Second Revision No. 1-NFPA 1600-2018 [Global Comment]

Throughout the document:

Change "emergency management and business continuity/continuity of operations programs" to "crisis/disaster/emergency management and business continuity/continuity of operations programs".

Change "emergency management and business continuity/continuity of operations community" to "crisis/disaster/emergency management and business continuity/continuity of operations community".

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Mar 27 12:19:59 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to align with the current title of the standard based on changes already made during the first draft. In general, the first draft placed greater emphasis on crisis management.

Response Message:

Second Revision No. 21-NFPA 1600-2018 [Global Comment]

Move Chapter 9 Execution to Chapter 7 and renumber subsequent sections.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:56:08 EDT 2018

Committee Statement

Committee Statement: The committee has reconsidered the best location for this Chapter and determined it to be Chapter 7. It also maintains alignment with the standard of Plan, Do, Check, Act.

Response Message:

Second Revision No. 28-NFPA 1600-2018 [Global Comment]

Throughout the document:

Change "the program" to "program".

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 10:41:35 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to allow the scope to be applied when "program" is used.

Response Message:

Second Revision No. 42-NFPA 1600-2018 [Global Comment]

See Attached new Annex L.

Supplemental Information

File Name	Description	Approved
SR_42_section_new_Annex_L.docx	New annex.--For staff use	
1600-Global_SR-42_Annex_L.docx	For ballot	

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Tue Apr 03 12:18:29 EDT 2018

Committee Statement

Committee Statement: Chapters 6, 8, and 9 of NFPA 1600, and especially §§ 6.6, 6.7, 6.8 and 6.9 along with Annexes A and K, require facilities to use coordinated planning, preparedness and operational practices. In each case, data interoperability is necessary for success. This annex was developed to assist practitioners to better understand the elements of data interoperability. The essence of data interoperability is the ability to share data with any organization across platforms in real time with minimal time of conversion. The ideal is to be able to use any software that can have immediate access to the data.

There are many software products marketed for data interoperability. This annex does not recommend any product, nor does it call for practitioners to acquire or rely on such a product. Instead, it provides criteria by which the organizations needs and capabilities are assessed and plans can be developed to fill capability gaps.

Proposed Draft Annex L - Emergency Management, Continuity, and Crisis Management Data Interoperability

Response Message:

Public Comment No. 1-NFPA 1600-2017 [Global Input]

Public Comment No. 5-NFPA 1600-2017 [Global Input]

Annex L Emergency Management, Continuity, and Crisis Management Data Interoperability

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

L.1 Interoperability.

Chapters 6, 8, and 9, in conjunction with the respective sections in Annex A as well as Annex K, required the organization to practice incident and resource management using situation analysis and coordination, emergency operations/response using situation analysis and crisis communication, and continuity using a variety of data and communication resources. In all these cases, the success of the activity depends upon good data kept in an interoperable system so that access by all those responsible for planning, making operational decisions, or communicating during a crisis have the same and current information.

Accordingly, the organization must create and maintain such a system. The vision of success for such a system is that the data it contains be accurate and updated, that it be accessible during planning as well as during a crisis, that it be easily used and accessed by the entire range of potential users, and that it be kept in a fashion that will maintain these traits during even catastrophic events.

While every organization working to comply with *NFPA 1600* will have its own set of critical data elements, there are some commonalities. For example, data elements that capture information on the organization's critical and time-sensitive processes and the status of key personnel will all be critical in following the requirements of Sections 6.6, 6.7, 6.8, and 6.9 regardless of the nature of the organization's operations.

Many users will immediately be drawn to software products to fill these needs. This annex does not recommend any software product nor does it necessarily stand for the proposition that software is the solution.

Instead, the organization must assess the hazards it might face and evaluate its current data interoperability capabilities in the arenas of emergency management, continuity, and crisis management. Most organizations will find that in comparison to the vision of success, their current data interoperability systems will have capability gaps.

The next step is to strategically plan to fill such gaps. While there is great temptation to reach for a quick solution, such solutions often bring their own additional capability gaps in the areas of financial burdens, the need for training and staffing support, the difficulties of system operation and maintenance, and the usefulness and reliability of the system during incidents. These new or additional capability gaps must be factored into the strategic plan.

As the vision of success notes as its first priority, data accuracy and updates are of paramount importance. It is pointless to have a wonderful software system if the data it contains is not accurate and updated. The practical aspects of data creation and maintenance must remain top of mind in the strategic planning process.

