NFPA 1600®

Standard on Disaster/Emergency Management and Business Continuity Programs

2010 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.

ISBN: 978-087765956-3 (Print)
ISBN: 978-161665005-6 (PDF) 12/09

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 by the NFPA. 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 02169-7471; email: stds_admin@nfpa.org

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

NFPA 1600®

Standard on

Disaster/Emergency Management and Business Continuity Programs

2010 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 and released by the Technical Correlating Committee on Emergency Management and Business Continuity. It was issued by the Standards Council on October 27, 2009, with an effective date of December 5, 2009, and supersedes all previous editions.

This edition of *NFPA 1600* was approved as an American National Standard on December 5, 2009.

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* has been reordered and expanded. Chapter 4, Program Management, was expanded to emphasize the importance of leadership and commitment; includes new requirements for defining performance objectives; and includes new requirements for records management. Finance and administration was also moved to the program management chapter. The most noticeable change from the 2007 edition is the rewriting of Chapter 5 into four chapters addressing planning, implementation, testing and exercises, and program improvement. The ordering of these chapters follows 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" are now a separate section within Chapter 5. Chapter 6, Implementation, includes a new section on employee assistance and support. Testing and exercising was expanded within the new Chapter 7, and evaluations and corrective action have been 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 includes a self-assessment checklist to help users evaluate conformity with the standard, and Annex D provides 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.

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]
Lloyd W. Bokman, Ohio Emergency Management Agency, OH [E]
Rep. National Association of Sara Title III Program Officials
Pete Brewster, U.S. Department of Veterans Affairs, WV [U]
Win Chaiyabhat, Aon Global Risk Consulting, ME [I]
Steven J. Charvat, University of Washington, WA [U]
Rep. International Association of Emergency Managers
Robert P. Fletcher, Jr., Readiness Consulting Services, MD [SE]
Robert Gazdik, Travelers Insurance Company, MN [I]
David Gluckman, Willis HRH N.A., NJ [I]
David Halstead, State of Florida, FL [E]
Rep. National Emergency Management Association
David J. Hiscott, Jr., ConocoPhillips Pipe Line Company, TX [U]
Rep. American Petroleum Institute
David R. Hood, Russell Phillips & Associates, LLC, NY [U]
Rep. NFPA Health Care Section
Michael W. Janko, The Goodyear Tire & Rubber Company, OH [U]
Gunnar J. Kuepper, Emergency and Disaster Management, Inc., CA [SE]
Edgar T. Ladouceur, Transport Canada, Canada [E]
Dana C. Lankhorst, MiddleOak, NH [I]
Dean R. Larson, Purdue University Calumet, IN [SE]
Ray S. Lazarus, Emergency Management Ontario, Canada [E]
Michael E. Martinet, County of Los Angeles, CA [E]
Ashley P. Moore, U.S. Department of Homeland Security/FEMA, DC [E]
Patricia A. Moore, Pat Moore Company, TX [SE]
Terry W. Moore, City of Houston, TX [U]
Rep. Emergency Management Association of Texas
Michael J. Morganti, Trinity, FL [SE]
Rep. Disaster Recovery Institute International
Melvyn Musson, Edward Jones Company, MO [U]
Ashley E. Newsome, Emergency Response Educators & Consultants, Inc., FL [SE]
Scott R. Nicoll, Chubb Group of Insurance Companies, NJ [I]
William G. Raisch, New York University, NY [SE]
Dale J. Romme, Hallmark Cards, Inc., MO [U]
Rep. NFPA Industrial Fire Protection Section
David M. Sarabacha, Deloitte & Touché LLP, WA [SE]
R. Ian Stronach, Alcan Inc., Canada [U]
MaryAnn E. Tierney, City of Philadelphia, PA [U]
Milt Wilson, Ontario Association of Fire Chiefs, Canada [U]

Alternates

Gregory T. Cybulski, Aon Corporation, NJ [I]
(Alt. to W. Chaiyabhat)
Steve Detwiler, Orange County Office of Emergency Management, FL [U]
(Alt. to S. J. Charvat)
Michael J. DuBose, Willis HRH N.A., NJ [I]
(Alt. to D. Gluckman)
Kenneth Katz, Travelers Insurance Company, NC [I]
(Alt. to R. Gazdik)
Shayne Mintz, Burlington Fire Department, Canada [U]
(Alt. to M. Wilson)
John Douglas Nelson, Business Continuity Solutions, Inc., CA [SE]
(Alt. to P. A. Moore)
Patricia Okolita, Hanover Insurance, MA [SE]
(Alt. to M. J. Morganti)
Robie Robinson, Dallas County, TX [U]
(Alt. to T. W. Moore)
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]
Carl Anthony Gibson, La Trobe University, Australia [E]
Graeme S. Jannaway, Jannaway & Associates, Canada [SE]
Gavin J. Love, WorleyParsons Pty Ltd., TX [SE]

David G. Trebisacci, 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

2010 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.

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

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, non-governmental organizations (NGO), and private entities on a local, regional, national, international, and global basis.

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 shall be located in an appendix or annex, footnote, or fine-print note and are not to be considered a part of the requirements of a standard.

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 impact of potential losses and maintain viable recovery strategies, recovery plans, and continuity of services.

3.3.3 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.

3.3.4* 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.

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

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

3.3.7 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.

3.3.8 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.

3.3.9* Exercise. Activity in which the entity's plan(s) is rehearsed in part or in whole to ensure that the plan(s) contains the appropriate information and produces the desired result when put into effect.

3.3.10 Impact Analysis [Business Impact Analysis (BIA)]. A management level analysis that identifies the impact of losing the entity's resources.

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

3.3.12 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.

3.3.13* 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.

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

3.3.15 Mitigation. Activities taken to reduce the impacts from hazards.

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

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

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

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

3.3.20* 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.

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

3.3.22 Risk Assessment. Process of hazard identification, probability analysis, vulnerability analysis, and impacts analysis.

3.3.23 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.

3.3.24 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) Policies, plans, and procedures to develop, implement, and maintain the program
(2) Resources to support the program
(3) Reviews and evaluations to ensure program effectiveness
(4) Correction of 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 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 for, 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. 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, objectives, and method of program evaluation
(3) Program plans and procedures that include the following:
    (a) Anticipated cost
    (b) Priority
    (c) Time schedule
    (d) Resources required
(4) Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5
(5) Program budget and schedule, including milestones
(6) Records management practices as required by Section 4.8

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 Performance Objectives.

4.6.1* The entity shall establish performance objectives for program requirements in accordance with Chapter 4 and program elements in accordance with Chapters 4 through 8.

4.6.2 The performance objectives shall depend on the results of the hazard identification, risk assessment, and business impact analysis.

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

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

4.7* Finance and Administration.

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

4.7.2 There shall be a responsive financial management and administrative framework that complies with the entity's program requirements and is uniquely linked to response, continuity, and recovery operations.

4.7.3 There shall be crisis management procedures to provide coordinated situation-specific authorization levels and appropriate control measures.

4.7.4 The framework shall provide 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.

4.7.5 The administrative process shall be documented through written procedures.

4.7.6 The program shall be capable of capturing financial data for future cost recovery, as well as identifying and accessing alternative funding sources and managing budgeted and specially appropriated funds.

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

4.7.8* The procedures specified in 4.7.7 shall include the following:

(1) Establishment and definition of responsibilities for the program finance authority, including its 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

4.8* Records Management.

4.8.1 The entity shall develop a records management program

4.8.2 Policies shall be created, approved, and enforced to address the following:

(1) Records classification
(2) Maintenance of confidentiality
(3) Maintenance of integrity incorporating audit trail
(4) Record retention
(5) Record storage
(6) Record archiving
(7) Record destruction
(8) Access control
(9) Document control

4.8.3 The entity shall apply the program to existing and newly created records.

4.8.4 The entity shall develop and enforce procedures coordinating the access and circulation of records within and outside of the organization.

4.8.5 The entity shall execute the records management program.

Chapter 5 Planning

5.1 Planning Process.

5.1.1* The program shall follow a planning process that develops strategic, crisis management, prevention, mitigation, emergency operations/response, continuity, and recovery plans.

5.1.2 Strategic planning shall define the vision, mission, and goals.

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

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

5.2 Common Plan Requirements.

5.2.1* Plans shall identify the functional roles and responsibilities of internal and external agencies, organizations, departments, and positions.

5.2.2 Plans shall identify lines of authority.

5.2.3 Plans shall identify lines of succession for the entity.

5.2.4 Plans shall identify interfaces to external organizations.

5.2.5 Plans shall identify the process for delegation of authority.

5.2.6 Plans shall identify logistics support and resource requirements.

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

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

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

5.3* Planning and Design.

5.3.1* The program shall include the requirements specified in Chapters 4 through 8, the scope of which shall be determined through an "all-hazards" approach, and the risk assessment.

5.3.2* The program requirements shall be applicable to prevention, mitigation, preparedness, response, continuity, and recovery.

5.4* Risk Assessment.

5.4.1* The entity shall conduct a risk assessment in accordance with Section 5.4 to identify strategies for prevention and mitigation and to gather information to develop plans for response, continuity, and recovery.

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

5.4.2.1* Hazards to be evaluated shall include the following:

(1) Natural hazards (geological, meteorological, and biological)
(2) Human-caused events (accidental and intentional)
(3) Technologically caused events (accidental and intentional)

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

5.4.3* The entity shall conduct an analysis of the impact of the hazards identified in 5.4.2 on the following:

(1) Health and safety of persons in the affected area at the time of the incident (injury and death)
(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
(9) Regulatory and contractual obligations
(10) Reputation of or confidence in the entity

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

5.5* Business Impact Analysis.

5.5.1 The entity shall conduct a business impact analysis (BIA).

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

5.5.3* The BIA shall identify those functions, processes, and applications that are critical to the entity and the point in time when the impact(s) of the interruption or disruption becomes unacceptable to the entity.

5.5.4* The BIA shall evaluate the potential loss of information and the point in time that defines the potential gap between the last backup of information and the time of the interruption or disruption.

5.5.5 The BIA developed in Section 5.5 shall be used in the development of plans to support the program.

5.5.6 The impact analysis required by 5.4.3 and the BIA required by Section 5.5 shall be permitted to be conducted in conjunction with each other or separately.

5.6 Prevention.

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

5.6.2* The prevention strategy shall be based on the information obtained from Section 5.4 and shall be kept current using the techniques of information collection and intelligence.

5.6.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, impact analysis, program constraints, operational experience, and cost benefit analysis.

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

5.7 Mitigation.

5.7.1* 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.

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

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

Chapter 6 Implementation

6.1* Resource Management.

6.1.1* The entity shall conduct a resource management needs assessment based on the hazards identified in 5.4.2.

6.1.2 The resource management 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 liability connected with using the involved resources
(3) Resources and any needed partnership arrangements essential to the program

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

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

6.1.5 Resource management shall include the following tasks:

(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

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

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

6.2* Mutual Aid/Assistance.

6.2.1 The need for mutual aid/assistance shall be determined.

6.2.2 If mutual aid/assistance is needed, agreements shall be established.

6.2.3* Mutual aid/assistance agreements shall be documented in the program.

6.3* Communications and Warning.

6.3.1* The entity shall determine communications and warning needs, based on required capabilities to execute plans.

6.3.2* Communications and warning systems shall be reliable, redundant, and interoperable.

6.3.3* Emergency communications and warning protocols and procedures shall be developed, tested, and used to alert stakeholders potentially impacted by an actual or impending incident.

6.3.4 Advisory and warning systems shall be integrated into planning and operational use.

6.3.5* The entity shall develop and maintain the following capabilities:

(1) Communications between the levels and functions of the organization and outside entities
(2) Documentation of communications
(3) Communications with emergency responders
(4) Central contact facility or communications hub

6.3.6 The entity shall establish, implement, and maintain procedures to disseminate warnings.

6.3.7 The entity shall develop procedures to advise the public, through authorized agencies, of threats to life, property, and the environment.

6.3.8* The entity shall disseminate warning information to stakeholders potentially impacted.

6.3.9 The entity shall document issued warnings.

6.4 Operational Procedures.

6.4.1 The entity shall develop, coordinate, and implement operational procedures to support the program and execute its plans.

6.4.2* Procedures shall be established and implemented for response to and recovery from the impact of hazards identified in 5.4.2.

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

6.4.4 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

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

6.4.6 On activation of a local emergency operations center (EOC), communications and coordination shall be established between the IMS and the EOC.

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

6.5 Emergency Response.

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

6.5.2* The plan shall identify actions to be taken to protect people (including those with special needs), property, operations, and the environment and to provide incident stabilization.

6.5.3 The plan shall include the following:

(1) Communication and warning in accordance with Section 6.3
(2) Crisis communication and public information in accordance with Section 6.8
(3) Protective actions for life safety
(4) Direction and control in accordance with Section 6.8
(5) Resource management in accordance with Sections 6.1 and 6.2
(6) Donation management in accordance with 6.1.7

6.6* Employee Assistance and Support.

