NFPA

1600®

Standard on Disaster/Emergency Management and Business Continuity/ Continuity of Operations Programs

2016

NFPA®

acp

DRI International Train. Prepare. Recover.

SAFETY ACT CERTIFIED

IAEM International Association of Emergency Managers

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 Standards"), 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 Standards.

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 Standards. The NFPA also makes no guaranty or warranty as to the accuracy or completeness of any information published herein.

In issuing and making NFPA Standards 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 Standards. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

REMINDER: UPDATING OF NFPA STANDARDS

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

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

To access the Document Information Page for a specific NFPA Standard, go to http://www.nfpa.org/docinfo to choose from the list of NFPA Standards or use the search feature on the right to select the NFPA Standard number (e.g., NFPA 101). The Document Information page includes postings of all existing Tentative Interim Amendments and Errata. It also includes the option to register for an "Alert" feature to receive an automatic email notification when new updates and other information are posted regarding the document.

ISBN: 978-145591313-8 (Print)
ISBN: 978-145591310-7 (PDF)

IMPORTANT NOTICES AND DISCLAIMERS CONCERNING NFPA® STANDARDS

ADDITIONAL NOTICES AND DISCLAIMERS

Updating of NFPA Standards

Users of NFPA codes, standards, recommended practices, and guides ("NFPA Standards") 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 or corrected by Errata. An official NFPA Standard 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 Standards

A statement, written or oral, that is not processed in accordance with Section 6 of the Regulations Governing the Development of NFPA Standards 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 Standard. The users of NFPA Standards 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 Standards.

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

Use of NFPA Standards 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 Standards, contact NFPA at the address below.

For Further Information

All questions or other communications relating to NFPA Standards 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 standards during regular revision cycles, should be sent to NFPA headquarters, addressed to the attention of the Secretary, Standards Council, NFPA, 1 Batterymarch Park, P.O. Box 9101, Quincy, MA 02269-9101; email: stds_admin@nfpa.org

For more information about NFPA, visit the NFPA website at www.nfpa.org. All NFPA codes and standards can be viewed at no cost at www.nfpa.org/freeaccess.

NFPA® 1600

Standard on
Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs
2016 Edition

About NFPA® 1600

This edition of NFPA 1600, *Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs,* was prepared by the Committee on Emergency Management and Business Continuity. It was issued by the Standards Council on November 14, 2015, with an effective date of December 4, 2015, and supersedes all previous editions.

This edition of *NFPA 1600* was approved as an American National Standard on December 4, 2015.

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-caused, and technological causes. The first edition of *NFPA 1600,* titled *Recommended Practice for Disaster Management,* was adopted by the NFPA membership in 1995.

The 2000 edition incorporated a “total program approach” for disaster/emergency management and business continuity programs. That edition provided a standardized basis for disaster/emergency management and business continuity programs in the private and public sectors by defining common program elements, techniques, and processes. Hazard mitigation was added to the standard for the protection of life and property. The annexes were also expanded to provide additional explanatory material. Significantly, the committee voted to move the document from a “recommended practice” to a “standard” by incorporating mandatory language (i.e., “shall” in place of “should”) in accordance with NFPA’s *Manual of Style*.

Reflecting contributions from the Federal Emergency Management Agency (FEMA), the National Emergency Management Association (NEMA), the International Association of Emergency Managers (IAEM), and private sector business continuity professionals, the 2004 edition was revised to define the elements of an emergency management and business continuity program to be used by the public and private sectors. Crosswalks between FEMA’s *Comprehensive Assessment for Readiness* (CAR), the Business Continuity Institute’s (BCI)

Good Practice Guidelines (GPG), Disaster Recovery Institute International's (DRII) *Ten Professional Practices,* and *NFPA 1600* were added to Annex A. Numerous other annexes were expanded. The 2004 edition also incorporated revised terminology and was reformatted to follow NFPA's *Manual of Style for NFPA Technical Committee Documents*.

A significant change to the 2007 edition was the expansion from the historical "four phases of emergency management" to include prevention, bringing the standard into alignment with the related disciplines and practices of risk management, security, and loss prevention. For the first time, the logos of the U.S. Department of Homeland Security (DHS), IAEM, and NEMA were added to the cover.

The 2010 edition of *NFPA 1600* was reordered and expanded to follow a program development process consistent with the "plan, do, check, act" continuous improvement process. Chapter 4, Program Management, was expanded to emphasize the importance of leadership and commitment; included new requirements for defining performance objectives; and included new requirements for records management. Finance and administration requirements also were moved to the program management chapter. Chapter 5 was rewritten into four chapters addressing planning, implementation, testing and exercises, and program improvement. Business impact analysis, which previously had been covered under the heading of "risk assessment," became a separate section within Chapter 5. Requirements for employee assistance and support were added to Chapter 6, Implementation. Requirements for testing and exercising were expanded within the new Chapter 7, and evaluations and corrective actions were incorporated into a new Chapter 8 on program improvement. A self-assessment checklist was added as Annex C to help users evaluate conformity with the standard, and Annex D provided a crosswalk between *NFPA 1600* and management system program elements. A significant addition to the annexes and an attractive option for those entities wishing to follow a "management system standard" was Annex F, NFPA 1600 2013 Edition as a Management System Standard. The annex enabled an entity to choose to adopt Annex F in place of the numbered chapters of the standard.

In November of 2009, *NFPA 1600* received designation and certification as anti-terrorism technology under the U.S. Federal SAFETY Act, and the SAFETY Act Certified™ seal was added to the cover of the 2010 edition along with the logos of the Association of Contingency Planners (ACP), DRII, and IAEM long-time supporters and contributors to the development of the standard.

The 2013 edition continued the reordering of the standard to align with a program development process and the continuous improvement process. Performance objectives were moved from Chapter 4, Program Management, to Chapter 5, Planning. Prevention and mitigation were moved from Chapter 5, Planning, to Chapter 6, Implementation. Resource management was split into resource needs assessment (Chapter 5, Planning) and resource management (Chapter 6, Implementation). Content on "communications and warning" and "crisis communications" was totally written into two sections: "Warning, Notifications, and Communications" and "Crisis Communications and Public Information." Requirements for business continuity and recovery were revised throughout the document, and new requirements for employee assistance and support were added. Chapter 7, Training and Education, was added to expand and clarify those requirements. In Chapter 9, the committee added program maintenance requirements. Annex A was reorganized, and new annexes were added.

The first notable change to the 2016 edition is the title. Recognizing that *NFPA 1600* is applicable to public sector continuity planning, commonly referred to as “Continuity of Operations Planning,” or “COOP,” the committee voted to change the title from *Standard on Disaster/Emergency Management and Business Continuity Programs to Standard on Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs*. The purpose of the standard has been changed to reflect the Committee’s decision to emphasize that the standard provides fundamental criteria for preparedness and that the program addresses prevention, mitigation, response, continuity, and recovery. In other words, “preparedness” is no longer just an element of the program — it is the program.

The committee has clarified crisis management planning to include issues that threaten the reputation and the strategic and intangible elements of the entity as a result of an event or a series of events that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders.

Business continuity is again a focus of the 2016 edition, and supply chain risk and information security are addressed in multiple places. Supply chain vulnerability assessment has been added to the section on risk assessment, assessment of the impact of the loss of “information” has been added to the requirements for the impact analysis, and planning for the security of information has been added to the continuity planning section. The business impact analysis section in Chapter 5 has been largely rewritten along with revised sections on continuity planning and recovery planning that provide more depth and differentiate “continuity” from “recovery.”

A significant change to the risk assessment requirements in Chapter 5, Planning, was the relocation of the detailed list of natural, human-caused, and technological hazards from Annex A to the requirements for risk assessment. The committee felt that the risk assessment is so important to the foundation of the program that users should evaluate all of the hazards on the list during the risk assessment process.

Annex C, Small Business Preparedness Guide, addresses a longstanding need for small business planning. A definition for persons with access and functional needs was added, and it supports new Annex J, Access and Functional Needs. Minor changes address the role of social media within crisis communications plans and capabilities.

Technical Committee on Emergency Management and Business Continuity

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

Richard R. Anderson, Anderson Risk Consultants, NJ [SE]

Pete Brewster, U.S. Department of Veterans Affairs, WV [U]

Andrew E. Cuthbert, Western Digital Corporation, CA [U]

Gregory T. Cybulski, Aon Corporation, NJ [I]

Steve Elliot, Elliot Consulting, FL [SE]
Rep. Association of Contingency Planners International, Inc.

David Gluckman, Willis Group, NJ [I]

Michael W. Janko, The Goodyear Tire & Rubber Company, OH [U]

Kenneth Katz, Travelers Insurance Company, NC [I]

Gunnar J. Kuepper, Emergency & Disaster Management, Inc., CA [SE]

Dana C. Lankhorst, MiddleOak, NH [I]

Richard J. Larkin, City of Saint Paul, MN [U]

Dean R. Larson, Larson Performance Consulting, IN [SE]

Ray S. Lazarus, Office of the Fire Marshal and Emergency Management, Canada [E]

Carrie M. Little, The City of Plano, TX [U]
Rep. International Association of Emergency Managers

Diane K. Mack, Indiana University, IN [U]

Breanna L. Medina, City of Rancho Cucamonga, CA [E]

Patricia A. Moore, Pat Moore Company, TX [SE]

Michael J. Morganti, DRI International, FL [SE]

Susana M. Mueller, Tampa Electric Company/TECO Energy, Inc., FL [U]

Jason C. Mumbach, Marsh Risk Consulting, CT [I]

Melvyn Musson, Edward Jones Company, MO [U]

Lee E. Newsome, Emergency Response Educators & Consultants, Inc., FL [SE]

Scott R. Nicoll, Chubb Group of Insurance Companies, FL [I]

Kelley Okolita, Cambia Health Solutions, FL [U]

Jo Robertson, Arkema Inc., PA [M]

David M. Sarabacha, Deloitte & Touche LLP, WA [SE]

Virginia Stouffer, Aforethought Consulting, LLC, PA [SE]

Brian Strong, CIT, FL [SE]

Joseph Bryan Travers, National Security Agency, MD [SE]

Bobby Williams, Fidelity Investments, TX [U]

Alternates

Chandra E. Fox, Emergency Services Coordinating Agency, WA [U]
(Alt. to Carrie M. Little)
Christian Gray, Cambia Health Solutions, UT [U]

(Alt. to Kelley Okolita)
Paul Grigg, Deloitte & Touche LLP, NJ [SE]
(Alt. to David M. Sarabacha)
Carey Ann Hamel, Aon Corporation, NH [I]
(Alt. to Gregory T. Cybulski)
Steven Majid, Shell Oil Company, TX [U]
(Voting Alt. to API Rep.)
John Douglas Nelson, Business Continuity Solutions, Inc., CA [SE]
(Alt. to Patricia A. Moore)
Teresa A. Newsome, Emergency Response Educators & Consultants, Inc., FL [SE]
(Alt. to Lee E. Newsome)
Manuel J. O'Bryant, Tampa Electric Company/TECO Energy, Inc., FL [U]
(Alt. to Susana M. Mueller)
Andrew M. Tait, Core Risks Ltd., PA [SE]
(Alt. to Richard R. Anderson)
Gary R. Villeneuve, DRI International, MI [SE]
(Alt. to Michael J. Morganti)
Lorraine E. Webb, Office of the Fire Marshal and Emergency Management, Canada [E]
(Alt. to Ray S. Lazarus)
Michael R. Zanotti, U.S. Department of Veterans Affairs, WV [U]
(Alt. to Pete Brewster)

Nonvoting

Carl Anthony Gibson, La Trobe University, Australia [E]

Graeme S. Jannaway, Jannaway Continuity Consulting, Inc., Canada [SE]
Rep. Canadian Standards Association

Gavin J. Love, WorleyParsons Pty Ltd., TX [SE]

Lloyd W. Bokman, Cedar Global Consulting, OH [SE]
(Member Emeritus)

Ryan Depew, 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.

NFPA® 1600
Standard on

Disaster/Emergency Management and Business Continuity/Continuity of Operations Programs
2016 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 Standards." They can also be obtained on request from NFPA or viewed at www.nfpa.org/disclaimers.

UPDATES, ALERTS, AND FUTURE EDITIONS: New editions of NFPA codes, standards, recommended practices, and guides (i.e., NFPA Standards) are released on scheduled revision cycles. This edition may be superseded by a later one, or it may be amended outside of its scheduled revision cycle through the issuance of Tentative Interim Amendments (TIAs). An official NFPA Standard at any point in time consists of the current edition of the document, together with any TIAs and Errata in effect. To verify that this document is the current edition or to determine if it has been amended by any TIAs or Errata, please consult the National Fire Codes® Subscription Service or visit the Document Information (DocInfo) pages on the NFPA website at www.nfpa.org/docinfo. In addition to TIAs and Errata, the DocInfo pages also include the option to sign up for Alerts for each document and to be involved in the development of the next edition.

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

A reference in brackets [ ] following a section or paragraph indicates material that has been extracted from another NFPA document. As an aid to the user, the complete title and edition of the source documents for extracts in mandatory sections of the document are given in Chapter 2 and those for extracts in informational sections are given in Annex K. Extracted text may be edited for consistency and style and may include the revision of internal paragraph references and other references as appropriate. Requests for interpretations or revisions of extracted text shall be sent to the technical committee responsible for the source document.

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

Chapter 1 Administration

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

1.2* Purpose. This standard provides the fundamental criteria for preparedness including the planning, implementation, assessment, and maintenance of programs for prevention, mitigation, response, continuity, and recovery.

1.3* Application. This document shall apply to public, private, and nonprofit and nongovernmental entities.

Chapter 2 Referenced Publications

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

2.2 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. An NFPA Standard, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements and that is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA Manuals of Style. When used in a generic sense, such as in the phrase “standards development process" or "standards development activities," the term "standards" includes all NFPA Standards, including Codes, Standards, Recommended Practices, and Guides.

3.3 General Definitions.

3.3.1* Access and Functional Needs. Persons requiring special accommodations because of health, social, economic, or language challenges.

3.3.2 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.

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

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

3.3.5 Capability. The ability to perform required actions.

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

3.3.7 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.

3.3.8* 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.

3.3.9 Crisis. An issue, event, or series of events that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders.

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

3.3.11 Damage Assessment. A determination of the effects of the incident on humans; on physical, operational, economic characteristics; and on the environment.

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

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

3.3.14* Exercise. A process to assess, train, practice, and improve performance in an entity.

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

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

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

3.3.18 Interoperability. The ability of diverse personnel, systems, and entities to work together seamlessly.

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

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

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

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

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

3.3.24* 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.

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

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

3.3.27 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.

3.3.28 Supply Chain. A network of individuals, entities, activities, information, resources, and technology involved in creating and delivering a product or service from supplier to end user.

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

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

Chapter 4 Program Management

4.1* Leadership and Commitment.

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

4.1.2 The leadership commitment shall include the following:

(1) Support the development, implementation, and maintenance of the program

(2) Provide necessary resources to support the program

(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness

(4) Support corrective action to address program deficiencies

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

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

4.3 Program Committee.

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

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

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

4.4 Program Administration.

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

(1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority

(2)* Program scope, goals, performance, objectives, and metrics for program evaluation

(3)* Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5

(4) Program budget and schedule, including milestones

(5) Program plans and procedures that include the following:

(a) Anticipated cost

(b) Priority

(c) Resources required

(6) Records management practices as required by Section 4.7

(7) Management of change

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

4.4.3* Program requirements shall be applicable to preparedness including the planning, implementation, assessment, and maintenance of programs for prevention, mitigation, response, continuity, and recovery.

4.5 Laws and Authorities.

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

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

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

4.6 Finance and Administration.

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

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

(1) Complies with the entity's program requirements

(2) Is uniquely linked to response, continuity, and recovery operations

(3) Provides for maximum flexibility to expeditiously request, receive, manage, and apply funds in a nonemergency environment and in emergency situations to ensure the timely delivery of assistance

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

4.6.4 Finance and administrative procedures shall include the following:

(1) Responsibilities for program finance authority, including reporting relationships to the program coordinator

(2)* Program procurement procedures

(3) Payroll

(4)* Accounting systems to track and document costs

(5) Management of funding from external sources

(6) Crisis management procedures that coordinate authorization levels and appropriate control measures

(7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery

(8) Identifying and accessing alternative funding sources

(9) Managing budgeted and specially appropriated funds

4.7* Records Management.

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

4.7.2 The program shall include the following:

(1) Identification of records (hard copy or electronic) vital to continue the operations of the entity

(2) Backup of records on a frequency necessary to meet program goals and objectives

(3) Validation of the integrity of records backup

(4) Implementation of procedures to store, retrieve, and recover records onsite or offsite

(5) Protection of records

(6) Implementation of a record review process

(7) Procedures coordinating records access

Chapter 5 Planning

5.1 Planning and Design Process.

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

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

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

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

5.1.5* Crisis management planning shall address an event, or series of events, that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders.