The strategic plan to fill gaps is a process. The organization must establish its data interoperability priorities. It is valid for an organization to prioritize communication during an incident while another might prioritize the value of data in continuity and recovery as long as these initial prioritizations are not viewed as completing the process. Planning to fill these gaps represent a process with many steps, all of which should demonstrate progress toward achieving the requirements of *NFPA 1600*.

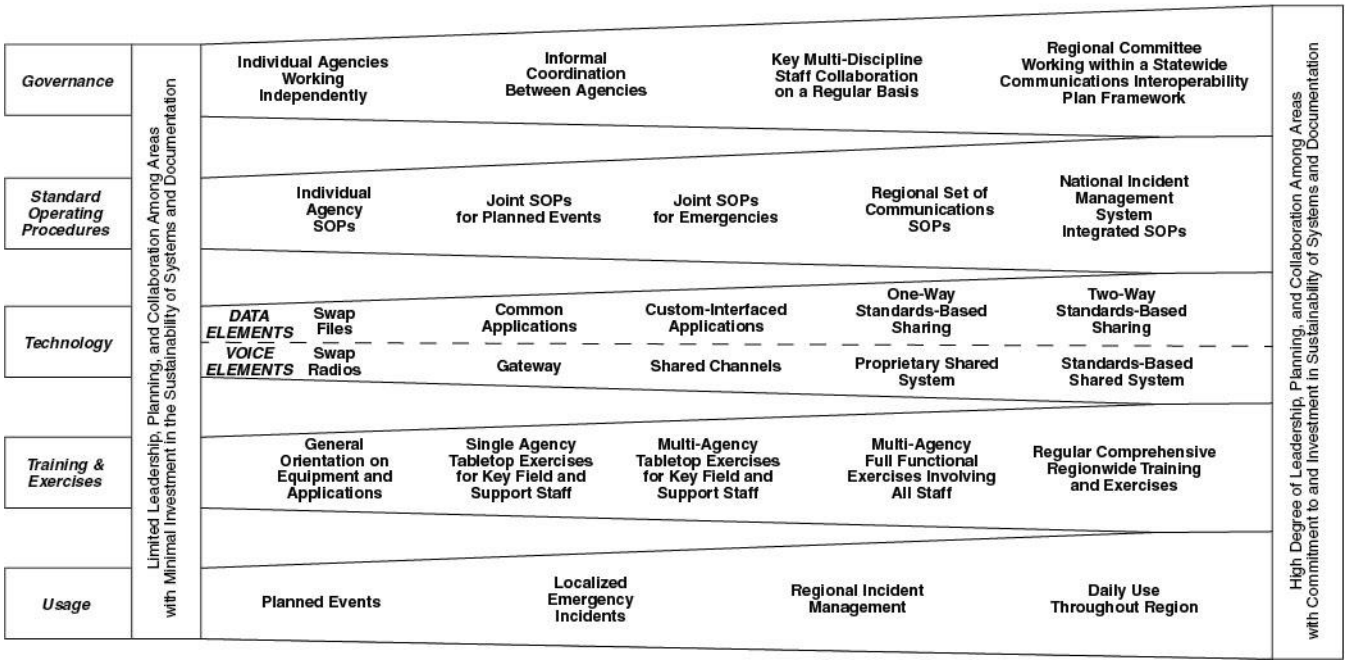
Data interoperability is such a key foundation for emergency management, continuity, and crisis management that the techniques required in Chapters 6, 8, and 9 must be applied to this function. For example, the base assumptions under which the system was created must be constantly reevaluated to determine if they are still valid. Points of failure must be identified and plans to bypass these failures put in place. The data interoperability system must be tested repeatedly under a variety of scenarios. Identifying failures, finding corrections, and implementing enhancements are as much a part of good data interoperability as they are of emergency management, continuity, and crisis management generally.

One example is DHS SAFECOM Interoperability Continuums, which could be particularly useful to share an early common view on data interoperability. (See Figure L.1.)

Figure L.1 DHS SAFECOM Interoperability Continuum.

Homeland Security

Interoperability Continuum



Second Revision No. 29-NFPA 1600-2018 [Detail]

In section E.6.1 Leadership and Commitment delete Note 2.

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Tue Apr 03 11:02:02 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to align with the NFPA Manual of Style (MOS).
Response Message:

Second Revision No. 2-NFPA 1600-2018 [Section No. 1.2]

1.2* Purpose.

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

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 crisis/ disaster/emergency management and business continuity/continuity of operations. NFPA 1616 is based upon an integrated program described in *NFPA 1600*.