6.6.1* The entity shall develop a strategy for employee assistance and support to include 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

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

6.7 Business Continuity and Recovery.

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

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

6.8* Crisis Communications and Public Information.

6.8.1* The entity shall develop a plan and procedures to disseminate and respond to requests for pre-incident, incident, and post-incident information to and from the following:

(1) Internal audiences, including employees
(2) External audiences, including the media and special needs populations

6.8.2* A capability shall be established and maintained to include the following:

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

6.8.3 The entity shall establish a physical or virtual information center.

6.9 Incident Management.

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

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

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

6.9.4 The entity shall coordinate the activities specified in 6.9.3 with stakeholders in the mitigation, preparedness, response, continuity, and recovery operations.

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

6.10* Emergency Operations Centers (EOCs).

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

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

6.11* Training and Education.

6.11.1* The entity shall develop and implement a training and education curriculum to support the program.

6.11.2 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.

6.11.3 The scope of the curriculum and frequency of instruction shall be identified.

6.11.4 Personnel shall be trained in the entity's IMS and other components of the program to the level of their involvement.

6.11.5 Records of training and education shall be maintained as specified in Section 4.8.

6.11.6 The curriculum shall comply with applicable regulatory and program requirements.

6.11.7* A public education program shall be implemented to communicate the following:

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

Chapter 7 Testing and Exercises

7.1 Entity Evaluation. The entity shall evaluate program plans, procedures, and capabilities through periodic testing and exercises.

7.2* Exercise Evaluation. Exercises shall be designed to evaluate program plans, procedures, and capabilities.

7.3* Methodology. Exercises shall provide a standardized methodology to practice procedures and interact with other entities in a controlled setting.

7.4 Frequency. Testing and exercises shall be conducted on the frequency needed to establish and maintain required capabilities.

7.5 Exercise Design. Exercises shall be designed to do the following:

(1) Evaluate the program
(2) Identify planning and procedural deficiencies
(3) Test or validate recently changed procedures or plans
(4) Clarify roles and responsibilities
(5) Obtain participant feedback and recommendations for program improvement
(6) Measure improvement compared to performance objectives
(7) Improve coordination between internal and external teams, organizations, and entities
(8) Validate training and education
(9) Increase awareness and understanding of hazards and the potential impacts of hazards on the entity
(10) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery

Chapter 8 Program Improvement

8.1* Program Reviews.

8.1.1 The entity shall improve effectiveness of the program through management review of the policies, performance objectives, evaluation of program implementation, and changes resulting from preventive and corrective action.

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

8.1.3 The program shall also be re-evaluated when any of the following occur:

(1) Regulatory changes
(2) Changes in hazards and potential impacts
(3) Resource availability or capability changes
(4) Organizational changes
(5)*Funding changes
(6) Infrastructure, economic, and geopolitical changes
(7) Changes in products or services
(8) Operational changes

8.1.4 Reviews shall be conducted based on post-incident analyses, lessons learned, and operational performance.

8.1.5 The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.8.

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

8.2* Corrective Action.

8.2.1* The entity shall establish a corrective action process.

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

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); business and industry; nongovernmental organizations; and individual citizens. Each of these entities has its own focus, unique missions and responsibilities, varied resources and capabilities, and operating principles and procedures.

A.1.2 This 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.

A.1.3 The application of *NFPA 1600* within the private sector is described in detail in a handbook, *Implementing NFPA 1600, National Preparedness Standard,* written by members of the Technical Committee on Emergency Management and Business Continuity, who are responsible for the standard. This handbook is available from the NFPA catalog of publications at www.nfpa.org.

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 author-

ity 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.

A.3.3.4 Continuity. An evolving concept that is linked to continuity is resilience. Organizational resilience is the ability of an entity to respond to the impact of an incident, continue to provide a minimum acceptable level of service 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(ies) in which the entity operates is resilient, entities should work with local stakeholders (including public, private, and voluntary organizations) to promote emergency management and business continuity processes. Entities that outsource any of their facilities or services should assist their suppliers in developing and maintaining these processes, and evaluate requiring their suppliers to maintain programs to assure organizational resilience to 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.3.3.9 Exercise. 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 with other agencies in a controlled setting. Participants identify and make recommendations to improve the overall program. The fundamental purpose is to improve the implementation of procedures. In support of that goal, an exercise should be used to achieve the following:

(1) Reveal planning weaknesses and strengths in the plan or standard operating procedures/standard operating guidelines (SOP/SOG), or to test and validate recently changed procedures
(2) Improve the coordination between various response organizations, elected officials, and community support organizations
(3) Validate the training of the critical elements of response (e.g., incident command, hazard recognition, evacuation, decontamination)
(4) Increase the entity's general awareness and understanding of the hazards present
(5) Identify additional resources, equipment, or personnel needed to prepare for and respond to an incident

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 involve invoking response and operational continuity procedures, but 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 identify those issues that might arise, prior to a real invocation.

A.3.3.11 Incident. Over the past 50 years, social scientists have studied disasters and have concluded that disasters are both quantitatively and qualitatively different from day-to-day incidents or emergencies. For example, during disasters, responding entities are forced into more and different kinds of interactions with other groups and may lose some of their autonomy and direct control over their own functioning. Other differences include the crossing of jurisdictional boundaries; a more coordinated relationship among public and private sector entities becomes necessary, and, performance standards for responding entities change to reflect disaster-relevant priorities. (Source: *Major Criteria for Judging Disaster Planning and Managing and Their Applicability in Developing Societies*)

A.3.3.13 Incident Management System (IMS). The incident management system is based on proven management characteristics. Each management characteristic contributes to the strength and efficiency of the overall system.

A description of 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 predesignated 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. The span of control of any individual with incident management supervisory responsibility should range from three to seven subordinates. The type of incident, 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 and is necessary to maintain communications connectivity and discipline and to enable common situational awareness and interaction. Preparedness planning has to 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 responsible for establishing command. When command is transferred, the process must 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 allows agencies with different legal, geographic, and functional authorities and responsibilities to work together effectively without affecting individual agency authority, responsibility, or accountability.

A.3.3.16 Mutual Aid/Assistance Agreement. The term *mutual aid/assistance agreement,* as used herein, includes cooperative agreements, partnership agreements, memoranda of understanding, intergovernmental compacts, or other terms commonly used for the sharing of resources.

A.3.3.18 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 both to human-caused incidents (such as terrorism, vandalism, sabotage, or human error) and naturally occurring incidents. Prevention of human-caused incidents can include applying intelligence and other information to a range of activities that includes such countermeasures as deterrence operations; heightened inspections; improved 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. Naturally occurring incidents such as floods can be "prevented" from causing harm by prohibiting people from building structures in areas prone to flooding. While the flooding cannot be stopped, the impact is.

A.3.3.19 Recovery. Recovery programs are designed to assist victims and their families, restore institutions to suitable economic growth and confidence, rebuild destroyed property, and reconstitute government operations and services. Recovery actions often continue long after the incident itself. Recovery programs include mitigation components designed to avoid damage from future incidents.

A.3.3.20 Resource Management. Resource management is a system for identifying available resources at all jurisdictional levels to enable timely and unimpeded access to resources needed to prepare for, respond to, or recover from an incident. 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. See *ASTM WK* 1652, *Standard Guide for Resource Management in Emergency Management and Homeland Security.*

A.3.3.21 Response. The term *response* of an entity refers to the response of an entity to an incident or other significant event that might impact the entity. Activities, tasks, programs, and systems can include the preserving of life, meeting basic human needs, preserving business operations, and protecting property and the environment. An incident response can include evacuating a facility, 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 identify and have access to applicable legal, regulatory, and other requirements to which the organization subscribes that are related to the organization's hazards, threats, and risks that are associated with its facilities, activities, functions, products, services, and supply chain, the environment, and stakeholders. The way these requirements apply to its hazards, threats, and risks, and their potential impact should be determined. The organization 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 program coordinator titles. It is recognized that different entities

use various forms and names for their program coordinator who performs the functions identified in the standard. An example of a title for the public sector is *emergency manager,* and an example of a title for the private sector is *business continuity manager.* A written position description should be provided.

A.4.3 Professional qualifications for emergency managers and business continuity professionals can be found in the DRII *Professional Practices for Business Continuity Practitioners* and the CEM® program.

A.4.3.1 Mandating that an entity have a program committee will, in some cases, violate the authorities under which the emergency management entity is established. Those organizations that can have, or want to have, a program committee that will provide advice and guidance should be encouraged to do so.

Advisory committees are administrative and assist the program coordinator in developing administrative priorities and in developing pre-incident resource allocation priorities, and, while the program committee and the program coordinator should be in agreement concerning such priorities, the program coordinator should have the final authority in deciding the course of the program during day-to-day operations. The program committee is for administrative activities and, unless identified as having a functional role or responsibility during incidents, is not consulted.

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. These authorities set the agendas for emergency management activities, and a program committee might not be appropriate.

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

A.4.4(2) The 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.4.5.1 Industry codes of practices and guidelines should also be considered. In the private sector, corporate policy might be the directives that must be followed.

A.4.5.2 The entity should consider local cultural and religious customs when developing the 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 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 as 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, and additional authority could be required to create a standing contingency fund to adequately support an emergency operation.

In the private sector, the governing factors can be industry codes of practice or regulations rather than statutory restrictions. A process should be established for periodic review of industry practices for compliance with the strategy, goals, and objectives of the entity.

Evolving best practices should be incorporated in the public and private sectors as applicable.

A.4.6.1 Performance objectives should be established for all elements in the program and should be linked to human performance. Without well-written performance objectives, measurement of performance and evaluation, when the performance is compared to criteria to determine if the performance meets expectations, is impossible.

Performance objectives should contain the following four essential parts:

(1) *Performer.* Specific identification of which person will perform the expected behavior.
(2) *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 must 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.
(3) *Conditions.* Specific identification of the exact location, tools, the equipment worn, and so forth, will be part of the observable, measurable behavior.
(4) *Criteria.* Specific criteria that will be compared with the observed behavior to determine if the performance objectives have been achieved during the expected behavior.

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 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 performance meets expectations.

A.4.6.3 An example of a technique for the development of objectives would be to utilize the "SMART" process for writing objectives in ICS-300, *Intermediate ICS for Expanding Incidents,* as follows:

(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.4.6.4 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 who are responding and stabilizing the incident," while long-term objectives might include "prevent environmental damage" and "comply with regulatory requirements."

A.4.7 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 should be included as a member 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.4.7.8 The entity should consider negotiating contracts for resources in advance of an incident.

A.4.7.8(4) Existing internal controls could be impacted by the same event necessitating a response. This opens the door for opportunistic fraud as we have seen in almost every large-scale event. It is important that the entity recognize the possibility of fraud occurring during this window of opportunity and take reasonable precautions.

A.4.8 Financial and administrative procedures are designed to aid in the capture, classification, and ongoing management of records throughout their life cycle. Such a system might be paper-based or might be based in a computer system, such as an electronic records management application.

Records management practices should include the following activities:

(1) Creating, approving, and enforcing records 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 SOPs
(4) Coordinating the access and circulation of records within and outside of 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 The assumptions used in preparation of all plans, especially those regarding hazard identification, risk assessment, and impact analysis, should be identified, reviewed, and included at the start of the planning process. Confidential or sensitive information can be redacted or protected.

A.5.2.1 An entity should coordinate regional planning approaches with other entities to better leverage resources.

A.5.2.7 The safety and health of personnel are critical to the successful execution of the program. Thus, consideration of the safety and health aspects for the performance expected is the responsibility of all personnel, not just the leadership. When every person accepts and performs as if safety and health are their personal responsibility, performance under hazardous conditions will minimize exposure and reduce the probably of incidents that result in injuries or impairment of health.

The exposure caused by performance in proximity to hazardous conditions is managed, in the ideal situation, by removing the hazards, and as a result the exposure is eliminated. In multiple elements of the program, elimination of hazards is not feasible, and controls must be instituted.

Hazard Control

Assess and mitigate hazards according to the hierarchy of controls specified in the paragraphs that follow:

Elimination or Substitution. Whenever possible, eliminate the hazard from the work area (e.g., repair or remove 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.

Engineering Controls. Take steps to reduce or eliminate exposure to a hazard through the use (or substitution) of engineered machinery or equipment, such as by guarding the pinch points associated with a machine's moving parts, providing ventilation to a permit-required confined space, using heavy equipment with temperature-controlled cabs, and placing barriers around the swing radius of rotating heavy equipment.

Work Practice or Administrative Controls. Implement work procedures that reduce the duration, frequency, and severity of exposure. For example, use well-rested crews and daylight hours to perform higher hazard or unfamiliar tasks, take frequent breaks during hot weather, remove nonessential personnel from the area during certain task/operations, and decontaminate equipment and personnel after contact with contaminated floodwater or chemicals. When possible, use water to suppress dust and work upwind in dusty conditions. Where extensive hot work is performed in the form of cutting and burning, use extended-length torch handles to increase the distance from the user's breathing zone to the generation of toxic fumes.