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

5.2* Risk Assessment.

5.2.1 The entity shall conduct a risk assessment.

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

5.2.2.1 Hazards to be evaluated shall include the following:

(1) Geological:

(a) Earthquake

(b) Landslide, mudslide, subsidence

(c) Tsunami

(d) Volcano

(2) Meteorological:

(a) Drought

(b) Extreme temperatures (hot, cold)

(c) Famine

(d) Flood, flash flood, seiche, tidal surge

(e) Geomagnetic storm

(f) Lightning

(g) Snow, ice, hail, sleet, avalanche

(h) Wildland fire

(i) Windstorm, tropical cyclone, hurricane, tornado, water spout, dust storm, sandstorm

(3) Biological:

(a) Food-borne illnesses

(b)* Infectious/communicable/pandemic diseases

(4) Accidental human-caused:

(a) Building/structure collapse

(b)* Entrapment

(c) Explosion/fire

(d) Fuel/resource shortage

(e)* Hazardous material spill or release

(f) Equipment failure

(g) Nuclear reactor incident

(h) Radiological incident

(i)* Transportation incident

(j) Unavailability of essential employee(s)

(k)* Water control structure failure

(l) Misinformation

(5) Intentional human-caused:

(a) Incendiary fire

(b) Bomb threat

(c) Demonstrations/civil disturbance/riot/insurrection

(d) Discrimination/harassment

(e) Disinformation

(f) Kidnapping/hostage

(g) Acts of war

(h) Missing person

(i)* Cyber security incidents

(j) Product defect or contamination

(k) Robbery/theft/fraud

(l) Strike or labor dispute

(m) Suspicious package

(n)* Terrorism

(o) Vandalism/sabotage

(p) Workplace/school/university violence

(6) Technological:

(a)* Hardware, software, and network connectivity interruption, disruption, or failure

(b)* Utility interruption, disruption, or failure

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

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

(1) Health and safety of persons in the affected area

(2) Health and safety of personnel responding to the incident

(3) Security of information

(4)* Continuity of operations

(5) Continuity of government

(6)* Property, facilities, assets, and critical infrastructure

(7) Delivery of the entity's services

(8) Supply chain

(9) Environment

(10)* Economic and financial conditions

(11) Legislated, regulatory, and contractual obligations

(12) Reputation of or confidence in the entity

(13) Work and labor arrangements

5.2.4 The risk assessment shall include an analysis of the escalation of impacts over time.

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

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

5.3 Business Impact Analysis (BIA).

5.3.1 The entity shall conduct a BIA that includes an assessment of how a disruption could affect an entity's operations, reputation, and market share, ability to do business, or relationships with key stakeholders and identifies the resources and capabilities that might be needed to manage the disruptions.

5.3.1.1* The BIA shall identify processes that are required for the entity to perform its mission.

5.3.1.2* The BIA shall identify the following resources that enable the processes:

(1) Personnel

(2) Equipment

(3) Infrastructure

(4) Technology

(5) Information

(6) Supply chain

5.3.2* The BIA shall evaluate the following:

(1) Dependencies

(2) Single-source and sole-source suppliers

(3) Single points of failure

(4) Potential qualitative and quantitative impacts from a disruption to the resources in 5.3.1.2

5.3.2.1* The BIA shall determine the point in time [recovery time objective (RTO)] when the impacts of the disruption become unacceptable to the entity.

5.3.3* The BIA shall identify the acceptable amount of data loss for physical and electronic records to identify the recovery point objective (RPO).

5.3.4* The BIA shall identify gaps between the RTOs and RPOs and demonstrated capabilities.

5.3.5* The BIA shall be used in the development of continuity and recovery strategies and plans.

5.3.6* The BIA shall identify critical supply chains, including those exposed to domestic and international risks, and the timeframe within which those operations become critical to the entity.

5.4 Resource Needs Assessment.

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

5.4.2 The resource needs assessment shall include the following:

(1)* Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed

(2) Quantity, response time, capability, limitations, cost, and liabilities

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

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

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

5.5 Performance Objectives.

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

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

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

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

Chapter 6 Implementation

6.1 Common Plan Requirements.

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

6.1.2 Plans shall identify and document the following:

(1) Assumptions made during the planning process

(2) Functional roles and responsibilities of internal and external entities

(3) Lines of authority

(4) The process for delegation of authority

(5) Lines of succession for the entity

(6) Liaisons to external entities

(7) Logistics support and resource requirements

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

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

6.2 Prevention.

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

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

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

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

6.3 Mitigation.

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

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

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

6.4 Crisis Communications and Public Information.

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

(1) Internal audiences, including employees

(2) External audiences, including the media, access and functional needs populations, and other stakeholders

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

(1)* Central contact facility or communications hub

(2) Physical or virtual information center

(3) System for gathering, monitoring, and disseminating information

(4) Procedures for developing and delivering coordinated messages

(5) Protocol to clear information for release

6.5 Warning, Notifications, and Communications.

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

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

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

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

6.5.5* Information shall be disseminated through the media, social media, or other means as determined by the entity to be the most effective.

6.6 Operational Procedures.

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

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

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

6.6.4 Procedures shall include the following:

(1) Control of access to the area affected by the incident

(2) Identification of personnel engaged in activities at the incident

(3) Accounting for personnel engaged in incident activities

(4) Mobilization and demobilization of resources

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

6.7 Incident Management.

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

6.7.1.1* Emergency Operations Centers (EOCs).

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

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

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

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

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

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

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

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

6.7.7 Resource management shall include the following tasks:

(1) Establishing processes for describing, taking inventory of, requesting, and tracking resources

(2) Resource typing or categorizing by size, capacity, capability, and skill

(3) Mobilizing and demobilizing resources in accordance with the established IMS

(4) Conducting contingency planning for resource deficiencies

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

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

6.8 Emergency Operations/Response Plan.

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

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

6.8.3* The plan shall identify actions for incident stabilization.

6.8.4 The plan shall include the following:

(1) Protective actions for life safety in accordance with 6.8.2.

(2) Warning, notifications, and communication in accordance with Section 6.5.

(3) Crisis communication and public information in accordance with Section 6.4

(4) Resource management in accordance with 6.7.7

(5) Donation management in accordance with 6.7.9

6.9* Continuity and Recovery.

6.9.1 Continuity.

6.9.1.1 Continuity plans shall include strategies to continue critical and time-sensitive processes and as identified in the BIA.

6.9.1.2* Continuity plans shall identify and document the following:

(1) Stakeholders that need to be notified

(2) Processes that must be maintained

(3) Roles and responsibilities of the individuals implementing the continuity strategies

(4) Procedures for activating the plan, including authority for plan activation

(5) Critical and time-sensitive technology, application systems, and information

(6) Security of information

(7) Alternative work sites

(8) Workaround procedures

(9) Vital records

(10) Contact lists

(11) Required personnel

(12) Vendors and contractors supporting continuity

(13) Resources for continued operations

(14) Mutual aid or partnership agreements

(15) Activities to return critical and time-sensitive processes to the original state

6.9.1.3 Continuity plans shall be designed to meet the RTO and RPO.

6.9.1.4 Continuity plans shall address supply chain disruption.

6.9.2 Recovery.

6.9.2.1 Recovery plans shall provide for restoration of processes, technology, information, services, resources, facilities, programs, and infrastructure.

6.9.2.2* Recovery plans shall document the following:

(1) Damage assessment

(2) Coordination of the restoration, rebuilding, and replacement of facilities, infrastructure, materials, equipment, tools, vendors, and suppliers

(3) Restoration of the supply chain

(4) Continuation of communications with stakeholders

(5) Recovery of critical and time-sensitive processes, technology, systems, applications, and information

(6) Roles and responsibilities of the individuals implementing the recovery strategies,

(7) Internal and external (vendors and contractors) personnel who can support the implementation of recovery strategies and contractual needs

(8) Adequate controls to prevent the corruption or unlawful access to the entity's data during recovery

(9) Compliance with regulations that would become applicable during the recovery

(10) Maintenance of pre-incident controls

6.10 Employee Assistance and Support.

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

(1)* Communications procedures

(2)* Contact information, including emergency contact outside the anticipated hazard area

(3) Accounting for persons affected, displaced, or injured by the incident

(4) Temporary, short-term, or long-term housing and feeding and care of those displaced by an incident

(5) Mental health and physical well-being of individuals affected by the incident

(6) Pre-incident and post-incident awareness

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

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

Chapter 7 Training and Education

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

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

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

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

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

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

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

(1) The potential impacts of a hazard

(2) Preparedness information

(3) Information needed to develop a preparedness plan

Chapter 8 Exercises and Tests

8.1 Program Evaluation.

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

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

8.1.3 Exercises and tests shall be documented.

8.2* Exercise and Test Methodology.

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

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

8.2.3 Tests shall be designed to demonstrate capabilities.

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

(1) Ensure the safety of people, property, operations, and the environment involved in the exercise or test

(2) Evaluate the program

(3) Identify planning and procedural deficiencies

(4) Test or validate recently changed procedures or plans

(5) Clarify roles and responsibilities

(6) Obtain participant feedback and recommendations for program improvement

(7) Measure improvement compared to performance objectives

(8)* Improve coordination among internal and external teams and entities

(9) Validate training and education

(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity

(11) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery

(12) Assess the ability of the team to identify, assess, and manage an incident

(13) Practice the deployment of teams and resources to manage an incident

(14) Improve individual performance

8.4* Exercise and Test Evaluation.

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

8.4.2 Tests shall be evaluated as either pass or fail.

8.5* Frequency.

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

Chapter 9 Program Maintenance and Improvement

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

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

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

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

(1) Regulations

(2) Hazards and potential impacts

(3) Resource availability or capability

(4) Entity's organization

(5)* Funding changes

(6) Infrastructure, including technology environment

(7) Economic and geographic stability

(8) Entity operations

(9) Critical suppliers

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

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

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

9.2* Corrective Action.

9.2.1* The entity shall establish a corrective action process.

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

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

Annex A Explanatory Material

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

A.1.1 The Emergency Management and Business Continuity/Continuity of Operations community comprises many different entities, including the government at distinct levels (e.g., federal, state/provincial, territorial, aboriginal, indigenous, tribal, and local levels); commercial business and industry; nonprofit and nongovernmental entities; and individual citizens. Each of these entities has its own focus, unique mission and responsibilities, varied resources and capabilities, and operating principles and procedures.

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

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

The application of *NFPA 1600* used with the United Nations Environmental Program APELL (Awareness and Preparedness for Emergencies at the Local Level) for Technological Hazards is described in Annex H. Annex H describes both international and domestic applications.

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

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

A.3.3.1 Access and Functional Needs. The terminology for this population continues to evolve. Similar terms include handicapped, disabled, special needs, vulnerable population, people with medical dependencies, specialty care population, and vulnerable persons. *(See Annex J.)*

A.3.3.3 Business Continuity/Continuity of Operations. Another term for business continuity/continuity of operations is *operational continuity* or *continuity of operations (COOP)*. In the public sector, the term *continuity of government (COG)* is also used. See also 3.3.8 and A.3.3.8.

A.3.3.8 Continuity. An evolving concept that is linked to continuity is resilience. Organizational resilience is the ability of an entity to withstand potential impacts of natural, human-caused, and technology-caused hazards; respond effectively when an incident occurs; continue to provide a minimum acceptable level of service during and in the immediate aftermath of the incident; and thereafter return conditions to a level that is acceptable to the entity. Entities generally are interdependent with a wider community. To ensure that the community in which the entity operates is resilient, entities should work with local stakeholders (including public, private, and not-for-profit organizations) to promote emergency management and business continuity/continuity of operations processes. Entities should evaluate their suppliers. The entity should request that the supplier develop and maintain programs and processes to ensure organizational resilience and their ability to provide critical services and goods during emergencies and disasters. Providing generic advice as well as more detailed assistance on a one-to-one basis to external stakeholders can ensure that businesses and government are resilient and can quickly restore a community's ability to function normally after an incident. The underlying strategy is to bring together all sectors to collaborate and share good practice. This concept can be referred to as “community resilience.”

A.3.3.14 Exercise. Exercise is the principal means of evaluating a program's ability to execute its response procedures. It allows the entity to practice procedures and interact in a controlled setting. Participants identify and make recommendations to improve the overall program. Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses, with the goal of achieving maximum performance.

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

A.3.3.17 Incident Management System (IMS). The incident management system is based on effective management characteristics that can be used by the public, private, and nonprofit sectors. For an IMS to work effectively, each management characteristic should contribute to the strength and efficiency of the overall system.

The following are commonly identified management characteristics:

(1) *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 A.3.3.17(2) through A.3.3.17(12).

(2) *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 entity establishes a process for gathering, sharing, and managing incident-related information and intelligence.

(3) *Modular Entity.* 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.

(4) *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.

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

(6) *Management by Objectives.* Management by objectives represents an approach that is communicated throughout the entire entity. This approach includes establishing overarching objectives for the following:

(a) Developing and issuing assignments, plans, procedures, and protocols

(b) Establishing specific, measurable objectives for various incident management functional activities and directing efforts to attain them in support of defined strategic objectives

(c) Documenting results to measure performance and facilitate corrective action

(7) *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.

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

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

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

(11) *Chain of Command and Unity of Command.* Chain of command refers to the orderly line of authority within the ranks of the incident management system. 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.

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

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

A.3.3.20 Mutual Aid/Assistance Agreement. The term *mutual aid/assistance agreement,* as used herein, includes cooperative agreements, partnership agreements, memoranda of understanding, memorandum of agreement, intergovernmental compacts, or other terms commonly used for the sharing of resources. Agreements can be executed between any combination of public, private, and not-for-profit entities.

A.3.3.22 Prevention. The term *prevention* refers to activities, tasks, programs, and systems intended to avoid or intervene in order to stop an incident from occurring.

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

A.3.3.23 Recovery. Recovery programs are designed to assist victims and their families, restore entities to suitable economic growth and confidence, relocate or rebuild destroyed property, and reconstitute government operations and services. Recovery actions can be short term or long term, often continuing long after the incident has ended. Recovery programs include mitigation components designed to avoid damage from future incidents.

A.3.3.24 Resource Management. This system includes a process for identifying, categorizing, ordering, mobilizing, tracking, and recovering and demobilizing resources, as well as a process for reimbursement for resources, as appropriate.

A.3.3.25 Response. The term *response* refers to the actions taken by an entity to an incident or event. Actions can include activities, tasks, programs, and systems to protect life safety, meet basic human needs, preserve operational capability, and protect property and the environment.

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

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

A.4.2 It is not the intent of this standard to restrict the users to the title *program coordinator*. It is recognized that different entities use various forms and names for the person who performs the program coordinator functions identified in the standard. Examples of titles are *emergency manager* (for the public sector), and *business continuity/continuity of operations manager* (for the private and nonprofit sectors). A written position description should be provided.

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

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

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

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

A.4.4.1(3) Industry codes of practices and guidelines and applicable regulations should also be considered along with any other directive established by the entity or the organization. In particular, applicable codes and ordinances can include requirements for the design or upgrade of protective and other building components to support emergency management (prevention, mitigation, response, continuity, and recovery).

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

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

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

In the case of private, nonprofit, and 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 because program requirements change to comply with changing roles and relationships in and among varying levels of government.

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

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

(1) The finance department could be considered for membership of the program committee.

(2) The finance department should be actively involved with identifying, prioritizing, and purchasing internal and external resources.

(3) The entity's financial opportunities or limitations should be identified within the strategic plan that defines the vision, mission, goals, and objectives of the program.

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

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

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

Records management practices should include the following activities:

(1) Creating, approving, and enforcing records management policies, including a classification system and a records retention policy

(2) Developing a records storage plan, including the short-term and long-term housing of physical records and digital information

(3) Identifying existing and newly created records and classifying and storing them according to standard operating procedures (SOPs)

(4) Coordinating the access and circulation of records within and outside the entity

(5) Executing a retention policy to archive and destroy records according to operational needs, operating procedures, statutes, and regulations

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

A.5.1.5 The majority of incidents that affect life, health, and safety are the purview of emergency response. A plan for returning to normal operation following a business disruption is the focus of business continuity/continuity of operations. The goal of crisis management is to minimize disruption and to influence the outcome of the crisis. The crisis management team, which is led by senior management, is responsible for the broad strategic decisions that affect the entity's reputation and for the long-term consequences of a severe incident.

Crises can create issues or threaten consequences that can disrupt the entity's ability to do business. They are best mitigated by proactively addressing such issues before they have escalated to a crisis. Recognizing the signs of a potential crisis and proactively addressing the issue(s) can help mitigate any damage to the reputation and finances of the entity.

When activated, the crisis management team is the ultimate authority on the entity's response to the crisis. The crisis management team's primary function is to identify, evaluate, and manage the strategic issues that impact the entity without becoming involved in the details of the on-site emergency response actions. The crisis management team focuses on forecasting consequences of the incident and is responsible for keeping other senior managers and executives informed of current and anticipated response activities as well as formulating long-term strategic response plans.

