evaluations and corrective action were incorporated into a new Chapter 8 on program improvement.

The long list of resources included with the annexes of prior editions was pared down, recognizing the difficulty of keeping information up to date in a triennial publication. Annex C included a self-assessment checklist to help users evaluate conformity with the standard, and Annex D provided a crosswalk between *NFPA 1600* and management system program elements.

In November of 2009, *NFPA 1600* received designation and certification as anti-terrorism technology under the SAFETY Act. The technical committee extends its appreciation to the U.S. Department of Homeland Security for authorizing the use of the SAFETY Act Certified™ seal on the cover of the 2010 edition.

The technical committee also expresses its appreciation to the Association of Contingency Planners (ACP), Disaster Recovery Institute International (DRII), and IAEM for their continued support in the development of *NFPA 1600,* and the use of their logos on the cover of the 2010 edition.

The 2013 edition has an array of changes. The committee reorganized specific chapters and improved the requirements for Business Continuity throughout the document. In Chapter 6, the role of the Emergency Operation Center (EOC) is more defined, and the important role that the EOC plays during an emergency is discussed. The committee also created a section on crisis communication and public information. A chapter on training and education has been added (Chapter 7). In Chapter 9, the committee added program maintenance requirements. Readers will notice that Annex A has been reorganized, and only supplementary material will be found there; the material that was removed from Annex A is now located in five new annexes. One of those new annexes, Annex E, provides a crosswalk between *NFPA 1600*, CSA Z1600, and DRII Professional Practices. Other new annexes include Annex F, Management System Standard; Annex G, Maturity Models; Annex H, APELL (Awareness and Preparedness for Emergencies at the Local Level), in response to the gas leak in Bhopal, India, in 1984; and Annex I, Family Preparedness.

Technical Committee on Emergency Management and Business Continuity

Donald L. Schmidt, *Chair*
Preparedness, LLC, MA [SE]

Charles P. Adams, Medina County Emergency Management Agency, OH [E]
Richard R. Anderson, Anderson Risk Consultants, NJ [SE]
Pete Brewster, U.S. Department of Veterans Affairs, WV [U]
Steven J. Charvat, University of Washington, WA [U]
Rep. International Association of Emergency Managers
Andrew E. Cuthbert, Western Digital Corporation, CA [U]
Gregory T. Cybulski, Aon Corporation, NJ [I]
Matthew Devine, Santa Rosa Fire Department, CA [E]
Michael J. DuBose, HUB International Limited, NJ [I]
Roderick J. Fraser, Jr., Boston Fire Department, MA [E]
David Gluckman, Willis Group, NJ [I]
David Halstead, State of Florida, FL [E]
Rep. National Emergency Management Association
David J. Hiscott, Jr., ConocoPhillips Transportation, TX [U]
Rep. American Petroleum Institute
George B. Huff, Jr., Administrative Office of the U.S. Courts, VA [U]
Michael W. Janko, The Goodyear Tire & Rubber Company, OH [U]
Kenneth Katz, Travelers Insurance Company, NC [I]
James A. Kelley, The Hartford Financial Services, CT [I]
Gunnar J. Kuepper, Emergency & Disaster Management, Inc., CA [SE]
Dana C. Lankhorst, MiddleOak, NH [I]
Richard J. Larkin, City of Saint Paul, Minnesota, MN [U]
Rep. Emergency Management Accreditation Program
Dean R. Larson, Larson Performance Consulting, IN [SE]
Ray S. Lazarus, Emergency Management Ontario, Canada [E]
Diane K. Mack, Indiana University, IN [U]
Patricia A. Moore, Pat Moore Company, TX [SE]
Michael J. Morganti, Disaster Recovery Institute International, FL [SE]
Rep. Disaster Recovery Institute International
Susana M. Mueller, Tampa Electric Company/TECO Energy, Inc., FL [U]
Melvyn Musson, Edward Jones Company, MO [U]
Ashley E. Newsome, Emergency Response Educators & Consultants, Inc., FL [SE]
Daniel Newton, Microsoft Corporation, WA [U]
Scott R. Nicoll, Chubb Group of Insurance Companies, NJ [I]
Jo Robertson, Arkema Inc., PA [M]
Dale J. Romme, Hallmark Cards, Inc., MO [U]
Rep. NFPA Industrial Fire Protection Section
David M. Sarabacha, Deloitte & Touché LLP, WA [SE]
Brian Strong, BlueCross BlueShield of Florida, FL [I]

Alternates

Traci Bishop, Microsoft Corporation, WA [U]
(Alt. to D. Newton)
Matthew DeFrain, Deloitte & Touché LLP, IL [SE]
(Alt. to D. M. Sarabacha)
Steve Elliot, Elliot Consulting, FL [SE]
(Alt.to ACPI Rep.)
Robert Gazdik, Travelers Insurance Company, MN [I]
(Alt. to K. Katz)
Francis E. McCarton, Boston Fire Department, MA [E]
(Alt. to R. J. Fraser, Jr.)
John Douglas Nelson, Business Continuity Solutions, Inc., CA [SE]
(Alt. to P. A. Moore)
Kelley Okolita, DRI International, FL [SE]
(Alt. to M. J. Morganti)
Lorraine E. Webb, Emergency Management Ontario, Canada [E]
(Alt. to R. S. Lazarus)
Michael R. Zanotti, U.S. Department of Veterans Affairs, WV [U]
(Alt. to P. Brewster)

Nonvoting

Donald P. Bliss, NI2 Center for Infrastructure Expertise, NH [RT]
John C. Fannin III, SafePlace Corporation, DE [SE]
Rep. TC on Premises Security
Carl Anthony Gibson, La Trobe University, Australia [E]
Graeme S. Jannaway, Jannaway Continuity Consulting, Inc., Canada [SE]
Rep. Canadian Standards Association
Gavin J. Love, WorleyParsons Pty Ltd., TX [SE]

Orlando P. Hernandez, NFPA Staff Liaison

This list represents the membership at the time the Committee was balloted on the final text of this edition. Since that time, changes in the membership may have occurred. A key to classifications is found at the back of the document.

NOTE: Membership on a committee shall not in and of itself constitute an endorsement of the Association or any document developed by the committee on which the member serves.

Committee Scope: This Committee shall have primary responsibility for documents on preparedness for, response to, and recovery from disasters resulting from natural, human, or technological events.

Contents

NFPA 1600

Standard on

Disaster/Emergency Management and Business Continuity Programs

2013 Edition

IMPORTANT NOTE: This NFPA document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notices and Disclaimers Concerning NFPA Documents." They can also be obtained on request from NFPA or viewed at www.nfpa.org/disclaimers.

NOTICE: An asterisk (*) following the number or letter designating a paragraph indicates that explanatory material on the paragraph can be found in Annex A.

Changes other than editorial are indicated by a vertical rule beside the paragraph, table, or figure in which the change occurred. These rules are included as an aid to the user in identifying changes from the previous edition. Where one or more complete paragraphs have been deleted, the deletion is indicated by a bullet (•) between the paragraphs that remain.

Information on referenced publications can be found in Chapter 2 and Annex J.

Chapter 1 Administration

1.1* Scope. This standard shall establish a common set of criteria for all hazards disaster/emergency management and business continuity programs, hereinafter referred to as "the program."

1.2* Purpose. This standard provides the fundamental criteria to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity, and recovery.

1.3* Application. This document shall apply to public, not-for-profit, and nongovernmental organizations (NGOs) and to private entities.

Chapter 2 Referenced Publications

2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document.

2.2 NFPA Publications. (Reserved)

2.3 Other Publications.

Merriam-Webster's Collegiate Dictionary, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2003.

2.4 References for Extracts in Mandatory Sections. (Reserved)

Chapter 3 Definitions

3.1 General. The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, shall be the source for the ordinarily accepted meaning.

3.2 NFPA Official Definitions.

3.2.1* Approved. Acceptable to the authority having jurisdiction.

3.2.2* Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure.

3.2.3 Shall. Indicates a mandatory requirement.

3.2.4 Should. Indicates a recommendation or that which is advised but not required.

3.2.5 Standard. A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the *Manual of Style for NFPA Technical Committee Documents*.

3.3 General Definitions.

3.3.1 All-Hazards. An approach for prevention, mitigation, preparedness, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused.

3.3.2* Business Continuity. An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

3.3.3 Business Impact Analysis. A management level analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources. The analysis may identify time-critical functions, recovery priorities, dependencies, and interdependencies so that recovery time objectives can be established and approved.

3.3.4 Capability. The ability to perform required actions.

3.3.5 Competence. Demonstrated ability to apply knowledge and skills to achieve intended results.

3.3.6 Continual Improvement. Recurring process of enhancing the management program in order to achieve improvements in overall performance consistent with the entity's policy, goals, and objectives.

3.3.7* Continuity. A term that includes business continuity, continuity of operations (COOP), operational continuity, succession planning, continuity of government (COG), which support the resilience of the entity.

3.3.8 Crisis Management. The ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputational impacts.

3.3.9 Damage Assessment. An appraisal or determination of the effects of the incident on humans; on physical, operational, economic characteristics; and on the environment.

3.3.10 Disaster/Emergency Management. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and to recover from, an incident that threatens life, property, operations, or the environment.

3.3.11 Entity. A governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has emergency management and continuity of operations responsibilities.

3.3.12* Exercise. A process to assess, train, practice, and improve performance in an organization.

3.3.13 Incident. An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe.

3.3.14 Incident Action Plan. A verbal plan, written plan, or combination of both that is updated throughout the incident and reflects the overall incident strategy, tactics, risk management, and member safety requirements developed by the incident commander.

3.3.15* Incident Management System (IMS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure and designed to aid in the management of resources during incidents.

3.3.16 Interoperability. The ability of diverse personnel, systems, and organizations to work together seamlessly.

3.3.17 Mitigation. Activities taken to reduce the impact from hazards.

3.3.18* Mutual Aid/Assistance Agreement. A prearranged agreement between two or more entities to share resources in response to an incident.

3.3.19 Preparedness. Ongoing activities, tasks, and systems to develop, implement, and maintain the program capabilities.

3.3.20* Prevention. Activities to avoid or stop an incident from occurring.

3.3.21* Recovery. Activities and programs designed to return conditions to a level that is acceptable to the entity.

3.3.22* Resource Management. A system for identifying available resources to enable timely access to resources needed to prevent, mitigate, prepare for, respond to, maintain continuity during, or recover from an incident.

3.3.23* Response. Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment.

3.3.24 Risk Assessment. The process of hazard identification and the analysis of probabilities, vulnerabilities, and impacts.

3.3.25 Situation Analysis. The process of collecting, evaluating, and disseminating information related to the incident, including information on the current and forecasted situation and on the status of resources for management of the incident.

3.3.26 Test. Procedure for evaluation with a pass or fail result.

3.3.27 Vital Records. Information critical to the continued operation or survival of an entity.

Chapter 4 Program Management

4.1* Leadership and Commitment.

4.1.1 The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents.

4.1.2 The leadership commitment shall include the following:

(1) Support the development, implementation, and maintenance of the program
(2) Provide necessary resources to support the program
(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness
(4) Support corrective action to address program deficiencies

4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.

4.2* Program Coordinator. The program coordinator shall be appointed by the entity's leadership and authorized to develop, implement, administer, evaluate, and maintain the program.

4.3 Program Committee.

4.3.1* A program committee shall be established by the entity in accordance with its policy.

4.3.2 The program committee shall provide input and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program.

4.3.3* The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.

4.4 Program Administration.

4.4.1 The entity shall have a documented program that includes the following:

(1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority
(2)*Program scope, goals, performance, objectives, and metrics for program evaluation
(3)*Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5
(4) Program budget and schedule, including milestones
(5) Program plans and procedures that include the following:
    (a) Anticipated cost
    (b) Priority
    (c) Resources required
(6) Records management practices as required by Section 4.7
(7) Change management process

4.4.2 The program shall include the requirements specified in Chapters 4 through 9, the scope of which shall be determined through an "all-hazards" approach and the risk assessment.

4.4.3* Program requirements shall be applicable to prevention, mitigation, preparedness, response, continuity, and recovery.

4.5 Laws and Authorities.

4.5.1 The program shall comply with applicable legislation, policies, regulatory requirements, and directives.

4.5.2 The entity shall establish and maintain a procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives.

4.5.3* The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.

4.6 Finance and Administration.

4.6.1 The entity shall develop finance and administrative procedures to support the program before, during, and after an incident.

4.6.2* There shall be a responsive finance and administrative framework that does the following:

(1) Complies with the entity's program requirements
(2) Is uniquely linked to response, continuity, and recovery operations
(3) Provides for maximum flexibility to expeditiously request, receive, manage, and apply funds in a nonemergency environment and in emergency situations to ensure the timely delivery of assistance

4.6.3 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles, governance requirements, and fiscal policy.

4.6.4 Finance and administrative procedures shall include the following:

(1) Responsibilities for program finance authority, including reporting relationships to the program coordinator
(2)*Program procurement procedures
(3) Payroll
(4)*Accounting systems to track and document costs
(5) Management of funding from external sources
(6) Crisis management procedures that coordinate authorization levels and appropriate control measures
(7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery
(8) Identifying and accessing alternative funding sources
(9) Managing budgeted and specially appropriated funds

4.7* Records Management.

4.7.1 The entity shall develop, implement, and manage a records management program to ensure that records are available to the entity following an incident.

4.7.2 The program shall include the following:

(1) Identification of records (hard copy or electronic) vital to continue the operations of the entity
(2) Backup of records on a frequency necessary to meet program goals and objectives
(3) Validation of the integrity of records backup
(4) Implementation of procedures to store, retrieve, and recover records onsite or offsite
(5) Protection of records
(6) Implementation of a record review process
(7) Procedures coordinating records access

Chapter 5 Planning

5.1 Planning and Design Process.

5.1.1* The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program.

5.1.2 Strategic planning shall define the entity's vision, mission, and goals of the program.

5.1.3 A risk assessment and a business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies.

5.1.4 A risk assessment, a BIA, and a resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans.

5.1.5 Crisis management planning shall address issues that threaten the strategic, reputational, and intangible elements of the entity.

5.1.6 The entity shall include key stakeholders in the planning process.

5.2* Risk Assessment.

5.2.1 The entity shall conduct a risk assessment to develop required strategies and plans.

5.2.2 The entity shall identify hazards and monitor those hazards and the likelihood of their occurrence.

5.2.2.1* Hazards to be evaluated shall include the following:

(1) Natural hazards (geologic, meteorologic, and biological)
(2) Human-caused events (accidental and intentional)
(3) Technology-caused events (accidental and intentional)

5.2.2.2 The vulnerability of people, property, operations, the environment, and the entity shall be identified, evaluated, and monitored.

5.2.3 The entity shall conduct an analysis of the impacts of the hazards identified in 5.2.2 on the following:

(1) Health and safety of persons in the affected area
(2) Health and safety of personnel responding to the incident
(3)*Continuity of operations
(4)*Property, facilities, assets, and critical infrastructure
(5) Delivery of the entity's services
(6) Supply chain
(7) Environment
(8)*Economic and financial conditions
(9) Regulatory and contractual obligations
(10) Reputation of or confidence in the entity

5.2.4* The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts.

5.2.5 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies.

5.3* Business Impact Analysis.

5.3.1 The entity shall conduct a BIA.

5.3.2 The BIA shall evaluate the potential impact resulting from interruption or disruption of individual functions, processes, and applications.

5.3.3* The BIA shall identify those functions, processes, infrastructure, systems, and applications that are critical to the entity and the point in time [recovery time objective (RTO)] when the impact of the interruption or disruption becomes unacceptable to the entity.

5.3.4 The BIA shall identify dependencies and interdependencies across functions, processes, and applications to determine the potential for compounding impact in the event of an interruption or disruption.

5.3.5* The BIA shall evaluate the potential loss of information and the point in time [recovery point objective (RPO)] that defines the potential gap between the last backup of information and the time of the interruption or disruption.

5.3.6* The BIA shall be used in the development of recovery strategies and plans to support the program.

5.4 Resource Needs Assessment.

5.4.1* The entity shall conduct a resource needs assessment based on the hazards identified in Section 5.2 and the business impact analysis in Section 5.3.

5.4.2 The resource needs assessment shall include the following:

(1)*Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed
(2) Quantity, response time, capability, limitations, cost, and liabilities

5.4.3* The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, and materials procured or donated to support the program.

5.4.4 Facilities capable of supporting response, continuity, and recovery operations shall be identified.

5.4.5* Agreements. The need for mutual aid/assistance or partnership agreements shall be determined; if needed, agreements shall be established and documented.

5.5 Performance Objectives.

5.5.1* The entity shall establish performance objectives for the program in accordance with Chapter 4 and the elements in Chapters 5 through 9.

5.5.2 The performance objectives shall address the results of the hazard identification, risk assessment, and business impacts analysis.

5.5.3 Performance objectives shall be developed by the entity to address both short-term and long-term needs.

5.5.4* The entity shall define the terms *short term* and *long term*.

Chapter 6 Implementation

6.1 Common Plan Requirements.

6.1.1* Plans shall address the health and safety of personnel.

6.1.2 Plans shall identify and document the following:

(1) Assumptions made during the planning process
(2) Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions
(3) Lines of authority
(4) The process for delegation of authority
(5) Lines of succession for the entity
(6) Liaisons to external entities
(7) Logistics support and resource requirements

6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.

6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.

6.2 Prevention.

6.2.1* The entity shall develop a strategy to prevent an incident that threatens life, property, and the environment.

6.2.2* The prevention strategy shall be kept current using the information collection and intelligence techniques.

6.2.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, an analysis of impacts, program constraints, operational experience, and a cost-benefit analysis.

6.2.4 The entity shall have a process to monitor the identified hazards and adjust the level of preventive measures to be commensurate with the risk.

6.3 Mitigation.

6.3.1* The entity shall develop and implement a mitigation strategy that includes measures to be taken to limit or control the consequences, extent, or severity of an incident that cannot be prevented.

6.3.2* The mitigation strategy shall be based on the results of hazard identification and risk assessment, an analysis of impact, program constraints, operational experience, and cost-benefit analysis.

6.3.3 The mitigation strategy shall include interim and long-term actions to reduce vulnerabilities.

6.4 Crisis Communications and Public Information.

6.4.1* The entity shall develop a plan and procedures to disseminate information to and respond to requests for information from the following audiences before, during, and after an incident:

(1) Internal audiences, including employees
(2) External audiences, including the media, functional needs populations, and other stakeholders

6.4.2* The entity shall establish and maintain a crisis communications or public information capability that includes the following:

(1)*Central contact facility or communications hub
(2) Physical or virtual information center
(3) System for gathering, monitoring, and disseminating information
(4) Procedures for developing and delivering coordinated messages
(5) Protocol to clear information for release

6.5 Warning, Notifications, and Communications.

6.5.1* The entity shall determine its warning, notification, and communications needs.