The controls start with identification of the hazard and the vulnerability of people potentially exposed. Safety and health controls include training, safety procedures, personal protective equipment (PPE), observations, and enforcement of safe behavior.

The performance of a program element that results in injury or impairment of health can overshadow the purpose of the element. For example, if someone is hurt during an exercise, the focus of the exercise will become the actual injury, and the original purpose is lost.

IMSs have trained, designated incident safety officers but safety must be a paramount concern of every person involved. As past emergency response activities have demonstrated, it is important to share hazard- and exposure-monitoring data among response and recovery organizations.

Operations during recovery operations can be particularly hazardous. Due to the nature of the recovery, the normal operations have been disrupted and the hazards are probably uncontrolled. Cleanup work of any kind is hazardous. Procedures and training are needed to help ensure safe performance of those engaged in cleanup after an incident.

Work conditions change drastically after hurricanes and other natural disasters. In the wake of a hurricane, response and recovery workers will face additional challenges, such as downed power lines, downed trees, and high volumes of construction debris, while performing an otherwise familiar task or operation.

Evaluate the work site to identify if safety or health hazards such as fall, electrocution, noise, and cut/laceration hazards; high ambient temperatures; hazardous substances; or infectious materials are present. As appropriate, conduct task-specific exposure monitoring during response and recovery activities.

Occupational exposure levels are set to protect employees from the short-term and long-term harmful health effects that might be associated with chemical (e.g., vapors, particulates, fibers) and physical (e.g., heat, noise, vibration) agents. Exposure limits can be expressed as 8-hour time-weighted averages, or can be expressed as shorter exposures, such as ceiling levels or 15-minute short-term exposure levels.

Occupational exposure levels should be determined when it is necessary to assess and evaluate specific employee exposure, investigate and resolve employee complaints or concerns, or to verify the adequacy of the implemented hazard control methods.

When problems are determined, corrective action should be aggressive and complete but should be carefully considered so as not to create a new set of hazards.

Personal Protective Equipment (PPE). If hazards cannot be engineered or administratively controlled, shield or isolate individuals from the chemical, physical, and biological hazards that might be encountered 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.

Engineering controls, administrative controls, and PPE are not mutually exclusive. Entities might need to use multiple types of controls to prevent employee overexposure.

A.5.2.8 Many entities have written one or more plan documents that comprise their program. 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 this section 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 they meet the needs of the entity.

A.5.2.9 Distributing plans internally or to key stakeholders could require an entity to exercise safeguards like obtaining confidentiality or nondisclosure agreements.

A.5.3 The entity should engage in regional planning, and it should be noted that most entities engage in multiple planning activities (e.g., mitigation and land use planning). 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 objectives, results of the hazard analysis, organizational culture and philosophy, and regulations.

A.5.3.1 Table A.5.3.1 is a cross-reference to the requirements of *NFPA 1600,* DRII *Professional Practices for Business Continuity Practitioners,* and CSA Z1600, *Emergency Management and Business Continuity Programs.*

A.5.3.2 Key program elements cross boundaries during prevention, mitigation, preparedness, response, continuity, and recovery. Each element should be considered interrelated and can be considered concurrently. The use of the terms *phases*, *elements*, or *components* varies from program to program.

A.5.4 A comprehensive risk assessment identifies the range of possible hazards, threats, or emergencies that have impacted or might impact the entity, surrounding area, or critical infrastructure supporting the entity. The potential impact of each hazard, threat, or emergency is determined by the severity of each and the vulnerability of people, property, operations, the environment, and the entity to each threat, hazard, or emergency. The risk assessment should categorize threats, hazards, or emergencies by both their relative frequency and severity, keeping in mind that there might be many possible combinations of frequency and severity for each. The entity should attempt to prevent, mitigate, prepare for, plan to respond to, and plan to recover from those threats, hazards, or emergencies that are able to significantly impact people, property, operations, the environment, or the entity itself.

Risk assessment is a process for identifying hazards and their relative probability of occurrence, identifying assets at risk, assessing the vulnerability of the assets at risk by the identified hazards, and quantifying the potential impact of the hazard on the assets. Many potential hazards should initially be assessed and a periodic reassessment is needed, as the entity and hazards will change over time.

This process should also include a business impact analysis (BIA) to identify critical business functions and the impact of losing those functions.

Information from the risk assessment and the BIA will help determine priorities for prevention and mitigation activities as well as prioritize development of plans and procedures.

A.5.4.1 A number of methodologies and techniques for risk assessment exist that range from simple to complex. These techniques and associated amplifying information include but are not limited to those specified in items (1) through (6), which follow:

(1) *What-If.* The purpose of the "what-if" analysis is to identify specific hazards or hazardous situations that could result in undesirable consequences. This technique has limited structure but relies on knowledgeable individuals who are familiar with the areas/operations/processes. The value of the end result is dependent on the team and the exhaustive nature of the questions they ask regarding the hazards.
(2) *Checklist.* A specific list of items is used to identify hazards and hazardous situations by comparing the current or projected situations with accepted standards. The value of the end result is dependent on the quality of the checklist and the experience/credentials of the checklist user.

Table A.5.3.1 ***NFPA 1600*, DRII Professional Practices, and CSA Z1600 Cross-Reference**

***NFPA 1600*-2010 Chapter/Section**	**DRII *Professional Practices for Business Continuity Practitioners*, 2008 Subject Area**	**CSA Z1600-08 *Emergency Management and Business Continuity Programs* Chapter/Section**
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	9. Crisis Communications 10. Coordinating with External Agencies	4.5 Laws and Authorities
4.6 Performance Objectives	1. Project Initiation and Management	4.4.3 Program Goals and Objectives
4.7 Finance and Administration	1. Project Initiation and Management	4.6 Financial Management
4.8 Records Management	BIA (B.2.f.)	4.4.6 Records management
5.1 Planning Process	2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plans	5.2 Planning Process
5.2 Common Plan Requirements	2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plans 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications	5.3 Common Plan Requirements
5.3 Planning and Design	1. Project Initiation and Management 2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Response and Operations 6. Business Continuity Plans	5. Planning
5.4 Risk Assessment	5. Risk Evaluation and Control	5.1 Hazard Identification, Risk Assessment, and Business Impact Analysis
5.5 Business Impact Analysis	3. Business Impact Analysis	5.1.3 Business Impact Analysis
5.6 Prevention	2. Risk Evaluation and Control	6.1.2 Prevention
5.7 Mitigation	2. Risk Evaluation and Control	6.1.3 Mitigation
6.1 Resource Management	1. Project Initiation and Management 3. Business Impact Analysis 6. Business Continuity Plans	6.2 Resource Management
6.2 Mutual Aid/Assistance	4. Business Continuity Strategies [B.2.f (iv)]	6.3 Mutual Aid/Mutual Assistance
6.3 Communications and Warning	5. Emergency Preparedness and Response 9. Crisis Communications	6.6 Communications and Warning

Table A.5.3.1 *Continued*

NFPA 1600-2010 Chapter/Section	DRII *Professional Practices for Business Continuity Practitioners*, 2008 Subject Area	CSA Z1600-08 *Emergency Management and Business Continuity Programs* Chapter/Section
6.4 Operational Procedures	5. Emergency Preparedness and Response 6. Business Continuity Plans 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications	6.7 Operational Procedures
6.5 Emergency Response	5. Emergency Preparedness and Response	6.4 Emergency Response
6.6 Employee Assistance and Support	5. Emergency Preparedness and Response (B.1.b ii, B.2.a)	
6.7 Business Continuity and Recovery	4. Developing Business Continuity Strategies 6. Developing and Implementing Business Continuity Plans	6.10 Business Continuity
6.8 Crisis Communications and Public Information	9. Public Relations and Crisis Coordination	6.6.7 Crisis Communications Capability 6.6.5 Public Awareness
6.9 Incident Management	5. Emergency Preparedness and Response	6.5 Incident Management
6.10 Emergency Operations Centers	5. Emergency Preparedness and Response	6.8 Facilities
6.11 Training and Education	7. Awareness and Training Programs	6.9 Training
Chapter 7 Testing and Exercises 7.1 Entity Evaluation 7.2 Exercise Evaluation 7.3 Methodology 7.4 Frequency 7.5 Exercise Design	8. Business Continuity Plan Exercise, Audit and Maintenance	Chapter 7 Exercises, Evaluations, and Corrective Actions
Chapter 8 Program Improvement	8. Business Continuity Plan Exercise, Audit and Maintenance	8.2 Continuous Improvement 7.4 Corrective Action
8.1 Program Reviews	8. Exercising and Maintaining Business Continuity Plans	
8.2 Corrective Action	8. Business Continuity Plan Exercise, Audit and Maintenance	7.4 Corrective Action

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

(3) *What-If/Checklist.* This technique is a combination of the what-if and checklist techniques and uses the strength of both techniques to complete the risk assessment. The what-if questions are developed, and the checklist(s) is to encourage the creativity of the what-if process, as well as to fill in any gaps in the process of developing questions. The value of the end result is dependent on the team and the exhaustive nature of the questions they ask regarding the hazards.

(4) *Hazard and Operability Study (HAZOP).* This technique requires an interdisciplinary team that is very knowledgeable of the areas/operations/processes to be assessed. This approach is thorough, time consuming, and costly. The value of the end result depends on the qualifications and experience of the team; the quality of the reference material available; the ability of the team to function as a team; and strong, positive leadership.

(5) *Failure Mode and Effects Analysis (FMEA).* Each element in a system is examined individually and collectively to determine the effect when one or more elements fail. This is a bottom-up approach; that is, the elements are examined and the effect of failure on the overall system is predicted. A small interdisciplinary team is required. This technique is best suited for assessing potential equipment failures. The value of the end result is dependent on the credentials of the team and scope of the system to be examined.

(6) *Fault-Tree Analysis (FTA):* This is a top-down approach where an undesirable event is identified and the range of potential causes that could lead to the undesirable event

is identified. The value of the end result is dependent on the competence in using the FTA process, on the credentials of the team, and on the depth of the team's analysis.

While any of the six techniques will identify the initial hazards that could affect the entity, consideration must also be given to those secondary hazards or cascading events that will occur that could cause additional impact to the entity. As an example, drought in the area which, on the surface, would cause concerns to those involved in agriculture, will also cause expansion of soils that can lead to failure of underground utilities such as water, electric, and communications systems.

A.5.4.2 The entity shall have a system to monitor the identified hazards and adjust the level of preventative measures to be commensurate with the risk.

A.5.4.2.1 The hazard identification should include the types of potential hazards that follow in items (1) through (3). This list is not all-inclusive but reflects the general categories that should be assessed in the hazard identification.

(1) Naturally occurring hazards that can occur without human influence and have potential direct or indirect impact on the entity (people, property, environment), such as the following:
   (a) Geological hazards (not including asteroids, comets, meteors), as follows:
      i. Earthquake
      ii. Tsunami
      iii. Volcano
      iv. Landslide, mudslide, subsidence
      v. Glacier, iceberg
   (b) Meteorological hazards, as follows:
      i. Flood, flash flood, seiche, tidal surge
      ii. Drought
      iii. Fire (forest, range, urban, wildland, urban interface)
      iv. Snow, ice, hail, sleet, avalanche
      v. Windstorm, tropical cyclone, hurricane, tornado, water spout, dust storm or sandstorm
      vi. Extreme temperatures (heat, cold)
      vii. Lightning strikes
      viii. Famine
      ix. Geomagnetic storm
   (c) Biological hazards, as follows:
      i. Emerging diseases that impact humans or animals [plague, smallpox, anthrax, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), pandemic disease, bovine spongiform encephalopathy (BSE, or mad cow disease)]
      ii. Animal or insect infestation or damage
(2) Human-caused events, such as the following:
   (a) Accidental hazards, as follows:
      i. Hazardous material (explosive, flammable liquid, flammable gas, flammable solid, oxidizer, poison, radiological, corrosive) spill or release
      ii. Explosion/fire
      iii. Transportation accident
      iv. Building/structure collapse
      v. Energy/power/utility failure
      vi. Fuel/resource shortage
      vii. Air/water pollution, contamination
      viii. Water control structure/dam/levee failure
      ix. Financial issues, economic depression, inflation, financial system collapse
      x. Communications systems interruptions
      xi. Misinformation
   (b) Intentional hazards, as follows:
      i. Terrorism (explosive, chemical, biological, radiological, nuclear, cyber)
      ii. Sabotage
      iii. Civil disturbance, public unrest, mass hysteria, riot
      iv. Enemy attack, war
      v. Insurrection
      vi. Strike or labor dispute
      vii. Disinformation
      viii. Criminal activity (vandalism, arson, theft, fraud, embezzlement, data theft)
      ix. Electromagnetic pulse
      x. Physical or information security breach
      xi. Workplace/school/university violence
      xii. Product defect or contamination
      xiii. Harassment
      xiv. Discrimination
(3) Technologically caused events that can be unrelated to natural or human-caused events, such as the following:
   (a) Central computer, mainframe, server, software, or application (internal/external) hazards
   (b) Ancillary support equipment hazards
   (c) Telecommunications hazards
   (d) Energy/power/utility hazards

A.5.4.3 The impact analysis (IA), sometimes called a business interruption study (BIS), provides an assessment of how key disruption risks could affect an entity's operations and identifies capabilities that are required to manage them.