Crisis management activities can include the following:

(1) Acting as a clearinghouse for all information

(2) Coordinating corporate support to the site of the incident

(3) Coordinating the response activities of a business group and corporate functional departments

(4) Coordinating the implementation of business continuity/continuity of operations or disaster recovery plans and management of business resumption issues stemming from an incident

(5) Supporting executives in crisis management activities

The crisis management team should address:

(1) Consequences of operational and business disruptions

(2) Implications of media, community, and government relationships

(3) Concerns about inter- and intra-organizational ramifications

(4) Impacts on strategic plans

(5) Consequences for labor and contractor relations

(6) Legal and financial liability

(7) Insurance implications

(8) Environmental issues

(9) Impacts on international relations

(10) Potential for industry-wide concerns

The roles and responsibilities of the crisis management team can include the following:

(1) Communicate with board of directors

(2) Define corporate policy

(3) Commit corporate assets

(4) Provide overall management and direction

(5) Set strategic direction of crisis response

A.5.2 Risk assessment is a process for identifying potential hazards/risk exposures and their relative probability of occurrence; identifying assets at risk; assessing the vulnerability of the assets exposed; and quantifying the potential impacts of the hazard/risk exposures on the assets. Periodic reassessment is needed when changes to the entity occur. Reassessment is also necessary because hazards/risk exposures change over time, and the collective knowledge of hazards/risk exposures develops over time.

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

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

(1) Determine the methodology the entity will use to conduct the assessment and determine whether the entity has the necessary expertise to perform the assessment.

(2) Consult with internal or external experts with the expertise to assess the vulnerability of the entity's assets from identified hazards.

(3) Identify and categorize assets (human resources, buildings, equipment, operations, technology, electronic information, suppliers, vendors, third-party service providers, etc.).

(4) Identify threats and hazards — natural, human caused (accidental and intentional), and technology caused.

(5) Evaluate hazard/risk exposures to which the entity is exposed.

(6) Assess the existing/current preventive measures and mitigation controls in place against credible threats.

(7) Categorize threats, hazard/risk exposures, and potential incidents by their relative frequency and severity. Keep in mind that there might be many possible combinations of frequency and severity for each, as well as cascading impacts.

(8) Evaluate the residual hazard/risk exposures (those that remain hazardous after prevention and mitigation activities).

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

A.5.2.2.1(3)(b) Avian flu, H1N1, plague, smallpox, anthrax, Ebola, West Nile virus, foot and mouth disease, severe acute respiratory syndrome (SARS), or bovine spongiform encephalopathy (BSE, Mad Cow Disease)

A.5.2.2.1(4)(b) Machinery, confined space, high angle, or water

A.5.2.2.1(4)(e) Flammable/combustible liquid; flammable/combustible gas; flammable solid; oxidizer; poison; explosive, radiological, or corrosive material

A.5.2.2.1(4)(i) Motor vehicle, railroad, watercraft, aircraft, pipeline

A.5.2.2.1(4)(k) Dam and levee

A.5.2.2.1(5)(i) Virus, worm, hacking, Trojan horse, botnets, phishing, spyware, malware, or denial of service

A.5.2.2.1(5)(n) Explosive, chemical, biological, radiological, nuclear, cyber, or electromagnetic pulse

A.5.2.2.1(6)(a) Outages, data corruption, deletion, loss of (Internet or intranet), loss of electronic data interchange or ecommerce, loss of domain name server (DNS), interdependencies, direct physical loss, vulnerability exploitation, loss of encryption, or improper system use by employee

A.5.2.2.1(6)(b) Telecommunications, electrical power, water, gas, steam, HVAC, pollution control system, sewage system, or other critical infrastructure

A.5.2.2.2 Supply chain interruption [e.g., loss of shipping or transportation, vendor failure (single or sole source provider)], including direct and indirect effects on the supply chain based on impacts from the expanded lists of hazards included in this document.

A.5.2.3(4) In order to maintain continuity of operations, the entity should identify essential or critical functions and processes, their recovery priorities, and their internal and external interdependencies, so that recovery time objectives can be set. Consideration also should be given to situations that cause the entity to become incapable of response or incapable of maintaining any continuity of operations for the foreseeable future. This process is called a business impact analysis (BIA) and is defined further in Section 5.3.

A.5.2.3(6) Assets include production machinery and processing equipment, tools, finished goods/inventory, raw materials, vehicles, electronic information, vital records, patents, intellectual property, and personnel/institutional knowledge. The analysis of impacts also should include evaluation of the infrastructure necessary to operate buildings, equipment, and technology.

A.5.2.3(10) Quantification of the potential economic and financial impacts resulting from property damage, interruption or disruption of operations, and environmental contamination provides input into the determination of where to invest in mitigation and planning efforts.

A.5.2.5 It is important to consider the cascading impacts of regional, national, or international incidents. One example is the cascading impacts of a hurricane. Direct impacts can include wind and flood damage. Secondary impacts can include telecommunications, electrical power, and transportation disruptions, both inside and outside the direct impact area. The earthquake and tsunami in Japan in 2011 resulted in supply chain interruptions around the world. The terrorist attacks of September 11, 2001, shut down air travel in the United States for days and impacted the financial markets.

A.5.3.1.1 Working with resources throughout the entity, identify all the entity's functions and related processes. In addition to human resources, and items such as organization charts, mission statement, operational procedures and so forth may assist the planner in identifying critical processes within the entity.

A.5.3.1.2 Working within each of the entity's operational areas, document the resources each process needs in order to operate successfully. For example, how many people are needed and what skill sets do they need? What equipment is needed to complete the process? What kind of infrastructure is required? What technology is required? What information is required? What suppliers are used by the process?

A.5.3.2 Determine the consequences of a disruption on the identified processes in financial, regulatory, customer and/or operational terms over defined periods as follows:

(1) Identify the interdependencies with key internal and external stakeholders, which could include mapping the nature of the interdependencies through the supply chain (inbound and outbound).

(2) Determine the current available resources provided by single source and sole source suppliers and the essential level of resources required to continue operations at a minimum acceptable level following a disruption. Identify the interruption potentials that describe the financial, regulatory, customer, or operational impacts, including potential bottlenecks, upstream and downstream supply chains, long lead time equipment, and single-source and sole-source suppliers.

(3) Identify the impacts resulting from single points of failure in resources needed to support the process. Examples include a process operating in only one site, single electrical feed to the building, single application that provides the ability to perform a task and the impact to the process if that single point fails to perform.

(4) Identify the potential impacts resulting from a disruption of functions and processes.

A.5.3.2.1 The RTO represents the maximum period of time the entity can tolerate the loss of capability. Determine the RTO for each process, based on the identified consequences and the critical success factors for the function. Determine the severity of the impact over time if the RTO is not met.

Correlate specific, infrastructure, systems, and applications with the operational processes they support and based on that information, assess the impact to the entity's operations due to disruption of those resources.

A.5.3.3 Identify the lines of process flow (material flow, information flow, people movement, cash flow) and time constraints. Typical output of the BIA will provide a process flow for the entire entity.

A.5.3.4 The RPO is the point in time from which data is recovered — "the last good backup offsite at the time of the event." Any activities that occurred after this point are lost and will need to be re-created by some other means. This includes activities occurring in technology applications, work in progress in operational areas, and vital records stored onsite. The amount of time between the RPO and the time of disruption equals the amount of loss sustained during the incident. It can be deemed as the acceptable amount of data loss.

The BIA should document the gap between what capabilities the entity has demonstrated and what it requires in order to meet the defined RTO and RPO. For example, if the BIA determined that an application required by a business process needs to be available RTO in 4 hours, yet the most recent recovery exercise for the application demonstrated the recovery took 12 hours, then there is a gap of 8 hours between what is needed and what has been demonstrated. Same is true of RPO. If the BIA identified that the process needed the data to be less than 24 hours old, yet the data is only backed up and sent off site weekly, that would indicate a gap of up to 6 days between the RPO needed and the RPO demonstrated.

A.5.3.5 Recovery strategies provide a means to restore operations quickly and effectively following a service disruption. The recovery strategies should consider the impacts of disruption and allowable outage times identified in the impact analysis, as well as cost, security, and integration with larger, entity-level recovery plans. RTOs and RPOs are often used as the basis for the development of recovery strategies and as a determinant as to when to implement the recovery strategies during a disaster situation. Three examples follow:

(1) An RTO in the range of a few minutes to hours might require that the operational process be fully functional in two geographically diverse sites that are fully equipped and staffed. In technology environments, this might require that two facilities either operate in parallel (active/active, mirroring) or at least duplicate the primary environment (active/passive, clustering or high availability).

(2) An RTO expressed in days to weeks can be sufficiently addressed by transferring the operations and staff to an alternative site, such as a commercial recovery facility or an internally developed and maintained hot, warm, or mobile site.

(3) An RTO expressed in months can be sufficiently addressed by a cold site that requires that all necessary equipment, technology, and supplies be re-established at the time of the event.

A.5.3.6 Identify the interruption potentials that describe the financial, regulatory, customer, or operational impacts, including potential bottlenecks, upstream and downstream supply chains, long lead time equipment, single-source and sole-source suppliers, and the RTO and RPO the entity would require from its suppliers. Work with suppliers to demonstrate their capability to meet the required RTO and RPO.

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

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

A.5.4.2(1) The resource needs assessment might include “credentialing,” which addresses the need for individuals licensed (e.g., doctors, engineers) in one jurisdiction (state or country) performing their professional duties (as volunteers or under mutual aid compacts) during an incident in a jurisdiction where they are not licensed or do not hold the proper credentials. Credentialing provides minimum professional qualifications, certifications, training, and education requirements that define the standards required for specific emergency response functional assignments.

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

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

(1) Locations, quantities, accessibility, operability, and maintenance of equipment

(2) Supplies (medical, personal hygiene, consumable, administrative, ice)

(3) Sources of energy (electrical, fuel)

(4) Emergency power

(5) Communications systems

(6) Food and water

(7) Technical information

(8) Clothing

(9) Shelter

(10) Specialized human resources (medical, faith-based, and volunteer entities; emergency management staff; utility workers; morticians; and private contractors)

(11) Employee and family assistance

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

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

The term *mutual aid/assistance agreement,* as used here, includes cooperative assistance agreements, intergovernmental compacts, or other terms commonly used for the sharing of resources. Partnerships can include any combination of public, private, and nonprofit entities or NGOs.

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

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

(1) Definitions of key terms used in the agreement, including *intellectual property, duration of the agreement*, and *duration of assistance*

(2) Roles and responsibilities of individual parties

(3) Procedures for requesting and providing assistance, including mobilization and demobilization

(4) Procedures, authorities, and rules for payment, reimbursement, and allocation of costs

(5) Notification procedures

(6) Protocols for interoperable communications

(7) Relationships with other agreements among entities

(8) Workers' compensation

(9) Treatment of liability and immunity

(10) Recognition of qualifications and certifications

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

(1) *Performance*. Specific identification of expected behavior that is observable and measurable. If the specific behavior is based on expected knowledge (cognitive process) or attitudes (emotions, feelings), indicator behaviors should be used, because knowledge and attitude performance objectives are not directly observable and, therefore, are not measurable. An indicator behavior is observable and is based on either cognitive or emotional processes.

(2) *Conditions*. Specific identification of exact location, tools, the equipment used, and so forth, that will be part of the observable, measurable behavior.

(3) *Criteria*. Specific criteria that will be used to compare the observed behavior so that it can be determined if the performance objectives have been achieved.

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

(1) ***S****pecific*. The wording must be precise and unambiguous in describing the objective.

(2) ***M****easurable*. The design and statement of objectives should make it possible to conduct a final accounting as to whether objectives were achieved.

(3) ***A****ction oriented*. The objective must have an action verb that describes the expected accomplishments.

(4) ***R****ealistic*. Objectives must be achievable with the resources that the entity can allocate or make available.

(5) ***T****ime sensitive*. Time frames should be specified (if applicable).

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

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

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

Hazard control begins with identification of the hazard and the vulnerability of people or assets potentially exposed and elimination or mitigation according to the hierarchy of controls as follows:

(1) *Elimination or substitution*. Whenever possible, the hazard should be eliminated from the work area (e.g., repairing or removing fallen electrical power lines before allowing other work to proceed in the area). Although desirable, elimination or substitution might not be options for most airborne/chemical hazards created by an incident.

(2) *Engineering controls*. Steps should be taken to reduce or eliminate exposure to a hazard through engineering controls such as the installation of ventilation systems, automatic sprinklers (building), or special protection systems.

(3) *Administrative controls*. Work practices should be implemented that reduce the duration, frequency, and severity of risk exposures. Safety and health controls include training, safety procedures, observations, and enforcement of safe behavior, for example, using well-rested crews and daylight hours to perform higher hazard or unfamiliar tasks, requiring frequent breaks during hot weather, removing nonessential personnel from the area during certain tasks/operations, and decontaminating equipment and personnel after contact with contaminated floodwater or chemicals, and when possible, using water to suppress dust and work upwind in dusty conditions.

(4) *Personal protective equipment (PPE)*. If hazard exposures cannot be engineered or administratively controlled, individuals should be shielded or isolated from chemical, physical, and biological hazards through the use of PPE. Careful selection and use of adequate PPE should protect the respiratory system, skin, eyes, face, hands, feet, head, body, and hearing. Examples of PPE are safety glasses and goggles for eyes, gloves for hands, and respirators to protect the lungs. Control of the hazard exposures should not stop with providing PPE.

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

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

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

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

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

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

(1) Security patrols inside and outside facilities; increased inspections of vehicles entering the facility; background checks of personnel

(2) Access controls, including perimeter fence line and gates, access control systems, camera surveillance, intruder detection systems (motion-sensing cameras, infrared detectors)

(3) Immunizations, isolation, or quarantine

(4) Land use restrictions to prevent development in hazard-prone areas, such as flooding areas or construction of hazardous materials facilities in areas near schools, in population centers, or in areas of identified critical infrastructure

(5) Uninterruptible power supply (UPS) to provide short-term backup power to critical electrical components, including the data center power distribution unit (PDU), desktop computers in time-sensitive operational areas, phone switchboard (PBX), the HVAC system, and safety controls such as elevators and emergency lighting

(6) Gasoline- or diesel-powered generators to provide long-term backup power

(7) Crime prevention through environmental design (CPTED), including site layout, landscape design, and exterior lighting

(8) Personnel management

(9) Background investigations

(10) Cyber security, including firewalls, intrusion detection, virus protection, password management, cryptographic key management, and access to information based on need to know

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

(1) Ongoing hazard identification

(2) Threat assessment

(3) Risk assessment

(4) Analysis of impacts

(5) Operational experience, including incident analysis

(6) Information collection and analysis

(7) Intelligence and information sharing

(8) Regulatory requirements

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

A.6.3.1 Mitigation strategies can include the following:

(1) Use of applicable building construction standards

(2) Hazard avoidance through appropriate land use practices

(3) Relocation, retrofitting, or removal of structures at risk

(4) Removal or elimination of the hazard

(5) Reduction or limitation of the amount or size of the hazard

(6) Segregation of the hazard from that which is to be protected

(7) Modification of the basic characteristics of the hazard

(8) Control of the rate of release of the hazard

(9) Provision of protective systems or equipment for both cyber risks and physical risks

(10) Establishment of hazard warning and communication procedures

(11) Redundancy or diversity of essential personnel, critical systems, equipment, information, operations, or materials

(12) Acceptance/retention/transfer of risk (insurance programs)

(13) Protection of competitive/proprietary information

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

(1) Explanation of hazard and vulnerabilities

(2) Quantification of the risk if unmitigated

(3) Anticipated cost

(4) Anticipated benefit

(5) Cost-benefit analysis

(6) Prioritization of projects based on probability of occurrence and severity of potential impacts

(7) Planned changes to the entity

(8) Project timeline

(9) Resources required

(10) Funding mechanism

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

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

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

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

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

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

A.6.5.2 Since warning, notification, and communications systems must be immediately available and functional to warn persons potentially at risk, to alert persons to respond, and to enable communications between responders, reliability of systems and equipment is critically important. Redundancy in systems and equipment provides assurance that essential warnings, notifications, and communications can be made. Systems and equipment must be interoperable to ensure that responders are able to communicate effectively during an incident. Also see 3.3.18, Interoperability.

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

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

A.6.5.5 A common format for gathering pertinent information (inbound messaging) and disseminating information (outbound messaging) is recommended. Use of social media can provide a distinct advantage to both inbound and outbound messaging, and should be considered a basic form of communication with external and internal audiences.