6.5.2* Warning, notification, and communications systems shall be reliable, redundant, and interoperable.

6.5.3* Emergency warning, notification, and communications protocols and procedures shall be developed, tested, and used to alert stakeholders potentially at risk from an actual or impending incident.

6.5.4 Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of prescripted information bulletins or templates.

6.6 Operational Procedures.

6.6.1 The entity shall develop, coordinate, and implement operational procedures to support the program.

6.6.2 Procedures shall be established and implemented for response to and recovery from the impact of hazards identified in 5.2.2.

6.6.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.

6.6.4 Procedures shall include the following:

(1) Control of access to the area affected by the incident
(2) Identification of personnel engaged in activities at the incident
(3) Accounting for personnel engaged in incident activities
(4) Mobilization and demobilization of resources

6.6.5 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.

6.7 Incident Management.

6.7.1* The entity shall develop an incident management system to direct, control, and coordinate response, continuity, and recovery operations.

6.7.1.1* Emergency Operations Centers (EOCs).

6.7.1.1.1* The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations.

6.7.1.1.2* The EOCs shall be permitted to be physical or virtual.

6.7.1.1.3 On activation of an EOC, communications and coordination shall be established between incident command and the EOC.

6.7.2 The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.

6.7.3 The entity shall establish procedures and policies for coordinating mitigation, preparedness, response, continuity, and recovery activities.

6.7.4 The entity shall coordinate the activities specified in 6.7.3 with stakeholders.

6.7.5 Procedures shall include a situation analysis that incorporates a damage assessment and a needs assessment to identify resources to support activities.

6.7.6* Emergency operations/response shall be guided by an incident action plan or management by objectives.

6.7.7 Resource management shall include the following tasks:

(1) Establishing processes for describing, taking inventory of, requesting, and tracking resources
(2) Resource typing or categorizing by size, capacity, capability, and skill
(3) Mobilizing and demobilizing resources in accordance with the established IMS
(4) Conducting contingency planning for resource deficiencies

6.7.8 A current inventory of internal and external resources shall be maintained.

6.7.9 Donations of human resources, equipment, material, and facilities shall be managed.

6.8 Emergency Operations/Response Plan.

6.8.1* Emergency operations/response plans shall define responsibilities for carrying out specific actions in an emergency.

6.8.2* The plan shall identify actions to be taken to protect people, including those with access and functional needs, property, operations, the environment, and the entity.

6.8.3* The plan shall identify actions for incident stabilization.

6.8.4 The plan shall include the following:

(1) Protective actions for life safety in accordance with 6.8.2.
(2) Warning, notifications, and communication in accordance with Section 6.5.
(3) Crisis communication and public information in accordance with Section 6.4
(4) Resource management in accordance with 6.7.7
(5) Donation management in accordance with 6.7.9

6.9 Business Continuity and Recovery.

6.9.1* The continuity plan shall include recovery strategies to maintain critical or time-sensitive functions and processes identified during the business impact analysis.

6.9.2* The continuity plan shall identify stakeholders that need to be notified; critical and time-sensitive applications; alternative work sites; vital records, contact lists, functions, and processes that must be maintained; and personnel, procedures, and resources that are needed while the entity is recovering.

6.9.3* The recovery plan shall provide for restoration of functions, services, resources, facilities, programs, and infrastructure.

6.10 Employee Assistance and Support.

6.10.1* The entity shall develop a strategy for employee assistance and support that includes the following:

(1)*Communications procedures
(2)*Contact information, including emergency contact outside the anticipated hazard area
(3) Accounting for persons affected, displaced, or injured by the incident
(4) Temporary, short-term, or long-term housing and feeding and care of those displaced by an incident
(5) Mental health and physical well-being of individuals affected by the incident
(6) Pre-incident and post-incident awareness

6.10.2 The strategy shall be flexible for use in all incidents.

6.10.3* The entity shall promote family preparedness education and training for employees.

Chapter 7 Training and Education

7.1* Curriculum. The entity shall develop and implement a competency-based training and education curriculum that supports all employees who have a role in the program.

7.2 Goal of Curriculum. The goal of the curriculum shall be to create awareness and enhance the knowledge, skills, and abilities required to implement, support, and maintain the program.

7.3 Scope and Frequency of Instruction. The scope of the curriculum and the frequency of instruction shall be identified.

7.4 Incident Management System Training. Personnel shall be trained in the entity's incident management system (IMS) and other components of the program to the level of their involvement.

7.5 Recordkeeping. Records of training and education shall be maintained as specified in Section 4.7.

7.6 Regulatory and Program Requirements. The curriculum shall comply with applicable regulatory and program requirements.

7.7* Public Education. A public education program shall be implemented to communicate the following:

(1) The potential impact of a hazard
(2) Preparedness information
(3) Information needed to develop a preparedness plan

Chapter 8 Exercises and Tests

8.1 Program Evaluation.

8.1.1 The entity shall evaluate program plans, procedures, training, and capabilities and promote continuous improvement through periodic exercises and tests.

8.1.2 The entity shall evaluate the program based on post-incident analyses, lessons learned, and operational performance in accordance with Chapter 9.

8.1.3 Exercises and tests shall be documented.

8.2* Exercise and Test Methodology.

8.2.1 Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting.

8.2.2 Exercises shall be designed to assess the maturity of program plans, procedures, and strategies.

8.2.3 Tests shall be designed to demonstrate capabilities.

8.3* Design of Exercises and Tests. Exercises shall be designed to do the following:

(1) Ensure the safety of people, property, operations, and the environment involved in the exercise or test
(2) Evaluate the program
(3) Identify planning and procedural deficiencies
(4) Test or validate recently changed procedures or plans
(5) Clarify roles and responsibilities
(6) Obtain participant feedback and recommendations for program improvement
(7) Measure improvement compared to performance objectives
(8) Improve coordination among internal and external teams, organizations, and entities
(9) Validate training and education
(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity
(11) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery
(12) Assess the ability of the team to identify, assess, and manage an incident
(13) Practice the deployment of teams and resources to manage an incident
(14) Improve individual performance

8.4 Exercise and Test Evaluation.

8.4.1 Exercises shall evaluate program plans, procedures, training, and capabilities to identify opportunities for improvement.

8.4.2 Tests shall be evaluated as either pass or fail.

8.5* Frequency.

8.5.1 Exercises and tests shall be conducted on the frequency needed to establish and maintain required capabilities.

Chapter 9 Program Maintenance and Improvement

9.1* Program Reviews. The entity shall maintain and improve the program by evaluating its policies, program, procedures, and capabilities using performance objectives.

9.1.1* The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action.

9.1.2* Evaluations shall be conducted on a regularly scheduled basis and when the situation changes to challenge the effectiveness of the existing program.

9.1.3 The program shall be re-evaluated when a change in any of the following impacts the entity's program:

(1) Regulations
(2) Hazards and potential impacts
(3) Resource availability or capability
(4) Entity's organization
(5)*Funding changes
(6) Infrastructure, including technology environment
(7) Economic and geographic stability
(8) Entity operations

9.1.4 Reviews shall include post-incident analyses, reviews of lessons learned, and reviews of program performance.

9.1.5 The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.7.

9.1.6 Documentation, records, and reports shall be provided to management for review and follow-up.

9.2* Corrective Action.

9.2.1* The entity shall establish a corrective action process.

9.2.2* The entity shall take corrective action on deficiencies identified.

9.3 Continuous Improvement. The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process.

Annex A Explanatory Material

Annex A is not a part of the requirements of this NFPA document but is included for informational purposes only. This annex contains explanatory material, numbered to correspond with the applicable text paragraphs.

A.1.1 The Emergency Management and Business Continuity community comprises many different entities, including the government at distinct levels (e.g., federal, state/provincial, territorial, tribal, indigenous, and local levels); commercial business and industry; not-for-profit and nongovernmental organizations; and individual citizens. Each of these entities has its own focus, unique mission and responsibilities, varied resources and capabilities, and operating principles and procedures.

A.1.2 The standard promotes a common understanding of the fundamentals of planning and decision making to help entities examine all hazards and produce an integrated, coordinated, and synchronized program for disaster/emergency management and business continuity.

A.1.3 The application of *NFPA 1600* within the private sector is described in detail in *Implementing NFPA 1600, National Preparedness Standard,* published by the National Fire Protection Association.

A.3.2.1 Approved. The National Fire Protection Association does not approve, inspect, or certify any installations, procedures, equipment, or materials; nor does it approve or evaluate testing laboratories. In determining the acceptability of installations, procedures, equipment, or materials, the authority having jurisdiction may base acceptance on compliance with NFPA or other appropriate standards. In the absence of such standards, said authority may require evidence of proper installation, procedure, or use. The authority having jurisdiction may also refer to the listings or labeling practices of an organization that is concerned with product evaluations and is thus in a position to determine compliance with appropriate standards for the current production of listed items.

A.3.2.2 Authority Having Jurisdiction (AHJ). The phrase "authority having jurisdiction," or its acronym AHJ, is used in NFPA documents in a broad manner, since jurisdictions and approval agencies vary, as do their responsibilities. Where public safety is primary, the authority having jurisdiction may be a federal, state, local, or other regional department or individual such as a fire chief; fire marshal; chief of a fire prevention bureau, labor department, or health department; building official; electrical inspector; or others having statutory authority. For insurance purposes, an insurance inspection department, rating bureau, or other insurance company representative may be the authority having jurisdiction. In many circumstances, the property owner or his or her designated agent assumes the role of the authority having jurisdiction; at government installations, the commanding officer or departmental official may be the authority having jurisdiction.

A.3.3.2 Business Continuity. Another term for business continuity is *operational continuity* or *continuity of operations (COOP).* In the public sector, the term *continuity of government (COG)* is also used. See also 3.3.7 and A.3.3.7.

A.3.3.7 Continuity. An evolving concept that is linked to continuity is resilience. Organizational resilience is the ability of an entity to withstand potential impacts of natural, human-caused, and technology-caused hazards; respond effectively when an incident occurs; continue to provide a minimum acceptable level of service during and in the immediate aftermath of the incident; and thereafter return conditions to a level that is acceptable to the entity. Entities generally are interdependent with a wider community. To ensure that the community in which the entity operates is resilient, entities should work with local stakeholders (including public, private, and not-for-profit organizations) to promote emergency management and business continuity processes. Entities should evaluate their suppliers. The entity should request that the supplier develop and maintain programs and processes to ensure organizational resilience and their ability to provide critical services and goods during emergencies and disasters. Providing generic advice as well as more detailed assistance on a one-to-one basis to external stakeholders can ensure that businesses and government are resilient and can quickly restore a community's ability to function normally after an incident. The underlying strategy is to bring together all sectors to collaborate and share good practice. This concept can be referred to as "community resilience."

A.3.3.12 Exercise. Exercise is the principal means of evaluating a program's ability to execute its response procedures. It allows the entity and stakeholder organizations to practice procedures and interact in a controlled setting. Participants identify and make recommendations to improve the overall program. Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses, with the goal of achieving maximum performance.

An exercise can include seminars, workshops, games, drills, tabletops, functional exercises, or full-scale exercises and involve the simulation of a response or operational continuity incident. Exercises can be announced or unannounced and involve participant role-play in order to identify issues that might arise in a real incident.

A.3.3.15 Incident Management System (IMS). The incident management system is based on effective management characteristics that can be used by the public, private, and not-for-profit sectors. For an IMS to work effectively each management characteristic should contribute to the strength and efficiency of the overall system.

A description of commonly identified management characteristics follows.

Common Terminology. Common terminology allows diverse incident management and support entities to work together across a wide variety of incident management functions and hazard scenarios. This common terminology is covered in the paragraphs that follow.

Organizational Functions. Major functions and functional units with domestic incident management responsibilities are named, and defined terminology for the organizational elements involved is standard and consistent. The incident management organization establishes a process for gathering, sharing, and managing incident-related information and intelligence.

Modular Organization. The organizational structure develops in a top-down, modular fashion that is based on the size and complexity of the incident, as well as the specifics of the hazard environment created by the incident. Where needed, separate functional elements can be established, each of which can be further subdivided to enhance external organizational management and external coordination.

Comprehensive Resource Management. Maintaining an accurate and up-to-date picture of resource utilization is a critical component of domestic incident management. Resource management includes processes for categorizing, ordering, dispatching, tracking, and recovering resources. It also includes processes for reimbursement for resources, as appropriate. Resources are defined as personnel, teams, equipment, supplies, and facilities available or potentially available for assignment or allocation in support of incident management and emergency response activities. Personnel and equipment should respond only when requested or when dispatched by an appropriate authority.

Incident Facilities. Various types of operational locations and support facilities are established in the vicinity of an incident to accomplish a variety of objectives, such as decontamination, donated goods processing, mass care, and evacuation. Typical facilities include incident command posts, bases, camps, staging areas, mass casualty triage areas, and other facilities as required.

Management by Objectives. Management by objectives represents an approach that is communicated throughout the entire organization. This approach includes establishing overarching objectives for the following:

(1) Developing and issuing assignments, plans, procedures, and protocols
(2) Establishing specific, measurable objectives for various incident management functional activities and directing efforts to attain them in support of defined strategic objectives
(3) Documenting results to measure performance and facilitate corrective action

Reliance on an Incident Action Plan. Incident action plans (IAPs) provide a coherent means of communicating the overall incident objectives in the context of both operational and support activities.

Manageable Span of Control. Span of control is key to effective and efficient incident management. Although effective span of control varies, the span of incident management supervisory responsibility in the public sector is typically three to seven subordinates. The type of incident, the nature of the task, hazards and safety factors, and distances between personnel and resources all influence span of control considerations.

Integrated Communications. Incident communications are facilitated through the development and use of a common communications plan and interoperable communications processes and architectures. This integrated approach links the operational and support units of the various agencies involved. It is necessary to maintain communications connectivity and discipline and to enable common situational awareness and interaction. Preparedness planning should address the equipment, systems, and protocols necessary to achieve integrated voice and data incident management communications.

Establishment and Transfer of Command. The command function has to be clearly established from the beginning of incident operations. The agency with primary jurisdictional authority over the incident designates the individual at the scene who will be responsible for establishing command. When command is transferred, the process should include a briefing that captures all essential information for continuing safe and effective operations.

Chain of Command and Unity of Command. Chain of command refers to the orderly line of authority within the ranks of the incident management organization. Unity of command means that every individual has a designated supervisor to whom he or she reports at the scene of the incident. These principles clarify reporting relationships and eliminate the confusion caused by multiple, conflicting directives. Incident managers at all levels have to be able to control the actions of all personnel under their supervision.

Unified Command (UC). In incidents involving multiple jurisdictions, a single jurisdiction with multi-agency involvement, or multiple jurisdictions with multi-agency involvement, unified command (UC) allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

Although a single Incident Commander normally handles the command function, an incident management system (IMS) can be expanded into a UC. The UC is a structure that brings together the incident commanders of all major organizations, which could include personnel from both private and public sectors involved in the incident, in order to coordinate an effective response while at the same time they carry out their own jurisdictional responsibilities. The UC links the organizations responding to the incident and provides a forum for the entities to make consensus decisions. Under the UC, the various jurisdictions and/or agencies and nongovernment responders blend together throughout the operation to create an integrated response team.

A.3.3.18 Mutual Aid/Assistance Agreement. The term *mutual aid/assistance agreement,* as used herein, includes cooperative agreements, partnership agreements, memoranda of understanding, memorandum of agreement, intergovernmental compacts, or other terms commonly used for the sharing of resources. Agreements can be executed between any combination of public, private, and not-for-profit entities.

A.3.3.20 Prevention. The term *prevention* refers to activities, tasks, programs, and systems intended to avoid or intervene in order to stop an incident from occurring.

Prevention can apply to accidental and intentional human-caused incidents and technology-caused incidents. Accident prevention and safety programs can reduce the frequency of workplace accidents. Prevention and deterrence of human-caused intentional incidents can include gathering intelligence and information and implementing countermeasures such as enhanced surveillance and security operations; investigations to determine the nature and source of the threat; and law enforcement operations directed at deterrence, preemption, interdiction, or disruption. Implementation of network and information security can help prevent penetration of networks and intercept malware. Analyses of the vulnerability of systems can identify means to prevent incidents caused by interruption, disruption, or failure of technology.

A.3.3.21 Recovery. Recovery programs are designed to assist victims and their families, restore entities to suitable economic growth and confidence, relocate or rebuild destroyed property, and reconstitute government operations and services. Recovery actions can be short term or long term, often continuing long after the incident has ended. Recovery programs include mitigation components designed to avoid damage from future incidents.

A.3.3.22 Resource Management. This system includes a process for identifying, categorizing, ordering, mobilizing, tracking, and recovering and demobilizing resources, as well as a process for reimbursement for resources, as appropriate.

A.3.3.23 Response. The term *response* refers to the actions taken by an entity to an incident or event. Actions can include activities, tasks, programs, and systems to protect life safety, meet basic human needs, preserve operational capability, and protect property and the environment.

An incident response can include protective actions for life safety (evacuation, shelter-in-place, and lockdown), conducting damage assessment, initiating recovery strategies, and any other measures necessary to bring an entity to a more stable status.

A.4.1 Leadership should research applicable legal, regulatory, and other industry requirements that are related to the hazards, threats, and risks associated with the entity's facilities, activities, functions, products, services, and supply chain; the environment; and stakeholders. The entity should document this information and keep it up to date.

A.4.2 It is not the intent of this standard to restrict the users to the title *program coordinator.* It is recognized that different

entities use various forms and names for the person who performs the program coordinator functions identified in the standard. Examples of titles are *emergency manager* (for the public sector), and *business continuity manager* (for the private sector). A written position description should be provided.

Certification programs for emergency managers and business continuity professionals can be found in the DRII *Professional Practices for Business Continuity Practitioners* and through FEMA's Emergency Management Institute and the Certified Emergency Manager (CEM) program administered by International Association of Emergency Managers (IAEM).

A.4.3.1 All state and local emergency management entities report to a higher authority and might include governors, adjutant generals, chief law enforcement officers, county commissions, or city commissions, among others. These authorities set the agendas for emergency management activities, and a program committee might not be appropriate. Mandating an entity to have a program committee might, in some cases, violate the authorities under which the emergency management entity is established. Those entities that can have, or want to have, a program committee that will provide advice and guidance should be encouraged to do so.

A.4.3.3 When the representation on the program committee is being determined, consideration should be given to public sector representation on a private sector committee and vice versa, which will help to establish a coordinated and cooperative approach to the program.