The Process

An impact analysis can be undertaken using engineering analysis, mathematical modeling, the stochastic process, simulations, surveys, questionnaires, interviews, structured workshops, or combinations thereof, to obtain an understanding of the critical processes, people/personnel, assets and resources, physical and non-physical properties, and the financial and operational effects of the loss of these elements, as well as the required recovery time frames and supporting resources.

The key steps are as follows:

(1) Based on the risk and vulnerability assessment, confirm the key processes and outputs of the organization to determine the criticality of the processes.
(2) Determine the consequences of a disruption of the identified critical processes in financial or operational terms, or both, over defined periods.
(3) Identify the interdependencies with key internal and external stakeholders, which could include mapping the nature of the interdependencies through the supply chain.
(4) Determine the current available resources and the essential level of resources required to continue to operate at a minimum acceptable level following a disruption.
(5) Identify ways to bypass problems ("workarounds") in processes currently in use or planned to be developed. Alternate processes might need to be developed where resources or capability are inaccessible or insufficient during the disruption.

(6) Determine the maximum acceptable down time (MAD) [or maximum acceptable outage time (MAO)] for each process, based on the identified consequences and the critical success factors for the function. The MAD (MAO) represents the maximum period of time the organization can tolerate the loss of capability.
(7) Confirm the current level of preparedness of the critical processes to manage a disruption. This might include evaluating the level of redundancy within the process (e.g., spare equipment) or the existence of alternate suppliers.

Outputs

The outputs are as follows:

(1) Financial impact to the organization or entity due to the particular risk needed to be mitigated, minimized, prevented, or avoided; therefore, cost justification made based on amount of impact determined
(2) Operational impact, including upstream and downstream operations and dependencies or cascading impact, or both, both internal and external to the entity
(3) Priority list of critical processes and associated interdependencies
(4) Documented financial and operational impacts from loss of the critical processes
(5) Supporting resources required for identified critical processes
(6) Outage timeframes for critical process and associated information and communication technologies (ICT) recovery time frames

The IA is a broad description and quantification of a potential event that can impact an entity. This analysis should provide a clear idea of the hazards that are most likely to occur; which entity facilities, functions, or services are affected, based on their vulnerability to a particular hazard; which actions will most effectively protect such facilities, functions, or services; and the potential impact on the entity in quantifiable terms.

Within the IA, the entity should consider the impact external to its area of influence that can affect the entity's ability to cope with an incident. One example is the cascade effect of a hurricane. Direct impact can include wind and flood damage. Secondary impact can include communications, power, and transportation disruptions, both inside and outside the direct impact area, and the potential impact on the entity in quantifiable terms.

Within the IA, the entity should also consider the following:

(1) Health and safety of persons in the affected area at the time of the incident (injury and death)
(2) Health and safety of personnel responding to the incident
(3) Continuity of operations

A.5.4.3(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 should also be given to situations that cause the entity to become incapable of response or be incapable of maintaining any continuity of operations for the foreseeable future.

A.5.4.3(4) Assets include data, information, vital records, patents, intellectual property, and institutional knowledge.

A.5.4.3(8) An economic and financial impact analysis allows the quantification of the impact without considering the cause of the incident. This analysis is closely related to the process of identifying essential or critical functions or processes and helps decide where to place the emphasis in planning efforts.

A.5.4.4 It is important to consider the regional, national, or international implications of a hazard's impact on a community, such as in New York City. A hazard that affects the New York Stock Exchange will have national and international impact that should be considered.

Cascading impacts are events following the primary hazard occurrence. An example would be a tornado that creates a power outage leading to the inability to dispense fuel thus curtailing transportation due to the lack of fuel for motor vehicles.

A.5.5 The overall goal of a BIA is to understand that if a business function failed, the impact that would that have on the overall operation of the entity.

The Process

The functional BIA is not based on any specific hazard or risk. The idea is to understand the impact that business function failure would have on the overall operation of the corporation or organization.

The analysis should consist of following two components:

(1) Understanding the business purpose and process by conducting the business process analysis (BPA), which identifies the lines of process flow (i.e., material flow, information flow, people movement, cash flow) and time constraints. This activity simply forces the planner to understand the reason for the existence of the company and the value proposition of its various departments toward that end. Typical output of the BPA analysis will provide, at a minimum, an interdepartmental process flow chart or map for an entire organization, identifying external dependencies.
(2) Understanding the high-level business interruption potentials by conducting the BIS, which identifies and describes the potential bottlenecks, upstream and downstream supply chains for single points of failure, long lead time or imported equipment, single-source and sole-source suppliers, time constraint processing (i.e., long batch time), and identifying interdependencies between internal and external entities and facilities. The BIS will also assist the planner in determining the existing vulnerabilities and the resiliency (i.e., level of redundancy) of the organization. This analysis can be assessed at multiple levels of complexity. The intent of the BIS is to depict the propagation of interruption through the business processes. It is recommended that the BIS initially be performed at two levels, which can be defined as follows:
    (a) Global dependencies, which are the dependencies between an organization's multiple facilities and external entities and are assessed to determine the propagation of interruptions. This study looks at the potential loss of a single facility and determines the impact to the overall corporation or organization. This facility might be a single building on a campus or a single site within a regional disaster. The BIS determines how this loss will impact the other facilities.
    (b) Inter-departmental dependencies, which are dependencies between departments and are assessed to determine the internal propagation of interruptions. By looking at the critical interdepartmental processes identified in the BPA, the BIS will analyze further to discover the critical components or critical pieces of equipment, information, utilities, infrastructure, vital records, or people that can impact the entire operation of the facility if interrupted.

(c) Upon the completion of the BPA and BIS, the planner can start using the necessary information and organizational knowledge to determine the impact of interruption(s) on the mission of the organization. Based on the available BPA/BIS business process knowledge, the BIA will assist the planner in determining individual recovery time objective (RTO) or MAD. The definition of these recovery objectives, in turn, defines the department/business unit prioritization within the organization. A typical analysis will include questions related to the following:

i. Understanding the operational impact and financial impact to the organization if the department or function fails to perform
ii. The seasonality impact profile
iii. Time-sensitive critical impact
iv. Amount of critical work backlog
v. Recovery resources and technology resources that are critical for department function and the escalation of these resources over time
vi. Whether any stand-alone personal computers or legacy equipment need to be considered for recovery
vii. Number of recovery resources and the escalation of the need for these resources over time, such as workstations; local area networks (LANs); storage area network (SAN); server, network and telecommunications infrastructure support; and so forth
viii. Any documented process bypass procedures
ix. Work-at-home possibilities
x. Workload shifting to other mutual aid facilities or entities (internal and external)
xi. Vital business records and time requirements
xii. Regulatory reporting with time constraints
xiii. Description of material/work inflows and material/work outflows to other entities, internal and external
xiv. Any previous business disruption experience
xv. Any known competitive issues analysis

Recovery objectives should also include consideration of the following:

(1) Physical, operational, and financial impact. For example, the currency exchange rate fluctuation, legal ramifications of import/export law changes, money transfer law changes, environmental law changes, and so forth, should also be considered.
(2) The results might be quantifiable or might be qualified on an ordinal scale.
(3) It must be as certain that the comparison of recovery objectives is done from the same perspective and assumptions; that is, comparing apples to apples, not apples to oranges.

Outputs

The outputs of functional BIA are as follows:

(1) Financial, operational, and other nontangible impacts to the organization from a worst-case failure of a department or function, or both
(2) Identification of all critical functions and their critical resources requirements
(3) Prioritized critical business units and functions recovery
(4) Understanding of the seasonal impact to operations for each business unit and function
(5) Determination of resources (people, vendors, equipment, data/information, funding, and time) required for resumption and recovery and their escalation sequence for deployment over time
(6) MAD and RTO for each business unit and function

The output information will help to achieve the following:

(1) Identify the company's mission critical operations.
(2) Identify the company's time-critical operations.
(3) Determine the MAD for each critical operation (both time critical and mission critical).
(4) Determine the interdependencies with internal business units and external units, upstream and downstream, between other facilities and the facility being analyzed, and between other companies both on the supply side and the customer side.
(5) Determine the recovery strategies and course of action, alternatives and repair/replace, as well as possible contingency plan for each critical operation if the operation ceases to function.
(6) Determine those functions that cannot be non-functional at any time or that have a recovery time objective of zero, thus requiring a mirrored or fail-over operation.

A.5.5.3 The recovery time objective is the period of time within which systems, applications, or functions must be recovered after an outage (e.g., one business day). RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether to implement the recovery strategies during a disaster situation.

A.5.5.4 The recovery point objective is the point within a data flow that will be used as a base to begin the recovery of data back to the state at the time of disruption. The gap between the recovery point objective and the state at the time of disruption equals the data loss sustained during the incident.

A.5.6.1 The prevention strategy should include the following:

(1) Deterrence operations (e.g., patrols inside and outside of facilities) and increased inspections of vehicles entering the facility or background checks of personnel, or both
(2) Provision of protective systems or equipment for physical or cyber risks [i.e., perimeter fence line and gates, access control systems, increased camera surveillance, intruder detection systems (motion-sensing cameras, infrared detectors)]
(3) Immunizations, isolation, or quarantine
(4) Threat assessment documentation
(5) 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.

A.5.6.2 Techniques to consider in a prevention strategy include the following:

(1) Ongoing hazard identification
(2) Threat assessment
(3) Risk assessment
(4) Impact analysis
(5) Program assessment
(6) Operational experience
(7) Ongoing incident analysis
(8) Information collection and analysis
(9) Intelligence and information sharing

An IA could include a cost benefit analysis. The cost benefit analysis should not be the overriding factor in establishing a prevention strategy.

A.5.7.1 The mitigation strategy should include the following:

(1) Explanation of hazard and vulnerability
(2) Quantified risk if unmitigated
(3) Strategy for mitigation project development
(4) Anticipated cost
(5) Anticipated benefit
(6) Cost benefit analysis
(7) Prioritization of projects
(8) Project time line
(9) Resources required
(10) Funding mechanism

A.5.7.2 The mitigation strategy should 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 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.5.7.3 The mitigation strategy should establish interim and long-term actions to reduce the severity of potential impacts from hazards.

A.6.1 The five key principles that underpin effective resource management are as follows:

(1) *Advance Planning.* Entities work together in advance of an incident to develop plans for managing and employing resources in a variety of possible circumstances.
(2) *Resource Identification and Ordering.* Entities use standardized processes and methodologies to order, identify, mobilize, dispatch, and track the resources required to support incident management activities.
(3) *Categorizing Resources.* Resources are categorized by size, capacity, capability, and skill.
(4) *Use of Agreements.* Mutual aid/assistance agreements and pre-incident agreements among all entities providing or requesting resources are necessary to enable effective and efficient resource management during incidents.
(5) *Effective Management of Resources.* Resource managers use validated practices to perform the following key resource management tasks systematically and efficiently:
    (a) Acquisition procedures. Used to obtain resources to support operational requirements.
    (b) Management information systems. Used to collect, update, and process data; track resources; and display their readiness status.
    (c) Ordering, mobilization, dispatching, and demobilization protocols. Used to request resources, prioritize requests, activate and dispatch resources to incidents, and return resources to normal status.

To the extent practical and feasible, an entity should type resources according to established definitions.

A resource should be available in a timely manner and should have the capability to perform its intended function.

Restriction on the use of the resource should be taken into account, and application of the resource should not incur more liability than would failure to use the resource. Finally, the cost of the resource should not outweigh the benefit.

A.6.1.1 A resource needs assessment should be done based on the hazards present and should be tied directly to the overall performance objectives established to deal with those hazards.

A.6.1.2(1) The assessment might include "credentialing," which addresses the question of 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.6.1.3 All program equipment should be checked and tested on a regularly scheduled basis to ensure it will function properly when required. This includes vehicles, PPE, radio, information technology equipment, and warning and alerting devices and equipment including sirens, special emergency response equipment, and so forth.

A.6.1.4 Resources for program administration, as well as emergency operations, should be specifically identified. Resources might be pre-positioned to expedite deployment. These resources 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, volunteer organizations, emergency management staff, utility workers, morticians, and private contractors)
(11) Employee and family assistance
(12) Specialized volunteer groups [Red Cross, amateur radio, religious relief organizations, charitable agencies, volunteer organization active in disaster (VOAD), community organization active in disaster (COAD), community emergency response team (CERT)]
(13) External entities at all levels of governance

A.6.2 Mutual aid/assistance agreements between entities are an effective means to obtain resources and should be developed whenever possible. Mutual aid/assistance 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.

Mutual aid/assistance 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 a mutual aid/assistance 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 all neighboring or nearby entities, as well as relevant private sector and nongovernmental organizations. States should participate in interstate compacts and look to establish intrastate agreements that encompass all local entities. Mutual aid/assistance agreements are also needed with private organizations, such as the International Red Cross, to facilitate the timely delivery of private assistance at the appropriate entity level during incidents.