Starting with the 2010 edition of *NFPA 1600*, the standard was organized in the Plan-Do-Check-Act (PDCA) format, as follows:

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

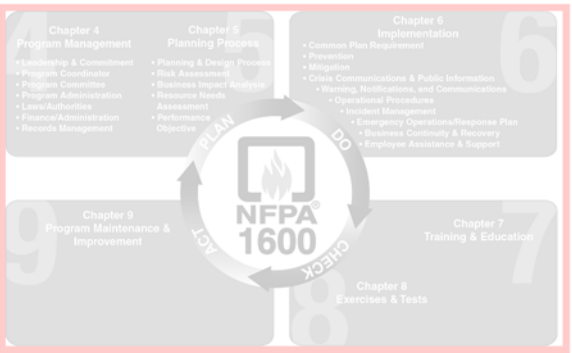
Do is executing the actions needed to achieve the desired outcome(s).

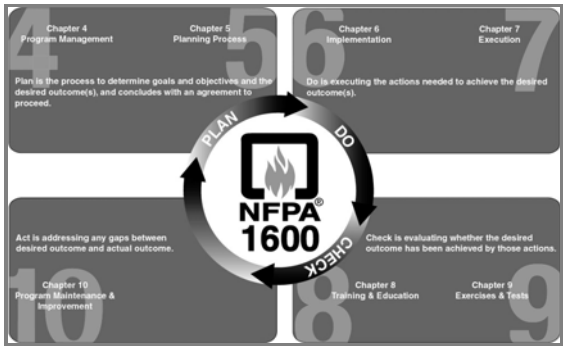
Check is evaluating whether the desired outcome(s) has been achieved by those actions.

Act is addressing any gaps between desired outcome(s) and actual outcome(s).

Figure A.1.2 depicts the PDCA cycle.

Figure A.1.2 The Plan-Do-Check-Act (PDCA) Cycle.





Supplemental Information

File Name	Description	Approved
1600_SR_3_A.1.2_Final.png	For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Mar 27 13:33:44 EDT 2018

Committee Statement

Committee Statement: Execution was added to align with changes made during the First Draft (i.e. the addition of Chapter 7).

Figure A.1.2: The committee has updated the image based on changes to the standard from the first draft. It correlates the chapters with the Plan, Do, Check, Act. It comes from the deming model of continuous improvement.

Response Message:

Second Revision No. 4-NFPA 1600-2018 [Section No. 1.3]

1.3* Application.

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

A.1.3

The application of *NFPA 1600* within the private sector is described in detail in the ~~*Implementing NFPA 1600, National Preparedness Standard,*~~ *NFPA 1600 Handbook* 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~~)~~ (APELL) for Technological Hazards is described in Annex G. Annex G describes both international and domestic applications.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Mar 27 14:21:33 EDT 2018

Committee Statement

Committee Statement: The annex has been updated to the most current publication in relation to NFPA 1600.

Response Message:

Second Revision No. 9-NFPA 1600-2018 [Section No. 3.3.15]

3.3.15 Incident.

An event that has the potential to cause interruption, disruption, loss, emergency, ~~crisis,~~ disaster, or catastrophe, and can escalate into a crisis.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:03:50 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction the committee made correct a typo.

Response Message:

Second Revision No. 11-NFPA 1600-2018 [Section No. 4.4.2]

4.4.2

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

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:20:52 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to comply with the NFPA Manual of Style (MOS).

Response Message:

Second Revision No. 12-NFPA 1600-2018 [Section No. 4.4.3]

4.4.3

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

4.4.4*

The program committee shall solicit applicable external representation.

A.4.4.4

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.

The entity should determine if local government agencies and nonprofit or nongovernmental organizations have adopted relevant local emergency response, preparedness, and resiliency policies, programs, or training efforts.

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Wed Mar 28 15:22:21 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to comply with the NFPA Manual of Style (MOS).
Response Message:

Second Revision No. 44-NFPA 1600-2018 [Section No. 6.9.4]

6.9.4*

The plan shall include the following:

(1) Protective actions for life safety in accordance with 6.9.2.

(2) Warning, notifications, and communication in accordance with Section 6.6.

(3) Crisis communication and public information in accordance with Section 6.5

(4) Resource management in accordance with 6.8.7

(5) Donation management in accordance with 6.8.9

A.6.9.4

The emergency operations/response plan should include data interoperability, which is the ability to share data with any organization across platforms in real time with minimal time of conversion. (See Annex L for more information.)

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 10 07:05:34 EDT 2018

Committee Statement

Committee Statement: The annex adds procedures to help emergency management, continuity, and crisis management

on the dissemination of information across multiple platforms. Note the committee reviewed and

adopted a version of this draft in the first meeting, but it was omitted in error.