A.4.4.1(2) Goals and objectives should be consistent with the entity's policy, vision, mission statement, roles and responsibilities, and enabling authority. Consideration should also be given to financial constraints, management support, regulatory requirements, and codes of practice.

A.4.4.1(3) Industry codes of practices and guidelines should also be considered. In the private sector, corporate policy might dictate the directives that should be followed.

The entity should consider local cultural and religious customs as well as demographics when developing the program.

A.4.4.3 Key program elements cross boundaries during prevention, mitigation, preparedness, response, continuity, and recovery. Each element should be considered interrelated with other elements and can be considered concurrently. The use of the terms, phases, elements, or components varies from program to program.

A.4.5.3 If, through exercise or incident analysis, program evaluation, or corrective action, limitations in the necessary laws and applicable authorities are discovered, a formal process should exist to amend them. This procedure should include an understanding of the procedures to influence the necessary changes to applicable legislation, policies, directives, standards, and industry codes of practice.

In the case of public/private entities, consideration should be made for periodic review of existing legislation, regulations, codes, and authorities to determine whether adequate flexibility exists to accommodate evolving programmatic policy or if new legislation should be developed and introduced through a legislative initiative. This is particularly relevant because program requirements change to comply with changing roles and relationships in and among varying levels of government.

For example, the entity might have the appropriate authority to conduct emergency operations but lack authority to take action prior to an event to mitigate the occurrence or the recurrence of an incident. In other cases, additional authorities could be needed to generate the necessary revenue to sustain a viable program or to create a standing contingency fund to adequately support an emergency operation.

A.4.6.2 In addition to having sound financial and administration procedures for daily operations, it is equally important to have procedures in place that will allow an entity to expedite financial decision making and ensure that proper accounting occurs. To develop proper financial and administration procedures, the following steps should be taken:

(1) The finance department could be considered for membership of the program committee.
(2) The finance department should be actively involved with identifying, prioritizing, and purchasing internal and external resources.
(3) The entity's financial opportunities or limitations should be identified within the strategic plan that defines the vision, mission, goals, and objectives of the program.

A.4.6.4(2) The entity should consider establishing contracts for resources in advance of an incident.

A.4.6.4(4) Existing internal controls that necessitate a response could be affected by the same event, which opens the door for opportunistic fraud. It is important that the entity recognize the possibility of fraud occurring during this window of opportunity and take reasonable precautions.

A.4.7 Records management is designed to aid in the identification, backup, protection, and access to paper-based and electronic records that are vital to the entity and required for the emergency management and business continuity program. It is not the intent of this section to require a records management program for all of the entity's records.

Records management practices should include the following activities:

(1) Creating, approving, and enforcing records management policies, including a classification system and a records retention policy
(2) Developing a records storage plan, including the short-term and long-term housing of physical records and digital information
(3) Identifying existing and newly created records and classifying and storing them according to standard operating procedures (SOPs)
(4) Coordinating the access and circulation of records within and outside the organization
(5) Executing a retention policy to archive and destroy records according to operational needs, operating procedures, statutes, and regulations

A.5.1.1 Assumptions used in preparation of plans, especially those regarding hazard identification, risk assessment, analysis of potential impacts, and the availability and capability of resources, should be identified, evaluated, and validated during the planning process. Confidential or sensitive information can be redacted or protected. Assumptions should be documented as required by 6.1.2(1).

A.5.2 Risk assessment is a process for identifying potential hazards/risk exposures and their relative probability of occurrence; identifying assets at risk; assessing the vulnerability of the assets exposed; and quantifying the potential impacts of the hazard/risk exposures on the assets. Periodic reassessment is

needed when changes to the entity occur. Reassessment is also necessary because hazards/risk exposures change over time, and the collective knowledge of hazards/risk exposures develops over time.

In addition to identifying hazards that could be the primary cause of an incident, consideration should also be given to those secondary hazards or cascading events that could cause additional impact to the entity and its assets. As an example, a fire could result in injury or death, property damage, interruption of operations, contamination of the environment, and negative attention on the entity.

A comprehensive risk assessment identifies the range of hazard/risk exposures, including threats, hazards, or disruptive incidents, that have impacted or might impact the entity, the surrounding area, or the critical infrastructure supporting the entity. The potential impact of each threat, hazard/risk exposure, or disruptive incident is determined by the capabilities of the perpetrator, the magnitude of the hazard, and the scope of the incident, as well as the vulnerability of people, property, technology, the environment, and the entity's operations to the threat, hazard, or incident and the adequacy of existing mitigation. There are multiple methods to perform a risk assessment, but the entity should adhere to the following steps for conducting a comprehensive risk assessment:

(1) Determine the methodology the entity will use to conduct the assessment and determine whether the entity has the necessary expertise to perform the assessment.
(2) Consult with internal or external experts with the expertise to assess the vulnerability of the entity's assets from identified hazards.
(3) Identify and categorize assets (human resources, buildings, equipment, operations, technology, electronic information, suppliers, vendors, third-party service providers, etc.).
(4) Identify threats and hazards — natural, human caused (accidental and intentional), and technology caused.
(5) Evaluate hazard/risk exposures to which the entity is exposed.
(6) Assess the existing/current preventive measures and mitigation controls in place against credible threats.
(7) Categorize threats, hazard/risk exposures, and potential incidents by their relative frequency and severity. Keep in mind that there might be many possible combinations of frequency and severity for each, as well as cascading impacts.
(8) Evaluate the residual hazard/risk exposures (those that remain hazardous after prevention and mitigation activities).

Information from the risk assessment and impact analysis will help determine priorities for prevention and mitigation activities as well as prioritize development of plans and procedures. The entity should attempt to prevent, mitigate, prepare for, plan to respond to, and plan to recover from incidents that have significant potential to impact people; property; operational capabilities, including technology; the environment; and the entity itself.

A.5.2.2.1 The following is an expanded list of hazards that should be considered during the risk assessment. Many hazards can be classified in multiple categories. A wildland fire might be caused by lightning or an intentional act. A fire in a chemical plant could be caused by human error or the failure of technology, such as a malfunctioning or improperly programmed control system. Hazards that should be considered during the risk assessment include natural hazards/risk exposures (geologic, meteorologic, and biological), human-caused events (accidental and intentional), and technology-caused incidents:

(1) Geologic hazards/risk exposures
  (a) Earthquake
  (b) Tsunami
  (c) Volcano
  (d) Landslide, mudslide, subsidence
(2) Meteorologic hazards/risk exposures
  (a) Flood, flash flood, seiche, tidal surge
  (b) Water control structure (e.g., dam, levee) failure
  (c) Drought
  (d) Snow, ice, hail, sleet, avalanche, arctic freeze
  (e) Windstorm, tropical cyclone, hurricane, tornado, water spout, duststorm, sandstorm
  (f) Extreme temperatures (heat, cold)
  (g) Wildland fire
  (h) Lightning strikes
  (i) Famine
  (j) Geomagnetic storm
(3) Biological hazards/risk exposures
  (a) Food-borne illnesses
  (b) Pandemic disease (e.g., avian flu, H1N1)
  (c) Infectious/communicable disease [e.g., plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), bovine spongiform encephalopathy (BSE, or Mad Cow Disease)]
(4) Accidental human-caused events
  (a) Hazardous material spill or release (flammable liquid; flammable gas; flammable solid; oxidizer; poison; explosive, radiological, or corrosive material)
  (b) Nuclear power plant incident, radiological incident
  (c) Explosion/fire
  (d) Transportation accident
  (e) Building/structure collapse
  (f) Entrapment and/or rescue (machinery, confined space, high angle, water)
  (g) Fuel/resource shortage
  (h) Mechanical breakdown
  (i) Transportation incidents (motor vehicle, railroad, watercraft, aircraft, pipeline)
  (j) Untimely death of employee
(5) Intentional human-caused events
  (a) Strike or labor dispute
  (b) Criminal activity (vandalism, sabotage, arson, robbery, theft, fraud, embezzlement, data theft, malfeasance)
  (c) Physical or information security breach
  (d) Lost person, child abduction, kidnapping, extortion, hostage incident, workplace/school/university violence, homicide
  (e) Product defect or contamination
  (f) Disinformation
  (g) Harassment
  (h) Discrimination
  (i) Demonstrations, civil disturbance, public unrest, mass hysteria, riot
  (j) Bomb threat, suspicious package
  (k) Terrorism (explosive, chemical, biological, radiological, nuclear, cyber, electromagnetic pulse)
  (l) Insurrection
  (m) Enemy attack, war
  (n) Arson
(6) Technology-caused incidents

(a) Computer systems [outages, hardware failure, data corruption, deletion, theft, loss of network connectivity (Internet or intranet), loss of electronic data interchange or ecommerce, loss of domain name server (DNS), virus, worm, Trojan horse, power surge, lightning, host site interdependencies, direct physical loss, water damage, cyber terrorism, vulnerability exploitation, botnets, hacking, phishing, spyware, malware, computer fraud, loss of encryption, denial of service, improper system use by employee, telecommunications interruption or failure, electricity brownout or blackout]
(b) Computer software or application interruption, disruption, or failure (internal/external)
(c) Loss, corruption, or theft of electronic information
(d) Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewage system, other critical infrastructure)

(7) Other hazards/risk exposures, such as supply chain interruption [loss of shipping or transportation, vendor failure (single or sole source provider)]

A.5.2.3(3) In order to maintain continuity of operations, the entity should identify essential or critical functions and processes, their recovery priorities, and their internal and external interdependencies, so that recovery time objectives can be set. Consideration also should be given to situations that cause the entity to become incapable of response or incapable of maintaining any continuity of operations for the foreseeable future. This process is called a business impact analysis (BIA) and is defined further in Section 5.3.

A.5.2.3(4) Assets include production machinery and processing equipment, tools, finished goods/inventory, raw materials, vehicles, electronic information, vital records, patents, intellectual property, and personnel/institutional knowledge. The analysis of impacts also should include evaluation of the infrastructure necessary to operate buildings, equipment, and technology.

A.5.2.3(8) Quantification of the potential economic and financial impacts resulting from property damage, interruption or disruption of operations, and environmental contamination provides input into the determination of where to invest in mitigation and planning efforts.

A.5.2.4 It is important to consider the cascading impact of regional, national, or international incidents. One example is the cascading impact of a hurricane. Direct impacts can include wind and flood damage. Secondary impacts can include telecommunications, electrical power, and transportation disruptions, both inside and outside the direct impact area. The earthquake and tsunami in Japan in 2011 resulted in supply chain interruptions around the world. The terrorist attacks of September 11, 2001, shut down air travel in the United States for days and impacted the financial markets.

A.5.3 The BIA provides an assessment of how key disruption risks could affect an entity's operations and identifies capabilities that might be needed to manage the disruptions.

The BIA Process. A BIA can be undertaken using engineering analysis, mathematical modeling, simulations, surveys, questionnaires, interviews, structured workshops, or a combination thereof, to identify the critical processes, people/personnel, assets and resources, physical and nonphysical properties, and the financial and operational effects of the loss of these elements, as well as the required recovery time frames and supporting resources.

Based on the risk and vulnerability assessments, the following steps should be taken to confirm the processes and outputs of the organization:

(1) Determine the consequences of a disruption on the identified processes in financial, regulatory, customer and/or operational terms over defined periods.
(2) Identify the interdependencies with key internal and external stakeholders, which could include mapping the nature of the interdependencies through the supply chain (both inbound and outbound).
(3) Determine the current available resources and the essential level of resources required to continue operation at a minimum acceptable level following a disruption.
(4) Identify ways to bypass problems ("workarounds") in processes that are currently in use or are planned to be developed. It might be necessary to develop alternative processes where resources or capability might be inaccessible or insufficient during the disruption.
(5) Determine the recovery time objective (RTO) for each process, based on the identified consequences and the critical success factors for the function. The RTO represents the maximum period of time the organization can tolerate the loss of capability.
(6) Determine the rate at which the severity of the impact increases over time if the RTO is not met.
(7) Confirm the current level of preparedness of the entity's processes to manage a disruption. This might include evaluating the level of redundancy within the process (e.g., spare equipment) or the existence of alternative suppliers.

The BIA processes should consist of the following three components:

(1) Identify the lines of process flow (i.e., material flow, information flow, people movement, cash flow) and time constraints. Typical output of the BIA will provide a process flow for the entire entity, identifying internal and external dependencies.
(2) Identify the interruption potentials that describe the financial, regulatory, customer, or operational impacts, including potential bottlenecks, upstream and downstream supply chains, single points of failure, long lead time or imported equipment, single-source and sole-source suppliers, time constraint processing (e.g., long batch times), and interdependencies between internal and external entities and facilities.
(3) Identify the entity's dependency on technology infrastructure, including systems and applications, by identifying the technology needed to continue time-sensitive operational processes; correlate specific technology components with the operational processes they support and based on that information, assess the impact to the entity's operations due to disruption of those components.

A typical BIA would supply the following information:

(1) The financial impact to the organization if the process fails to perform, for example:
(a) Loss of sales
(b) Fines or penalties incurred
(c) Overtime pay
(d) Additional costs to recover
(e) Loss of raw materials/finished products

(2) The regulatory or legal impact, for example:
(a) Failure to meet reporting requirements
(b) Failure to meet contractual commitments
(c) Potential lawsuits

(3) Customer impact, for example:
  (a) How soon customers will know a problem exists and how worried they will be
  (b) Impact to a customer's supply chain
  (c) Potential for a customer to take its business elsewhere
  (d) Harm that could be caused to the customer
  (e) Impact to brand
  (f) Impact to reputation
(4) Operational impact, for example:
  (a) Seasonal impact
  (b) Backlog impact
  (c) Workload changes
  (d) Overtime
  (e) Employee morale
(5) The RTO required for the process in order to meet the operational level acceptable to the entity
(6) Resources required to continue or resume time-sensitive processes and the escalation of resource needs over time, for example:
  (a) Technology infrastructure components, systems, and applications including:
    i. RTO of the required technology components
    ii. Interdependency among different technology components
    iii. Core infrastructure, systems, and services such as network components, directory services, etc., that are essential for recovery of other technology components
    iv. Recovery point objectives (RPOs) for data (the maximum amount of acceptable data loss)
  (b) Vital records requirements
  (c) Equipment requirements such as printers, fax machines, scanners, mail sorters, postage meters, time stamps, forklifts, ladders, and tools
  (d) Desktop requirements such as computers, telephones
  (e) Supplies such as paper, envelopes, letterhead, forms
  (f) Regulatory reporting requirements
  (g) Description of internal and external dependencies
  (h) Previous disruption experience
  (i) Known competitive issues analysis

The outputs of the BIA typically would include the following:

(1) Financial, operational, regulatory, customer, and other tangible and nontangible impact to the entity
(2) Identification of all time-sensitive processes and their critical resources requirements
(3) Identification of time-sensitive technology components essential to recover the operational processes
(4) Prioritization of processes to be recovered
(5) Prioritization of the technology components in alignment with operational processes
(6) Identification of key internal and external interdependencies of operational units, functions, processes, critical resources, and technology components
(7) Identification of seasonal impact to operations for each operational process
(8) Determination of resources (people, vendors, equipment, technology, data/information, funding, and time) required for resumption and recovery
(9) RTO for each process

The output information of the BIA will help to achieve the following:

(1) Identify the entity's critical operations
(2) Identify the entity's time-sensitive operations
(3) Determine the RTO for each critical operation
(4) Determine the internal and external dependencies
(5) Determine whether the recovery of each dependent component is in alignment with process RTO
(6) Determine the critical resources (people, vendors, equipment, technology, data/information, funding, and time) required to support the entity's mission

A.5.3.3 RTOs are often used as the basis for the development of recovery strategies and as a determinant as to when to implement the recovery strategies during a disaster situation. Three examples follow:

(1) An RTO in the range of a few minutes to hours might require that the operational process be fully functional in two geographically diverse sites that are fully equipped and staffed. In technology environments, this might require that two facilities either operate in parallel (active/active, e.g., mirroring) or at least duplicate the primary environment (active/passive, e.g., clustering or high availability).
(2) An RTO expressed in hours to days can be sufficiently addressed by transferring the operations and staff to an alternative site, such as a commercial recovery facility or an internally developed and maintained hot, warm, or mobile site.
(3) An RTO expressed in weeks can be sufficiently addressed by a cold site that requires that all necessary equipment, technology, and supplies be re-established at the time of the event.

A.5.3.5 The RPO is the point in time from which data are recovered, "the last good backup offsite at the time of the event." Any activities that occurred after this point are lost and will need to be re-created by some other means. This includes activities occurring in technology applications, work in progress in operational areas, and vital records stored onsite. The gap between the RPO and the time of disruption equals the amount of loss sustained during the incident. It can be deemed as an acceptable amount of data loss.

A.5.3.6 Recovery strategies provide a means to restore operations quickly and effectively following a service disruption. The recovery strategies should consider the impacts of disruption and allowable outage times identified in the impact analysis, as well as cost, security, and integration with larger, entity-level recovery plans.

A.5.4.1 The entity should identify the resources necessary to support the program, plan for and procure needed resources, effectively manage resources that have been acquired to support operational needs, and establish mutual aid/partnership agreements as necessary. Resources should be available within the required time frame as required for emergency operations/response and to meet recovery time objectives. Resources should have the capability to perform their intended function.

Scenarios developed during the risk assessment and business impact analysis should be used to identify resources needed by the program. Resources for emergency operations/response to protect life safety, stabilize the incident, and protect property should be identified. Resources required to execute recovery strategies within the recovery time objective also should be identified. The resource needs assessment should identify resource requirements necessary to achieve performance objectives.

A.5.4.2(1) The resource needs assessment might include "credentialing," which addresses the need for individuals licensed

(e.g., doctors, engineers) in one jurisdiction (state or country) performing their professional duties (as volunteers or under mutual aid compacts) during an incident in a jurisdiction where they are not licensed or do not hold the proper credentials. Credentialing provides minimum professional qualifications, certifications, training, and education requirements that define the standards required for specific emergency response functional assignments.

A.5.4.3 All program equipment should be checked and tested on a regularly scheduled basis to ensure it will function properly when required. This might include vehicles, personal protective equipment (PPE), radio, information technology equipment, and warning and alerting devices and equipment, including sirens, special emergency response equipment, and so forth.

Resources can be prepositioned to expedite deployment. These resources can include the following:

(1) Locations, quantities, accessibility, operability, and maintenance of equipment
(2) Supplies (medical, personal hygiene, consumable, administrative, ice)
(3) Sources of energy (electrical, fuel)
(4) Emergency power
(5) Communications systems
(6) Food and water
(7) Technical information
(8) Clothing
(9) Shelter
(10) Specialized human resources (medical, faith-based, and volunteer organizations; emergency management staff; utility workers; morticians; and private contractors)
(11) Employee and family assistance

A.5.4.5 Mutual aid/assistance or partnership agreements between entities are an effective means to obtain resources and should be developed whenever possible.