A.6.2.3 Mutual aid/assistance agreements should include the following elements or provisions:

(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.6.3 The organization should create a basic communications structure and make it flexible enough to expand to fit the needs of the individual 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. For specific information on communications and warning and emergency public information, see Section 6.3 as well as pages 168, 169, 175, 178 of *Implementing NFPA 1600 National Preparedness Standard*.

A.6.3.1 The entity should determine communications and warning needs based on its hazard identification and risk assessment process and preparedness plans, procedures, public education programs, and emergency information programs.

A.6.3.2 Entities should evaluate the need for alternative methods or redundant systems to overcome the failure or inadequacy of communications and warning capabilities.

A.6.3.3 Emergency communication, warning protocols, and procedures should identify the message content that needs to be sent, requested, and received between levels and functions of the entity and outside entities and identify the communication mechanisms (human, systems, tools, networks) to execute said communication.

A.6.3.5 Means of maintaining capability includes redundant or multiple systems. For specific information on communications and warning and emergency public information, see Section 6.3.

A.6.3.8 Key stakeholders may vary depending on the organization. Typical stakeholders for many organizations include the media, government, customers, employees, community, and investors.

A.6.4.2 Recovery planning for the public and private sector will normally bring the entity, infrastructure, and individuals back to pre-incident conditions, including implementation of mitigation measures, to facilitate short-term and long-term recovery.

The recovery plan should include the following:

(1) Critical infrastructure
(2) Telecommunications and cyber systems
(3) Distribution systems or networks for essential goods, or both
(4) Transportation systems, networks, and infrastructure
(5) Facilities
(6) Psychosocial services
(7) Health services
(8) Continuity of operations

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

(1) Vital personnel, systems, operations, records, and equipment identified in Section 5.6
(2) Priorities for restoration and mitigation
(3) Acceptable downtime before restoration to a minimal level
(4) Minimum of 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 volunteer, contractual, and entity resources
(4) Opportunities for mitigation

A.6.4.3 The term *property conservation* means minimizing property damage.

A.6.4.7 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. These include business continuity plans, business resumption plans, and disaster recovery plans. In addition, within the public sector, continuity of operations (COOP) plans might use BIA to identify critical governmental functions.

Business continuity planning in the private sector incorporates both the initial activities to respond to an emergency situation and the restoration of the business and its functions to pre-incident levels. As a result, there are differences and similarities between public sector recovery plans and private sector business continuity plans.

Specific areas to consider in continuity plans include the following:

(1) *Succession.* To ensure that the leadership will continue to function effectively under emergency conditions. When practical, there is a designation of at least three successors for each position. Provisions have been made to deal with vacancies and other contingencies, such as absence or inability to act.
(2) *Pre-Delegation of Emergency Authorities.* To ensure that sufficient enabling measures are in effect to continue operations under emergency conditions. Emergency authorities have been enacted that specify the essential duties to be performed by the leadership during the emergency period and that enable the leadership to act if other associated entities are disrupted, and to re-delegate with appropriate limitations.

A.6.5.1 The management functions of the IMS (command, operations, planning, logistics, and finance/administration) can be used to structure the emergency operations/response plan. This approach can improve understanding and effective use of both the IMS and emergency operations response plan.

Emergency action steps are actions that facilitate the ability of personnel to respond quickly and efficiently to incidents. Checklists, action lists, or SOPs, or both, have been written that identify emergency assignments, responsibilities, and emergency duty locations. Procedures should also exist for alerting, notifying, locating, and recalling key members of the entity. The SOPs and notification procedures should be integrated.

A.6.5.2 Special needs populations are populations whose members might have additional needs before, during, or after an incident in one or more of the following functional areas:

(1) Maintaining independence
(2) Communication
(3) Transportation
(4) Supervision
(5) Medical care

Individuals in need of additional response assistance might include those who have disabilities, including physical, mental health, development and learning, visual, auditory, or nonvisible disability; live in institutionalized settings; are elderly; are children; are from diverse cultures and have limited proficiency in local language; or are transportation disadvantaged.

A.6.6 Employee assistance and support might be called human continuity, human impact, workforce continuity, human aspects of business continuity, and so forth. Employee assistance and support is the ability to provide assistance and support to the entity's employees and their families/significant others affected by the incident.

A.6.6.1 Communications procedures are the method that the entity and its employees will use to inform employees of the program pre-event, and to inform employees that the program is activated and available post-event. The employee should notify the entity of the need for assistance through the communications system established. 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 business functions are interrupted at a site and staff have been sent home as well as 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 *(See pages 148–150 of Implementing NFPA 1600 National Preparedness Standard for more information.)*

There are situations where customers, vendors, and other parties might be located at the entity's facility and the program should include the ability to provide assistance.

A.6.6.1(2) The entity should develop policies and procedures to store, retrieve, and control access of personal information when needed in an emergency situation, including systems to facilitate reunification of family members.

A.6.7.1 Key stakeholders from both internal and external entities should be considered.

Alternative operating or backup facilities. Provisions should also exist for alternative site(s) for departments or agencies having emergency functions or continuing operations.

Vital records. The measures that are taken by the entity to protect vital records (e.g., financial data, personnel records, and engineering drawings) that the entity should have in order to continue functioning during emergency conditions and to protect the rights and interests of the entity. Procedures have been put in place to ensure the selection, preservation, and availability of records essential to the effective functioning of the entity under emergency conditions and to maintain the continuity of operations. Protection of records should comply with applicable laws [Health Insurance Portability and Accountability Act (HIPAA) or other privacy laws].

Protection of resources, facilities, and personnel. The measures that are taken to deploy resources and personnel in a manner that will provide redundancy to ensure the entity can continue to function during emergency conditions. Plans and procedures are in place to ensure the protection of personnel, facilities, and resources so the entity can operate effectively. The entity should have the ability to allocate needed resources and restore functions during and after incidents. Plans should address deployment procedures to relocate/replicate resources or facilities, increase protection of facilities, and inform and train personnel in protective measures. Preparedness should be increased based on the threat level.

A.6.8 Risk communication is affected by the characteristics of the source, the message, the channel(s), and the characteristics of the receivers. Public response to warning messages has been extensively studied and there are several important dimensions to understand. First, the existence of myths that persist about disaster behavior that influences both senders and receivers, such as people will obey the advice of authorities, the public is immobilized by shock, they will panic, and so forth. Second, the choices of sources, channels, and messages will produce different effects on recipients, and recipients' receptivity varies with regards to the sources, channels, and messages. Third, warning messages are more likely to evoke timely and effective action if they create a perception of the threat as imminent and severe consequences. Fourth, protective actions are more likely to be taken if the recommended action does not involve large costs, significant time or effort, need for specialized knowledge, or cooperation with others. Fifth, if conflict exists between the messages of different sources, the result will be inaction. Research has also shown that family groups will try to re-unite prior to taking protective action. *(Adapted from Major Criteria for Judging Disaster Planning and Managing and Their Applicability in Developing Societies.)*

A.6.8.1 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. *(See Chapter 8 of Implementing NFPA 1600 National Preparedness Standard for more information.)* 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 should also be incorporated into the process to better ensure a two-way dialogue. This can be done through pamphlets, speaker's bureaus, the Internet, community meetings, newsletters, and other means. *(See page 178 of Implementing NFPA 1600 National Preparedness Standard for more information.)*

A.6.8.2 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. *(See Chapter 8 of Implementing NFPA 1600 National Preparedness Standard for more information.)* Information or tools that can be prepared in advance, such as prescripted 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. *(See pages 180–182 in Implementing NFPA 1600 National Preparedness Standard for more information on templates and the approval process.)*

A.6.8.2(1) 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. *(See pages 176–177 of Implementing NFPA 1600 National Preparedness Standard for more information.)*

A.6.9.1 An IMS would be used to systematically identify management functions assigned to various personnel. 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 IMS is designed to enable effective and efficient domestic incident management by integrating a combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure. It is normally structured to facilitate activities in five major functional areas: command, operations, planning, logistics, and finance and administration. See the definition of the term *incident management system* in 3.3.13 and additional information in A.3.3.13. The IMS should be based on proven management characteristics. Each management characteristic contributes to the strength and efficiency of the overall system.

An example of an approved IMS would be the National Incident Management System (NIMS), as used in the United States, or its equivalent in other countries.

A.6.9.2 An incident management system should be able to effectively manage multi-jurisdictional and multi-agency events by the following means:

(1) Pre-event planning
(2) Integrating flexibility and scalability
(3) Designating clearly the roles and responsibilities, including command, lines of authority, and supporting roles
(4) Providing scalable communications systems, including common terminology
(5) Integrating risk management into the regular functions of incident management
(6) Implementing planning into every element of the system and the use of an IAP
(7) Implementing a strong logistics support system
(8) Providing finance/administrative services where necessary

Effectively managing resources from multiple sources includes record keeping, tracking assignments, deploying and demobilizing resources, designating facilities, implementing and maintaining accountability, and tracking.

A.6.9.5 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 with reliance on an IAP, which provides a coherent means of communicating the overall incident objectives in the contexts of both operational and support activities

The mission defines the current state of the entity, the vision establishes where the entity wants to be, and the goals are the broad statements of how the entity will accomplish both the mission and the vision. The goals might be short term and long term.

Goals are general guidelines designed to communicate the desired outcome and are not typically measurable but are broad statements of what the entity wants to accomplish. An example of a goal would be that the continuity of operation of the entity would not be interrupted as a result of an incident.

A.6.10 An emergency operations centers (EOC) is the physical location at which the coordination and support of incident management activities take place.

Facilities should be capable of accommodating any combination of essential representatives who are identified in the entity's plan. Facilities should have adequate work space, communications, and backup utilities and should meet other basic human needs for each representative.

EOCs should be organized by major functional discipline services, by jurisdiction, or by some combination of jurisdiction, function, or discipline. For complex incidents, EOCs should be staffed by personnel representing multiple jurisdictions, functional disciplines, and resources.

The physical size, staffing, and equipping of an EOC will depend on the size of the entity, resources available, and anticipated incident management support required. EOCs should be organized and staffed to provide coordination and support to the incident. The specific organizational structure used for the EOC should include, but not limited to, the following core functions:

(1) Coordination capabilities
(2) Communications that are reliable and redundant in capabilities
(3) Resource dispatching and tracking
(4) Information collection, analysis, and dissemination
(5) Joint information activities

EOCs can be permanent organizations and facilities or can be established to meet temporary, short-term needs.

The efficient functioning of the EOCs frequently depends on the existence of mutual aid/assistance agreements and joint communications protocols among participating agencies.

IMS field organizations should establish communications with the activated EOC, either directly or through their parent organizations.

A.6.10.1 Primary and alternative emergency operations centers are a facility or capability from which direction and control are exercised during an incident. This type of center or

capability is designated to ensure that the capacity exists for the leadership to direct and control operations from a centralized facility or capability in the event of an incident.

Other facilities might include alternative EOCs to ensure that facilities are available and located so that they are not impacted by the same event. This might also include department operations centers (DOCs), which focus on internal agency incident management and response and are linked to and, in most cases, are physically represented in a higher level EOC. Incident command posts (ICPs) should also be linked to DOCs and EOCs to ensure effective and efficient incident management.

An ICP located at or in the immediate vicinity of an incident site, although primarily focused on the tactical on-scene response, can perform an EOC-like function in smaller-scale incidents or during the initial phase of the response to larger, more complex events. EOCs, or those centers to support larger, more complex events, are established in a central or permanently established facility at a higher level of organization within a jurisdiction.

A.6.10.2 Virtual EOCs or DOCs capable of accomplishing the core functions might also meet the requirement.

A.6.11 Training addresses known knowledge, skill, and ability requirements while education addresses unknown knowledge, skill, and ability requirements.

A.6.11.1 A performance-based curriculum is a program based on competencies and implemented with goals, objectives, and references to be used to measure and evaluate compliance. The performance-based curriculum is implemented and ensures that specified goals and objectives are met. The curriculum allows for the use of equivalencies that demonstrate compliance. The following describes the instructional system design (ISD) use of a performance-based curriculum instructional design model, commonly known as ADDIE (Analysis Design Development Implementation Evaluation):

(1) Establish goals
(2) Analyze the current levels of performance and identify the desire levels
(3) Write performance objectives that include specific expected behavior, conditions under which the behavior is expected, and specific criteria for the behavior
(4) Design evaluation first and instruction and instructional strategies second
(5) Develop the instruction, including all learning support materials
(6) Implement the instruction
(7) Evaluate the learning
(8) Determine follow-up corrective action, if necessary

All personnel designated to perform specific task(s) should demonstrate competence to safely perform those tasks and meet the expected criteria identified in performance objectives. Competency-based performance is an accepted concept in public, private, and not-for-profit entities. One comprehensive definition of "competency" is: "A cluster of related knowledge, skills, and attitudes that affects a major part of one's job (a role or responsibility), that correlates with performance on the job, that can be measured against well-accepted standards, and that can be improved via training and development" (*Training*, July 1996). An "essential" competency is critical for an employee to perform safely, effectively meeting the criteria identified in the performance objective. Competencies are gained through a multitude of ways: life experience, formal education, apprenticeship, on-the-job experience, self-help programs, and training and development programs. All of these together might contribute to competence in performing a designated task.