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

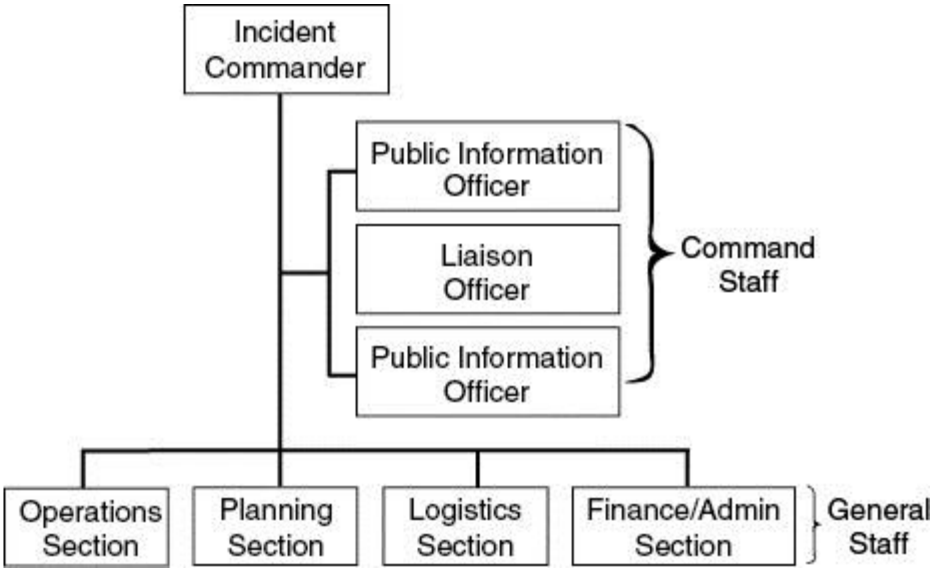
A.6.7.1 An incident management system (IMS) should be used to manage an incident. The system used varies among entities and among jurisdictions within entities. In minor incidents, IMS functions might be handled by one person: the incident commander or equivalent designee.

An example of a public sector IMS would be the National Incident Management System (NIMS) used in the United States or similar systems in other countries, such as the Gold-Silver-Bronze system in the United Kingdom. In the Incident Command System (ICS) portion of NIMS, incident management is structured to facilitate activities in five major functional areas: command, operations, planning, logistics, and finance and administration.

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

For private sector or nonprofit entities, it is acceptable for the IMS to be organized in whatever way best fits the organizational structure, as long as it is clear how the entity will coordinate its operations with public sector resources arriving at the incident scene.

FIGURE A.6.7.1 Diagram of Incident Command System.



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

A.6.7.1.1.1 The requirement to establish primary and alternate EOCs is intended to ensure that the capacity exists to support operations from a centralized facility or virtual capability. The primary and alternate EOCs should be located so both are not impacted by the same event and at least one EOC will be operational. Alternate EOCs can include site or department EOCs, which focus on internal department or agency incident management and are linked to and, in most cases, physically represented in a higher level EOC.

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

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

A.6.7.3 Common prevention strategies and techniques as outlined in A.6.2.1 and A.6.2.2 typically occur prior to the occurrence of an incident. There are occasions, however, where an incident management system is activated to manage a planned event, as well as to prevent the occurrence of incidents that might impact the event. It might also be necessary to activate an incident management system in the face of a threat, with the purpose of preventing such a threat from occurring. Should prevention measures not be successful, response and recovery measures can be implemented to deal with the consequences of an incident.

A.6.7.6 In larger scale incidents a formal incident action plan *(see 3.3.16)* is developed and approved by the incident commander. In small-scale incidents, objectives are established by the incident commander and verbally communicated. Operations are then managed by command to achieve the objectives.

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

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

(1) Visually impaired

(2) Hearing impaired

(3) Mobility impaired

(4) Single working parent

(5) Language competency

(6) People without vehicles

(7) People with special dietary needs

(8) People with medical conditions

(9) People with intellectual disabilities

(10) People with dementia

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

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

A.6.9 Examples of strategies, options and alternatives for manufacturing, health care, education, service, or other facilities, include the following:

(1) Strategies for disruption or loss of operational site:

(a) Transfer of workload and staff to a surviving site

(b) Contracted alternate site

(c) Reciprocal agreement with a similar entity

(d) Dedicated alternate site

(e) Mobile facility

(f) Remote access/work from home

(g) Resources acquired at the time of disruption

(h) Mutual aid agreement

(i) Finished goods buyback

(j) Real location of surviving capacity

(k) Stockpile critical equipment and inventory

(2) Third-party (vendor provided/extended enterprise) recovery strategy options:

(a) Multiple sourcing

(b) Alternate sourcing

(c) Service level agreement

(d) In-source (do not outsource)

(3) Technical recovery alternatives:

(a) Commercial vendor (hot site)

(b) Resources acquired at time of disruption

(c) Quick-ship equipment

(d) Dual data center with active/active

(e) Dual data center with active/passive

(f) Outsourcing with a service level agreement (cloud computing)

(g) Stockpiled equipment

(h) Manual workarounds or alternate systems

(4) Backup strategies for records:

(a) Electronic storage

(b) Synchronous replication

(c) Asynchronous replication

(d) Electronic journaling

(e) Standby database

(f) Electronic vaulting

(g) Tape backup

(h) Full backup

(i) Differential backup

(j) Incremental backup

(k) Salvage

(5) Hard-copy storage:

(a) Film

(b) Fiche

(c) Photocopy

(d) Scan

(e) Salvage

Plans should include the following:

(1) Facilities and equipment

(2) Critical infrastructure

(3) Telecommunications and cyber protection systems

(4) Distribution systems for essential goods

(5) Transportation systems, networks, and infrastructure

(6) Human resources

(7) Psychosocial services

(8) Health services

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

(1) Critical personnel, systems, operations, records, and equipment

(2) Priorities for restoration and mitigation

(3) Acceptable downtime before restoration to a minimal level

(4) Minimal functions, services, and resources needed to provide for the restoration of facilities, processes, 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 contractual and entity resources

(4) Opportunities for mitigation

A.6.9.1.2 Plans for business continuity/continuity of operations of government and continuity of operations are generally similar in intent and less similar in content. Continuity plans have various names in public, private, and nonprofit sectors, including business continuity/continuity of operations plans, business resumption plans, and disaster recovery plans.

A.6.9.2.2 Recovery planning for public, private, and nonprofit sectors should provide for continuity of operations to return the entity, infrastructure, and individuals back to an acceptable level. This includes implementation of mitigation measures to facilitate short-term and long-term recovery.

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

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

Various communications methodologies can be established, including the following:

(1) Automated notification systems or call centers

(2) Email, web site, or voicemail broadcasts

(3) Call lists

(4) Social media

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

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

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

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

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

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

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

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

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

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

(1) Reveal planning weaknesses and strengths in plans, standard operating procedures (SOPs), and standard operating guidelines (SOGs) and to test and validate recently changed procedures

(2) Improve the coordination among various response entities, elected officials, and community support entities

(3) Validate the training for response (e.g., incident command, hazard recognition, evacuation, decontamination) and recovery

(4) Increase the entity's general awareness of the hazards

(5) Identify additional resources, equipment, or personnel needed to prepare for, respond to, and recover from an incident

(6) Include activities performed for the purpose of training and conditioning team members and personnel in appropriate actions

(7) Practice improvisation of activities in a safe environment (Improvisation might be necessary in actual disruptive events because predictions of disruptions are usually flawed.)

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

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

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

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

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

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

A.8.3(8) Coordination between internal and external teams, entities, and entities is one of the primary objectives of exercises and tests. Such teams could include, but are not limited to, incident command management/structure; response organizational structure; emergency support functions; internal/external coordinators or liaisons; all elements of the supply chain, including critical suppliers, purchasing, human resources, and communications (including marketing, website, and social media) teams.

A.8.4 The Homeland Security Exercise Evaluation Program (HSEEP) provides a guide for designing, developing, and evaluating various types of exercises.

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

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

(1) Measurement, sometimes called “assessment” or “observation,” is the function in which the personnel accurately determine exactly what organizational performance has occurred.

(2) Evaluation is the function in which the observed performance is compared with criteria, sometimes called “standards” or “competencies,” to determine if the actual organizational performance meets expectations.

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

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

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

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

Corrective actions should be identified by the following:

(1) Changes to regulations, policy, plans, or procedures

(2) Additions or modifications to facilities, systems, or equipment

(3) Results of exercises and testing

(4) After-action reviews of actual incidents

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

The task group should take the following actions:

(1) Develop options for appropriate corrective action

(2) Make recommendations for a preferred option

(3) Develop an implementation plan, including training if required

(4) Ensure that during the next exercise the corrective actions are evaluated to determine if the corrective actions have been successful

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

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

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

(2) Review of corrective action issues from previous evaluations and identification of possible solutions to the problem

(3) Selection of a corrective action strategy and prioritization of the actions to be taken, as well as an associated schedule for completion

(4) Provision of authority and resources to the individual assigned responsibility and accountability for implementation, so that the designated change can be accomplished

(5) Identification of the resources required to implement the strategy

(6) Check of the progress of completing the corrective action

(7) Forwarding of problems that need to be resolved by higher authorities to the level of authority that can resolve the problem

(8) Once the problem is solved, testing of the solution through exercising

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

Annex B Self-Assessment for Conformity with *NFPA 1600,* 2016 Edition

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

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

Table B.1 Self-Assessment Tool for Conformity with the 2016 Edition of *NFPA 1600*

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
Chapter 4 Program Management **4.1* Leadership and Commitment.** **4.1.1** The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents.			
4.1.2 The leadership commitment shall include the following:			

(1) Support the development, implementation, and maintenance of the program			
(2) Provide necessary resources to support the program			
(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness			
(4) Support corrective action to address program deficiencies			
4.1.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program.			
4.2* Program Coordinator. The program coordinator shall be appointed by the entity's leadership and authorized to develop, implement, administer, evaluate, and maintain the program.			
4.3 Program Committee. **4.3.1*** A program committee shall be established by the entity in accordance with its policy.			
4.3.2 The program committee shall provide input and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program.			
4.3.3* The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation.			
4.4 Program Administration. **4.4.1** The entity shall have a documented program that includes the following: (1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority			
(2)* Program scope, goals, performance, objectives, and metrics for program evaluation			
(3)* Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.5			
(4) Program budget and schedule, including milestones			

(5) Program plans and procedures that include the following:			
(a) Anticipated cost			
(b) Priority			
(c) Resources required			
(6) Records management practices as required by Section 4.7			
(7) Management of change			
4.4.2 The program shall include the requirements specified in Chapters 4 through 9, the scope of which shall be determined through an “all-hazards” approach and the risk assessment.			
4.4.3* Program requirements shall be applicable to preparedness including the planning, implementation, assessment, and maintenance of programs for prevention, mitigation, response, continuity, and recovery.			
4.5 Laws and Authorities. **4.5.1** The program shall comply with applicable legislation, policies, regulatory requirements, and directives.			
4.5.2 The entity shall establish, maintain, and document procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives.			
4.5.3* The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice.			
4.6 Finance and Administration. **4.6.1** The entity shall develop finance and administrative procedures to support the program before, during, and after an incident.			
4.6.2* There shall be a responsive finance and administrative framework that does the following: (1) Complies with the entity's program requirements			
(2) Is uniquely linked to response, continuity, and recovery operations			
(3) Provides for maximum flexibility to expeditiously request, receive, manage, and			

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

(4) Implementation of procedures to store, retrieve, and recover records onsite or offsite			
(5) Protection of records			
(6) Implementation of a record review process			
(7) Procedures coordinating records access			
Chapter 5 Planning **5.1 Planning and Design Process.** **5.1.1*** The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program.			
5.1.2 Strategic planning shall define the entity's vision, mission, and goals of the program.			
5.1.3 A risk assessment and a business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies.			
5.1.4 A risk assessment, a BIA, and a resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans.			
5.1.5* Crisis management planning shall address an event, or series of events, that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders.			
5.1.6 The entity shall include key stakeholders in the planning process.			
5.2* Risk Assessment. **5.2.1** The entity shall conduct a risk assessment.			
5.2.2 The entity shall identify hazards and monitor those hazards and the likelihood and severity of their occurrence over time. **5.2.2.1** Hazards to be evaluated shall include the following:			
(1) Geological:			
(a) Earthquake			
(b) Landslide, mudslide, subsidence			
(c) Tsunami			
(d) Volcano			

(2) Meteorological:			
(a) Drought			
(b) Extreme temperatures (hot, cold)			
(c) Famine			
(d) Flood, flash flood, seiche, tidal surge			
(e) Geomagnetic storm			
(f) Lightning			
(g) Snow, ice, hail, sleet, avalanche			
(h) Wildland fire			
(i) Windstorm, tropical cyclone, hurricane, tornado, water spout, dust storm, sandstorm			
(3) Biological:			
(a) Food-borne illnesses			
(b)* Infectious/communicable/pandemic diseases			
(4) Accidental human-caused:			
(a) Building/structure collapse			
(b)* Entrapment			
(c) Explosion/fire			
(d) Fuel/resource shortage			
(e)* Hazardous material spill or release			
(f) Equipment failure			
(g) Nuclear reactor incident			
(h) Radiological incident			
(i)* Transportation incident			
(j) Unavailability of essential employee(s)			
(k)* Water control structure failure			
(l) Misinformation			
(5) Intentional human-caused:			
(a) Incendiary fire			
(b) Bomb threat			
(c) Demonstrations/civil disturbance/riot/insurrection			
(d) Discrimination/harassment			
(e) Disinformation			
(f) Kidnapping/hostage			

(g) Acts of war			
(h) Missing person			
(i)* Cyber security incidents			
(j) Product defect or contamination			
(k) Robbery/theft/fraud			
(l) Strike or labor dispute			
(m) Suspicious package			
(n)* Terrorism			
(o) Vandalism/sabotage			
(p) Workplace/school/university violence			
(6) Technological:			
(a)* Hardware, software, and network connectivity interruption, disruption, or failure			
(b)* Utility interruption, disruption, or failure			
5.2.2.2* The vulnerability of people, property, operations, the environment, the entity, and the supply chain operations shall be identified, evaluated, and monitored.			
5.2.3 The entity shall conduct an analysis of the impacts of the hazards identified in 5.2.2 on the following: (1) Health and safety of persons in the affected area			
(2) Health and safety of personnel responding to the incident			
(3) Security of information			
(4)* Continuity of operations			
(5) Continuity of government			
(6)* Property, facilities, assets, and critical infrastructure (7) Delivery of the entity's services			
(8) Supply chain			
(9) Environment			
(10)* Economic and financial conditions			
(11) Legislated, regulatory, and contractual obligations			
(12) Reputation of or confidence in the entity			
(13) Work and labor arrangements			

5.2.4 The risk assessment shall include an analysis of the escalation of impacts over time.			
5.2.5* The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts.			
5.2.6 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies.			
5.3 Business Impact Analysis (BIA). **5.3.1** The entity shall conduct a BIA that includes an assessment of how a disruption could affect an entity's operations, reputation, and market share, ability to do business, or relationships with key stakeholders and identifies the resources and capabilities that might be needed to manage the disruptions.			
5.3.1.1 The BIA shall identify processes that are required for the entity to perform its mission.			
5.3.1.2 The BIA shall identify the following resources that enable the processes: (1) Personnel			
(2) Equipment			
(3) Infrastructure			
(4) Technology			
(5) Information			
(6) Supply chain			
5.3.2* The BIA shall evaluate the following: (1) Dependencies			
(2) Single-source and sole-source suppliers			
(3) Single points of failure			
(4) Potential qualitative and quantitative impacts from a disruption to the resources in 5.3.1.2			
5.3.3* The BIA shall identify the acceptable amount of data loss for physical and electronic records to identify the recovery point objective (RPO).			
5.3.4* The BIA shall identify gaps between the RTOs and RPOs and demonstrated capabilities.			

5.3.5* The BIA shall be used in the development of continuity and recovery strategies and plans.			
5.3.6* The BIA shall identify critical supply chains, including those exposed to domestic and international risks, and the timeframe within which those operations become critical to the entity.			
5.4 Resource Needs Assessment.			
5.4.1* The entity shall conduct a resource needs assessment based on the hazards identified in Section 5.2 and the business impact analysis in Section 5.3.			
5.4.2 The resource needs assessment shall include the following: (1)* Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed			
(2) Quantity, response time, capability, limitations, cost, and liabilities			
5.4.3* The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, and materials procured or donated to support the program.			
5.4.4 Facilities capable of supporting response, continuity, and recovery operations shall be identified.			
5.4.5* The need for mutual aid/assistance or partnership agreements shall be determined; if needed, agreements shall be established and documented.			
5.5 Performance Objectives. **5.5.1*** The entity shall establish performance objectives for the program in accordance with Chapter 4 and the elements in Chapters 5 through 9.			
5.5.2 The performance objectives shall address the results of the hazard identification, risk assessment, and business impact analysis.			
5.5.3 Performance objectives shall be developed by the entity to address both short-term and long-term needs.			