Agreements should be in writing, be reviewed by legal counsel, be signed by a responsible official, define liability, and detail funding and cost arrangements.

The term *mutual aid/assistance agreement*, as used here, includes cooperative assistance agreements, intergovernmental compacts, or other terms commonly used for the sharing of resources. Partnerships can include any combination of public, private, and not-for-profit entities or nongovernmental organizations (NGOs).

Mutual aid/assistance and partnership agreements are the means for one entity to provide resources, facilities, services, and other required support to another entity during an incident. Each entity should be party to the agreement with appropriate entities from which they expect to receive or to which they expect to provide assistance during an incident. This would normally include neighboring or nearby entities, as well as relevant private sector and NGOs. States should participate in interstate compacts and look to establish intrastate agreements that encompass all local entities. Mutual aid/assistance agreements with NGOs, such as the International Red Cross/Red Crescent, can be helpful in facilitating the timely delivery of private assistance.

If mutual aid/assistance is needed, agreements should include the following:

(1) Definitions of key terms used in the agreement, including *intellectual property, duration of the agreement*, and *duration of assistance*
(2) Roles and responsibilities of individual parties
(3) Procedures for requesting and providing assistance, including mobilization and demobilization
(4) Procedures, authorities, and rules for payment, reimbursement, and allocation of costs
(5) Notification procedures
(6) Protocols for interoperable communications
(7) Relationships with other agreements among entities
(8) Workers' compensation
(9) Treatment of liability and immunity
(10) Recognition of qualifications and certifications

A.5.5.1 Performance objectives should be established for all elements in the program and should be linked to human performance. Without well-written performance objectives, measurement and evaluation of performance, when the performance is compared to criteria to determine if the performance meets expectations, are impossible. Performance objectives should contain the following three essential parts:

(1) *Performance.* Specific identification of expected behavior that is observable and measurable. If the specific behavior is based on expected knowledge (cognitive process) or attitudes (emotions, feelings), indicator behaviors should be used, because knowledge and attitude performance objectives are not directly observable and, therefore, are not measurable. An indicator behavior is observable and is based on either cognitive or emotional processes.
(2) *Conditions.* Specific identification of exact location, tools, the equipment used, and so forth, that will be part of the observable, measurable behavior.
(3) *Criteria.* Specific criteria that will be used to compare the observed behavior so that it can be determined if the performance objectives have been achieved.

An example of a technique for the development of performance objectives is the "SMART" acronym for checking:

(1) ***S****pecific.* The wording must be precise and unambiguous in describing the objective.
(2) ***M****easurable.* The design and statement of objectives should make it possible to conduct a final accounting as to whether objectives were achieved.
(3) ***A****ction oriented.* The objective must have an action verb that describes the expected accomplishments.
(4) ***R****ealistic.* Objectives must be achievable with the resources that the entity can allocate or make available.
(5) ***T****ime sensitive.* Time frames should be specified (if applicable).

A.5.5.4 Time frames defining short-term and long-term performance objectives should be developed by the entity. Examples of short-term objectives might include "stabilize the incident" and "support entities that are responding to and stabilizing the incident," while long-term objectives might include "prevent environmental damage" and "comply with regulatory requirements."

A.6.1.1 The safety and health of personnel are critical to the successful execution of the program. When every person accepts and performs as if safety and health are their personal responsibility, hazardous exposures will be minimized and the probability of accidents and incidents will be reduced.

Hazard/risk exposure can be eliminated or minimized by removing the hazards or by not performing the hazardous task. However, complete elimination of risk is not always be feasible, and controls should then be instituted.

Hazard control begins with identification of the hazard and the vulnerability of people or assets potentially exposed

and elimination or mitigation according to the hierarchy of controls as follows:

(1) *Elimination or substitution.* Whenever possible, the hazard should be eliminated from the work area (e.g., repairing or removing fallen electrical power lines before allowing other work to proceed in the area). Although desirable, elimination or substitution might not be options for most airborne/chemical hazards created by an incident.
(2) *Engineering controls.* Steps should be taken to reduce or eliminate exposure to a hazard through engineering controls such as the installation of ventilation systems, automatic sprinklers (building), or special protection systems.
(3) *Administrative controls.* Work practices should be implemented that reduce the duration, frequency, and severity of risk exposures. Safety and health controls include training, safety procedures, observations, and enforcement of safe behavior, for example, using well-rested crews and daylight hours to perform higher hazard or unfamiliar tasks, requiring frequent breaks during hot weather, removing nonessential personnel from the area during certain tasks/operations, and decontaminating equipment and personnel after contact with contaminated floodwater or chemicals, and when possible, using water to suppress dust and work upwind in dusty conditions.
(4) *Personal protective equipment (PPE).* If hazard exposures cannot be engineered or administratively controlled, individuals should be shielded or isolated from chemical, physical, and biological hazards through the use of PPE. Careful selection and use of adequate PPE should protect the respiratory system, skin, eyes, face, hands, feet, head, body, and hearing. Examples of PPE are safety glasses and goggles for eyes, gloves for hands, and respirators to protect the lungs. Control of the hazard exposures should not stop with providing PPE.

Incident management systems (IMSs) have trained, designated incident safety officers, but hazard exposure control should be a paramount concern of every person involved.

Recovery operations can be particularly hazardous. Due to the nature of the recovery, normal operations might be disrupted and the hazards uncontrolled. For example, work conditions change drastically after hurricanes and other natural disasters. In the wake of a hurricane, response and recovery workers face additional challenges, such as downed power lines, downed trees, and high volumes of construction debris, while performing an otherwise familiar task or operation. Procedures and training are needed to help ensure safe performance of those engaged in cleanup after an incident.

Corrective actions to eliminate or mitigate hazard exposure should be aggressive and complete, but they also should be carefully considered before implementation so as not to create a new set of hazard exposures.

A.6.1.3 Many entities have written one or more plan documents for their programs. For example, environmental health and safety, security, emergency response, business continuity, and crisis communications plans are written by private sector organizations. Some plans exist at the corporate level (e.g., crisis management) to direct the efforts of senior management. Within the public sector, mitigation, emergency management, continuity of operations, and other plans are written. The committee's intent in 6.1.3 is to provide flexibility for the user to create needed program plans. However, development of all plans should be coordinated, and plans should be sufficiently connected to ensure that they meet the needs of the entity.

A.6.1.4 Distributing plans internally or to key stakeholders could require an entity to exercise safeguards like obtaining confidentiality or nondisclosure agreements. Multi-organizational coordination of the planning process and plans ensures no duplication, improves understanding, increases support, and ensures that all stakeholders have a voice [e.g., the National Incident Management System (NIMS)]. The extent of planning requirements will depend on the program's performance objectives, results of the hazard analysis, and the entity's culture, philosophy, and regulations.

A.6.2.1 Common prevention and deterrence strategies include the following:

(1) Security patrols inside and outside facilities; increased inspections of vehicles entering the facility; background checks of personnel
(2) Access controls, including perimeter fence line and gates, access control systems, camera surveillance, intruder detection systems (motion-sensing cameras, infrared detectors)
(3) Immunizations, isolation, or quarantine
(4) Land use restrictions to prevent development in hazard-prone areas, such as flooding areas or construction of hazardous materials facilities in areas near schools, in population centers, or in areas of identified critical infrastructure
(5) Uninterruptible power supply (UPS) to provide short-term backup power to critical electrical components, including the data center power distribution unit (PDU), desktop computers in time-sensitive operational areas, phone switchboard (PBX), the HVAC system, and safety controls such as elevators and emergency lighting
(6) Gasoline- or diesel-powered generators to provide long-term backup power
(7) Crime prevention through environmental design (CPTED), including site layout, landscape design, and exterior lighting
(8) Personnel management
(9) Background investigations
(10) Cyber security, including firewalls, intrusion detection, virus protection, password management, cryptographic key management, and access to information based on need to know

A.6.2.2 Techniques to consider in a prevention strategy include the following:

(1) Ongoing hazard identification
(2) Threat assessment
(3) Risk assessment
(4) Analysis of impacts
(5) Operational experience, including incident analysis
(6) Information collection and analysis
(7) Intelligence and information sharing
(8) Regulatory requirements

The cost-benefit analysis should not be the overriding factor in establishing a prevention strategy. Other considerations have indirect benefits that are difficult to quantify (e.g., safety, property conservation).

A.6.3.1 Mitigation strategies can include the following:

(1) Use of applicable building construction standards
(2) Hazard avoidance through appropriate land use practices
(3) Relocation, retrofitting, or removal of structures at risk

(4) Removal or elimination of the hazard
(5) Reduction or limitation of the amount or size of the hazard
(6) Segregation of the hazard from that which is to be protected
(7) Modification of the basic characteristics of the hazard
(8) Control of the rate of release of the hazard
(9) Provision of protective systems or equipment for both cyber risks and physical risks
(10) Establishment of hazard warning and communication procedures
(11) Redundancy or diversity of essential personnel, critical systems, equipment, information, operations, or materials
(12) Acceptance/retention/transfer of risk (insurance programs)
(13) Protection of competitive/proprietary information

A.6.3.2 Development of the mitigation strategy should consider the following:

(1) Explanation of hazard and vulnerabilities
(2) Quantification of the risk if unmitigated
(3) Anticipated cost
(4) Anticipated benefit
(5) Cost-benefit analysis
(6) Prioritization of projects based on probability of occurrence and severity of potential impacts
(7) Planned changes to the entity
(8) Project timeline
(9) Resources required
(10) Funding mechanism

A.6.4.1 The crisis communications plan should include a preestablished structure and process for gathering and disseminating emergency or crisis information to both internal and external stakeholders. The communications plan should identify not only key stakeholders but also who on the communications team is responsible for tailoring and communicating appropriate information to each stakeholder group before, during, and after an incident. Formal awareness initiatives should be established in advance of an emergency with the intention of reaching populations that could be impacted by a risk or hazard. A means of collecting inquiries and responding to concerns from the public also should be incorporated into the process to better ensure a two-way dialogue. This can be done through pamphlets, websites, social media, community meetings, newsletters, and other means.

A.6.4.2 The entity should create a basic communications structure that is flexible enough to expand and contract to fit the needs of the situation. Communications activities should be coordinated not only among the various communications functions that have been activated but also with the site team and response organization.

A joint information center (JIC) can be established during incident operations to support the coordination and dissemination of critical emergency as well as public affairs information from all communications operations related to the incident, including federal, state, local, and tribal public information officers (PIOs) as well as private entity or corporate communications staff. The JIC can be physical or virtual.

A.6.4.2(1) Stakeholder liaisons and others tasked with communications responsibilities should coordinate information through a central communications hub to ensure an organized, integrated, and coordinated mechanism for the delivery of understandable, timely, accurate, and consistent information to all parties. Information or tools that can be prepared in advance, such as pre-scripted information bullets or template press releases, can help speed the release of information. Similarly, narrowing the time between when information becomes known and when it is approved for release to the public can be a critical factor in shaping public opinion.

A.6.5.1 The entity should determine warning, notification, and communications needs based on the hazards and potential impacts identified during the risk assessment and the capabilities required to execute response, crisis communications, continuity, and recovery plans, procedures, and public education/emergency information programs.

Warning systems can include fire alarm, emergency voice communication, public address, mass notification, and other systems designed to warn building occupants, people on a campus, or citizens in the community that there is a threat or hazard and to take protective action. Notification systems are used to alert members of response, continuity, and recovery teams as well as external resources (public emergency services), regulators, management, and so forth. Communications needs include two-way radio systems, and wired and wireless voice and data communications, among other systems.

A.6.5.2 Since warning, notification, and communications systems must be immediately available and functional to warn persons potentially at risk, to alert persons to respond, and to enable communications between responders, reliability of systems and equipment is critically important. Redundancy in systems and equipment provides assurance that essential warnings, notifications, and communications can be made. Systems and equipment must be interoperable to ensure that responders are able to communicate effectively during an incident. Also see 3.3.16, Interoperability.

A.6.5.3 The entity should identify the circumstances requiring emergency communication and the stakeholders that would need to be warned. Protocols defining the circumstances and procedures for implementing communications should be established in advance, tested, and maintained. Scripting templates for likely message content and identification of the best communication mechanisms in advance reduce the time necessary to communicate and enhance the effectiveness of messages.

Stakeholders will vary depending on the entity. Typical stakeholders for many entities include the media, government, customers, employees and their families, vendors, suppliers, community, visitors, and investors.

A.6.6.3 The term *property conservation* means minimizing property damage. Actions can be taken in advance of a forecast event such as a hurricane (e.g., boarding up windows) and during and following the incident (e.g., using water vacuums to remove water that has entered a building). Also see Section 6.8 for details on protective actions for life safety, incident stabilization, and other guidance.

A.6.7.1 An incident management system (IMS) should be used to manage an incident. The system used varies among entities and among jurisdictions within entities. In minor incidents, IMS functions might be handled by one person: the incident commander or equivalent designee.

An example of an effective public sector IMS would be the National Incident Management System (NIMS) used in the United States or its equivalent in other countries. In the Incident Command System (ICS) portion of NIMS, incident management is structured to facilitate activities in five

major functional areas: command, operations, planning, logistics, and finance and administration. For private sector entities, it is acceptable for the IMS to be organized in whatever way best fits the organizational structure, as long as it is clear how the entity will coordinate its operations with public sector resources arriving at the incident scene.

Figure A.6.7.1 illustrates private sector functions under the ICS. All positions would not be filled for all incidents. In addition, the number of positions reporting to any supervisor should not exceed the "manageable span of control" within the ICS. The intent of Figure A.6.7.1 is to show how positions for different scenarios would be organized under the ICS. In addition, the figure illustrates that the organization can grow as the scale of the incident and the resources needed to manage the incident expand.

It is common to find that environmental, health, and safety professionals within private industry fill positions, including "Safety Officer," as well as positions within "Operations." Public affairs and media relations staff would likely fill the "Public Information" position. Facilities management, engineering, and operations typically staff "Operations" as well. Personnel trained to provide first aid and administer CPR would staff the "Medical" function. Security would fill the "Security" function. Finance staff, including insurance and risk management staff, would likely fill positions under "Finance & Administration." Supply chain personnel would have the ideal expertise to staff the "Logistics" section. "Planning" could be filled by staff with planning expertise.

It is not the intent that Figure A.6.7.1 suggest that every entity must include all of the functions in its response, continuity, or recovery organization. Each entity is unique and should structure its teams and IMS to best fit its needs. Many of the positions can be combined and filled by a single person.

A.6.7.1.1 An emergency operations center (EOC) is the location where the coordination and support of incident management activities take place. The EOC should have adequate workspace, communications, and backup utilities and should meet basic human needs. For complex incidents, EOCs might need to be staffed by personnel representing multiple jurisdictions, sectors, functional disciplines, and resources. The physical size, staffing, and equipping of an EOC will depend on the size of the entity, the resources available and the anticipated incident management support required. EOCs can be permanent facilities or can be established to meet temporary, short-term needs.

A.6.7.1.1.1 The requirement to establish primary and alternate EOCs is intended to ensure that the capacity exists to support operations from a centralized facility or virtual capability. The primary and alternate EOCs should be located so both are not impacted by the same event and at least one EOC will be operational. Alternate EOCs can include site or department EOCs,

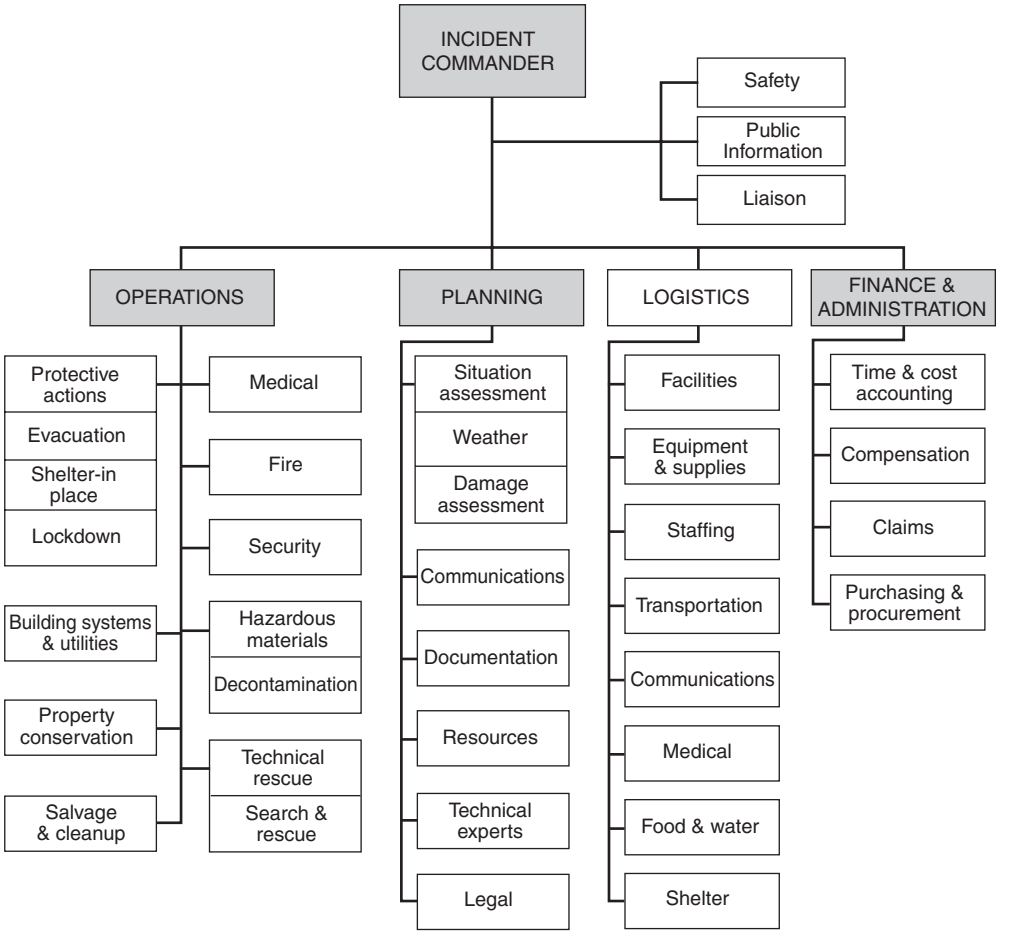

FIGURE A.6.7.1 Diagram of Incident Command System.

which focus on internal department or agency incident management and are linked to and, in most cases, physically represented in a higher level EOC.