A.6.11.7 Information that should be included in public outreach and awareness efforts include regulatory disclosures such as those required by the 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. See also A.6.8.

A.7.2 An exercise is an instrument used to train for, assess, practice, and improve performance in prevention, protection, response, and recovery capabilities in a risk-free 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.

Note: An exercise is also an excellent way to demonstrate community resolve to prepare for disastrous events.

(See U.S. Department of Homeland Security Exercise and Evaluation Program.)

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.

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 with other agencies 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 the plan or SOPs/standard operating guidelines (SOGs), or to test and validate recently changed procedures
(2) Improve the coordination between various response organizations, elected officials, and community support organizations
(3) Validate the training of the critical elements of response, (e.g., incident command, hazard recognition, evacuation, decontamination)
(4) Increase the entity's general awareness and understanding of the hazards present
(5) Identify additional resources, equipment, or personnel, needed to prepare for and respond to an incident

A.7.3 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 involve invoking response and operational continuity procedures, but 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 the issues that arise, prior to a real invocation.

Exercises should include, but not be limited to, tabletops, simulations, and full operational exercises. Exercises are generally divided into the three types specified in the paragraphs that follow.

Tabletop. The basic purpose of a tabletop exercise is to solve problems in a group discussion. This normally provides key individuals an opportunity to evaluate coordination, review plan, and SOP elements, and prepare for larger and more complex exercises. Tabletop exercises do not involve response personnel or equipment but are designed to allow for problem solving to occur through discussion. Each problem or element of the exercise must be given adequate time for discussion to allow for complete problem solution.

Functional. Functional exercises are a hands-on activity that is designed to evaluate a limited number of functions within the overall plan and does require the use of response personnel and equipment, as well as the coordination needed for those functions. Several functional exercises might be needed to test specific areas of the plan independently for appropriate evaluation.

Full-scale. Full-scale exercises are designed to physically test a major portion of the plan, bringing together the functional elements tested during the previous functional exercises. These exercises typically requires the activation of an EOC to coordinate the activities of all entities involved.

A.8.1 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.8.1.2 The program should be reviewed on a regularly scheduled basis, after the entity changes 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.8.1.3(5) Many emergency management entities and programs in both the public and private sector are supported in part by grants from government entities or private sources.

A.8.2 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 using the following three categories:

(1) Plan or SOPs revisions
(2) Training and exercises
(3) Equipment additions or modifications and facilities

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 do the following:

(1) Develop options for appropriate corrective action.
(2) Make recommendations for a preferred option.
(3) Develop an implementation plan, and include 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 should establish a change management process (i.e., a process involving all sectors of a 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.8.2.1 The corrective action program should include the following:

(1) Development of a problem statement that states the problem and identifies its impact
(2) Review of the past history 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 to 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 that level of authority that can resolve the problem
(8) Testing of the solution through exercising once the problem is solved

A.8.2.2 The appropriate corrective actions might not be taken due to budgetary or other constraints or will be deferred as a part of the long-range capital project. However, temporary actions might be adopted during the time it takes to fund and implement the desired option.

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 it must be used wisely and correctly, just as any tool should be used. 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).

Not all search engines are equally created; some are better than others. Often there is a tendency to use Google exclusively. Though Google is an excellent tool for researching the Internet, it is not the only search engine.

Search directories are not search engines. Do not let the similarity of the search fields mislead. When a search directory is used, an index handpicked by a human is used. Search engines search a database of the full text of web pages automatically harvested from the web pages available. When a search engine is used, the search is using 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 (directory.google.com)
(3) Infomine (infomine.ucr.edu)
(4) Internet Public Library (www.ipl.org)
(5) Librarians' Internet Index (lii.org)
(6) Open Directory (www.dmoz.org)
(7) Yahoo search (yahoo.com/dir)
(8) The WWW virtual library (vlib.org)
(9) BUBL Countries (bubl.ac.uk/link/world/index.html) (This is an extensive collection of Internet resources on countries.)
(10) InfoPlease Countries of the World (www.infoplease.com/countries.html) See also under InfoPlease in General Information. This source, as well as similar sources, such as the BBC Country Reports, will use the CIA World Factbook as a source for its information.
(11) The World Factbook, a handbook of economic, political, and geographic intelligence. Central Intelligence Agency (CIA) (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. The print version is published every year).

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

American Waterworks Association:
http://www.awwa.org/files/Utilities_Helping_Utilities.pdf

Congressional Research Service:
http://www.fas.org/irp/crs/RL32527.pdf

Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada:
http://www.csps-efpc.gc.ca/Research/publications/pdfs/crisis_e.pdf

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

Disaster Research Center: http://www.udel.edu/DRC/

EMAP:
http://www.wvdhsem.gov/Training/Assessing%20Public%20Awareness%20-%20final.pdf

Emergency Management and Civil Protection Act and Regulation (Ontario):
(http://www.search.e-laws.gov.on.ca/en/isysquery/8f3d252e-16c8-4764-ae6f-648f6147659a/2/frame/?search=browseStatutes&context

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

Emergency Risk Management Applications Guide (Australia):
(http://www.ema.gov.au/agd/EMA/rwpattach.nsf/VAP/(383B7EDC29CDE21FBA276BBBCE12CDC0)~Manual+05a.pdf/$file/Manual+05a.pdf

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

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

FEMA:
http://www.fema.gov/plan/gaheop.shtm

FEMA:
http://www.usfa.dhs.gov/downloads/pdf/publications/fa-197-508.pdf

Fire Marshal of Ontario:
http://www.ofm.gov.on.ca/english/FireProtection/munguide/04-05-12.asp

Florida Department of Education:
http://132.170.176.110/disasterPrep/prep.html#plan

Governor's Office of Emergency Services – California:
http://www.oes.ca.gov/Operational/OESHome.nsf/PDF/Emergency%20Managers%20Mutual%20Aid%20Guidance/$file/EMMAGuidance.pdf

Guide for All-Hazard Emergency Operations Planning (FEMA):
http://www.fema.gov/plan/gaheop.shtm

Hardened First Responder Facility (FEMA):
http://www.fema.gov/library/viewRecord.do?id=1782

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
Institute of Risk Management: Risk Management Standard (UK):
http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf
International Society for Performance Improvement
http://www.ispi.org/
Marin County, California — Office of Education:
http://mcoeweb.marin.k12.ca.us/emerprep/MCOE2008EmerPlan.doc
Mitigation Best Practices Search (FEMA):
http://www.fema.gov/mitigationbp/index.jsp
National Incident Management System (NIMS) page (FEMA):
http://www.fema.gov/emergency/nims/
Natural Hazards Research and Information Applications Center:
http://www.colorado.edu/hazards/
New York State Department of Health (EMS):
http://www.health.state.ny.us/nysdoh/ems/policy/89-02.htm
NIMS Resource Management (FEMA):
http://www.fema.gov/emergency/nims/mutual_aid.shtm
Pennsylvania Emergency Management Agency:
http://www.pema.state.pa.us/pema/cwp/browse.asp?a=205&bc=0&c=35245
Records Management Guide (National Archives):
http://www.archives.gov/records-mgmt/publications/agency-recordkeeping-requirements.html
Resource Management (Mutual Aid) (FEMA):
http://www.fema.gov/emergency/nims/rm/ma.shtm
Risk Management Standard (Australia):
http://www.riskmanagement.com.au/
State Emergency Management Committee (New South Wales Government):
http://www.emergency.nsw.gov.au/semc
University of Delaware:
http://www.udel.edu/DRC/current_projects/Severe%20Weather%20and%20Integrated%20Warning%20Systems.ppt#6
University of Toronto:
http://www.utoronto.ca/security/documentation/business_continuity/dis_rec_plan.htm
Washington Military Department, Emergency Management Division:
http://emd.wa.gov/plans/documents/MutualAidHandbook.pdf
Wildland Firefighting:
http://www.fireleadership.gov/toolbox/documents/SOPWorkbook.pdf
http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-35982721F5AA/0/SOP.pdf
Writing Guide for Standard Procedures (Homeland Security):
http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-35982721F5AA/0/SOP.pdf