5.5.4* The entity shall define the terms *short term* and *long term*.			
Chapter 6 Implementation **6.1 Common Plan Requirements.**			
6.1.1* Plans shall address the health and safety of personnel.			
6.1.2 Plans shall identify and document the following:			
(1) Assumptions made during the planning process			
(2) Functional roles and responsibilities of internal and external entities			
(3) Lines of authority			
(4) The process for delegation of authority			
(5) Lines of succession for the entity			
(6) Liaisons to external entities			
(7) Logistics support and resource requirements			
6.1.3* Plans shall be individual, integrated into a single plan document, or a combination of the two.			
6.1.4* The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required.			
6.2 Prevention. **6.2.1*** The entity shall develop a strategy to prevent an incident that threatens life, property, operations, information, and the environment.			
6.2.2* The prevention strategy shall be kept current using the information collection and intelligence techniques.			
6.2.3 The prevention strategy shall be based on the results of hazard identification and risk assessment, an analysis of impacts, program constraints, operational experience, and cost-benefit analysis.			
6.2.4 The entity shall have a process to monitor the identified hazards and adjust the level of preventive measures to be commensurate with the risk.			
6.3 Mitigation.			

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

6.5.3* Emergency warning, notification, and communications protocols and procedures shall be developed, tested, and used to alert stakeholders potentially at risk from an actual or impending incident.			
6.5.4 Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of prescripted information bulletins or templates.			
6.5.5 Information shall be disseminated through the media, social media, or other means as determined by the entity to be the most effective.			
6.6 Operational Procedures. **6.6.1** The entity shall develop, coordinate, and implement operational procedures to support the program.			
6.6.2 Procedures shall be established and implemented for response to and recovery from the impacts of hazards identified in 5.2.2.			
6.6.3* Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity.			
6.6.4 Procedures shall include the following:			
(1) Control of access to the area affected by the incident			
(2) Identification of personnel engaged in activities at the incident			
(3) Accounting for personnel engaged in incident activities			
(4) Mobilization and demobilization of resources			
6.6.5 Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation.			
6.7 Incident Management.			
6.7.1* The entity shall develop an incident management system to direct, control, and coordinate response, continuity, and recovery operations.			
6.7.1.1* Emergency Operations Centers (EOCs).			

6.7.1.1.1* The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations.			
6.7.1.1.2* The EOCs shall be permitted to be physical or virtual.			
6.7.1.1.3 On activation of an EOC, communications and coordination shall be established between incident command and the EOC.			
6.7.2 The incident management system shall describe specific entity roles, titles, and responsibilities for each incident management function.			
6.7.3* The entity shall establish procedures and policies for coordinating prevention, mitigation, preparedness, response, continuity, and recovery activities.			
6.7.4 The entity shall coordinate the activities specified in 6.7.3 with stakeholders.			
6.7.5 Procedures shall include a situation analysis that incorporates a damage assessment and a needs assessment to identify resources to support activities.			
6.7.6* Emergency operations/response shall be guided by an incident action plan or management by objectives.			
6.7.7 Resource management shall include the following tasks: (1) Establishing processes for describing, taking inventory of, requesting, and tracking resources			
(2) Resource typing or categorizing by size, capacity, capability, and skill			
(3) Mobilizing and demobilizing resources in accordance with the established IMS			
(4) Conducting contingency planning for resource deficiencies			
6.7.8 A current inventory of internal and external resources shall be maintained.			
6.7.9 Donations of human resources, equipment, material, and facilities shall be managed.			
6.8 Emergency Operations/Response Plan.			

6.8.1* Emergency operations/response plans shall define responsibilities for carrying out specific actions in an emergency.			
6.8.2* The plan shall identify actions to be taken to protect people, including people with disabilities and others access and functional needs, information, property, operations, the environment, and the entity.			
6.8.3* The plan shall identify actions for incident stabilization.			
6.8.4 The plan shall include the following: (1) Protective actions for life safety in accordance with 6.8.2			
(2) Warning, notifications, and communication in accordance with Section 6.5			
(3) Crisis communication and public information in accordance with Section 6.4			
(4) Resource management in accordance with 6.7.7			
(5) Donation management in accordance with 6.7.9			
6.9 Continuity and Recovery.			
6.9.1 Continuity.			
6.9.1.1 Continuity plans shall include strategies to continue critical and time-sensitive processes and as identified in the BIA.			
6.9.1.2* Continuity plans shall identify and document the following: (1) Stakeholders that need to be notified			
(2) Processes that must be maintained			
(3) Roles and responsibilities of the individuals implementing the continuity strategies			
(4) Procedures for activating the plan, including authority for plan activation			
(5) Critical and time-sensitive technology, application systems, and information			
(6) Security of information			
(7) Alternative work sites			
(8) Workaround procedures			
(9) Vital records			
(10) Contact lists			

(11) Required personnel			
(12) Vendors and contractors supporting continuity			
(13) Resources for continued operations			
(14) Mutual aid or partnership agreements			
(15) Activities to return critical and time-sensitive processes to the original state			
6.9.1.3 Continuity plans shall be designed to meet the RTO and RPO.			
6.9.1.4 Continuity plans shall address supply chain disruption.			
6.9.2 Recovery.			
6.9.2.1 Recovery plans shall provide for restoration of processes, technology, information, services, resources, facilities, programs, and infrastructure.			
6.9.2.2* Recovery plans shall document the following:			
(1) Damage assessment			
(2) Coordination of the restoration, rebuilding, and replacement of facilities, infrastructure, materials, equipment, tools, vendors, and suppliers			
(3) Restoration of the supply chain			
(4) Continuation of communications with stakeholders			
(5) Recovery of critical and time-sensitive processes, technology, systems, applications, and information			
(6) Roles and responsibilities of the individuals implementing the recovery strategies,			
(7) Internal and external (vendors and contractors) personnel who can support the implementation of recovery strategies and contractual needs			
(8) Adequate controls to prevent the corruption or unlawful access to the entity’s data during recovery			
(9) Compliance with regulations that would become applicable during the recovery			
(10) Maintenance of pre-incident controls			
6.10* Employee Assistance and Support.			

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

7.7* Public Education. A public education program shall be implemented to communicate the following: (1) Potential hazard impacts			
(2) Preparedness information			
(3) Information needed to develop a preparedness plan			
Chapter 8 Exercises and Tests **8.1 Program Evaluation.** **8.1.1** The entity shall evaluate program plans, procedures, training, and capabilities and promote continuous improvement through periodic exercises and tests.			
8.1.2 The entity shall evaluate the program based on post-incident analyses, lessons learned, and operational performance in accordance with Chapter 9.			
8.1.3 Exercises and tests shall be documented.			
8.2* Exercise and Test Methodology. **8.2.1** Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting.			
8.2.2 Exercises shall be designed to assess the maturity of program plans, procedures, and strategies.			
8.2.3 Tests shall be designed to demonstrate capabilities.			
8.3* Design of Exercises and Tests. Exercises shall be designed to do the following: (1) Ensure the safety of people, property, operations, and the environment involved in the exercise or test			
(2) Evaluate the program			
(3) Identify planning and procedural deficiencies			
(4) Test or validate recently changed procedures or plans			
(5) Clarify roles and responsibilities			
(6) Obtain participant feedback and recommendations for program improvement			

(7) Measure improvement compared to performance objectives			
(8)* Improve coordination between internal and external teams and entities			
(9) Validate training and education			
(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity			
(11) Identify additional resources and assess the capabilities of existing resources, including personnel and equipment needed for effective response and recovery			
(12) Assess the ability of the team to identify, assess, and manage an incident			
(13) Practice the deployment of teams and resources to manage an incident			
(14) Improve individual performance			
8.4* Exercise and Test Evaluation. **8.4.1** Exercises shall evaluate program plans, procedures, training, and capabilities to identify opportunities for improvement.			
8.4.2 Tests shall be evaluated as either pass or fail.			
8.5* Frequency.			
8.5.1 Exercises and tests shall be conducted on the frequency needed to establish and maintain required capabilities.			
Chapter 9 Program Maintenance and Improvement **9.1* Program Reviews.** The entity shall maintain and improve the program by evaluating its policies, program, procedures, and capabilities using performance objectives.			
9.1.1* The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action.			
9.1.2* Evaluations shall be conducted on a regularly scheduled basis and when the situation changes to challenge the effectiveness of the existing program.			

9.1.3 The program shall be re-evaluated when a change in any of the following impacts the entity's program: (1) Regulations			
(2) Hazards and potential impacts			
(3) Resource availability or capability			
(4) Entity's organization			
(5)* Funding changes			
(6) Infrastructure, including technology environment			
(7) Economic and geographic stability			
(8) Entity operations			
(9) Critical suppliers			
9.1.4 Reviews shall include post-incident analyses, reviews of lessons learned, and reviews of program performance.			
9.1.5 The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section 4.7.			
9.1.6 Documentation, records, and reports shall be provided to management for review and follow-up.			
9.2* Corrective Action. **9.2.1*** The entity shall establish a corrective action process.			
9.2.2* The entity shall take corrective action on deficiencies identified.			
9.3 Continuous Improvement. The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process.			

Annex C Small Business Preparedness Guide

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

C.1 Figure C.1 shows a sample small business preparedness guide.

FIGURE C.1 Sample Small Business Preparedness Guide.

Small Business Preparedness Guide

NFPA 1600 is intended to meet the unique needs of all entities, regardless of size. The objective for small businesses or entities might be to simply increase preparedness. The following guidance material is intended to highlight and simplify key aspects of NFPA 1600® where small entities might wish to focus their preparedness efforts.

This guidance material can help an entity better identify where it needs to focus to protect its assets (people, property, operations); continue to provide goods and/or services; maintain cash flow; preserve its competitive advantage and reputation; and provide the ability to meet legal, regulatory, financial, and contractual obligations.
Key sections of NFPA 1600 are mentioned in parentheses for easy reference.

Program Management (Chapter 4) Leadership and Commitment (Section 4.1)

The entity's leadership should demonstrate commitment to its emergency management/business continuity program by taking an active role. In small entities, the owner or organizational leader might be responsible for the entire program.
Has someone been appointed to be responsible for developing and maintaining the organization's program? Yes No

Planning (Chapter 5)

Document your emergency management/business continuity plans and procedures. Plans can be simple but should consider:

- How the entity will respond to an emergency or disaster (emergency operations/response)
- What the entity needs to communicate, who the organization needs to communicate with, and how the entity will go about communicating with those stakeholders (crisis communications and some degree crisis management)
- How the entity will recover from a disaster (recovery) and keep its business operations going after a disaster happens (continuity)
- What the entity can do to prevent a disaster in the first place (prevention) or limit the damage when a disaster does happen (mitigation)
- How all these plans fit together and how they provide for the future of the organization (strategic/crisis management)

We have reviewed and documented basic steps to take in an emergency - such as an evacuation route and a meeting place. Yes No

We have contact lists for all employees, customers, and key vendors. Yes No

We have outlined the steps for restoring the business if we lose computers/technology. Yes No

Risk Assessment (Section 5.2)

Identify which hazards are most likely to occur and which will have the biggest consequences or be most severe for the entity if they do occur. The intent of a risk assessment is to help an entity better allocate its resources by being cognizant of and focusing attention on prevention, mitigation, preparation, and a plan on how to recover from the highest risk threats.

Additional considerations for small entities include:

- Natural hazard recognition - Business owners/operators should be cognizant of any natural hazards that their location is exposed to such as floods, hurricanes, and earthquakes. Local emergency management and insurance companies should be able to provide this information. Make sure the building's construction and location is resistant to such hazards.

- Exposure - Exposure is "what's nearby that can hurt you." It could be an adjacent combustible building, wildfire potential, or a hazardous occupancy nearby (e.g., a chemical plant or a gas station). It could also be a nearby river that poses a flood risk. To evaluate an entity's exposure, go up on the roof and look around the facility. Then walk inside and around the facility and consider the potential hazards - an oven fire in a restaurant, faulty wiring, equipment failure that could bring manufacturing to a standstill. Finally, drive around the block or area that borders the facility. Ask the question, "What can hurt me or my facility?"

See 5.2.2.1 for a list of common hazards to consider including natural hazards, human-caused events, and technology-caused incidents.

We have reviewed which hazards are most likely to occur in our area and consider these hazards when we do our planning. Yes No

We have reviewed the potential hazards posed by neighbors and taken that into consideration as well. Yes No

Business Impact Analysis (Section 5.3)

Identify critical business operations and analyze the impact of losing them. This is helpful to better prioritize plans and procedures, especially if resources are limited. Think through the steps an entity will need to take to continue to operate if hazards/impacts occur.

Additional considerations for small entities include:

- Backup data- If it's critical or important to an entity, then it should be backed up. How frequently the backup occurs is dictated by the amount of data that can be lost without inflicting unreasonable damage to the entity (usually measured in dollar amounts, reputation, etc.).

- Backup hardware- Backed-up data is only half the equation. How will the backed-up data be processed or accessed?

We have backups of inventory records identifying how much is on hand and where it is.
Yes No

We have backups of accounts receivable and accounts payable information identifying who and how much. Yes No

We have backups of client names and contact information (e-mail, address, phone numbers, etc.).
Yes No

We have backups of other information critical to the organization, such as equipment lists, drawings, specifications, etc. Yes No

We have determined the availability of equipment to access the data we backed up.
Yes No

<u>Resource Needs Assessment (Section 5.4)</u>

What resources will be needed to resume operation if a hazard occurs? What training is needed? We have determined where resources will come from if we need to resume operation following an incident and we have a location to store physical resources and supplies. Yes No

<u>Additional considerations for small entities include:</u>

- Fire prevention program – Fire is the most common and significant threat to most businesses. Owner/operators can reduce the probability of fire by implementing fire safety programs, especially where flammable liquids or gasses are handled.

- Automatic sprinklers - Locating a business or operation in buildings that are fully protected by automatic sprinklers significantly reduces an entity's exposure to a catastrophic incident. Many natural catastrophes are often compounded by fire.

We have a fire safety program. Yes No

We have automatic sprinklers.
Yes No

- Adequate insurance - Business interruption (BI) and extra expense (EE) coverage is often overlooked. "All risk" policies should be considered as well, as they are more expansive and in some cases allow for customization. In all cases, policyholders should know what is included in their policy and determine what can or should be added, based on their specific needs.

- If an entity's premises are damaged as a result of a covered loss and can operate at a temporary location, extra expense coverage might cover the costs above and beyond normal operating expenses. Among other things, it could cover the cost of relocation, rent for the temporary location, and advertising to bring back customers or those that utilize the entity's services.

- Business interruption insurance (also known as business income insurance) compensates an entity for lost income if it has to vacate the premises due to a covered loss under the property insurance policy, such as a fire. Business interruption coverage might provide compensation for lost profits - based on the entity's financial records - had the event not happened. It also covers continuing operating expenses, such as utilities and rent on the property, which continue to accrue even though business activities have been temporarily suspended.

- Entities that depend heavily on suppliers should consider contingent business interruption (CBI) insurance and contingent extra expense coverage. CBI and contingent extra expense coverage reimburse lost profits and extra expenses resulting from an interruption of business at the premises of a customer or supplier. It is possible to get protection against a set list of suppliers or in some cases to purchase blanket coverage protecting any supplier's shutdown.

We have adequate insurance coverage for our needs. Yes No

We have BI insurance. Yes No

We have extra expense insurance. Yes No

- Emergency services preplan - It can be helpful to make sure that local emergency services (fire rescue, police, hazmat, etc.) become familiar with an entity's operations and the challenges service providers might face when they arrive. It's also an opportunity to clarify any expectations the entity has of the service providers and vice versa.

If we have hazards on site, or pose a potential hazard to our neighbors as a result of our operations, we have shared this information with the fire department and invited them for a meeting to discuss. Yes No

Implementation (Chapter 6)

An entity does not need to have separate emergency response, incident management, and business continuity/recovery plans, but those who have a role in implementing the plans should be aware of what is expected of them.

Plans should focus on prevention and mitigation of the hazards, risks, vulnerabilities, and impacts that have been identified.

Do all employees know how to respond to any incident? Yes No

Communications (Sections 6.4 and 6.5)

Identify the entity's most important audiences (employees, customers, media, investors, regulators, vendors, etc.) and predetermine how to communicate with them following an emergency or disaster.

The simplest way to determine who the entity's key stakeholders are is to consider who is most important to the organization, who is most interested in the organization, or who could be hurt by problems that befall the organization.

Determine how you will notify key audiences of an emergency. Make sure there is a backup. Plan how critical information will be provided to employees as well as key external audiences.

Figure out how to coordinate dissemination of that information to ensure it is consistent.

Additional considerations for small entities include:

- Employee contact info.- Ensure emergency contact information has been gathered and a means of communicating with employees has been established. Has a process been devised to make sure employees can be accounted for in a disaster?

- Media contacts - Most entities use the media for promotion (e.g., TY, radio, print, social websites). The same media can be used to help recover from a crisis. Pre-planning how the entity will communicate in a crisis situation is key.

- Customer lists - Every entity has clients or customers who have an interest in the organization.

Being able to communicate very quickly after an incident allows the entity to help their clients and customers understand what has happened and how it will affect them, and also provides an opportunity to reassure them that the organization will be there to meet their needs. These lists can be used for e-mail blasts or informational mailings.