On-scene incident command posts (ICPs), which are located at or in the immediate vicinity of an incident site, should be linked to EOCs to ensure communications and effective and efficient incident management. An ICP is focused primarily on the tactical on-scene response but can be used to function as an EOC-like function in smaller-scale incidents or during the initial phase of the response to larger, more complex events.

A.6.7.1.1.2 Virtual EOCs that link team members located in separate locations via conference call, web meeting, and or other electronic meeting tool meet the requirements of this section.

A.6.7.6 In larger scale incidents a formal incident action plan *(see 3.3.14)* is developed and approved by the incident commander. In small-scale incidents, objectives are established by the incident commander and verbally communicated. Operations are then managed by command to achieve the objectives.

A.6.8.1 Emergency action plans should be based on the hazard scenarios developed during the risk assessment to accomplish established program goals. Plans should define responsibilities for warning persons at risk or potentially at risk, alerting responders, and notifying those who must be made aware of the incident. Plans should also define specific functional roles and responsibilities for protection of life safety, incident stabilization to the extent the entity is required or chooses, and property conservation. Documentation such as checklists, emergency action guides, and standard operating procedures (SOPs) should identify emergency assignments, responsibilities, and emergency duty locations. The SOPs and notification procedures should be integrated.

A.6.8.2 Protective actions for life safety include evacuation, shelter-in-place, and lockdown and depend upon the nature and location of the threat or hazard. Action should include defining the protocols and procedures for warning people at risk or potentially at risk and the actions that should be taken to protect their safety. Special attention might be needed to address the needs of people with access and functional needs (for guidance, see http://www.fema.gov/plan/prepare/specialplans.shtm). Emergency plans should address those who might have additional needs before, during, or after an incident in one or more of the following functional areas:

(1) Visually impaired
(2) Hearing impaired
(3) Mobility impaired
(4) Single working parent
(5) Language competency
(6) People without vehicles
(7) People with special dietary needs
(8) People with medical conditions
(9) People with intellectual disabilities
(10) People with dementia

Persons with access and functional needs can include those who reside in institutionalized settings, the elderly, children, and those from diverse cultures who have limited proficiency in the local language.

A.6.8.3 Incident stabilization is the action taken to prevent an incident from growing and to minimize the potential impact on life, property, operations, and the environment. Incident stabilization can include many different functions depending upon the nature and location of the threat or hazard, the magnitude of the incident, the actual and potential impact of the incident, applicable regulations that could dictate minimum response capabilities, the entity's program goals, and the resources available to the entity for incident response. Examples of incident stabilization activities are listed under "Operations" in Figure A.6.7.1.

A.6.9.1 Examples of recovery strategies options/alternatives include the following:

(1) Recovery strategies for loss of operational site
  (a) Transfer of workload to a surviving site
  (b) Transfer of staff and workload to a surviving site
  (c) Contracted alternate site with a vendor
  (d) Reciprocal agreement with a like organization
  (e) Dedicated alternate site
  (f) Mobile facility
  (g) Remote access/work from home
  (h) Resources acquired at the time of disruption
  (i) Mutual aid agreement
(2) Technical recovery alternatives
  (a) Commercial vendor (hot site)
  (b) Resources acquired at time of disruption
  (c) Quick-ship equipment
  (d) Dual data center with active/active
  (e) Dual data center with active/passive
  (f) Outsourcing with a service level agreement (cloud computing)
  (g) Stockpiled equipment
  (h) Manual workarounds or alternate systems
(3) Backup strategies for records
  (a) Electronic storage
  (b) Synchronous replication
  (c) Asynchronous replication
  (d) Electronic journaling
  (e) Standby database
  (f) Electronic vaulting
  (g) Tape backup
  (h) Full backup
  (i) Differential backup
  (j) Incremental backup
  (k) Salvage
  (l) Hard-copy storage
  (m) Film
  (n) Fiche
  (o) Photocopy
  (p) Scan
  (q) Salvage
(4) Third-party (vendor provided/extended enterprise) recovery strategy options
  (a) Multiple sourcing
  (b) Alternate sourcing
  (c) Service level agreement
  (d) In-source (do not outsource)

A.6.9.2 Plans for business continuity, continuity of government, and continuity of operations are generally similar in intent and less similar in content. Continuity plans have various names in both the public and private sectors, including business continuity plans, business resumption plans, and disaster recovery plans.

A.6.9.3 Recovery planning for the public and private sectors should provide for continuity of operations to return the entity, infrastructure, and individuals back to an acceptable level. This includes implementation of mitigation measures to facilitate short-term and long-term recovery.

The recovery plan should include the following:

(1) Facilities and equipment
(2) Critical infrastructure
(3) Telecommunications and cyber protection systems
(4) Distribution systems for essential goods
(5) Transportation systems, networks, and infrastructure
(6) Human resources
(7) Psychosocial services
(8) Health services

Short-term goals and performance objectives should be established and include the following:

(1) Vital personnel, systems, operations, records, and equipment
(2) Priorities for restoration and mitigation
(3) Acceptable downtime before restoration to a minimal level
(4) Minimal functions, services, and resources needed to provide for the restoration of facilities, programs, and infrastructure

Long-term goals and objectives should be based on the entity's strategic plan and include the following:

(1) Management and coordination of activities
(2) Funding and fiscal management
(3) Management of volunteers (both affiliated and spontaneous), contractual, and entity resources
(4) Opportunities for mitigation

A.6.10.1 Employee assistance and support might also be called human continuity, human impact, workforce continuity, human aspects of continuity, and so forth. Employee assistance and support includes the entity's employees and their families or significant others affected by the incident.

A.6.10.1(1) Communications procedures are the methods that the entity and its employees will use to inform employees of the program before an event occurs and to inform employees that the program is activated and available following the occurrence of an event. Employees should have a means of notifying the entity of the need for assistance through the communications system established. Similarly, the entity should develop a means of communicating with employees when operations are interrupted at a site and the staff has been sent home and how communications will be made to employees when the interruption has occurred outside normal business hours.

Various communications methodologies can be established, including the following:

(1) Automated notification systems or call centers
(2) Email, web site, or voicemail broadcasts
(3) Call lists
(4) Social media

There are situations in which customers, vendors, and other parties might be located at the entity's facility, and the program should include the ability to provide assistance for them as well.

A.6.10.1(2) The entity should develop policies and procedures to store, retrieve, and control access to personal information when needed in an emergency situation, including systems to facilitate reunification of family members.

A.6.10.3 Family preparedness is an ongoing process to educate and train individuals to plan for and take steps during an emergency. *(See Annex I for more information.)*

A.7.1 Competency-based education and training programs focus on the specific knowledge elements, skills, and/or abilities that are objective, that is, measurable or demonstrable, on the job. Education is usually focused on unknown risk exposures. Training is instruction that imparts and/or maintains the skills necessary for individuals and teams to perform their assigned system responsibilities and is usually focused on known risk exposures. The learning objectives of training should be competency-based and the criteria related to the relevant competencies. Competency is based on demonstrated performance to achieve designated goals.

All personnel designated to perform specific task(s) should demonstrate competence to perform the tasks and meet the expected criteria identified in the performance objectives. Competency is defined as demonstrated performance to achieve designated objectives. Competencies are mastered through a multitude of ways: life experience, education, apprenticeship, on-the-job experience, self-help programs, and training and development programs.

A.7.7 Information that should be included in public outreach and awareness efforts include regulatory disclosures such as those required by the SARA Title III [(Emergency Planning and Community Right-to-Know Act (EPCRA)], the Community Awareness Emergency Response (CAER), and the Clery Act. Other nonregulatory examples of awareness that might be included in public education include severe weather outreach and alerts, shelter-in-place, and evacuation.

A.8.2 An exercise is an instrument used to train for, assess, practice, and improve performance in prevention, protection, response, and recovery capabilities in a risk-managed environment. Exercises can be used for testing and validating policies, plans, procedures, training, equipment, and interagency agreements; clarifying and training personnel in roles and responsibilities; improving interagency coordination and communications; identifying gaps in resources; improving individual performance; and identifying opportunities for improvement.

A test/testing is a unique and particular type of exercise that incorporates an expectation of a pass or fail element within the goal or objectives established. An exercise is also an excellent way to demonstrate community resolve to prepare for disastrous events.

Exercise and testing might be synonymous in certain areas; however, there are times they are not synonymous. As an example, testing of a data center recovery plan will need to have an indication of success or failure.

An exercise is the principal means of testing a program's ability to implement its response procedures. It allows the entity and other agencies and organizations to practice procedures and interact in a controlled setting. Participants identify and make recommendations to improve the overall program. The fundamental purpose is to improve implementation procedures. In support of that goal, an exercise should be used to achieve the following:

(1) Reveal planning weaknesses and strengths in plans, standard operating procedures (SOPs), and standard operating guidelines (SOGs) and to test and validate recently changed procedures
(2) Improve the coordination among various response organizations, elected officials, and community support organizations
(3) Validate the training for response (e.g., incident command, hazard recognition, evacuation, decontamination) and recovery

(4) Increase the entity's general awareness of the hazards
(5) Identify additional resources, equipment, or personnel needed to prepare for, respond to, and recover from an incident
(6) Include activities performed for the purpose of training and conditioning team members and personnel in appropriate actions
(7) Practice improvisation of activities in a safe environment (Improvisation might be necessary in actual disruptive events because predictions of disruptions are usually flawed.)

A.8.3 An exercise can involve invoking response and operational continuity procedures, but it is more likely to involve the simulation of a response or operational continuity incident, or both, announced or unannounced, in which participants role-play in order to assess, prior to a real invocation, issues that arise. Exercises should include, but not be limited to, orientation seminars, drills, tabletop exercises, functional exercises, and full-scale exercises.

Orientation Seminar. The orientation seminar is an overview or introduction. Its purpose is to familiarize participants with roles, plans, procedures, or equipment. It can also be used to resolve questions of coordination and assignment of responsibilities.

Drill. A drill is a coordinated, supervised exercise activity normally used to test a single specific operation or function. With a drill, there is no attempt to coordinate organizations or fully activate the EOC. Its role in an exercise program is to practice and perfect one small part of the response plan and help prepare for more extensive exercises, in which several functions will be coordinated and tested. The effectiveness of a drill is its focus on a single, relatively limited portion of the overall emergency management system. It makes possible a tight focus on a potential problem area.

Tabletop exercise. A tabletop exercise is a facilitated analysis of an emergency situation in an informal, relatively stress-free environment. It is designed to elicit constructive discussion as participants examine and resolve problems based on existing operational plans and identify where those plans need to be refined. The success of the exercise is largely determined by group participation in the identification of problem areas.

Functional exercise. A functional exercise is a fully simulated interactive exercise that tests the capability of an organization to respond to a simulated event. The exercise tests multiple functions of the organization's operational plan. It is a coordinated response to a situation in a time-pressured, realistic simulation

Full-scale exercise. A full-scale exercise simulates a real event as closely as possible. It is designed to evaluate the operational capability of emergency management systems in a highly stressful environment that simulates actual response conditions. To accomplish this realism, it can include the mobilization and actual movement of emergency personnel, equipment, and resources. Ideally, the full-scale exercise should test and evaluate most functions of the emergency management plan or operational plan.

A.8.5 Where no frequency is established, a minimum annual frequency of exercises and testing is recommended.

A.9.1 Performance improvement is based on the following two distinct but interrelated functions:

(1) Measurement, sometimes called "assessment" or "observation," is the function in which the personnel accurately determine exactly what organizational performance has occurred.
(2) Evaluation is the function in which the observed performance is compared with criteria, sometimes called "standards" or "competencies," to determine if the actual organizational performance meets expectations.

A.9.1.1 Improvements to the program can be made in many ways, such as following an exercise or test of the program, following an actual event that required one or more of the program elements to be activated or through a scheduled periodic review of the program.

A.9.1.2 The program should be reviewed on a regularly scheduled basis, after major changes to or within the entity (e.g., new facility, process, product, policy), after scheduled exercises (testing of the program), or following an incident that required a part of the plan associated with the program to be utilized. Consideration should be given to the use of external evaluators.

A.9.1.3(5) Many emergency management entities and programs in both the public and private sectors are supported in part by grants from government entities or private sources. A change in grant assistance could materially impact the entity's program, necessitating an evaluation of the program.

A.9.2 The corrective action process should follow a review of the program or follow an actual event or exercise to identify program deficiencies and take necessary corrective actions to address such deficiencies. The corrective action program should include techniques to manage the capabilities improvement process. The corrective action program should begin following the "after-action" discussion/critique of the incident or exercise or should take place during the incident if a lengthy or extended event is being managed. During the evaluation process, deficiencies that require improvement should be identified. Process deficiencies should be identified within one or more of the program elements found in this standard.

Corrective actions should be identified by the following:

(1) Changes to regulations, policy, plans, or procedures
(2) Additions or modifications to facilities, systems, or equipment
(3) Results of exercises and testing
(4) After-action reviews of actual incidents

A task group should be assigned to each identified area of noted deficiency to develop the necessary actions for improvement, and a time schedule for development of the necessary corrective action should be established.

The task group should take the following actions:

(1) Develop options for appropriate corrective action
(2) Make recommendations for a preferred option
(3) Develop an implementation plan, including training if required
(4) Ensure that during the next exercise the corrective actions are evaluated to determine if the corrective actions have been successful

The entity should establish a process to identify the root cause of the deficiencies noted. The entity also should establish a change management process (i.e., a process involving all sectors of an entity's operations in which changes to the operations are reflected in the plan and, vice versa, changes in the plan are reflected in the entity's operations).

A.9.2.1 The corrective action process should include the following:

(1) Development of a problem statement that states the problem and identifies its impact

(2) Review of corrective action issues from previous evaluations and identification of possible solutions to the problem
(3) Selection of a corrective action strategy and prioritization of the actions to be taken, as well as an associated schedule for completion
(4) Provision of authority and resources to the individual assigned responsibility and accountability for implementation, so that the designated change can be accomplished
(5) Identification of the resources required to implement the strategy
(6) Check of the progress of completing the corrective action
(7) Forwarding of problems that need to be resolved by higher authorities to the level of authority that can resolve the problem
(8) Once the problem is solved, testing of the solution through exercising

A.9.2.2 The appropriate corrective actions might not be taken due to budgetary or other constraints or might be deferred as a part of the long-range capital project. However, temporary actions could be adopted until the desired option is funded and implemented.

Annex B Program Development Resources

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

B.1 Using the Internet. The Internet is an invaluable tool that has become a necessity for the program developer, maintainer, and assessor. The content of the *NFPA 1600* annexes has changed based on the context of the widespread competence and use of the Internet for research.

The Internet can be a great tool for finding information, but like any tool it must be used wisely and correctly. Because virtually anyone can publish information on the Internet, the information must be used with care. The best advice is to attempt to find the same information from two different web sites (not two different pages on the same web site). It is important to check the date the information was posted. Business continuity and emergency management information has changed drastically in the years since 9/11 and Hurricane Katrina. Though some information does not change, the prudent user of the Internet should check the date to avoid using out-of-date information.

A search engine is an Internet tool that locates web pages and sorts them according to specified key words. As with any tool, it is a good idea to read the directions for each search engine to ensure the best use. The three most common search engines are Google (www.google.com), Yahoo! Search (www.yahoo.com), and Ask.com (www.ask.com). Some search engines are better than others. Often there is a tendency to use Google exclusively. Google is an excellent tool for researching the Internet, but it is not the only search engine.

Search directories are not search engines, and the similarity of the search fields can be misleading. A search directory is an index handpicked by a human. Search engines search a database of the full text of web pages automatically harvested from the web pages available. A search engine uses a somewhat outdated copy of the real web page, not the actual pages. However, search engines produce valuable information and should not be ignored.

The following list is provided as a starting resource for building programs:

(1) Digital Librarian (www.digital-librarian.com)
(2) Google (www.directory.google.com)
(3) Infomine (http://infomine.ucr.edu)
(4) Internet Public Library (www.ipl.org)
(5) Open Directory (www.dmoz.org)
(6) Yahoo search (http://diryahoo.com)
(7) The WWW virtual library (http://vlib.org)
(8) BUBL Countries Catalogue of Internet resources by country (http://bubl.ac.uk/link/world/index.html)
(9) InfoPlease Countries of the World (www.infoplease.com/countries.html) (See also under InfoPlease General Information.) This source, as well as similar sources, such as the BBC Country Reports, uses *The CIA World Factbook* as a source for its information.
(10) *The CIA World Factbook*, a handbook of economic, political, and geographic intelligence (https://www.cia.gov/library/publications/the-world-factbook/index.html) (Excellent source of country information, including background information on countries not limited to geography, demographics, disaster, economy, political, transportation, and military information. The online version is updated continuously, while the print version is published every year.)

B.2 Web Sites and Documents of Interest. Web sites are included here as examples of program development resources available on the Internet. Inclusion in this annex does not constitute an endorsement. The user is cautioned that web site addresses change, and a search engine might be needed to locate the correct URL.

American Waterworks Association, "Utilities Helping Utilities: An Action Plan for Mutual Aid and Assistance Networks for Water and Wastewater Utilities": http://www.awwa.org/files/Utilities_Helping_Utilities.pdf

Congressional Research Service, "Emergency Communications: The Emergency Alert System (EAS) and All-Hazard Warnings": http://www.fas.org/irp/crs/RL32527.pdf

Crisis Communications Plan Template (Canadian Centre for Emergency Preparedness): http://www.ccep.ca/templates/ccplan.rtf

Disaster Research Center, University of Delaware: http://www.udel.edu/DRC/Emergency Management and Civil Protection Act and Regulation (Ontario): http://www.search.e-laws.gov.on.ca/en/isysquery/78ea6acf-3e22-41e7-8d1b-66282cd4213f/3/doc/?search=browseStatutes&context=#hit1

Emergency Management Assessment Program (EMAP): http://www.emaponline.org/

Emergency Management Competencies: http://training.fema.gov/EMIWeb/edu/EMCompetencies.asp

Emergency Management Institute (FEMA) IS-120 Introduction to Exercises: http://emilms.fema.gov/IS120A/index.htm

Emergency Management Institute homepage (FEMA): http://training.fema.gov/

Emergency Manager Toolkit (FEMA): http://training.fema.gov/EMIWeb/IS/is1Toolkit/unit2.htm

Emergency Program Manager: Knowledge, Skills, and Abilities: http://training.fema.gov/EMIWeb/edu/EmergProgMgr.doc

Enterprise Preparedness (International Center for Enterprise Preparedness): http://www.nyu.edu/intercep

EPA Risk Assessment Portal: http://www.epa.gov/risk/

FEMA: Developing Effective Standard Operating Procedures for Fire and EMS Departments: http://www.usfa.dhs.gov/downloads/pdf/publications/fa-197-508.pdf

Hazard Mitigation Planning (FEMA): http://www.fema.gov/plan/mitplanning/index.shtm

Homeland Exercise and Security Evaluation Program: https://hseep.dhs.gov/pages/1001_HSEEP7.aspx

ICS All-Hazard Core Competencies (FEMA): http://www.fema.gov/library/viewRecord.do?id=2948

http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf

International Standards Organization (ISO): http://www.iso.org

Mitigation Best Practices Search (FEMA): http://www.fema.gov/mitigationbp/index.jsp

National Incident Management System (NIMS) Resource Center: http://www.fema.gov/emergency/nims/

Natural Hazards Center, University of Colorado: http://www.colorado.edu/hazards/

New York State Department of Health (EMS) EMS Mutual Aid Planning Guidelines: http://www.health.state.ny.us/nysdoh/ems/policy/89-02.htm

Ready Business, Federal Emergency Management Agency (FEMA): http://www.ready.gov/business

Records Managers (National Archives): http://www.archives.gov/records-mgmt/

Risk Management Standard (Australia): http://www.riskmanagement.com.au/

Disaster Recovery Planning, University of Toronto: http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm

Washington Military Department, Emergency Management Division, Mutual Aid and Interlocal Agreement Handbook: http://emd.wa.gov/plans/documents/MutualAidHandbook.pdf

Annex C Self-Assessment for Conformity with *NFPA 1600*, 2013 Edition

This annex is not a part of the requirements of this NFPA document but is included for informational purposes only.