Annex C Self Assessment for Conformity with *NFPA 1600*, 2010 Edition

C.1 Table C.1 shows a self-assessment tool that is intended to assist entities in determining conformity with the requirements of the standard. 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 indicate 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 2010 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) Policies, plans, and procedures to develop, implement and maintain the program (2) Resources to support the program (3) Reviews and evaluations to ensure program effectiveness (4) Correction of deficiencies				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
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 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 for, 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. 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, objectives, and method of program evaluation				
(3) Program plans and procedures that include the following: (a) Anticipated cost				
(b) Priority				
(c) Time schedule				
(d) Resources required				
(4) Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5.				
(5) Program budget and schedule, including milestones				
(6) Records management practices as required by Section 4.8				
4.5 Laws and Authorities. **4.5.1*** The program shall comply with applicable legislation, policies, regulatory requirements, and directives.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
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 Performance Objectives. **4.6.1*** The entity shall establish performance objectives for program requirements in accordance with Chapter 4 and program elements in accordance with Chapters 4 through 8.				
4.6.2 The performance objectives shall depend on the results of the hazard identification, risk assessment, and business impact analysis.				
4.6.3* Performance objectives shall be developed by the entity to address both short term and long term needs.				
4.6.4* The entity shall define the terms *short-term* and *long-term*.				
4.7 Finance and Administration. **4.7.1** The entity shall develop financial and administrative procedures to support the program before, during, and after an incident.				
4.7.2 There shall be a responsive financial management and administrative framework that complies with the entity's program requirements and is uniquely linked to response, continuity, and recovery operations.				
4.7.3 There shall be crisis management procedures to provide coordinated situation-specific authorization levels and appropriate control measures.				
4.7.4 The framework shall provide 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.				
4.7.5 The administrative process shall be documented through written procedures.				
4.7.6 The program shall be capable of capturing financial data for future cost recovery, as well as identifying and accessing alternative funding sources and managing budgeted and specially appropriated funds.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
4.7.7 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles and other fiscal policy.				
4.7.8* The procedures specified in 4.7.7 shall include the following: (1) Establishment and definition of responsibilities for the program finance authority, including its 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				
4.8 Records Management. **4.8.1** The entity shall develop a records management program				
4.8.2 Policies shall be created, approved, and enforced to address the following: (1) Records classification				
(2) Maintenance of confidentiality				
(3) Maintenance of integrity incorporating audit trail				
(4) Record retention				
(5) Record storage				
(6) Record archiving				
(7) Record destruction				
(8) Access control				
(9) Document control				
4.8.3 The entity shall apply the program to existing and newly created records.				
4.8.4 The entity shall develop and enforce procedures coordinating the access and circulation of records within and outside of the organization.				
4.8.5 The entity shall execute the records management program.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
Chapter 5 Planning **5.1 Planning Process.** **5.1.1*** The program shall follow a planning process that develops strategic, crisis management, prevention, mitigation, emergency operations/response, continuity, and recovery plans.				
5.1.2 Strategic planning shall define the vision, mission, and goals.				
5.1.3 Crisis management planning shall address issues that threaten the strategic, reputational, and intangible elements of the entity.				
5.1.4 The entity shall include key stakeholders in the planning process.				
5.2 Common Plan Requirements. **5.2.1*** Plans shall identify the functional roles and responsibilities of internal and external agencies, organizations, departments, and positions.				
5.2.2 Plans shall identify lines of authority.				
5.2.3 Plans shall identify lines of succession for the entity.				
5.2.4 Plans shall identify interfaces to external organizations.				
5.2.5 Plans shall identify the process for delegation of authority.				
5.2.6 Plans shall identify logistics support and resource requirements.				
5.2.7* Plans shall address the health and safety of personnel.				
5.2.8* Plans shall be individual, integrated into a single plan document, or a combination of the two.				
5.2.9* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.				
5.3 Planning and Design. **5.3.1*** The program shall include the requirements specified in Chapters 4 through 8, the scope of which shall be determined through an "all-hazards" approach, and the risk assessment.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
5.3.2* The program requirements shall be applicable to prevention, mitigation, preparedness, response, continuity, and recovery.				
5.4* Risk Assessment. **5.4.1*** The entity shall conduct a risk assessment in accordance with Section 5.4 to identify strategies for prevention and mitigation and to gather information to develop plans for response, continuity, and recovery.				
5.4.2* The entity shall identify hazards and monitor those hazards and the likelihood of their occurrence.				
5.4.2.1* Hazards to be evaluated shall include the following: (1) Natural hazards (geological, meteorological, and biological)				
(2) Human-caused events (accidental and intentional)				
(3) Technologically caused events (accidental and intentional)				
5.4.2.2 The vulnerability of people, property, the environment, and the entity shall be identified, evaluated, and monitored.				
5.4.3 The entity shall conduct an analysis of the impact of the hazards identified in 5.4.2 on the following: (1) Health and safety of persons in the affected area at the time of the incident (injury and death)				
(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				
(9) Regulatory and contractual obligations				
(10) Reputation of or confidence in the entity				
5.4.4* The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
5.5* Business Impact Analysis. **5.5.1** The entity shall conduct a business impact analysis (BIA).				
5.5.2 The BIA shall evaluate the potential impacts resulting from interruption or disruption of individual functions, processes, and applications.				
5.5.3* The BIA shall identify those functions, processes, and applications that are critical to the entity and the point in time when the impact(s) of the interruption or disruption becomes unacceptable to the entity.				
5.5.4* The BIA shall evaluate the potential loss of information and the point in time which defines the potential gap between the last backup of information and the time of the interruption or disruption.				
5.5.5 The BIA developed in 5.5 shall be used in the development of plans to support the program.				
5.5.6 The impact analysis required by 5.4.3 and the BIA required by 5.5 shall be permitted to be conducted in conjunction or separately.				
5.6 Prevention. **5.6.1*** The entity shall develop a strategy to prevent an incident that threatens life, property, and the environment.				
5.6.2* The prevention strategy shall be based on the information obtained from Section 5.4 and shall be kept current using the techniques of information collection and intelligence.				
5.6.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, impact analysis, program constraints, operational experience, and cost benefit analysis.				
5.6.4 The entity shall have a process to monitor the identified hazards and adjust the level of preventive measures to be commensurate with the risk.				
5.7 Mitigation. **5.7.1*** 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.				
5.7.2* The mitigation strategy shall be based on the results of hazard identification and risk assessment, impact analysis, program constraints, operational experience, and cost benefit analysis.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
5.7.3* The mitigation strategy shall include interim and long-term actions to reduce vulnerabilities.				
Chapter 6 Implementation **6.1* Resource Management.** **6.1.1*** The entity shall conduct a resource management needs assessment based on the hazards identified in 5.4.2.				
6.1.2 The resource management 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 liability connected with using the involved resources				
(3) Resources and any needed partnership arrangements essential to the program				
6.1.3* The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, materials, and facilities procured or donated to support the program.				
6.1.4* Facilities capable of supporting response, continuity, and recovery operations shall be identified.				
6.1.5 Resource management shall include the following tasks: (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 incident management system				
(4) Conducting contingency planning for resource deficiencies				
6.1.6 A current inventory of internal and external resources shall be maintained.				
6.1.7 Donations of human resources, equipment, material, and facilities shall be managed.				
6.2* Mutual Aid/Assistance. **6.2.1** The need for mutual aid/assistance shall be determined.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.2.2 If mutual aid/assistance is needed, agreements shall be established.				
6.2.3* Mutual aid/assistance agreements shall be documented in the program.				
6.3* Communications and Warning. **6.3.1*** The entity shall determine communications and warning needs, based on required capabilities to execute plans.				
6.3.2* Communications and warning systems shall be reliable, redundant, and interoperable.				
6.3.3* Emergency communications and warning protocols and procedures shall be developed, tested, and used to alert stakeholders potentially impacted by an actual or impending incident.				
6.3.4 Advisory and warning systems shall be integrated into planning and operational use.				
6.3.5* The entity shall develop and maintain the following capabilities: (1) Communications between the levels and functions of the organization and outside entities				
(2) Documentation of communications				
(3) Communications with emergency responders				
(4) Central contact facility or communications hub				
6.3.6 The entity shall establish, implement and maintain procedures to disseminate warnings.				
6.3.7 The entity shall develop procedures to advise the public, through authorized agencies, of threats to life, property, and the environment.				
6.3.8* The entity shall disseminate warning information to stakeholders potentially impacted.				
6.3.9 The entity shall document issued warnings.				
6.4 Operational Procedures. **6.4.1*** The entity shall develop, coordinate, and implement operational procedures to support the program and execute its plans.				
6.4.2* Procedures shall be established and implemented for response to and recovery from the impact of hazards identified in 5.4.2.				
6.4.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.4.4* 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				
6.4.5 Procedures shall include a situation analysis that incorporates a damage assessment and a needs assessment to identify resources to support activities.				
6.4.6 On activation of a local emergency operations center (EOC), communications and coordination shall be established between the incident management system (IMS) and the EOC.				
6.4.7 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.				
6.5 Emergency Response. **6.5.1*** Emergency operations/response plans shall assign responsibilities for carrying out specific actions in an emergency.				
6.5.2* The plan shall identify actions to be taken to protect people (including those with special needs), property, operations, and the environment and to provide incident stabilization.				
6.5.3 The plan shall include the following: (1) Communication and warning in accordance with Section 6.3				
(2) Crisis communication and public information in accordance with Section 6.8				
(3) Protective actions for life safety				
(4) Direction and control in accordance with Section 6.8				
(5) Resource management in accordance with Section 6.1 and 6.2				
(6) Donation management in accordance with Section 6.1.7				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.6* Employee Assistance and Support **6.6.1*** The entity shall develop a strategy for Employee Assistance and Support to include 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, 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				
6.6.2 The strategy shall be flexible for use in all incidents.				
6.7 Business Continuity and Recovery. **6.7.1*** The continuity plan shall identify stakeholders that need to be notified; critical and time-sensitive applications; alternative work sites; vital records, contact lists, processes and functions that must be maintained; and personnel, procedures, and resources that are needed while the entity is recovering.				
6.7.2 The recovery plan shall provide for restoration of functions, services, resources, facilities, programs, and infrastructure.				
6.8* Crisis Communications and Public Information **6.8.1*** The entity shall develop a plan and procedures to disseminate and respond to requests for pre-incident, incident, and post-incident information to and from the following: (1) Internal audiences including employees				
(2) External audiences including the media and special needs populations				
6.8.2* A capability shall be established and maintained to include the following: (1) Central contact facility				
(2) System for gathering, monitoring, and disseminating information				
(3) Procedures for developing and delivering coordinated messages				
(4) Pre-scripted information bulletins or templates				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
(5) Protocol to coordinate and clear information for release				
6.8.3* The entity shall establish a physical or virtual information center.				
6.9 Incident Management **6.9.1*** The entity shall develop an incident management system to direct, control, and coordinate response and recovery operations.				
6.9.2* The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function.				
6.9.3 The entity shall establish procedures and policies for coordinating mitigation, preparedness, response, continuity and recovery activities.				
6.9.4 The entity shall coordinate the activities specified in 6.9.3 with stakeholders in the mitigation, preparedness, response, continuity, and recovery operations.				
6.9.5* Emergency operations/response shall be guided by an incident action plan or management by objectives.				
6.10* Emergency Operations Centers (EOCs) **6.10.1*** The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations.				
6.10.2* The EOCs shall be permitted to be physical or virtual.				
6.11* Training and Education **6.11.1*** The entity shall develop and implement a training and education curriculum to support the program.				
6.11.2 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.				
6.11.3 The scope of the curriculum and frequency of instruction shall be identified.				

(continues)

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
6.11.4 Personnel shall be trained in the entity's incident management system and other components of the program to the level of their involvement.				
6.11.5 Records of training and education shall be maintained as specified in Section 4.8.				
6.11.6 The curriculum shall comply with applicable regulatory and program requirements.				
6.11.7* A public education program shall be implemented to communicate the following: (1) Potential hazard impacts				
(2) Preparedness information				
(3) Information needed to develop a preparedness plan				
Chapter 7 Testing and Exercises **7.1 Entity Evaluation.** The entity shall evaluate program plans, procedures, and capabilities through periodic testing and exercises.				
7.2* Exercise Evaluation. Exercises shall be designed to evaluate program plans, procedures, and capabilities.				
7.3* Methodology. Exercises shall provide a standardized methodology to practice procedures and interact with other entities in a controlled setting.				
7.4 Frequency. Testing and exercises shall be conducted on the frequency needed to establish and maintain required capabilities.				
7.5 Exercise Design. Exercises shall be designed to do the following: (1) Evaluate the program				
(2) Identify planning and procedural deficiencies				
(3) Test or validate recently changed procedures or plans				
(4) Clarify roles and responsibilities				
(5) Obtain participant feedback and recommendations for program improvement				
(6) Measure improvement compared to performance objectives.				
(7) Improve coordination between internal and external teams, organizations, and entities				
(8) Validate training and education				

Table C.1 *Continued*

NFPA 1600 Program Elements	Conforming	Partially Conforming	Nonconforming	Comments
(9) Increase awareness and understanding of hazards and the potential impacts of hazards on the entity				
(10) Identify additional resources and assess the capabilities of existing resources including personnel and equipment needed for effective response and recovery				
Chapter 8 Program Improvement **8.1 Program Reviews.** **8.1.1** The entity shall improve effectiveness of the program through management review of the policies, performance objectives, evaluation of program implementation, and changes resulting from preventive and corrective action.				
8.1.2* Reviews shall be conducted on a regularly scheduled basis, and when the situation changes to evaluate the effectiveness of the existing program.				
8.1.3 The program shall also be re-evaluated when any of the following occur: (1) Regulatory changes				
(2) Changes in hazards and potential impacts				
(3) Resource availability or capability changes				
(4) Organizational changes				
(5)* Funding changes				
(6) Infrastructure, economic, and geopolitical changes				
(7) Changes in products or services				
(8) Operational changes				
8.1.4 Reviews shall be conducted based on post-incident analyses, lessons learned, and operational performance.				
8.1.5* The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.8.				
8.1.6 Documentation, records, and reports shall be provided to management for review and follow-up.				
8.2* Corrective Action. **8.2.1*** The entity shall establish a corrective action process.				
8.2.2* The entity shall take corrective action on deficiencies identified.				

Annex D Management System Guidelines

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

D.1 This annex is an example of a type B management system guideline. To implement *NFPA 1600* as a Type A management requirement standard (*see ISO Guide 72, Guidelines for the Justification and Development of Management System Standards*), the implementation should be by directive from an authority having jurisdiction and criteria for each program element should be developed and approved by that same authority. Table D.1 provides a list of program elements and their location in the 2010 edition of *NFPA 1600*. This annex was developed using the same ISO guidance used by ISO/TC 223, *Societal Security*.

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

Table D.1 A Guide to Implementing the 2010 Edition of *NFPA 1600*

Program Elements	Location in *NFPA 1600*, 2010 Edition
1. Introduction	
1.1 Scope	1.1, 1.2, 1.3
1.2 Normative Reference	2.1, 2.3, 2.4
1.3 Terms and Definitions	3.1, 3.2, 3.3
1.4 General Principles	
2. Policy	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8
3. Planning	5.1, 5.2, 5.3, 5.4, 5.5, 5.6
4. Implement and Operation	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10
5. Performance Assessment	7.1, 7.2, 7.3, 7.4
6. Improvement	8.2
7. Management Review	8.1

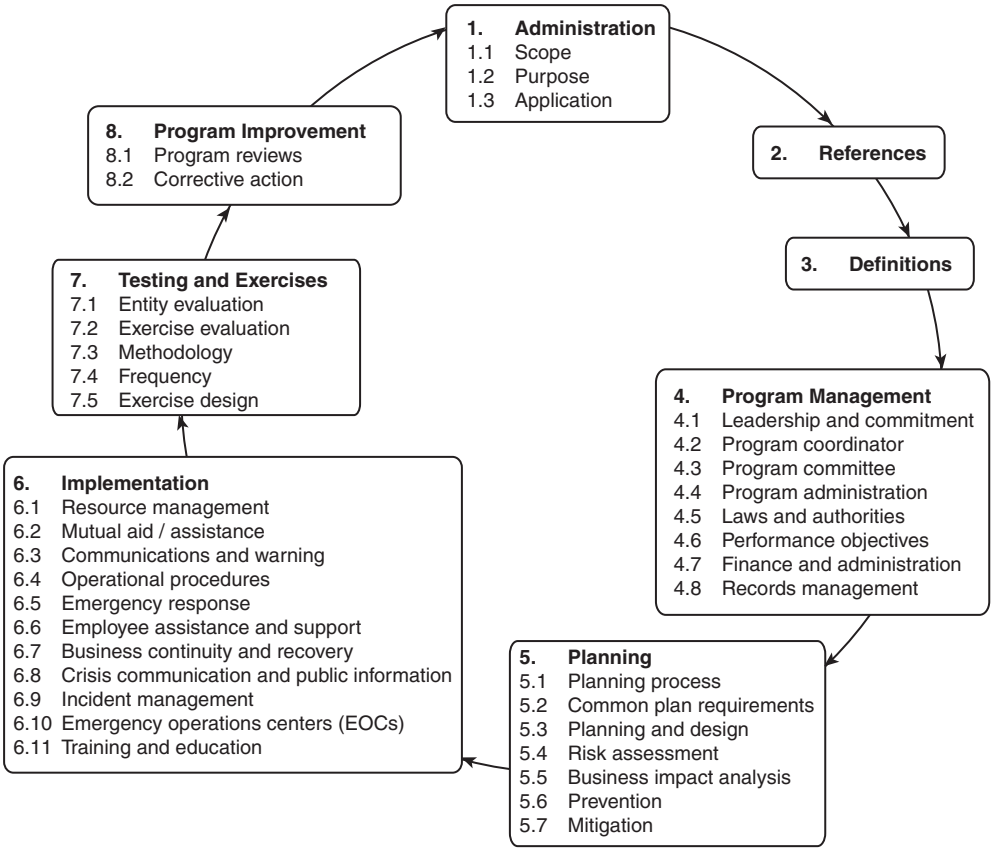

FIGURE D.1 The Plan-Do-Check-Act (PDCA) Cycle.