- E-mail - Here's where backup data comes in. Blasts to the entity's clients/customers lets them know the entity's status.

- Social media -   Same as for e-mail.

We have employee contact lists and have determined how to account for employees following a emergency or disaster. Yes No

We have key customer/supplier/vendor contact lists as well and have determined how to coordinate a steady stream of information to them? Yes No

Emergency Operations/Response (Section 6.8)

Identify emergency actions to protect people and stabilize the emergency. Anyone tasked with a role will need a copy of the parts of the action plan that pertain to them.

Additional considerations for small entities include:

- 911/alarms - Simple procedures such as knowing to call 911 or to activate manual alarms should be communicated to all personnel via orientation and follow-up training. Fast response can mean the difference between life and death, and it can minimize property damage.

- Evacuation plan - Every organization should have an evacuation plan. Exits should be well marked and kept clear.

Evacuation drills should be conducted on a .regular basis under realistic conditions.

We have provided emergency procedure orientation as well as follow-up training to all personnel. Yes No

We conduct evacuation drills on a regular basis. Yes No

Business Continuity and Recovery (Section 6.9)

Determine how to recover critical or time-sensitive processes as quickly as possible after a disaster. Stipulate roles and responsibilities - not only the jobs that have to be done and who will do those jobs, but also who will be in charge if the owner or manager is not available during an emergency or disaster.

Additional considerations for small entities include:

- Location strategy - If the entity loses its facility, where will it relocate?
    - Do you know your building, utility, and infrastructure needs, including the following:
        - Purchasing – what is the local commercial real estate market like?
        - Leasing/renting - is it possible on a short-term or mid-term basis?
        - Consider a mutual aid agreement with a similar entity
    - Allow employees to work from home, when applicable
- Processing strategy - How will the entity continue to provide goods or services to its clients/customers?
- Outsourcing - Is there a way to provide goods or services through a third-party vendor?
- Mutual aid - Is there a similar provider who can fill the entity's needs by agreement and the entity would reciprocate if the roles were reversed?

We have determined where to relocate if we are not able to operate out of our facility following a disaster. Yes No

We have determined how to continue to provide goods and services to our clients/customers following a disaster. O Yes O No

Training and Education (Chapter 7) and Exercises and Tests (Chapter 8)

Regardless of the size of the entity, periodic awareness, exercises, and tests can be helpful to do the following:

- Practice responses
- Validate plans/procedures
- Ensure those tasked with a response are clear on what is expected of them
- Improve hazard awareness
- Identify any capability gaps or needed resource improvements

For small entities, this could entail periodic testing of the following:

- IT backups to ensure they are adequately capturing information
- Fire drills

We train/drill on plans/procedures as part of new employee orientation with annual updates. Yes No

Program Maintenance and Improvement (Chapter 9)

Regularly review plans and procedures with an eye toward identifying ways to improve the program. Triggers for program improvement include, but are not limited to, the following:

- Identification of new hazards or exposures
- Addition (or elimination) of regulations or resources
- Budget changes
- Addition (or elimination) of products or services
- Personnel turnover

We review the program at least annually to identify improvements? Yes No

Resources

There are free planning resources available through various sources. For example, the Metropolitan Washington Council of Governments has an online tool available that walks small business owners through the process. The tool provides simple directions for plugging in appropriate information and generates a simple printable plan tailored for the entity. [http://www.mwcog.ogr/secmi ty/security/continuity /intro.asp]

Similarly, the Insurance Institute for Business & Home Safety has an "Open for Business®" planning toolkit, available free of charge. Open for Business EZ® is composed of a workbook, a multimedia trainer series to help users manage their time and walk through the planning process, and some Advanced Track materials. In addition, it provides mitigation tips for protecting property from natural hazard events.[www.DisasterSafety.org/business_protection]

Ready.gov is a free planning website sponsored by FEMA. There are resources to help develop a business continuity plan and information to plan and prepare for events.

ReadyRating.org is a tool developed by the Red Cross to help with preparing for emergency and disasters.

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

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

D.1 Starting with the 2010 edition of *NFPA 1600*, the standard was organized in the PDCA format.

Plan is the process to determine goals and objectives and the desired outcome(s), and concludes with an agreement to proceed.

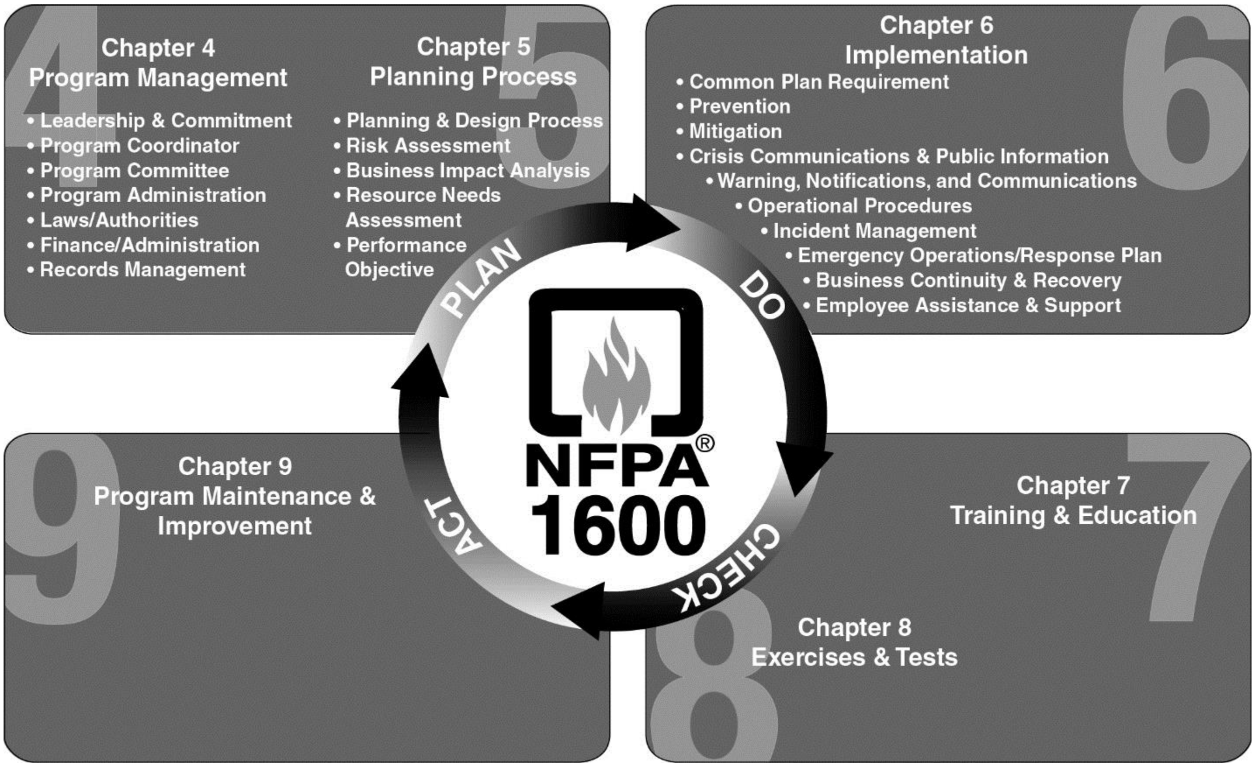
Do is executing the actions needed to achieve the desired outcome(s)

Check is evaluating whether the desired outcome has been achieved by those actions

Act is addressing any gaps between desired outcome and actual outcome

Figure D.1 depicts the PDCA cycle.

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



Annex E Crosswalk Between *NFPA 1600* and DRII Professional Practices, CSA Z1600, and Federal Continuity Directive 1

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

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

Table E.1(a) Cross-Reference of *NFPA 1600* to DRII Professional Practices

NFPA 1600 (2016) Chapter/Section	DRII *Professional Practices for Business Continuity Practitioners* (2012) Subject Area

Chapter 4 Program Management	
4.1 Leadership and Commitment	1. Project Initiation and Management
4.2 Program Coordinator	1. Project Initiation and Management
4.3 Program Committee	1. Project Initiation and Management
4.4 Program Administration	1. Project Initiation and Management
4.5 Laws and Authorities	1. Program Initiation and Management 3. Business Impact Analysis 9. Crisis Communications 10. Coordinating with External Agencies
4.6 Finance and Administration	1. Project Initiation and Management
4.7 Records Management	3. Business Impact Analysis
Chapter 5 Planning	
5.1 Planning and Design Process	2. Risk Evaluation and Control
	3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation
5.2 Risk Assessment	2. Risk Evaluation and Control
5.3 Business Impact Analysis	3. Business Impact Analysis
5.4 Resource Needs Assessment	1. Program Initiation and Management 2. Risk Evaluation and Control 3. Business Impact Analysis 5. Emergency Response and Operations 6. Business Continuity Plan Development and Implementation
5.5 Performance Objectives	1. Project Initiation and Management
Chapter 6 Implementation	
6.1 Common Plan Requirements	1. Project Initiation 2. Risk Evaluation and Control 3. Business Impact Analysis 4. Business Continuity Strategies 5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program

	8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications 10. Coordination with External Agencies
6.2 Prevention	2. Risk Evaluation and Control 5. Emergency Response and Operations
6.3 Mitigation	2. Risk Evaluation and Control 5. Emergency Response and Operations 9. Crisis Communications
6.4 Crisis Communications and Public Information	5. Emergency Response and Operations 6. Business Continuity Plan Development and Implementation 9. Crisis Communications 10. Coordination with External Agencies
6.5 Warning, Notifications, and Communications	5. Emergency Preparedness and Response 7. Awareness and Training Program 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications 10. Coordinating with External Agencies
6.6 Operational Procedures	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications
6.7 Incident Management	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 9. Crisis Communications 10. Coordinating with External Agencies
6.8 Emergency Operations/Response Plan	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program

	8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications
6.9 Business Continuity and Recovery	4. Business Continuity Strategies 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications
6.10 Employee Assistance and Support	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications 10. Coordinating with External Agencies
Chapter 7 Training and Education	8. Business Continuity Plan Exercise, Audit and Maintenance
7.1 Training and Education Curriculum	
7.2 Goal of the Curriculum	
7.3 Scope and Frequency of Instruction	5. Emergency Preparedness and Response
7.4 Incident Management System Training	5. Emergency Preparedness and Response 10. Coordination with External Agencies
7.5 Recordkeeping	
7.6 Regulatory and Program Requirements	10. Coordination with External Agencies
7.7 Public Education	
Chapter 8 Exercises and Tests	5. Emergency Preparedness and Response 8. Business Continuity Plan Exercise, Audit and Maintenance 10. Coordination with External Agencies
8.1 Program Evaluation	
8.2 Exercise and Test Methodology	
8.3 Design of Exercises and Tests	
8.4 Exercise and Test Evaluation	
8.5 Frequency	

Chapter 9 Program Maintenance and Improvement	5. Emergency Preparedness and Response 6. Business Continuity Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, Audit and Maintenance 9. Crisis Communications 10. Coordinating with External Agencies
9.1 Program Reviews	
9.2 Corrective Action	
9.3 Continuous Improvement	

DRII: DRI International, Inc.

Table E.1(b) Cross-Reference of *NFPA 1600–13* to CSA Z1600–14

***NFPA 1600* (2013) Chapter/Section**	**CSA Z1600-14, Emergency Management and Business Continuity Programs Chapter/Section**
Chapter 4 Program Management	**4 Program Management**
4.1 Leadership and Commitment	4.1 Leadership and Commitment
4.2 Program Coordinator	4.2 Program Coordinator
4.3 Program Committee	4.3 Program Committee
4.4 Program Administration	4.4 Program Administration
4.5 Laws and Authorities	4.5 Compliance with Laws and Authorities
4.6 Finance and Administration	4.6 Financial Management
4.7 Records Management	4.4.6 Records Management
Chapter 5 Planning	**5 Planning**
5.1 Planning and Design Process	5.1 Planning Process
5.2 Risk Assessment	5.3 Risk Assessment
5.3 Business Impact Analysis	5.4 Impact Analysis
5.4 Resource Needs Assessment	4.7 Resources
	5.4.3 6.2.7 Resource Management
5.5 Performance Objectives	4.4.3 Goals, Objectives, and Performance Measures
Chapter 6 Implementation	**6 Implementation**
6.1 Common Plan Requirements	5.2 Common Plan Requirements

	5.5.2 Prevention 5.5.3 Mitigation 6.1.2 Prevention 6.1.3 Mitigation
6.4 Crisis Communications and Public Information	5.5.8 Communications
	6.2.5.2 Communications Assessment 6.2.5.3 Communication Systems 6.2.5.4 Communication Procedures 6.2.5.6 Emergency Communication and Warning Capability 6.2.5.7 Emergency Information 6.2.5.8 Crisis Information 6.3.5 Communications 6.3.6 Emergency Information
6.5 Warning, Notifications, and Communications	6.2.5 Communication and Warning 6.2.5.6 Emergency Communication and Warning Capability
6.6 Operational Procedures	6.3.1 Operational Procedures
6.7 Incident Management	6.5 Incident Management System
6.8 Emergency Operations/Response Plan	5.5.5 Response 6.2.4 Response Plan
	6.3 Response
6.9 Business Continuity and Recovery	6.10 Business Continuity 5.5.6 Continuity 6.2.6 Continuity 6.3.3 Continuity 5.5.7 Recovery 6.4 Recovery 6.4.1 Recovery Procedures 6.4.2 Recovery Assessment
6.10 Employee Assistance and Support	—
Chapter 7 Training and Education	
7.1 Curriculum	6.2.8.2
7.2 Goal of the Curriculum	—

7.3 Scope and Frequency of Instruction	6.2.8.3
7.4 Incident Management System Training	—
7.5 Recordkeeping	6.2.8.4
7.6 Regulatory and Program Requirements (pertaining to training curriculum)	4.5 Compliance with Laws and Authorities (pertaining to overall program)
7.7 Public Education	6.2.5.5 Public Awareness and Education
	6.3.7 Public Awareness
Chapter 8 Exercises and Tests	**7 Program Evaluation**
8.1 Program Evaluation	7.1 Evaluation
8.2 Exercise and Test Methodology	—
8.3 Design of Exercises and Tests	—
8.4 Exercise and Test Evaluation	7.2 Exercises and Tests
	7.2.1 Exercises
	7.2.2 Tests
8.5 Frequency	—
Chapter 9 Program Maintenance and Improvement	**8 Management Review**
9.1 Program Reviews	8 Management Review
	8.1 Senior Management Review
	7.3 Audit and Review
9.2 Corrective Action	7.4 Corrective Action
9.3 Continuous Improvement	8.2 Continual Improvement

Table E.1(c) Cross-Reference of *NFPA 1600* to FCD-1

***NFPA 1600* (2016)** **Chapter/Section**	**Federal Continuity Directive 1 Chapter/Section**
Chapter 4 Program Management	**8 Program Management**
4.1 Leadership and Commitment	9 Elements of a Viable Continuity Capability (9.b Orders of Succession and 9.c Delegations of Authority) 12 Roles and Responsibilities (assigned responsibilities are outlined in NSPD-51/HSPD-20 and the NCPIP)
4.2 Program Coordinator	9 Elements of a Viable Continuity Capability (9.g Human Resources)
4.3 Program Committee	—
4.4 Program Administration	8 Program Management

4.5 Laws and Authorities	—
4.6 Finance and Administration	—
4.7 Records Management	9 Elements of a Viable Continuity Capability (9.f Essential Records Management)
Chapter 5 Planning	**8 Program Management**
5.1 Planning and Design Process	
5.2 Risk Assessment	8 Program Management (Risk Management)
5.3 Business Impact Analysis	9 Elements of a Viable Continuity Capability (9.a Essential Functions)
5.4 Resource Needs Assessment	—
5.5 Performance Objectives	—
Chapter 6 Implementation	**11 Continuity Plan Operational Phases and Implementation**
6.1 Common Plan Requirements	8 Program Management (Annex A Program Plans and Procedures)
6.2 Prevention	—
6.3 Mitigation	—
6.4 Crisis Communications and Public Information	9 Elements of a Viable Continuity Capability (9.e Continuity Communications)
6.5 Warning, Notifications, and Communications	
6.6 Operational Procedures	8 Program Management (Annex A Program Plans and Procedures)
6.7 Incident Management	—
6.8 Emergency Operations/Response Plan	—
6.9 Business Continuity and Recovery	8 Program Management (Annex A Program Plans and Procedures) 9 Elements Of A Viable Continuity Capability (9.j Reconstitution)
6.10 Employee Assistance and Support	9 Elements of a Viable Continuity Capability (9.g Human Resources)
Chapter 7 Training and Education	**9 Elements of a Viable Continuity Capability (9.h Tests, Training, and Exercises)**
7.1 Curriculum	
7.2 Goal of Curriculum	
7.3 Scope and Frequency of Instruction	
7.4 Incident Management System Training	
7.5 Recordkeeping	
7.6 Regulatory and Program Requirements	

7.7 Public Education	
Chapter 8 Exercises and Tests	**9 Elements of a Viable Continuity Capability (9.h Tests, Training, and Exercises)**
8.1 Program Evaluation	
8.2 Exercise and Test Methodology	
8.3 Design of Exercises and Tests	
8.4 Exercise and Test Evaluation	
8.5 Frequency	
Chapter 9 Program Maintenance and Improvement	**11 Continuity Plan Operational Phases and Implementation**
9.1 Program Reviews	
9.2 Corrective Action	
9.3 Continuous Improvement	
—	9 Elements of a Viable Continuity Capability (9.d Continuity Facilities)
—	9 Elements of a Viable Continuity Capability (9.i Devolution of Control and Direction)
—	10 Coordination with Tribal, State, Territorial, Local Governments and the Private Sector

Annex F *NFPA 1600* 2016, Edition as an MSS.