C.1 Table C.1 shows a self-assessment tool that is intended to assist entities in determining conformity with the requirements of *NFPA 1600*. The table includes a list of hazards from Annex A and also repeats text from the body of the standard where needed to make the self-assessment tool more user friendly. Users of this self-assessment tool can indicate conformity, partial conformity, or nonconformity as well as evidence of conformity, corrective action, task assignment, a schedule for action, or other information in the Comments column.

Table C.1 Self-Assessment Tool for Conformity with the 2013 Edition of *NFPA 1600*.

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
Chapter 4 Program Management **4.1* Leadership and Commitment.** **4.1.1** The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents.				
4.1.2 The leadership commitment shall include the following: (1) Support the development, implementation, and maintenance of the program				
(2) Provide necessary resources to support the program				
(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness				
(4) Support corrective action to address program deficiencies				
4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.				
4.2* Program Coordinator. The program coordinator shall be appointed by the entity's leadership and authorized to develop, implement, administer, evaluate, and maintain the program.				
4.3* Program Committee. **4.3.1*** A program committee shall be established by the entity in accordance with its policy.				
4.3.2 The program committee shall provide input, and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
4.3.3* The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.				
4.4 Program Administration. **4.4.1** The entity shall have a documented program that includes the following: (1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority				
(2) Program scope, goals, performance objectives, and metrics for program evaluation				
(3) Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5				
(4) Program budget and schedule, including milestones				
(5) Program plans and procedures that include the following: (a) Anticipated cost				
(b) Priority				
(c) Resources required				
(6) Records management practices as required by Section 4.7				
(7) Change management process				
4.4.2 The program shall include the requirements specified in Chapters 4 through 9, the scope of which shall be determined through an "all-hazards" approach and the risk assessment.				
4.4.3* Program requirements shall be applicable to prevention, mitigation, preparedness, response, continuity, and recovery.				
4.5 Laws and Authorities. **4.5.1** The program shall comply with applicable legislation, policies, regulatory requirements, and directives.				
4.5.2 The entity shall establish and maintain a procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives.				
4.5.3* The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.				
4.6 Finance and Administration. **4.6.1** The entity shall develop finance and administrative procedures to support the program before, during, and after an incident.				
4.6.2* There shall be a responsive finance and administrative framework that does the following: (1) Complies with the entity's program requirements				
(2) Is uniquely linked to response, continuity, and recovery operations				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
(3) Provides for maximum flexibility to expeditiously request, receive, manage, and apply funds in a nonemergency environment and in emergency situations to ensure the timely delivery of assistance				
4.6.3 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles, governance requirements, and fiscal policy.				
4.6.4 Finance and administrative procedures shall include the following: (1) Responsibilities for program finance authority, including reporting relationships to the program coordinator				
(2)* Program procurement procedures				
(3) Payroll				
(4)* Accounting systems to track and document costs				
(5) Management of funding from external sources				
(6) Crisis management procedures that coordinate authorization levels and appropriate control measures				
(7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery				
(8) Identifying and accessing alternative funding sources				
(9) Managing budgeted and specially appropriated funds				
4.7* Records Management. **4.7.1** The entity shall develop, implement, and manage a records management program to ensure that records are available to the entity following an incident.				
4.7.2 The program shall include the following: (1) Identification of records (hard copy or electronic) vital to continue the operations of the entity				
(2) Backup of records on a frequency necessary to meet program goals and objectives				
(3) Validation of the integrity of records backup				
(4) Implementation of procedures to store, retrieve, and recover records onsite or offsite				
(5) Protection of records				
(6) Implementation of a record review process				
(7) Procedures coordinating records access				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
Chapter 5 Planning **5.1 Planning and Design Process.** **5.1.1*** The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program.				
5.1.2 Strategic planning shall define the entity's vision, mission, and goals of the program.				
5.1.3 A risk assessment and business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies.				
5.1.4 A risk assessment, a BIA, and resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans.				
5.1.5 Crisis management planning shall address issues that threaten the strategic, reputational, and intangible elements of the entity.				
5.1.6 The entity shall include key stakeholders in the planning process.				
5.2* Risk Assessment. **5.2.1*** The entity shall conduct a risk assessment to develop required strategies and plans.				
5.2.2 The entity shall identify hazards and monitor those hazards and the likelihood of occurrence.				
5.2.2.1* Hazards to be evaluated shall include the following: (1) Natural hazards (geological, meteorologic, and biological) Geologic hazards/risk exposures				
– Earthquake				
– Tsunami				
– Volcano				
– Landslide, mudslide, subsidence				
Meteorologic hazards/risk exposures – Flood, flash flood, seiche, tidal surge				
– Water control structure/dam/levee failure				
– Drought				
– Snow, ice, hail, sleet, avalanche, arctic freeze				
– Windstorm, tropical cyclone, hurricane, tornado, water spout, dust/sand storm				
– Extreme temperatures (heat, cold)				
– Wildland fire				
– Lightning strikes				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
– Famine				
– Geomagnetic storm				
Biological hazards/risk exposures – Food-borne illnesses				
– Pandemic disease (avian flu, H1N1, etc.)				
– Infectious/communicable disease [plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), BSE (Mad Cow Disease)]				
(2) Human-caused events (accidental and intentional) Accidental – Hazardous material spill or release (explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, radiological, corrosive)				
– Nuclear power plant incident, radiological incident				
– Explosion/fire				
– Transportation accident				
– Building/structure collapse				
– Entrapment and or rescue–machinery, confined space, high angle, water				
– Fuel/resource shortage				
– Mechanical breakdown				
– Transportation incidents (motor vehicle, railroad, watercraft, aircraft, pipeline)				
– Untimely death of employee				
Intentional – Strike or labor dispute				
– Criminal activity (vandalism, sabotage, arson, robbery, theft, fraud, embezzlement, data theft, malfeasance)				
– Physical or information security breach				
– Lost person, child abduction, kidnapping, extortion, hostage incident, workplace/school/university violence, homicide				
– Product defect or contamination				
– Disinformation				
– Harassment				
– Discrimination				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
– Demonstrations, civil disturbance, public unrest, mass hysteria, riot				
– Bomb threat, suspicious package				
– Terrorism (explosive, chemical, biological, radiological, nuclear, cyber, electromagnetic pulse)				
– Insurrection				
– Enemy attack, war				
– Arson				
(3) Technology-caused events (accidental and intentional) – Computer systems (outages, hardware failure, data corruption, deletion, or theft, loss of network connectivity (internet or intranet), loss of electronic data interchange or ecommerce, loss of domain name server (DNS), virus, worm, Trojan horse, power surge, lightning, host site interdependencies, direct physical loss, water damage, cyber terrorism, vulnerability exploitation, botnets, hacking, phishing, spyware, malware, computer fraud, loss of encryption, denial of service, improper system use by employee, telecommunications interruption or failure, internet service provider, electricity brownout or blackout)				
– Computer software or application interruption, disruption or failure (internal/external)				
– Loss, corruption, or theft of electronic information				
– Utility interruption or failure (telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewage system, other critical infrastructure)				
Other hazards/risk exposures – Supply chain interruption (loss of shipping or transportation, vendor failure (single- or sole-source provider)				
5.2.2.2 The vulnerability of people, property, operations, the environment, and the entity shall be identified, evaluated, and monitored.				
5.2.3 The entity shall conduct an analysis of the impacts of the hazards identified in 5.2.2 on the following: (1) Health and safety of persons in the affected area				
(2) Health and safety of personnel responding to the incident				
(3)* Continuity of operations				
(4)* Property, facilities, assets, and critical infrastructure				
(5) Delivery of the entity's services				
(6) Supply chain				
(7) Environment				
(8)* Economic and financial condition				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
(9) Regulatory and contractual obligations				
(10) Reputation of or confidence in the entity				
5.2.4* The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts.				
5.2.5 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies.				
5.3* Business Impact Analysis. **5.3.1** The entity shall conduct a business impact analysis (BIA).				
5.3.2 The BIA shall evaluate the potential impacts resulting from interruption or disruption of individual functions, processes, and applications.				
5.3.3* The BIA shall identify those functions, processes, infrastructure, systems, and applications that are critical to the entity and the point in time (recovery time objective) when the impact of the interruption or disruption becomes unacceptable to the entity.				
5.3.4 The BIA shall identify dependencies and interdependencies across functions, processes, and applications, to determine the potential for compounding impacts in the event of an interruption or disruption.				
5.3.5* The BIA shall evaluate the potential loss of information and the point in time (recovery point objective) that defines the potential gap between the last backup of information and the time of the interruption or disruption.				
5.3.6* The BIA developed in Section 5.3 shall be used in the development of recovery strategies and plans to support the program.				
5.3.7 The analysis of impacts required by 5.2.3 and the BIA required by Section 5.3 shall be conducted jointly or separately.				
5.4 Resource Needs Assessment. **5.4.1*** The entity shall conduct a resource needs assessment based on the hazards identified in Section 5.2 and the business impact analysis in Section 5.3.				
5.4.2 The resource needs assessment shall include the following: (1)* Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed				
(2) Quantity, response time, capability, limitations, cost, and liabilities				
5.4.3* The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, and materials procured or donated to support the program.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
5.4.4 Facilities capable of supporting response, continuity, and recovery operations shall be identified.				
5.4.5* The need for mutual aid/assistance or partnership agreements shall be determined.				
5.4.5.1* If needed, agreements shall be established and documented.				
5.5 Performance Objectives. **5.5.1*** The entity shall establish performance objectives for the program in accordance with the requirements in Chapter 4 and the elements in Chapters 5 through 9.				
5.5.2 The performance objectives shall address the results of the hazard identification, risk assessment, and business impact analysis.				
5.5.3 Performance objectives shall be developed by the entity to address both short-term and long-term needs.				
5.5.4* The entity shall define the terms *short term* and *long term*.				
Chapter 6 Implementation **6.1 Common Plan Requirements.** **6.1.1*** Plans shall address the health and safety of personnel.				
6.1.2 Plans shall identify and document the following: (1) Assumptions made during the planning process				
(2) Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions				
(3) Lines of authority				
(4) The process for delegation of authority				
(5) Lines of succession for the entity				
(6) Liaisons to external entities				
(7) Logistics support and resource requirements				
6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.				
6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.				
6.2 Prevention. **6.2.1*** The entity shall develop a strategy to prevent an incident that threatens life, property, and the environment.				
6.2.2* The prevention strategy shall be based on the information obtained from Section 5.2 and shall be kept current using the techniques of information collection and intelligence.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.2.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, an analysis of impacts, program constraints, operational experience, and cost benefit analysis.				
6.2.4 The entity shall have a process to monitor the identified hazards and adjust the level of preventive measures to be commensurate with the risk.				
6.3 Mitigation. **6.3.1*** The entity shall develop and implement a mitigation strategy that includes measures to be taken to limit or control the consequences, extent, or severity of an incident that cannot be prevented.				
6.3.2* The mitigation strategy shall be based on the results of hazard identification and risk assessment, an analysis of impacts, program constraints, operational experience, and cost benefit analysis.				
6.3.3 The mitigation strategy shall include interim and long-term actions to reduce vulnerabilities.				
6.4 Crisis Communications and Public Information.				
6.4.1* The entity shall develop a plan and procedures to disseminate information to and respond to requests for information from the following audiences before, during, and after an incident: (1) Internal audiences, including employees				
(2) External audiences, including the media, functional needs population, and other stakeholders				
6.4.2* The entity shall establish and maintain a crisis communications or public information capability that includes the following: (1)* Central contact facility or communications hub				
(2) Physical or virtual information center				
(3) System for gathering, monitoring, and disseminating information				
(4) Procedures for developing and delivering coordinated messages				
(5) Pre-scripted information bulletins or templates				
(6) Protocol to clear information for release				
6.5 Warning, Notifications, and Communications.				
6.5.1* The entity shall determine warning, notification, and communications needs.				
6.5.2* Warning, notification, and communications systems shall be reliable, redundant, and interoperable.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.5.3* The entity shall develop and test warning, notification, and communications protocols and procedures to alert stakeholders potentially at risk from an actual or impending incident.				
6.5.4 Procedures shall include issuing warnings through authorized agencies if required by law.				
6.6 Operational Procedures. **6.6.1** The entity shall develop, coordinate, and implement operational procedures to support the program.				
6.6.2 Procedures shall be established and implemented for response to and recovery from the impacts of hazards identified in 5.2.2.				
6.6.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.				
6.6.4 Procedures shall include the following: (1) Control of access to the area affected by the incident				
(2) Identification of personnel engaged in activities at the incident				
(3) Accounting for personnel engaged in incident activities				
(4) Mobilization and demobilization of resources				
6.6.5 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.				
6.7 Incident Management.				
6.7.1* The entity shall develop an incident management system to direct, control, and coordinate response, continuity, and recovery operations.				
6.7.1.1* Emergency Operations Centers (EOCs).				
6.7.1.1.1* The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations.				
6.7.1.1.2* The EOCs shall be permitted to be physical or virtual.				
6.7.1.1.3 On activation of an emergency operations center (EOC), communications and coordination shall be established between incident command and the EOC.				
6.7.2 The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.				
6.7.3 The entity shall establish procedures and policies for coordinating mitigation, preparedness, response, continuity, and recovery activities.				
6.7.4 The entity shall coordinate the activities specified in 6.7.3 with stakeholders.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.7.5 Procedures shall include a situation analysis that incorporates a damage assessment and a needs assessment to identify resources to support activities.				
6.7.6* Emergency operations/response shall be guided by an incident action plan or management by objectives.				
6.7.7 Resource management shall include the following: (1) Establishing processes for describing, taking inventory of, requesting, and tracking resources				
(2) Resource typing or categorizing resources by size, capacity, capability, and skill				
(3) Mobilizing and demobilizing resources in accordance with the established IMS				
(4) Conducting contingency planning for resource deficiencies				
6.7.8 A current inventory of internal and external resources shall be maintained.				
6.7.9 Donations of human resources, equipment, material, and facilities shall be managed.				
6.8 Emergency Operations/Response Plan.				
6.8.1* Emergency operations/response plans shall define responsibilities for carrying out specific actions in an emergency.				
6.8.2* The plan shall identify actions to be taken to protect people including those with access and functional needs, property, operations, the environment, and the entity.				
6.8.3* The plan shall identify actions for incident stabilization.				
6.8.4 The plan shall include the following: (1) Protective actions for life safety in accordance with 6.8.2				
(2) Warning, notifications, and communication in accordance with Section 6.5				
(3) Crisis communication and public information in accordance with Section 6.4				
(4) Resource management in accordance with 6.7.7				
(5) Donation management in accordance with 6.7.9				
6.9.1* The continuity plan should include recovery strategies to maintain critical or time-sensitive functions and processes identified during the business impact analysis.				
6.9.2* The continuity plan shall identify stakeholders that need to be notified; critical and time-sensitive applications; alternative work sites; vital records, contact lists, functions, and processes, that must be maintained; and personnel, procedures, and resources that are needed while the entity is recovering.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.9.3* The recovery plan shall provide for restoration of functions, services, resources, facilities, programs, and infrastructure.				
6.10* Employee Assistance and Support. **6.10.1*** The entity shall develop a strategy for employee assistance and support that includes the following: (1) Communications procedures				
(2)* Contact information, including emergency contact outside anticipated hazard area				
(3) Accounting for persons affected, displaced, or injured by the incident				
(4) Temporary, short-term, or long-term housing, and feeding and care of those displaced by an incident				
(5) Mental health and physical well-being of individuals affected by the incident				
(6) Pre-incident and post-incident awareness				
6.10.2 The strategy shall be flexible for use in all incidents.				
6.10.3* The entity shall promote family preparedness education and training for employees.				
Chapter 7 Training and Education **7.1* Training and Education Curriculum.** The entity shall develop and implement a competency-based training and education curriculum that supports all employees who have a role in the program.				
7.2 Goal of the Curriculum. The goal of the curriculum shall be to create awareness and enhance the knowledge, skills, and abilities required to implement, support, and maintain the program.				
7.3 Scope and Frequency of Instruction. The scope of the curriculum and frequency of instruction shall be identified.				
7.4 Incident Management System Training. Personnel shall be trained in the entity's incident management system (IMS) and other components of the program to the level of their involvement.				
7.5 Recordkeeping. Records of training and education shall be maintained as specified in Section 4.7.				
7.6 Regulatory and Program Requirements. The curriculum shall comply with applicable regulatory and program requirements.				
7.7* Public Education. A public education program shall be implemented to communicate: (1) Potential hazard impacts				
(2) Preparedness information				
(3) Information needed to develop a preparedness plan				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
Chapter 8 Exercises and Tests **8.1 Program Evaluation.** **8.1.1** The entity shall evaluate program plans, procedures, training, and capabilities and promote continuous improvement through periodic exercises and tests.				
8.1.2 The entity shall evaluate the program based on post-incident analyses, lessons learned, and operational performance in accordance with Chapter 9.				
8.1.3 Exercises and tests shall be documented.				
8.2* Exercise and Test Methodology. **8.2.1** Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting.				
8.2.2 Exercises shall be designed to assess the maturity of program plans, procedures, and strategies.				
8.2.3 Tests shall be designed to demonstrate capabilities.				
8.3* Design of Exercises and Tests.				
8.3.1 Exercises and tests shall be designed to: (1) Ensure the safety of people, property, operations, and the environment involved in the exercise or testing				
(2) Evaluate the program				
(3) Identify planning and procedural deficiencies				
(4) Test or validate recently changed procedures or plans				
(5) Clarify roles and responsibilities				
(6) Obtain participant feedback and recommendations for program improvement				
(7) Measure improvement compared to performance objectives				
(8) Improve coordination between internal and external teams, organizations, and entities				
(9) Validate training and education				
(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity				
(11) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery				
(12) Assess the ability of the team to identify, assess, and manage an incident				
(13) Practice the deployment of teams and resources to manage an incident				
(14) Improve individual performance				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
8.4 Exercise and Test Evaluation. **8.4.1** Exercises shall evaluate program plans, procedures, training, and capabilities to identify opportunities for improvement.				
8.4.2 Tests shall be evaluated as either pass or fail.				
8.5* Frequency.				
8.5.1 Exercises and tests shall be conducted on the frequency needed to establish and maintain required capabilities.				
Chapter 9 Program Maintenance and Improvement **9.1* Program Reviews.** The entity shall maintain and improve the program by evaluating its policies, program, procedures, and capabilities using performance objectives.				
9.1.1* The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action.				
9.1.2* Evaluations shall be conducted on a regularly scheduled basis, and when the situation changes to challenge the effectiveness of the existing program.				
9.1.3 The program shall be re-evaluated when a change in any of the following impacts the entity's program: (1) Regulations				
(2) Hazards and potential impacts				
(3) Resource availability or capability				
(4) Entity's organization				
(5)* Funding				
(6) Infrastructure, including technology environment				
(7) Economy and geopolitical stability				
(8) Entity operations				
9.1.4 Reviews shall include post-incident analyses, reviews of lessons learned, and reviews of program performance.				
9.1.5 The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.7.				
9.1.6 Documentation, records, and reports shall be provided to management for review and follow-up.				
9.2* Corrective Action. **9.2.1*** The entity shall establish a corrective action process.				
9.2.2* The entity shall take corrective action on deficiencies identified.				
9.3 Continuous Improvement. The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process.				