Annex E Informational References

E.1 Referenced Publications. The documents or portions thereof listed in this annex are referenced within the informational sections of this standard and are not part of the requirements of this document unless also listed in Chapter 2 for other reasons.

E.1.1 NFPA Publications. National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

Schmidt, Donald L. (editor), *Implementing NFPA 1600 National Preparedness Standard*, 2007.

E.1.2 Other Publications.

E.1.2.1 ASTM Publications. ASTM International, 100 Barr Harbor Drive, P.O. Box C700, West Conshohocken, PA 19428-2959.

ASTM WK 16252, *Standard Guide for Resource Management in Emergency Management and Homeland Security.*

E.1.2.2 CSA Publications. Canadian Standards Association, 5060 Spectrum Way, Mississauga, ON, L4W 5N6, Canada.

CSA Z1600, *Emergency Management and Business Continuity Programs*, 2008.

E.1.2.3 DRII Publications. DRI International, 1115 Broadway, 12th Floor, New York, NY 10010.

Professional Practices for Business Continuity Practitioners, 2008.

E.1.2.4 DHS Publications. DHS Integration Center, U.S. Department of Homeland Security, FEMA 500 C Street SW, Washington, DC, 20472.

NIMS DHS ICS-300, *Intermediate ICS for Expanding Incidents*, 2008.

E.1.2.5 ISO Publications. International Organization for Standardization, 1, ch. De la Voie-Creuse, Case postale 56, CH-1211 Geneva 20, Switzerland.

ISO Guide 72, *Guidelines for the Justification and Development of Management System Standards.*

ISO/TC 223, Societal Security.

E.1.2.6 U.S. Department of Homeland Security. U.S. Department of Homeland Security Exercise and Evaluation Program, Washington, DC., https://hseep.dhs.gov/pages/1001_HSEEP7.aspx

E.1.2.7 Other Publications.

Quarantelli, E.L. 1998. *Major Criteria for Judging Disaster Planning and Managing and Their Applicability in Developing Societies,* Newark, DE: Disaster Research Center, University of Delaware.

Training, July 1996.

E.2 Informational References. The following documents or portions thereof are listed here as informational resources only. They are not a part of the requirements of this document.

ARMA International, 11880 College Blvd, Suite 450, Overland Park, KS 66210.

ANSI/ARMA 5-2003. *Vital Records: Identifying, Managing, and Recovering Business-Critical Records, ARMA International*, 2003.

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

National Incident Management System (NIMS), http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

Contingency Planning Guide for Information Technology (IT) Systems, National Institute of Standards and Technology, NIST Special Publication 800-34, http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf.

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Recommendations of the National Institute of Standards and Technology, Special Publication 800-84, http://csrc.nist.gov/publications/nistpubs/800-84/SP800-84.pdf.

Building An Information Technology Security Awareness and Training Program, National Institute of Standards and Technology, Special Publication 800-50, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology, SP 800-100, http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf.

Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, SP 800-30, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf.

Generally Accepted Principles and Practices for Securing Information Technology Systems, National Institute of Standards and Technology, SP 800-14, http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.

An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, SP 800-12, http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.

"Emergency Preparedness for People with Disabilities," 2001.

Emergency Evacuation Planning Guide For People with Disabilities, National Fire Protection Association, http://www.nfpa.org/assets/files/PDF/Forms/EvacuationGuide.pdf.

People with disabilities, Online resources from the National Fire Protection Association, http://www.nfpa.org/categoryList.asp?categoryID=824.

Saving Lives: Including People with Disabilities in Emergency Planning, National Council on Disability Emergency Procedures for Employees with Disabilities in Office Occupancies, U.S. Fire Administration, http://www.ncd.gov/newsroom/publications/2005/saving_lives.htm

E.3 References for Extracts in Informational Sections. (Reserved)

Index

Sequence of Events Leading to Issuance of an NFPA Committee Document

Step 1: Call for Proposals

- Proposed new Document or new edition of an existing Document is entered into one of two yearly revision cycles, and a Call for Proposals is published.

Step 2: Report on Proposals (ROP)

- Committee meets to act on Proposals, to develop its own Proposals, and to prepare its Report.
- Committee votes by written ballot on Proposals. If two-thirds approve, Report goes forward. Lacking two-thirds approval, Report returns to Committee.
- Report on Proposals (ROP) is published for public review and comment.

Step 3: Report on Comments (ROC)

- Committee meets to act on Public Comments to develop its own Comments, and to prepare its report.
- Committee votes by written ballot on Comments. If two-thirds approve, Report goes forward. Lacking two-thirds approval, Report returns to Committee.
- Report on Comments (ROC) is published for public review.

Step 4: Technical Report Session

- "*Notices of intent to make a motion"* are filed, are reviewed, and valid motions are certified for presentation at the Technical Report Session. ("Consent Documents" that have no certified motions bypass the Technical Report Session and proceed to the Standards Council for issuance.)
- NFPA membership meets each June at the Annual Meeting Technical Report Session and acts on Technical Committee Reports (ROP and ROC) for Documents with "certified amending motions."
- Committee(s) vote on any amendments to Report approved at NFPA Annual Membership Meeting.

Step 5: Standards Council Issuance

- Notification of intent to file an appeal to the Standards Council on Association action must be filed within 20 days of the NFPA Annual Membership Meeting.
- Standards Council decides, based on all evidence, whether or not to issue Document or to take other action, including hearing any appeals.

Committee Membership Classifications

The following classifications apply to Technical Committee members and represent their principal interest in the activity of the committee.

M *Manufacturer:* A representative of a maker or marketer of a product, assembly, or system, or portion thereof, that is affected by the standard.

U *User:* A representative of an entity that is subject to the provisions of the standard or that voluntarily uses the standard.

I/M *Installer/Maintainer:* A representative of an entity that is in the business of installing or maintaining a product, assembly, or system affected by the standard.

L *Labor:* A labor representative or employee concerned with safety in the workplace.

R/T *Applied Research/Testing Laboratory:* A representative of an independent testing laboratory or independent applied research organization that promulgates and/or enforces standards.

E *Enforcing Authority:* A representative of an agency or an organization that promulgates and/or enforces standards.

I *Insurance:* A representative of an insurance company, broker, agent, bureau, or inspection agency.

C *Consumer:* A person who is, or represents, the ultimate purchaser of a product, system, or service affected by the standard, but who is not included in the *User* classification.

SE *Special Expert:* A person not representing any of the previous classifications, but who has a special expertise in the scope of the standard or portion thereof.

NOTES;
1. "Standard" connotes code, standard, recommended practice, or guide.
2. A representative includes an employee.
3. While these classifications will be used by the Standards Council to achieve a balance for Technical Committees, the Standards Council may determine that new classifications of members or unique interests need representation in order to foster the best possible committee deliberations on any project. In this connection, the Standards Council may make appointments as it deems appropriate in the public interest, such as the classification of "Utilities" in the National Electrical Code Committee.
4. Representatives of subsidiaries of any group are generally considered to have the same classification as the parent organization.

NFPA Document Proposal Form

NOTE: All Proposals must be received by 5:00 pm EST/EDST on the published Proposal Closing Date.

For further information on the standards-making process, please contact the Codes and Standards Administration at 617-984-7249 or visit www.nfpa.org/codes.

For technical assistance, please call NFPA at 1-800-344-3555.

FOR OFFICE USE ONLY

Log #: _____

Date Rec'd: _____

Please indicate in which format you wish to receive your ROP/ROC ☐ **electronic** ☐ **paper** ☒ **download**
(Note: If choosing the download option, you must view the ROP/ROC from our website; no copy will be sent to you.)

Date April 1, 200X **Name** John J. Doe **Tel. No.** 716-555-1234

Company Air Canada Pilot's Association **Email**

Street Address 123 Summer Street Lane **City** Lewiston **State** NY **Zip** 14092

******If you wish to receive a hard copy, a street address MUST be provided. Deliveries cannot be made to PO boxes.***

Please indicate organization represented (if any)

1. (a) NFPA Document Title National Fuel Gas Code **NFPA No. & Year** 54, 200X Edition

(b) Section/Paragraph 3.3

2. Proposal Recommends (check one): ☐ new text ☒ revised text ☐ deleted text

3. Proposal (include proposed new or revised wording, or identification of wording to be deleted): [Note: Proposed text should be in legislative format; i.e., use underscore to denote wording to be inserted (inserted wording) and strike-through to denote wording to be deleted (~~deleted wording~~).]

Revise definition of effective ground-fault current path to read:

3.3.78 Effective Ground-Fault Current Path. An intentionally constructed, permanent, low impedance electrically conductive path designed and intended to carry ~~underground~~ electric fault current ~~conditions~~ from the point of a ground fault on a wiring system to the electrical supply source.

4. Statement of Problem and Substantiation for Proposal: (Note: State the problem that would be resolved by your recommendation; give the specific reason for your Proposal, including copies of tests, research papers, fire experience, etc. If more than 200 words, it may be abstracted for publication.)

Change uses proper electrical terms.

5. Copyright Assignment

(a) ☐ **I am the author of the text or other material (such as illustrations, graphs) proposed in the Proposal.**

(b) ☒ **Some or all of the text or other material proposed in this Proposal was not authored by me. Its source is as follows:** (please identify which material and provide complete information on its source)

ABC Co.

I hereby grant and assign to the NFPA all and full rights in copyright in this Proposal and understand that I acquire no rights in any publication of NFPA in which this Proposal in this or another similar or analogous form is used. Except to the extent that I do not have authority to make an assignment in materials that I have identified in (b) above, I hereby warrant that I am the author of this Proposal and that I have full power and authority to enter into this assignment.

Signature (Required) _____

PLEASE USE SEPARATE FORM FOR EACH PROPOSAL

Mail to: Secretary, Standards Council · National Fire Protection Association
1 Batterymarch Park · Quincy, MA 02169-7471 OR
Fax to: (617) 770-3500 OR Email to: proposals_comments@nfpa.org

NFPA Document Proposal Form

NOTE: All Proposals must be received by 5:00 pm EST/EDST on the published Proposal Closing Date.

For further information on the standards-making process, please contact the Codes and Standards Administration at 617-984-7249 or visit www.nfpa.org/codes.

For technical assistance, please call NFPA at 1-800-344-3555.

FOR OFFICE USE ONLY

Log #: _____

Date Rec'd: _____

Please indicate in which format you wish to receive your ROP/ROC ☐ electronic ☐ paper ☐ download
(Note: If choosing the download option, you must view the ROP/ROC from our website; no copy will be sent to you.)

Date _____ **Name** _____ **Tel. No.** _____

Company _____ **Email** _____

Street Address _____ **City** _____ **State** _____ **Zip** _____

******If you wish to receive a hard copy, a street address MUST be provided. Deliveries cannot be made to PO boxes.***

Please indicate organization represented (if any) _____

1. (a) NFPA Document Title _____ **NFPA No. & Year** _____

(b) Section/Paragraph _____

2. Proposal Recommends (check one): ☐ new text ☐ revised text ☐ deleted text

3. Proposal (include proposed new or revised wording, or identification of wording to be deleted): [Note: Proposed text should be in legislative format; i.e., use underscore to denote wording to be inserted (inserted wording) and strike-through to denote wording to be deleted (~~deleted wording~~).]

4. Statement of Problem and Substantiation for Proposal: (Note: State the problem that would be resolved by your recommendation; give the specific reason for your Proposal, including copies of tests, research papers, fire experience, etc. If more than 200 words, it may be abstracted for publication.)

5. Copyright Assignment

(a) ☐ I am the author of the text or other material (such as illustrations, graphs) proposed in the Proposal.

(b) ☐ Some or all of the text or other material proposed in this Proposal was not authored by me. Its source is as follows: (please identify which material and provide complete information on its source)

_____

I hereby grant and assign to the NFPA all and full rights in copyright in this Proposal and understand that I acquire no rights in any publication of NFPA in which this Proposal in this or another similar or analogous form is used. Except to the extent that I do not have authority to make an assignment in materials that I have identified in (b) above, I hereby warrant that I am the author of this Proposal and that I have full power and authority to enter into this assignment.

Signature (Required) _____

PLEASE USE SEPARATE FORM FOR EACH PROPOSAL

Mail to: Secretary, Standards Council · National Fire Protection Association
1 Batterymarch Park · Quincy, MA 02169-7471 OR
Fax to: (617) 770-3500 OR Email to: proposals_comments@nfpa.org