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

F.1 Introduction.

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

This annex was created using the *ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2014, Annex SL.9 High level structure, identical core text and common terms and core definitions for use in Management Systems Standards*. Cross-references to *NFPA 1600* Chapters 1 through 9 are provided in brackets. Paragraphs without a cross-reference are part of the ISO identical text for management system standards (MSS), common management system (MS) terms, and core definitions from the *ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2014, Annex SL Appendix 2.*

F.2 Scope. [Chapter 1]

F.2.1 Scope. This standard shall establish a common set of criteria for all-hazards disaster/emergency management and business continuity/continuity of operations programs, hereinafter referred to as “the program.” [1.1]

F.2.2 Purpose. This standard provides the fundamental criteria for preparedness including the planning, implementation, assessment, and maintenance of programs for prevention, mitigation, response, continuity, and recovery. [1.2]

F.2.3 Application. This document shall apply to public, private, and nonprofit entities and nongovernmental entities (NGOs). [1.3]

F.3 Normative References. [Chapter 2]

F.3.1 General. The documents or portions thereof listed in this chapter are referenced within this standard and shall be considered part of the requirements of this document. [2.1]

F.3.2 NFPA Publications. (Reserved) [2.2]

F.3.3 Other Publications. *Merriam-Webster's Collegiate Dictionary*, 11th edition, Merriam-Webster, Inc., Springfield, MA, 2003. [2.3]

F.3.4 References for Extracts in Mandatory Sections. (Reserved) [2.4]

F.4 Terms and Definitions. [Chapter 3]

F.4.1 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. [3.1]

F.4.2 NFPA Official Definitions. [3.2]

F.4.2.1 Approved. Acceptable to the authority having jurisdiction. [3.2.1]

F.4.2.2 Authority Having Jurisdiction (AHJ). An organization, office, or individual responsible for enforcing the requirements of a code or standard, or for approving equipment, materials, an installation, or a procedure. [3.2.2]

F.4.2.3 Shall. Indicates a mandatory requirement. [3.2.3]

F.4.2.4 Should. Indicates a recommendation or that which is advised but not required. [3.2.4]

F.4.2.5 Standard. An NFPA Standard, the main text of which contains only mandatory provisions using the word “shall” to indicate requirements and that is in a form generally suitable for mandatory reference by another standard or code or for adoption into law. Nonmandatory provisions are not to be considered a part of the requirements of a standard and shall be located in an appendix, annex, footnote, informational note, or other means as permitted in the NFPA Manuals of Style. When used in a generic sense, such as in the phrase “standards development process” or “standards development activities,” the term “standards” includes all NFPA Standards, including Codes, Standards, Recommended Practices, and Guides. [3.2.5]

F.4.3 General Definitions. [3.3]

F.4.3.1 Access and Functional Needs. Persons requiring special accommodations because of health, social, economic, or language challenges. [3.3.1]

F.4.3.2 All-Hazards. An approach for prevention, mitigation, response, continuity, and recovery that addresses a full range of threats and hazards, including natural, human-caused, and technology-caused. [3.3.3]

F.4.3.3 Business Continuity/Continuity of Operations. An ongoing process to ensure that the necessary steps are taken to identify the impacts of potential losses and maintain viable recovery strategies, recovery plans, and continuity of operations. [3.3.3]

F.4.3.4 Business Impact Analysis (BIA). A management level analysis that identifies, quantifies, and qualifies the impacts resulting from interruptions or disruptions of an entity's resources. The analysis may identify time-critical functions, recovery priorities, dependencies, and interdependencies so that recovery time objectives can be established and approved. [3.3.4]

F.4.3.5 Capability. The ability to perform required actions. [3.3.5]

F.4.3.6 Competence. Demonstrated ability to apply knowledge and skills to achieve intended results. [3.3.6]

F.4.3.7 Continual Improvement. Recurring process of enhancing the management program in order to achieve improvements in overall performance consistent with the entity's policy, goals, and objectives. [3.3.7]

F.4.3.8 Continuity. A term that includes business continuity/continuity of operations (COOP), operational continuity, succession planning, continuity of government (COG), which support the resilience of the entity. [3.3.8]

F.4.3.9 Crisis. An issue, event, or series of events that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders. [3.3.9]

F.4.3.10 Crisis Management. The ability of an entity to manage incidents that have the potential to cause significant security, financial, or reputational impacts. [3.3.10]

F.4.3.11 Damage Assessment. A determination of the effects of the incident on humans, on physical, operational, economic characteristics: and on the environment. [3.3.11]

F.4.3.12 Disaster/Emergency Management. An ongoing process to prevent, mitigate, prepare for, respond to, maintain continuity during, and to recover from an incident that threatens life, property, operations, information, or the environment. [3.3.12]

F.4.3.13 Entity. A governmental agency or jurisdiction, private or public entity, partnership, nonprofit organization, or other organization that has emergency management and continuity of operations responsibilities. [3.3.13]

F.4.3.14 Exercise. A process to assess, train, practice, and improve performance in an organization. [3.3.14]

F.4.3.15 Incident. An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe. [3.3.15]

F.4.3.16 Incident Action Plan. A verbal plan, written plan, or combination of both, that is updated throughout the incident and reflects the overall incident strategy, tactics, risk management, and member safety requirements approved by the incident commander. [3.3.16]

F.4.3.17 Incident Management System (IMS). The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational structure and designed to aid in the management of resources during incidents. [3.3.17]

F.4.3.18 Interoperability. The ability of diverse personnel, systems, and organizations to work together seamlessly. [3.3.18]

F.4.3.19 Mitigation. Activities taken to reduce the impacts from hazards. [3.3.19]

F.4.3.20 Mutual Aid/Assistance Agreement. A prearranged agreement between two or more entities to share resources in response to an incident. [3.3.20]

F.4.3.21 Preparedness. Ongoing activities, tasks, and systems to develop, implement, and maintain the program. [3.3.21]

F.4.3.22 Prevention. Activities to avoid or stop an incident from occurring. [3.3.22]

F.4.3.23 Recovery. Activities and programs designed to return conditions to a level that is acceptable to the entity. [3.3.23]

F.4.3.24 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. [3.3.24]

F.4.3.25 Response. Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, or the environment. [3.3.25]

F.4.3.26 Risk Assessment. The process of hazard identification, and the analysis of probabilities, vulnerabilities, and impacts. [3.3.26]

F.4.3.27 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. [3.3.27]

F.4.3.28 Supply Chain. A network of individuals, organizations, activities, information, resources, and technology involved in creating and delivering a product or service from supplier to end user. [3.3.28]

F.4.3.29 Test. Procedure for evaluation with a pass or fail result. [3.3.29]

F.4.3.30 Vital Records. Information critical to the continued operation or survival of an entity. [3.3.30]

F.4.4 ISO Terms and Definitions. For the purposes of this document, the following terms and definitions apply.

F.4.4.1 Organization. Person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives (F.4.4.8).

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

F.4.4.2 Interested Party (Preferred Term) Stakeholder (Admitted Term). Person or *organization* (F.4.4.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity.

F.4.4.3 Requirement. Need or expectation that is stated, generally implied or obligatory.

Note 1: “Generally implied” means that it is custom or common practice for the entity and interested parties that the need or expectation under consideration is implied.

Note 2: A specified requirement is one that is stated, for example in documented information.

F.4.4.4 Management System. Set of interrelated or interacting elements of an *entity* (F.4.4.1) to establish *policies* (F.4.4.7), and *objectives* (F.4.4.8), and *processes* (F.4.4.12) to achieve those objectives.

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

Note 2: The system elements include the entity's structure, roles and responsibilities, planning and operation.

Note 3: The scope of a entity system might include the whole of the entity, specific and identified functions of the entity, specific and identified sections of the entity, or one or more functions across a group of entities.

F.4.4.5 Top Management. Person or group of people who directs and controls an *organization* (F.4.4.1) at the highest level.

Note 1: Top management has the power to delegate authority and provide resources within the entity.

Note 2: If the scope of the *management system* (F.4.4.4) covers only part of an entity, then top management refers to those who direct and control that part of the entity.

F.4.4.6 Effectiveness. Extent to which planned activities are realized and planned results achieved.

F.4.4.7 Policy. Intentions and direction of an *entity* (F.4.4.1), as formally expressed by its *top management* (F.4.4.5).

F.4.4.8 Objective. Result to be achieved.

Note 1: An objective can be strategic, tactical, or operational.

Note 2: Objectives can relate to different disciplines (such as financial, health and safety, and environmental goals) and can apply at different levels [such as strategic, entity-wide, project, product, and *process* (F.4.4.12)].

Note 3: An objective can be expressed in other ways, for example, for example as an intended outcome, a purpose, an operational criterion, as a disaster/emergency management and business continuity/continuity of operations objective, or by the use of other words with similar meaning (e.g., aim, goal, or target).

Note 4: In the context of disaster/emergency management and business continuity/continuity of operations management systems, disaster/emergency management and business continuity/continuity of operations objectives are set by the entity, consistent with the disaster/emergency management and business continuity/continuity of operations policy, to achieve specific results.

F.4.4.9 Risk. Effect of uncertainty.

Note 1: An effect is a deviation from the expected — positive and/or negative.

Note 2: Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.

Note 3: Risk is often characterized by reference to potential “events” (as defined in ISO Guide 73:2009,) and “consequences” (as defined in ISO Guide 73:2009,), or a combination of these.

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

F.4.4.10 Competence. Ability to apply knowledge and skills to achieve intended results.

F.4.4.11 Documented Information. Information required to be controlled and maintained by an entity (F.4.4.1) and the medium on which it is contained.

Note 1: Documented information can be in any format and media, and from any source.

Note 2: Documented information can refer to the following:

(1) The *management system* (F.4.4.4), including related *processes* (F.4.4.12)

(2) Information created in order for the entity to operate (documentation)

(3) Evidence of results (records)

F.4.4.12 Process. Set of interrelated or interacting activities that transforms inputs into outputs.

F.4.4.13 Performance. Measurable result.

Note 1: Performance can relate either to quantitative or qualitative findings.

Note 2: Performance can relate to the management of activities, *processes* (F.4.4.10), products (including services), systems or (F.4.4.1).

F.4.4.14 Outsource (Verb). Make an arrangement where an external *entity* (F.4.4.1) performs part of an entity's function or *process* (F.4.4.12).

Note: An external entity is outside the scope of the *management system* (F.4.4.10), although the outsourced function or process is within the scope.

F.4.4.15 Monitoring. Determining the status of a system, a process (F.4.4.12), or an activity.

Note: To determine the status, there might be a need to check, supervise or critically observe.

F.4.4.16 Measurement. *Process* (F.4.4.12) to determine a value.

F.4.4.17 Audit. Systematic, independent, and documented *process* (F.4.4.12) for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

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

Note 2: An internal audit is conducted by the entity itself, or by an external party on its behalf.

Note 3: “Audit evidence” and “audit criteria” are defined in ISO 19011.

F.4.4.18 Conformity. Fulfillment of a *requirement* (F.4.4.3).

F.4.4.19 Nonconformity. Non-fulfillment of a *requirement* (F.4.4.3).

F.4.4.20 Corrective Action. Action to eliminate the cause of a *nonconformity*) and to prevent recurrence.

F.4.4.21 Continual Improvement. Recurring activity to enhance *performance* (F.4.4.13).

F.5 Context of the Entity.

F.5.1 Understanding the Entity and Its Context. The entity shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its disaster/emergency management and business/continuity of operations continuity management system.

F.5.2 Understanding the Needs and Expectations of Interested Parties. The entity shall determine:

(1) The interested parties that are relevant to the disaster/emergency management and business continuity/continuity of operations management system

(2) The relevant requirements of these interested parties.

F.5.3 Determining the Scope of the Disaster/Emergency and Business Continuity/Continuity of Operations Management System. The entity shall determine the boundaries and applicability of the disaster/emergency management and business continuity/continuity of operations management system to establish its scope. When determining this scope the entity shall consider:

(1) The external and internal issues referred to in F.4.1

(2) The requirements referred to in Section F.5.2

The scope shall be available as documented information.

F.5.4 Disaster/Emergency Management and Business Continuity/Continuity of Operations Management System. The entity shall, establish, implement, maintain and continually improve a disaster/emergency management and business continuity/continuity of operations management system, including the processes needed and their interactions, in accordance with the requirements of this International Standard.

F.5.5 Laws and Authorities. [4.5]

F.5.5.1 The program shall comply with applicable legislation, policies, regulatory requirements, and directives. [4.5.1]

F.5.5.2 The entity shall establish maintain, and document procedure(s) to comply with applicable legislation, policies, regulatory requirements, and directives. [4.5.2]

F.5.5.3 The entity shall implement a strategy for addressing the need for revisions to legislation, regulations, directives, policies, and industry codes of practice. [4.5.3]

F.6 Leadership.

F.6.1 Leadership and Commitment. Top management shall demonstrate leadership and commitment with respect to the disaster/emergency management and business continuity/continuity of operations management system by:

(1) Ensuring that the disaster/emergency management and business continuity/continuity of operations policy and objectives are established and are compatible with the strategic direction of the entity.

(2) Ensuring the integration of the disaster/emergency management and business continuity/continuity of operations management system requirements into the entity's business processes;

(3) Ensuring that the resources needed for the disaster/emergency management and business continuity/continuity of operations management system are available

(4) Communicating the importance of effective disaster/emergency management and business continuity/continuity of operations management and of conforming to the requirements

(5) Ensuring that the disaster/emergency management and business continuity/continuity of operations management system achieves its intended outcome(s)

(6) Directing and supporting persons to contribute to the effectiveness of the disaster/emergency management and business continuity/continuity of operations management system

(7) Promoting continual improvement

Supporting other relevant management roles to demonstrate leadership as it applies to the position's areas of responsibility.

Note 1: Reference to "business" in this International Standard can be interpreted broadly to mean those activities that are core to the purposes of the entity's existence.

Note 2: Reference to "business" in this International Standard should be interpreted broadly to mean those activities that are core to the purposes of the organization's existence.

F.6.2 Leadership and Commitment. [4.1]

F.6.2.1 The entity leadership shall demonstrate commitment to the program to prevent, mitigate the consequences of, prepare for, respond to, maintain continuity during, and recover from incidents. [4.1.1]

F.6.2.2 The leadership commitment shall include the following: [4.1.2]

(1) Support the development, implementation, and maintenance of the program

(2) Provide necessary resources to support the program

(3) Ensure the program is reviewed and evaluated as needed to ensure program effectiveness

(4) Support corrective action to address program deficiencies

F.6.2.3 The entity shall adhere to policies, execute plans, and follow procedures developed to support the program. [4.1.3]

F.6.3 Policy. Top management shall establish a disaster/emergency management and business continuity/continuity of operations policy that:

(1) Is appropriate to the purpose of the entity

(2) Provides a framework for setting disaster/emergency management and business continuity/continuity of operations objectives

(3) Includes a commitment to satisfy applicable requirements

(4) Includes a commitment to continual improvement of the disaster/emergency management and business continuity/continuity of operations management system

The disaster/emergency management and business continuity/continuity of operations policy shall:

(1) Be available as documented information

(2) Be communicated within the entity

(3) Be available to interested parties, as appropriate

F.6.3.1 Program Administration. [4.4]

F.6.3.1.1 The entity shall have a documented program that includes the following: [4.4.1]

(1) Executive policy, including vision, mission statement, roles, and responsibilities, and enabling authority

(2) Program scope, goals, performance objectives, and metrics for program evaluation

(3) Applicable authorities, legislation, regulations, and industry codes of practice as required by F.5.5

(4) Program budget and schedule, including milestones

(5) Program plans and procedures that include the following:

  (a) Anticipated cost

  (b) Priority

  (c) Resources required

(6) Records management practices as required by F.8.5.4

(7) Management of change

F.6.3.1.2 The program shall include the requirements specified in Sections F.5 to F.11, the scope of which shall be determined through an "all-hazards" approach, and the risk assessment. [4.4.2]

F.6.3.1.3 Program requirements shall be applicable for preparedness including the planning, implementation, assessment, and maintenance of programs for prevention, mitigation, preparedness, response, continuity, and recovery. [4.4.3]

F.6.4 Organizational Roles, Responsibilities, and Authorities. Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the entity.