Annex D Plan-Do-Check-Act (PDCA) Cycle

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

D.1 The Plan-Do-Check-Act (PDCA) (*see Figure D.1*), also known as the Deming or Shewhart cycle, is a four-step problem-solving process typically used for business process improvement and quality assurance management.

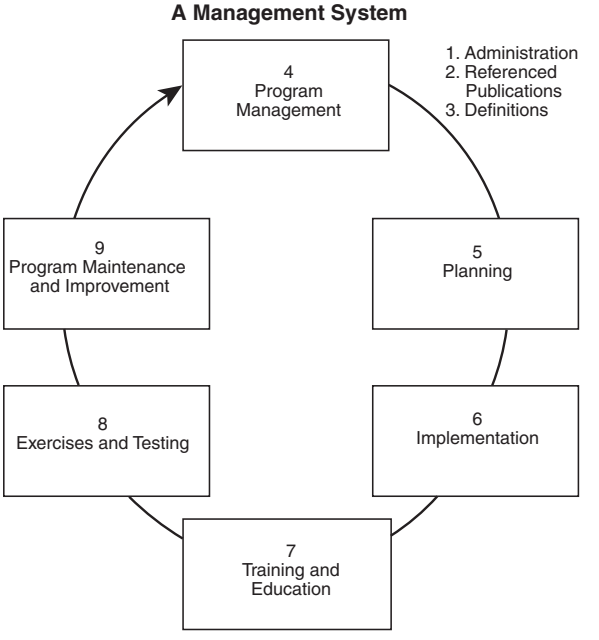

FIGURE D.1 The Plan-Do-Check-Act (PDCA) Cycle.

Annex E Crosswalk Between *NFPA 1600*, DRII, and CSA Z1600

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

E.1 Annex E is a cross-reference to the requirements of *NFPA 1600; Disaster Recovery Institute International Professional Practices for Business Continuity Practitioners*; and CSA Z1600, *Emergency Management and Business Continuity Programs. (See Table E.1)*. This crosswalk is intended purely as a high-level comparison of the component section of the indicated standards. Reference should be made the actual details in each section if a full comparison is needed.

Table E.1 Cross-Reference of *NFPA 1600* to DRII Professional Practices and CSA Z1600

NFPA 1600 (2013) Chapter/Section	DRII Professional Practices for Business Continuity Practitioners (2012) Subject Area	CSA Z1600-08 Emergency Management and Business Continuity Programs Chapter/Section
Chapter 4 Program Management		**4 Program Management**
4.1 Leadership and Commitment	1. Project Initiation and Management	4.1 Leadership and Commitment
4.2 Program Coordinator	1. Project Initiation and Management	4.2 Program Coordinator
4.3 Program Committee	1. Project Initiation and Management	4.3 Advisory Committee
4.4 Program Administration	1. Project Initiation and Management	4.4 Program Administration
4.5 Laws and Authorities	1. Program Initiation and Management 3. Business Impact Analysis 9. Crisis Communications 10. Coordinating with External Agencies	4.5 Laws and Authorities
4.6 Finance and Administration	1. Project Initiation and Management	4.6 Financial Management
4.7 Records Management	3. Business Impact Analysis	4.4.6 Records Management
Chapter 5 Planning		**5 Planning**
5.1 Planning and Design Process	2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation	5.2 Planning Process

(continues)

Table E.1 *Continued*

NFPA 1600 (2013) Chapter/Section	DRII Professional Practices for Business Continuity Practitioners (2012) Subject Area	CSA Z1600-08 Emergency Management and Business Continuity Programs Chapter/Section
5.2 Risk Assessment	2. Risk Evaluation and Control	5.1.1 Hazard Identification 5.1.2 Risk Assessment
5.3 Business Impact Analysis	3. Business Impact Analysis	5.1.3 Business Impact Analysis (BIA)
5.4 Resource Needs Assessment	1. Program Initiation and Management 3. Business Impact Analysis 6 Business Continuity Plan Development and Implementation	6.2 Resource Management 6.3 Mutual Aid/Mutual Assistance
5.5 Performance Objectives	1. Project Initiation and Management	4.4.3 Program Goals and Objectives
Chapter 6 Implementation		**6 Implementation**
6.1 Common Plan Requirements	2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications	5.3 Common Plan Requirements
6.2 Prevention	2. Risk Evaluation and Control	6.1.2 Prevention
6.3 Mitigation	2. Risk Evaluation and Control	6.1.3 Mitigation
6.4 Crisis Communications and Public Information	6. Business Continuity Plan Development and Implementation 9. Crisis Communications	6.6 Communications and Warning
6.5 Warning, Notifications, and Communications	5. Emergency Preparedness and Response 9. Crisis Communications 10. Coordinating with External Agencies	6.6.4 Public Warning
6.6 Operational Procedures	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications	6.7 Operational Procedures
6.7 Incident Management	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 9. Crisis Communications	6.5 Incident Management 6.8 Facilities

Table E.1 *Continued*

NFPA 1600 (2013) Chapter/Section	DRII Professional Practices for Business Continuity Practitioners (2012) Subject Area	CSA Z1600-08 Emergency Management and Business Continuity Programs Chapter/Section
6.8 Emergency Operations/Response Plan	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 9. Crisis Communications	6.4 Emergency Response
6.9 Business Continuity and Recovery	4. Business Continuity Strategies 6. Business Continuity Plan Development and Implementation	6.10 Business Continuity 6.11 Recovery
6.10 Employee Assistance and Support	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation	-
Chapter 7 Training and Education	8. Business Continuity Plan Exercise, Audit and Maintenance	6.9 Training
7.1 Training and Education Curriculum		6.9.1
7.2 Goal of the Curriculum		6.9.2
7.3 Scope and Frequency of Instruction		6.9.3
7.4 Incident Management System Training		-
7.5 Recordkeeping		6.9.4
7.6 Regulatory and Program Requirements		4.5.1 Compliance
7.7 Public Education		6.6.5 Public Awareness
Chapter 8 Exercises and Tests	8. Business Continuity Plan Exercise, Audit and Maintenance	**7 Exercises, Evaluations, and Corrective Actions**
8.1 Program Evaluation		7.1
8.2 Exercise and Test Methodology		-
8.3 Design of Exercises and Tests		7.2
8.4 Exercise and Test Evaluation		7.1
8.5 Frequency		7.1
Chapter 9 Program Maintenance and Improvement	8. Business Continuity Plan Exercise, Audit and Maintenance	**8 Management Review**
9.1 Program Reviews		8.1
9.2 Corrective Action		7.4 Corrective Action
9.3 Continuous Improvement		8.2 Continuous Improvement

DRII: DRI International, Inc.; CSA: Canadian Standards Association.

Annex F *NFPA 1600* 2013 Edition as a Management System Standard

This annex is not a part of the recommendations of this NFPA document but is included for informational purposes only.

Information in this annex is intended to be adopted by the entity at its discretion, replacing Chapters 1 through 9. Although this annex is written in mandatory language, it is not intended to be enforced or applied unless specifically adopted by the entity, thereby replacing Chapters 1–9 and becoming the full requirements of the standard. A management system is defined as a framework of processes designed to ensure the achievement of an entity's "business" objectives. By adopting this annex, the entity is committing to using a management system standard for implementation and maintenance of the program.

This annex was created using the Draft ISO Guide 83, *High level structure and identical text for management system standards and common core management system terms and definitions.* Cross-references to NFPA 1600 Chapters 1 through 9 are provided in brackets. Paragraphs without a cross-reference are part of the ISO identical text for management system standards (MSS), common management system (MS) terms, and core definitions from the Draft ISO Guide 83.

F.1 Scope. [Chapter 1]

F.1.1 Scope. This standard shall establish a common set of criteria for all-hazards disaster/emergency management and business continuity programs, hereinafter referred to as "the program." [1.1]

F.1.2 Purpose. This standard provides the fundamental criteria for a management system designed to develop, implement, assess, and maintain the program for prevention, mitigation, preparedness, response, continuity, and recovery. [1.2]

F.1.3 Application. This document shall apply to public, not-for-profit, nongovernmental organizations (NGOs), and private entities. [1.3]

F.2 Normative References. [Chapter 2]

F.2.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document. [2.1]

F.2.2 NFPA Publications. (Reserved) [2.2]

F.2.3 Other Publications. [2.3] *Merriam-Webster's Collegiate Dictionary*, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2003.

F.2.4 References for Extracts in Mandatory Sections. (Reserved) [2.4]

F.3 Terms and Definitions. [Chapter 3]

F.3.1 General. The definitions contained in this chapter shall apply to the terms used in this standard. Where terms are not defined in this chapter or within another chapter, they shall be defined using their ordinarily accepted meanings within the context in which they are used. *Merriam-Webster's Collegiate Dictionary*, 11th edition, shall be the source for the ordinarily accepted meaning.

F.3.2 NFPA Official Definitions. [3.2]

F.3.2.1 Approved. Acceptable to the authority having jurisdiction. [3.2.1]

F.3.2.2 Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure. [3.2.2]

F.3.2.3 Shall. Indicates a mandatory requirement. [3.2.3]

F.3.2.4 Should. Indicates a recommendation or that which is advised but not required. [3.2.4]

F.3.2.5 Standard. A document, the main text of which contains only mandatory provisions using the word "shall" to indicate requirements and which is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the *Manual of Style for NFPA Technical Committee Documents.* [3.2.5]

F.3.3 General Definitions. [3.3]

F.3.3.1 All-Hazards. An approach for prevention, mitigation, preparedness, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused. [3.3.1]

F.3.3.2 Business Continuity. An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services. [3.3.2]

F.3.3.3 Business Impact Analysis. A management level analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources. The analysis may identify time-critical functions, recovery priorities, dependencies, and interdependencies so that recovery time objectives can be established and approved. [3.3.3]

F.3.3.4 Capability. The ability to perform required actions. [3.3.4]

F.3.3.5 Competence. Demonstrated ability to apply knowledge and skills to achieve intended results. [3.3.5]

F.3.3.6 Continual Improvement. Recurring process of enhancing the management program in order to achieve improvements in overall performance consistent with the entity's policy, goals, and objectives. [3.3.6]

F.3.3.7 Continuity. A term that includes business continuity, continuity of operations (COOP), operational continuity, succession planning, and continuity of government (COG), which support the resilience of the entity. [3.3.7]

F.3.3.8 Crisis Management. The ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputational impact. [3.3.8]

F.3.3.9 Damage Assessment. An appraisal or determination of the effects of the incident on humans, on physical, operational, economic characteristics, and on the environment. [3.3.9]

F.3.3.10 Disaster/Emergency Management. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and recover from an incident that threatens life, property, operations, or the environment. [3.3.10]

F.3.3.11 Entity. A governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has emergency management and continuity of operations responsibilities. [3.3.11]

F.3.3.12 Exercise. A process to assess, train, practice, and improve performance in an entity. [3.3.12]

F.3.3.13 Incident. An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe. [3.3.13]

F.3.3.14 Incident Action Plan. A verbal plan, written plan, or combination of both, that is updated throughout the incident and reflects the overall incident strategy, tactics, risk management, and member safety that are developed by the incident commander. [3.3.14]

F.3.3.15 Incident Management System (IMS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure, designed to aid in the management of resources during incidents. [3.3.15]

F.3.3.16 Interoperability. The ability of diverse personnel, systems, and organizations to work together seamlessly. [3.3.16]

F.3.3.17 Mitigation. Activities taken to reduce the impacts from hazards. [3.3.17]

F.3.3.18 Mutual Aid/Assistance Agreement. A prearranged agreement between two or more entities to share resources in response to an incident. [3.3.18]

F.3.3.19 Preparedness. Ongoing activities, tasks, and systems to develop, implement, and maintain the program capabilities. [3.3.19]

F.3.3.20 Prevention. Activities to avoid or stop an incident from occurring. [3.3.20]

F.3.3.21 Recovery. Activities and programs designed to return conditions to a level that is acceptable to the entity. [3.3.21]

F.3.3.22 Resource Management. A system for identifying available resources to enable timely access to resources needed to prevent, mitigate, prepare for, respond to, maintain continuity during, or recover from an incident. [3.3.22]

F.3.3.23 Response. Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment. [3.3.23]

F.3.3.24 Risk Assessment. Process of hazard identification, and the analysis or probabilities, vulnerability, and impacts. [3.3.24]

F.3.3.25 Situation Analysis. The process of collecting, evaluating, and disseminating information related to the incident, including information on the current and forecasted situation, and on the status of resources for management of the incident. [3.3.25]

F.3.3.26 Test. Procedure for evaluation with a pass or fail result. [3.3.26]

F.3.3.27 Vital Records. Information critical to the continued operation or survival of an entity. [3.3.27]

F.3.4 ISO Terms and Definitions. For the purposes of this document, the following terms and definitions apply.

NOTE 1 The following terms and definitions constitute an integral part of the "common text" for management systems standards.

NOTE 2 Bold type in a definition indicates a cross-reference to another term defined in this clause, and the number reference for the term is given in parentheses.

F.3.4.1 Terms Related to "Plan."

F.3.4.1.1 Organization. Person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives (F.3.4.1.4).

NOTE The concept of organization includes, but is not limited to sole-trader, company, corporation, firm, enterprise, authority, partnership, charity or institution, or part or combination thereof, whether incorporated or not, public or private.

F.3.4.1.2 Risk. Effect of uncertainty on objectives (F.3.4.1.4).

NOTE 1 An effect is a deviation from the expected – positive and/or negative.

NOTE 2 Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process (F.3.4.2.2)). An objective can be expressed in other ways, e.g. as an intended outcome, a purpose, an operational criterion, as a disaster/emergency management and business continuity objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

NOTE 3 Risk is often characterized by reference to potential events (Guide 73, 3.5.1.3) and consequences (Guide 73, 3.6.1.3), or a combination of these.

NOTE 4 Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated likelihood (Guide 73, 3.6.1.1) of occurrence.

NOTE 5 Uncertainty is the state, even partial, of efficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

NOTE 6 In the context of disaster/emergency management and business continuity management system standards disaster/emergency management and business continuity objectives are set by the organization, consistent with the disaster/emergency management and business continuity policy, to achieve specific results. When applying the term risk and components of risk management, this should be related to the objectives of the organization that include, but are not limited to the disaster/emergency management and business continuity objectives as specified in F.6.2 of the common MSS text.

F.3.4.1.3 Policy. Intentions and direction of an organization (F.3.4.1.1 as formally expressed by its top management (F.3.4.1.1).

F.3.4.1.4 Objective. Result to be achieved.

NOTE 1 An objective can be strategic, tactical, or operational.

NOTE 2 An objective can be expressed in other ways, e.g., as an intended outcome, a purpose, an operational criterion; as a disaster/emergency management and business continuity objective or by the use of other words with similar meaning (e.g. aim, goal, or target).

F.3.4.1.5 Top management. Person or group of people who directs and controls an organization (F.3.4.1.1) at the highest level.

NOTE 1 Top management has the power to delegate authority and provide resources within the organization.

NOTE 2 An organization can for this purpose be identified by reference to the scope of the implementation of a management system (F.3.4.2.1).

F.3.4.1.6 Interested party (preferred term), stakeholder (admitted term). Person or group of people that holds a view that can affect the organization (F.3.4.1.1).

F.3.4.1.7 Requirement. Obligatory need or expectation that is stated or implied.

F.3.4.2 Terms Related to "Do."

F.3.4.2.1 Management system. Set of interrelated or interacting elements of an organization (F.3.4.1.1) to establish policies (F.3.4.1.3) and objectives (F.3.4.1.4), and processes (F.3.4.2.2) to achieve those objectives.

NOTE 1 A management system can address a single discipline or several disciplines.

NOTE 2 The system elements include the organization's structure, roles and responsibilities, planning, operation, etc.

NOTE 3 The scope of a management system may include the whole of the organization, specific and identified functions of the organization, specific and identified sections of the organization, or one or more functions across a group of organizations.

F.3.4.2.2 Process. Set of interrelated or interacting activities which transforms inputs into outputs.

F.3.4.2.3 Competence. Ability to apply knowledge and skills to achieve intended results.

F.3.4.2.4 Documented information. Information required to be controlled and maintained by an organization (F.3.4.1.1).

NOTE 1 Documented information can be in any format and media and from any source.

NOTE 2 Documented information can, e.g., refer to – the management system (F.3.4.2.1), including related processes (F.3.4.2.2); – information created in order for the organization to operate; – evidence of results achieved.

F.3.4.2.5 Performance. Measurable result.

NOTE 1 Performance can relate either to quantitative or qualitative findings.

NOTE 2 Performance can relate to the management of activities, processes (F.3.4.2.2), products (including services), systems or organizations (F.3.4.1.1).

F.3.4.2.6 Outsource (verb). Make an arrangement where an external organization (F.3.4.1.1) performs part of an organization's function or process (F.3.4.2.2.

NOTE An external organization is outside the scope of the management system (F.3.4.2.1), although the outsourced function or process is within the scope.

F.3.4.3 Terms Related to "Check."

F.3.4.3.1 Monitoring. Determining the status of a system, a process (F.3.4.2.2) or an activity.

NOTE To determine the status there may be a need to check, supervise or critically observe.

F.3.4.3.2 Measurement. Process (F.3.4.2.2) to determine a value.

F.3.4.3.3 Audit. Systematic, independent, and documented process (F.3.4.2.2) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

NOTE 1 An audit can be an internal audit (first party) or an external audit (second party or third party), and it can be a combined audit (combining two or more disciplines).

NOTE 2 "Audit evidence" and "audit criteria" are defined in ISO 19011.

F.3.4.3.4 Effectiveness. Extent to which planned activities are realized and planned results achieved.

F.3.4.3.5 Conformity. Fulfillment of a requirement (F.3.4.1.7).

F.3.4.3.6 Nonconformity. Non-fulfillment of a requirement (F.3.4.1.7).

F.3.4.4 F.3.4.4 Terms Related to "Act."

F.3.4.4.1 Correction. Action to eliminate a detected nonconformity (F.3.4.3.6)

F.3.4.4.2 Corrective action. Action to eliminate the cause of a nonconformity (F.3.4.3.6) and to prevent recurrence.

NOTE In the case of other undesirable outcomes, action is necessary to minimize or eliminate the causes and to reduce the impact or prevent recurrence. Such actions fall outside the concept of "corrective action" in the sense of this definition.

F.3.4.4.3 Continual improvement. Recurring activity to enhance performance (F.3.4.2.5).

F.4 Context of the Organization.

F.4.1 Understanding the Organization and Its Context. The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcomes of its disaster/emergency management and business continuity management system.

These issues shall be taken into account when establishing, implementing, maintaining and improving the organization's disaster/emergency management and business continuity management system.

F.4.2 Understanding the Needs and Expectations of Interested Parties. When establishing its disaster/emergency management and business continuity program, the entity shall determine:

(1) Its relevant interested parties and
(2) Their requirements (i.e. their needs and expectations whether stated, implied or obligatory)

F.4.3 Determining the Scope of the Management System. The organization shall determine the scope of the disaster/emergency management and business continuity management system, such that the boundaries and applicability of the management system can be clearly communicated to relevant internal and external parties. When determining the scope of the management system the organization shall consider:

(1) The external and internal issues referred to in Section F.4.1
(2) The requirements referred to in Section F.4.2

F.4.4 Disaster/Emergency Management and Business Continuity Management System. The organization shall, establish, implement, maintain and improve disaster/emergency management and business continuity management system in accordance with the requirements of this International Standard including the processes needed and their interactions.

F.4.5 Laws and Authorities. [4.5]

F.4.5.1 The program shall comply with applicable legislation, policies, regulatory requirements, and directives. [4.5.1]

F.4.5.2 The entity shall establish and maintain a procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives. [4.5.2]

F.4.5.3 The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice. [4.5.3]

F.5 Leadership.

F.5.1 General. Persons in top management and other relevant management roles throughout the organization shall demonstrate leadership with respect to the disaster/emergency management and business continuity management system.

NOTE: This can be shown, for example, by motivating and empowering persons to contribute to the effectiveness of the disaster/emergency management and business continuity management system.

F.5.2 Management Commitment.

F.5.2.1 Top management shall demonstrate its commitment by:

(1) Ensuring the disaster/emergency management and business continuity management system is compatible with the strategic direction of the organization;
(2) Integrating the disaster/emergency management and business continuity management system requirements into the organization's business processes;
(3) Providing the resources to establish, implement, maintain, and continually improve the disaster/emergency management and business continuity management system;
(4) Communicating the importance of effective disaster/emergency management and business continuity management and conforming to the disaster/emergency management and business continuity management system requirements;
(5) Ensuring that the disaster/emergency management and business continuity management system achieves its intended outcomes;
(6) Directing and supporting continual improvement

NOTE: reference to "business" in this International Standard should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

F.5.2.2 Leadership and Commitment. [4.1]

F.5.2.2.1 The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents. [4.1.1]

F.5.2.2.2 The leadership commitment shall include the following: [4.1.2]

(1) Support the development, implementation, and maintenance of the program
(2) Provide necessary resources to support the program
(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness
(4) Support corrective action to address program deficiencies

F.5.2.2.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program. [4.1.3]

F.5.3 Policy.

F.5.3.1 Top management shall establish a disaster/emergency management and business continuity policy. The policy shall:

(1) Be appropriate to the purpose of the organization;
(2) Provide the framework for setting disaster/emergency management and business continuity objectives;
(3) Include a commitment to satisfy applicable requirements;
(4) Include a commitment to continual improvement of the disaster/emergency management and business continuity program and management system;
(5) Be communicated within the organization;
(6) Be available to interested parties, as appropriate.

F.5.3.2 The organization shall retain documented information on the disaster/emergency management and business continuity policy.

F.5.3.3 Program Administration. [4.4]

F.5.3.3.1 The entity shall have a documented program that includes the following: [4.4.1]

(1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority
(2) Program scope, goals, performance objectives, and metrics for program evaluation
(3) Applicable authorities, legislation, regulations, and industry codes of practice as required by F.4.5
(4) Program budget and schedule, including milestones
(5) Program plans and procedures that include:
    (a) Anticipated cost
    (b) Priority
    (c) Resources required
(6) Records management practices as required by F.7.5.4
(7) Change management process

F.5.3.3.2 The program shall include the requirements specified in Sections F.4 to F.10, the scope of which shall be determined through an "all-hazards" approach, and the risk assessment. [4.4.2]

F.5.3.3.3 Program requirements shall be applicable to prevention, mitigation, preparedness, response, continuity, and recovery. [4.4.3]

F.5.4 Organizational Roles, Responsibilities and Authorities.

F.5.4.1 Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization.

F.5.4.2 Top management shall assign the responsibility and authority for

(1) Ensuring that the disaster/emergency management and business continuity management system conforms to the requirements of this International Standard
(2) Reporting on the performance of the disaster/emergency management and business continuity management system to top management

F.5.4.3 Program Coordinator. The program coordinator shall be appointed by the entity's leadership and authorized to develop, implement, administer, evaluate, and maintain the program. [4.2]

F.5.4.4 Program Committee. [4.3]

F.5.4.4.1 A program committee shall be established by the entity in accordance with its policy. [4.3.1]

F.5.4.4.2 The program committee shall provide for, and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program. [4.3.2]

F.5.4.4.3 The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation. [4.3.3]

F.6 Planning. [Chapter 5]

F.6.1 Actions to Address Risks and Opportunities.

F.6.1.1 The organization shall consider the issues referred to in Section 4.1 and the requirements referred to in Section 4.2 and determine the risks and opportunities that need to be addressed to:

(1) Assure the management system can achieve its intended outcome(s)
(2) Prevent undesired effects
(3) Realize opportunities for improvement.

F.6.1.2 The organization shall:

(1) Evaluate the need to plan actions to address these risks and opportunities, and
(2) Where applicable
    (a) Integrate and implement these actions into its disaster/emergency management and business continuity management system processes (see F.8.1)
    (b) Ensure information will be available to evaluate if the actions have been effective (see F.9.1)

F.6.2 Disaster/Emergency Management and Business Continuity Objectives and Plans to Achieve Them.

F.6.2.1 Top management shall ensure that disaster/emergency management and business continuity objectives are established and communicated for relevant functions and levels within the organization.

F.6.2.2 The disaster/emergency management and business continuity objectives shall:

(1) Be consistent with the disaster/emergency management and business continuity policy
(2) Be measurable (if practicable)
(3) Take into account applicable requirements
(4) Be monitored and updated as appropriate

F.6.2.3 The organization shall retain documented information on the disaster/emergency management and business continuity objectives.

F.6.2.4 To achieve its disaster/emergency management and business continuity objectives, the organization shall determine:

(1) Who will be responsible
(2) What will be done
(3) What resources will be required
(4) When it will be completed
(5) How the results will be evaluated

F.6.2.5 Performance Objectives. [5.5]

F.6.2.5.1 The entity shall establish performance objectives for the program in accordance with the requirements in Section 5 and the elements in Sections 6 through 10. [5.5.1]

F.6.2.5.2 The performance objectives shall address the results of the hazard identification, risk assessment, and business impact analysis. [5.5.2]

F.6.2.5.3 Performance objectives shall be developed by the entity to address both short-term and long-term needs. [5.5.3]

F.6.2.5.4 The entity shall define the terms *short term* and *long term*. [5.5.4]

F.6.3 Planning and Design Process. [5.1]

F.6.3.1 The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program. [5.1.1]

F.6.3.2 Strategic planning shall define the entity's vision, mission, and program goals. [5.1.2]

F.6.3.3 Risk assessment and business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies. [5.1.3]

F.6.3.4 Risk assessment, business impact analysis, and resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans. [5.1.4]

F.6.3.5 Crisis management planning shall address issues that threaten the strategic, reputational, and intangible elements of the entity. [5.1.5]

F.6.3.6 The entity shall include key stakeholders in the planning process. [5.1.6]

F.6.4 Risk Assessment. [5.2]

F.6.4.1 The entity shall conduct a risk assessment in accordance with Section 5.4 to develop required strategies and plans. [5.2.1]

F.6.4.2 The entity shall identify hazards and monitor those hazards and the likelihood of occurrence. [5.2.2]

F.6.4.2.1 Hazards to be evaluated shall include the following: [5.2.2.1]

(1) Natural hazards (geologic, meteorologic, and biological)
(2) Human-caused events (accidental and intentional)
(3) Technology-caused events (accidental and intentional)

F.6.4.2.2 The vulnerability of people, property, the environment, and the entity shall be identified, evaluated, and monitored. [5.2.2.2]

F.6.4.3 The entity shall conduct an analysis of the impact of the hazards identified in F.6 on:

(1) Health and safety of persons in the affected area
(2) Health and safety of personnel responding to the incident
(3) Continuity of operations
(4) Property, facilities, assets, and critical infrastructure
(5) Delivery of the entity's services
(6) Supply chain
(7) Environment
(8) Economic and financial conditions
(9) Regulatory and contractual obligations
(10) Reputation of or confidence in the entity

F.6.4.4 The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts. [5.2.4]

F.6.4.5 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies. [5.2.5]

F.6.5 Business Impact Analysis. [5.3]

F.6.5.1 The entity shall conduct a business impact analysis (BIA). [5.3.1]

F.6.5.2 The BIA shall evaluate the potential impact resulting from interruption or disruption of individual functions, processes, and applications. [5.3.2]

F.6.5.3 The BIA shall identify those functions, processes, infrastructure, systems, and applications that are critical to the entity and the point in time (recovery time objective) when the impact of the interruption or disruption becomes unacceptable to the entity. [5.3.3]

F.6.5.4 The BIA shall identify dependencies and interdependencies across functions, processes, and applications, to determine the potential for compounding impacts in the event of an interruption or disruption. [5.3.4]

F.6.5.5 The BIA shall evaluate the potential loss of information and the point in time (recovery point objective) that defines the potential gap between the last backup of information and the time of the interruption or disruption.

F.6.5.6 The BIA developed in Section F.6.5 shall be used in the development of recovery strategies and plans to support the program.

F.6.5.7 The analysis of impacts required by F.6.5.3 and the BIA required by Section F.6.5 shall be conducted jointly or separately.

F.7 Support.

F.7.1 Resources. The organization shall determine and provide the resources needed for the disaster/emergency management and business continuity management system.

F.7.1.1 Resource Needs Assessment. [5.4]

F.7.1.1.1 The entity shall conduct a resource needs assessment based on the hazards identified in F.6.4 and the business impact analysis in F.6.5. [5.4.1]

F.7.1.1.2 The resource needs assessment shall include: [5.4.2]

(1) Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed.
(2) Quantity, response time, capability, limitations, cost, and liabilities.

F.7.1.1.3 The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, and materials procured or donated to support the program. [5.4.3]

F.7.1.1.4 Facilities capable of supporting response, continuity, and recovery operations shall be identified. [5.4.4]

F.7.1.1.5 The need for mutual aid/assistance or partnership agreements shall be determined. [5.4.5]

F.7.1.1.5.1 If needed, agreements shall be established and documented. [5.4.5.1]

F.7.1.2 Resource Management.

F.7.1.2.1 Resource management shall include the following tasks: [6.7.7]

(1) Establishing processes for describing, taking inventory of, requesting, and tracking resources
(2) Resource typing or categorizing resources by size, capacity, capability, and skill
(3) Mobilizing and demobilizing resources in accordance with the established IMS
(4) Conducting contingency planning for resource deficiencies

F.7.1.2.2 A current inventory of internal and external resources shall be maintained. [6.7.8]

F.7.1.2.3 Donations of human resources, equipment, material, and facilities shall be managed. [6.7.9]

F.7.1.3 Finance and Administration. [4.6]

F.7.1.3.1 The entity shall develop finance and administrative procedures to support the program before, during, and after an incident. [4.6.1]

F.7.1.3.2 There shall be a responsive finance management and administrative framework that: [4.6.2]

(1) Complies with the entity's program requirements
(2) Is uniquely linked to response, continuity, and recovery operations
(3) Provides for maximum flexibility to expeditiously request, receive, manage, and apply funds in a non-emergency environment and in emergency situations to ensure the timely delivery of assistance

F.7.1.3.3 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles, governance, requirements, and fiscal policy. [4.6.3]

F.7.1.3.4 Finance and administrative procedures shall include the following: [4.6.4]

(1) Responsibilities for program finance authority, including reporting relationships to the program coordinator
(2) Program procurement procedures
(3) Payroll
(4) Accounting systems to track and document costs
(5) Management of funding from external sources
(6) Crisis management procedures that coordinate authorization levels and appropriate control measures
(7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery
(8) Identifying and accessing alternative funding sources
(9) Managing budgeted and specially appropriated funds

F.7.2 Competence.

F.7.2.1 The organization shall:

(1) Determine the necessary competence of person(s) doing work under its control that affects its disaster/emergency management and business continuity performance.
(2) Ensure these persons are competent on the basis of appropriate education, training, or experience.
(3) Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.
(4) Retain appropriate documented information as evidence of competence.

NOTE: Applicable actions may include, for example: the provision of training to, the mentoring of, or the re-assignment of current employees; or the hiring or contracting of competent persons.

F.7.2.2 Training [Chapter 7]

F.7.2.2.1 Training and Education Curriculum. The entity shall develop and implement a competency-based training and education curriculum that supports all employees who have a role in the program. [7.1]

F.7.2.2.2 Goal of the Curriculum. The goal of the curriculum shall be to create awareness and enhance the knowledge, skills, and abilities required to implement, support, and maintain the program. [7.2]

F.7.2.2.3 Scope and Frequency of Instruction. The scope of the curriculum and frequency of instruction shall be identified. [7.3]

F.7.2.2.4 Incident Management System Training. Personnel shall be trained in the entity's incident management system (IMS) and other components of the program to the level of their involvement. [7.4]

F.7.2.2.5 Recordkeeping. Records of training and education shall be maintained as specified in Section F.7.5.5. [7.5]

F.7.2.2.6 Regulatory and Program Requirements. The curriculum shall comply with applicable regulatory and program requirements. [7.6]

F.7.2.2.7 Public Education. A public education program shall be implemented to communicate the following: [7.7]

(1) Potential hazard impacts
(2) Preparedness information
(3) Information needed to develop a preparedness plan

F.7.3 Awareness. Persons doing work under the organization's control shall be aware of:

(1) The disaster/emergency management and business continuity policy
(2) Their contribution to the effectiveness of the disaster/emergency management and business continuity management system, including the benefits of improved disaster/emergency management and business continuity performance
(3) The implications of not conforming with the disaster/emergency management and business continuity management system requirements

F.7.4 Communication.

F.7.4.1 The organization shall determine the need for internal and external communications relevant to the disaster/emergency management and business continuity management system including:

(1) What to communicate
(2) When to communicate
(3) To whom it will communicate

F.7.4.2 Crisis Communications and Public Information. [6.4]

F.7.4.2.1 The entity shall develop a plan and procedures to disseminate information to and respond to requests for information from the following audiences before, during, and after an incident: [6.4.1]

(1) Internal audiences, including employees
(2) External audiences, including the media, functional needs population, and other stakeholders

F.7.4.2.2 The entity shall establish and maintain a crisis communications or public information capability that includes the following: [6.4.2]

(1) Central contact facility or communications hub
(2) Physical or virtual information center
(3) System for gathering, monitoring, and disseminating information
(4) Procedures for developing and delivering coordinated messages
(5) Pre-scripted information bulletins or templates
(6) Protocol to clear information for release

F.7.4.3 Warning, Notifications, and Communications. [6.5]

F.7.4.3.1 The entity shall determine warning, notification, and communications needs. [6.5.1]

F.7.4.3.2 Warning, notification, and communications systems shall be reliable, redundant, and interoperable. [6.5.2]

F.7.4.3.3 The entity shall develop and test warning, notification, and communications protocols and procedures to alert stakeholders potentially at risk from an actual or impending incident. [6.5.3]

F.7.4.3.4 Procedures shall include issuing warnings through authorized agencies if required by law. [6.5.4]

F.7.5 Documented Information.

F.7.5.1 General The organization's disaster/emergency management and business continuity management system shall include:

(1) Documented information required by this International Standard
(2) Documented information determined by the organization as being required for the effectiveness of the disaster/emergency management and business continuity management system

F.7.5.2 Common Plan Requirements. [6.1]

F.7.5.2.1 Plans shall address the health and safety of personnel. [6.1.1]

F.7.5.2.2 Plans shall identify and document the following: [6.1.2]

(1) Assumptions made during the planning process
(2) Functional roles and responsibilities of internal and external agencies, organizations, departments, and positions
(3) Lines of authority
(4) The process for delegation of authority
(5) Lines of succession for the entity
(6) Liaisons to external entities
(7) Logistics support and resource requirements

F.7.5.2.3 Plans shall be individual, integrated into a single plan document, or a combination of the two.

F.7.5.2.4 The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required. [6.1.4]

F.7.5.3 Create and Update The process for creating and updating documented information shall ensure appropriate:

(1) Identification and description (e.g. a title, date, author, number)
(2) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic)
(3) Review and approval for adequacy