Top management shall assign the responsibility and authority for:

(1) Ensuring that the disaster/emergency management and business continuity/continuity of operations management system conforms to the requirements of this International Standard

(2) Reporting on the performance of the disaster/emergency management and business continuity/continuity of operations management system to top management

F.6.4.1 Program Coordinator. The program coordinator shall be appointed by the entity's leadership and authorized to develop, implement, administer, evaluate, and maintain the program. [4.2]

F.6.4.2 Program Committee. [4.3]

F.6.4.2.1 A program committee shall be established by the entity in accordance with its policy. [4.3.1]

F.6.4.2.2 The program committee shall provide input, and/or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program. [4.3.2]

F.6.4.2.3 The program committee shall include the program coordinator and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity and shall solicit applicable external representation. [4.3.3]

F.7 Planning. [Chapter 5]

F.7.1 Actions to Address Risks and Opportunities. When planning for the disaster/emergency management and business continuity/continuity of operations management system, the entity shall consider the issues referred to in Section 5.1 and the requirements referred to in Section 5.2 and determine the risks and opportunities that need to be addressed to:

(1) Give assurance that the disaster/emergency management and business continuity/continuity of operations management system can achieve its intended outcome(s).

(2) Prevent, or reduce, undesired effects.

(3) Achieve continual improvement.

The entity shall plan:

(1) Actions to address these risks and opportunities

(2) How to:

  (a) Integrate and implement the actions into its disaster/emergency management and business continuity/continuity of operations management system processes

  (b) Evaluate if the effectiveness of these actions have been effective

F.7.2 Disaster/Emergency Management and Business Continuity/Continuity of Operations Objectives and Planning to Achieve Them.

F.7.2.1 The entity shall establish disaster/emergency management and business continuity/continuity of operations objectives at relevant functions and levels.

The disaster/emergency management and business continuity/continuity of operations objectives shall:

(1) Be consistent with the disaster/emergency management and business continuity/continuity of operations policy

(2) Be measurable (if practicable)

(3) Take into account applicable requirements

(4) Be monitored

(5) Be communicated

(6) Updated as appropriate

The entity shall retain documented information on the disaster/emergency management and business continuity/continuity of operations objectives.

When planning how to achieve its disaster/emergency management and business continuity/continuity of operations objectives, the entity shall determine:

(1) What will be done

(2) What resources will be required

(3) Who will be responsible

(4) When it will be completed

(5) How the results will be evaluated

F.7.2.2 Performance Objectives. [5.5]

F.7.2.2.1 The entity shall establish performance objectives for the program in accordance with Section F.5 and the elements in Sections F.7through F.11. [5.5.1]

F.7.2.2.2 The performance objectives shall address the results of the hazard identification, risk assessment, and business impact analysis. [5.5.2]

F.7.2.2.3 Performance objectives shall be developed by the entity to address both short-term and long-term needs. [5.5.3]

F.7.2.2.4 The entity shall define the terms *short term* and *long term*. [5.5.4]

F.7.3 Planning and Design Process. [5.1]

F.7.3.1 The program shall follow a planning process that develops strategies, plans, and required capabilities to execute the program. [5.1.1]

F.7.3.2 Strategic planning shall define the entity's vision, mission, and goals of the program. [5.1.2]

F.7.3.3 Risk assessment and business impact analysis (BIA) shall develop information to prepare prevention and mitigation strategies. [5.1.3]

F.7.3.4 A risk assessment, BIA, and resource needs assessment shall develop information to prepare emergency operations/response, crisis communications, continuity, and recovery plans. [5.1.4]

F.7.3.5 Crisis management planning shall address an event, or series of events, that severely impacts or has the potential to severely impact an entity's operations, reputation, market share, ability to do business, or relationships with key stakeholders. [5.1.5]

F.7.3.6 The entity shall include key stakeholders in the planning process. [5.1.6]

F.7.4 Risk Assessment. [5.2]

F.7.4.1 The entity shall conduct a risk assessment. [5.2.1]

F.7.4.2 The entity shall identify hazards and monitor those hazards and the likelihood and severity of their occurrence over time. [5.2.2]

F.7.4.2.1 Hazards to be evaluated shall include the following: [5.2.2.1]

(1) Geological:

- (a) Earthquake
- (b) Landslide, mudslide, subsidence
- (c) Tsunami
- (d) Volcano

(2) Meteorological:

- (a) Drought
- (b) Extreme temperatures (hot, cold)
- (c) Famine
- (d) Flood, flash flood, seiche, tidal surge
- (e) Geomagnetic storm
- (f) Lightning
- (g) Snow, ice, hail, sleet, avalanche
- (h) Wildland fire
- (i) Windstorm, tropical cyclone, hurricane, tornado, water spout, dust storm, sandstorm

(3) Biological:

- (a) Food-borne illnesses
- (b) Infectious/communicable/pandemic diseases

(4) Accidental human-caused:

- (a) Building/structure collapse
- (b) Entrapment
- (c) Explosion/fire
- (d) Fuel/resource shortage

(e) Hazardous material spill or release

(f) Equipment failure

(g) Nuclear reactor incident

(h) Radiological incident

(i) Transportation incidents

(j) Unavailability of essential employee(s)

(k) Water control structure failure

(l) Misinformation

(5) Intentional human-caused:

(a) Incendiary fire

(b) Bomb threat

(c) Demonstrations/civil disturbance/riot/insurrection

(d) Discrimination/harassment

(e) Disinformation

(f) Kidnapping/hostage

(g) Acts of war

(h) Missing person

(i) Cyber security incidents

(j) Product defect or contamination

(k) Robbery/theft/fraud

(l) Strike or labor dispute

(m) Suspicious package

(n) Terrorism

(o) Vandalism/sabotage

(p) Workplace/school/university violence

(6) Technological:

(a) Hardware, software, and network connectivity interruption, disruption, or failure

(b) Utility interruption, disruption, or failure

F.7.4.2.2 The vulnerability of people, property, operations, the environment, the entity, and the supply chain operations shall be identified, evaluated, and monitored. [5.2.2.2]

F.7.4.3 The entity shall conduct an analysis of the impact of the hazards identified in F.7 on the following: [5.2.3]

(1) Health and safety of persons in the affected area

(2) Health and safety of personnel responding to the incident

(3) Security of information

(4) Continuity of operations

(5) Continuity of government

(6) Property, facilities, assets, and critical infrastructure

(7) Delivery of the entity's services

(8) Supply chain

(9) Environment

(10) Economic and financial conditions

(11) Regulatory and contractual obligations

(12) Reputation of or confidence in the entity

(13) Work and labor arrangements

F.7.4.4 The risk assessment shall include an analysis of the escalation of impacts over time. [5.2.4]

F.7.4.5 The analysis shall evaluate the potential effects of regional, national, or international incidents that could have cascading impacts. [5.2.5]

F.7.4.6 The risk assessment shall evaluate the adequacy of existing prevention and mitigation strategies. [5.2.6]

F.7.5 Business Impact Analysis (BIA). [5.3]

F.7.5.1 The entity shall conduct a (BIA) that includes an assessment of how a disruption could affect the entity's operations, reputation, market share, ability to do business relationships with key stakeholders and identify the resources and capabilities needed to manage the disruptions. [5.3.1]

F.7.5.1.1 The BIA shall identify processes that are required for the entity to perform its mission. [5.3.1.1]

F.7.5.1.2 The BIA shall identify the following resources that enable the processes: [5.3.1.2]

(1) Personnel

(2) Equipment

(3) Infrastructure

(4) Technology

(5) Information

(6) Supply chain

F.7.5.2 The BIA shall evaluate the following: [5.3.2]

(1) Dependencies

(2) Single-source and sole-source suppliers

(3) Single points of failure

(4) Potential qualitative and quantitative impacts from a disruption to the resources in F.7.5.1.2

F.7.5.2.1 The BIA determine the point in time [recovery time objective(RTO)] when the impacts of the disruption become unacceptable to the entity. [5.3.2.1]

F.7.5.3 The BIA shall identify the acceptable amount of data loss for physical and electronic records to identify recovery point objective (RPO). [5.3.3]

F.7.5.4 The BIA identify gaps between the RTOs and RPOs and demonstrated capabilities. [5.3.4]

F.7.5.5 The BIA shall be used in the development of continuity and recovery strategies and plans. [5.3.5]

F.7.5.6 The BIA shall identify critical supply chains, including those exposed to domestic and international risks, and the timeframe within which those operations become critical to the entity. [5.3.6]

F.8 Support.

F.8.1 Resources. The entity shall determine and provide the resources needed for the establishment, implementation, maintenance, and continual improvement of the disaster/emergency management and business continuity/continuity of operations management system.

F.8.1.1 Resource Needs Assessment. [5.4]

F.8.1.1.1 The entity shall conduct a resource needs assessment based on the hazards identified in F.7.4 and the business impact analysis in F.7.5. [5.4.1]

F.8.1.1.2 The resource needs assessment shall include the following: [5.4.2]

(1) Human resources, equipment, training, facilities, funding, expert knowledge, materials, technology, information, intelligence, and the time frames within which they will be needed

(2) Quantity, response time, capability, limitations, cost, and liabilities

F.8.1.1.3 The entity shall establish procedures to locate, acquire, store, distribute, maintain, test, and account for services, human resources, equipment, and materials procured or donated to support the program. [5.4.3]

F.8.1.1.4 Facilities capable of supporting response, continuity, and recovery operations shall be identified. [5.4.4]

F.8.1.1.5 Agreements. The need for mutual aid/assistance or partnership agreements shall be determined; if needed, agreements shall be established and documented. [5.4.5]

F.8.1.2 Resource Management.

F.8.1.2.1 Resource management shall include the following tasks: [6.7.7]

(1) Establishing processes for describing, taking inventory of, requesting, and tracking resources

(2) Resource typing or categorizing resources by size, capacity, capability, and skill

(3) Mobilizing and demobilizing in accordance with the established IMS

(4) Conducting contingency planning for resource deficiencies

F.8.1.2.2 A current inventory of internal and external resources shall be maintained. [6.7.8]

F.8.1.2.3 Donations of human resources, equipment, material, and facilities shall be managed. [6.7.9]

F.8.1.3 Finance and Administration. [4.6]

F.8.1.3.1 The entity shall develop finance and administrative procedures to support the program before, during, and after an incident. [4.6.1]

F.8.1.3.2 There shall be a responsive finance and administrative framework that does the following: [4.6.2]

(1) Complies with the entity's program requirements

(2) Is uniquely linked to response, continuity, and recovery operations

(3) Provides for maximum flexibility to expeditiously request, receive, manage, and apply funds in a nonemergency environment and in emergency situations to ensure the timely delivery of assistance

F.8.1.3.3 Procedures shall be created and maintained for expediting fiscal decisions in accordance with established authorization levels, accounting principles, governance, requirements, and fiscal policy. [4.6.3]

F.8.1.3.4 Finance and administrative procedures shall include the following: [4.6.4]

(1) Responsibilities for program finance authority, including reporting relationships to the program coordinator

(2) Program procurement procedures

(3) Payroll

(4) Accounting systems to track and document costs

(5) Management of funding from external sources

(6) Crisis management procedures that coordinate authorization levels and appropriate control measures

(7) Documenting financial expenditures incurred as a result of an incident and for compiling claims for future cost recovery

(8) Identifying and accessing alternative funding sources

(9) Managing budgeted and specially appropriated funds

F.8.2 Competence. The entity shall:

(1) Determine the necessary competence of person(s) doing work under its control that affects its disaster/emergency management and business continuity/continuity of operations performance

(2) Ensure that these persons are competent on the basis of appropriate education, training, or experience

(3) Where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken

(4) Retain appropriate documented information as evidence of competence

Note: Applicable actions can include, for example, the provision of training to, the mentoring of, or the re-assignment of currently employed persons; or the hiring or contracting of competent persons.

F.8.2.1 Training [Chapter 7]

F.8.2.1.1 Curriculum. The entity shall develop and implement a competency-based training and education curriculum that supports all employees who have a role in the program. [7.1]

F.8.2.1.2 Goal of the Curriculum. The goal of the curriculum shall be to create awareness and enhance the knowledge, skills, and abilities required to implement, support, and maintain the program. [7.2]

F.8.2.1.3 Scope and Frequency of Instruction. The scope of the curriculum and the frequency of instruction shall be identified. [7.3]

F.8.2.1.4 Incident Management System Training. Personnel shall be trained in the entity's incident management system (IMS) and other components of the program to the level of their involvement. [7.4]

F.8.2.1.5 Recordkeeping. Records of training and education shall be maintained as specified in Section F.8.5.5. [7.5]

F.8.2.1.6 Regulatory and Program Requirements. The curriculum shall comply with applicable regulatory and program requirements. [7.6]

F.8.2.1.7 Public Education. A public education program shall be implemented to communicate the following: [7.7]

(1) The potential impacts of a hazard

(2) Preparedness information

(3) Information needed to develop a preparedness plan

F.8.3 Awareness. Persons doing work under the entity's control shall be aware of:

(1) The disaster/emergency management and business continuity/continuity of operations policy

(2) Their contribution to the effectiveness of the disaster/emergency management and business continuity/continuity of operations management system, including the benefits of improved disaster/emergency management and business continuity/continuity of operations performance

(3) The implications of not conforming with the disaster/emergency management and business continuity/continuity of operations management system requirements

F.8.4 Communication. The entity shall determine the internal and external communications relevant to the disaster/emergency management and business continuity/continuity of operations management system, including:

(1) On what it will communicate

(2) What to communicate

(3) With whom to communicate

(4) How to communicate

F.8.4.1 Crisis Communications and Public Information. [6.4]

F.8.4.1.1 The entity shall develop a plan and procedures to disseminate information to and respond to requests for information from the following audiences before, during, and after an incident: [6.4.1]

(1) Internal audiences, including employees

(2) External audiences, including the media, access and functional needs populations, and other stakeholders

F.8.4.1.2 The entity shall establish and maintain a crisis communications or public information capability that includes the following: [6.4.2]

(1) Central contact facility or communications hub

(2) Physical or virtual information center

(3) System for gathering, monitoring, and disseminating information

(4) Procedures for developing and delivering coordinated messages

(5) Protocol to clear information for release

F.8.4.2 Warning, Notifications, and Communications. [6.5]

F.8.4.2.1 The entity shall determine its warning, notification, and communications needs. [6.5.1]

F.8.4.2.2 Warning, notification, and communications systems shall be reliable, redundant, and interoperable. [6.5.2]

F.8.4.2.3 Emergency warning, notification, and communications protocols and procedures shall be developed, tested, and used to alert stakeholders potentially at risk from an actual or impending incident. [6.5.3]

F.8.4.2.4 Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of prescripted information bulletins or templates. [6.5.4]

F.8.5 Documented Information.

F.8.5.1 General. The entity's disaster/emergency management and business continuity/continuity of operations management system shall include:

(1) Documented information required by this International Standard;

(2) Documented information determined by the entity as being required for the effectiveness of the disaster/emergency management and business continuity/continuity of operations management system.

Note: The extent of documented information for a disaster/emergency management and business continuity/continuity of operations management system can differ from one entity to another due to:

(1) The size of entity and its type of activities, processes, products, and services

(2) The complexity of processes and their interactions

(3) The competence of persons

F.8.5.2 Common Plan Requirements. [6.1]

F.8.5.2.1 Plans shall address the health and safety of personnel. [6.1.1]

F.8.5.2.2 Plans shall identify and document the following:

(1) Assumptions made during the planning process

(2) Functional roles and responsibilities of internal and external agencies, entities, departments, and positions

(3) Lines of authority

(4) The process for delegation of authority

(5) Lines of succession for the entity

(6) Liaisons to external entities

(7) Logistics support and resource requirements [6.1.2]

F.8.5.2.3 Plans shall be individual, integrated into a single plan document, or a combination of the two. [6.1.3]

F.8.5.2.4 The entity shall make sections of the plans available to those assigned specific tasks and responsibilities therein and to key stakeholders as required. [6.1.4]

F.8.5.3 Creating and Updating. When creating and updating documented information the entity shall ensure appropriate:

(1) Identification and description (e.g., a title, date, author, number, or reference number)

(2) Format (e.g., language, software version, graphics) and media (e.g., paper, electronic)

(3) Review and approval for suitability and adequacy

F.8.5.4 Control of Documented Information. Documented information required by the disaster/emergency management and business continuity/continuity of operations management system and by this International Standard shall be controlled to ensure:

(1) It is available and suitable for use, where and when it is needed

(2) It is adequately protected (e.g., from loss of confidentiality, improper use, or loss of integrity)

For the control of documented information, the entity shall address the following activities, as applicable:

(1) Distribution, access, retrieval and use

(2) Storage and preservation, including preservation of legibility

(3) Control of changes (e.g., version control)

(4) Retention and disposition.