Response Message:

Second Revision No. 23-NFPA 1600-2018 [Section No. 9.4]

7.4 Activate Incident Management ~~Plan~~ System .

7.4.1

The entity shall execute procedures from the documented plans in accordance with ~~the following:~~ Sections 6.5, 6.8, 6.9, and 6.10.

~~Crisis Communications and Public Information~~

~~Section Incident Management~~

~~Section Emergency Operations/Response Plan~~

~~Section , Continuity and Recovery~~

.

7.4.2

The entity shall execute its incident management ~~plan~~ system and activities in support of established objectives and tasks.

7.4.3

On activation of an emergency operations center (EOC), communications and coordination shall be established between incident command and the EOC.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 16:03:12 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to align with terminology in Chapter 6. The changes are necessary for consistency within the standard.

Response Message:

Second Revision No. 7-NFPA 1600-2018 [Section No. 10.1.2]

10.1.2*

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

A.10.1.2

The program should be reviewed on a regularly scheduled basis, after major changes to or within the entity (e.g., new facility, process, product, or policy), after scheduled exercises (i.e., 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.

The program might also need to be reviewed based on lessons learned from external influences, such as relevant changes to one of the standards referenced in Annex D .

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 14:42:27 EDT 2018

Committee Statement

Committee Statement: Per the NFPA Manual of Style (MOS) the committee is including a reference to Annex D to point the user to further guidance.

Response Message:

Second Revision No. 24-NFPA 1600-2018 [Section No. 10.1.5]

10.1.5

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

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 16:05:14 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to align with changes from the first draft.

Response Message:

Second Revision No. 10-NFPA 1600-2018 [Section No. A.4.1]

A.8.2

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

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:17:42 EDT 2018

Committee Statement

Committee Statement: The committee is moving the annex to the correct location based on changes from the First Draft.

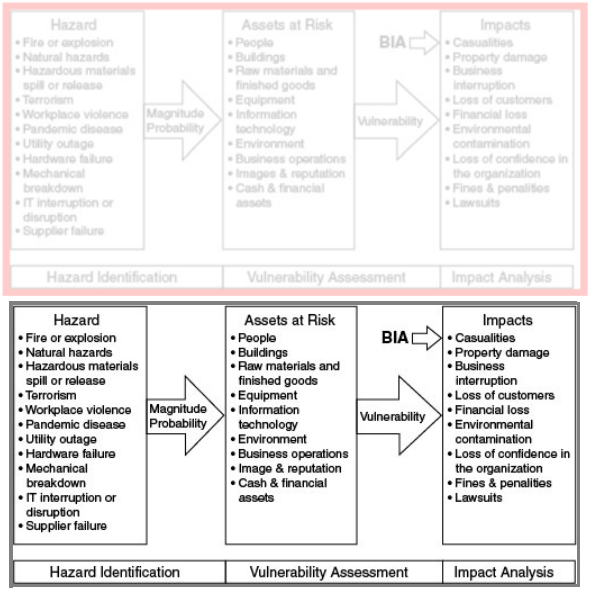
Response Message:

Second Revision No. 26-NFPA 1600-2018 [Section No. A.5.1.3]

A.5.1.3

The results of a risk assessment and an impact analysis identify the highest potential risks and the risks with the highest impact into the entity. This will allow the entity to focus prevention and mitigation measures on those risks that are likeliest to occur and/or those that would have the greatest impact. *(See Figure A.5.1.3.)*

Figure A.5.1.3 Risk Assessment Process.



Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 16:29:48 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction.

Response Message:

Second Revision No. 38-NFPA 1600-2018 [Section No. A.6.1.1]

A.6.1.1

The plan developed by the program needs to address the safety and health of personnel and needs to be part of prevention and mitigation planning, emergency response and operations planning, and continuity and recovery planning.

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. See Annex K for additional information on alerting and warning systems.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 12:03:26 EDT 2018

Committee Statement

Committee Statement: Per the NFPA Manual of Style (MOS), the committee is including a reference to Annex K to point the user to further guidance.

Response Message:

Second Revision No. 37-NFPA 1600-2018 [Section No. A.6.6.5]

A.6.6.5

A common format for gathering pertinent information (i.e., inbound messaging) and disseminating information (i.e., 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. See Annex J for additional information on social media in emergency management.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:57:23 EDT 2018

Committee Statement

Committee Statement: Per the NFPA Manual of Style (MOS), the committee is including a reference to Annex J to point the user to further guidance.

Response Message:

Second Revision No. 13-NFPA 1600-2018 [Section No. A.6.8.1]

A.6.8.1

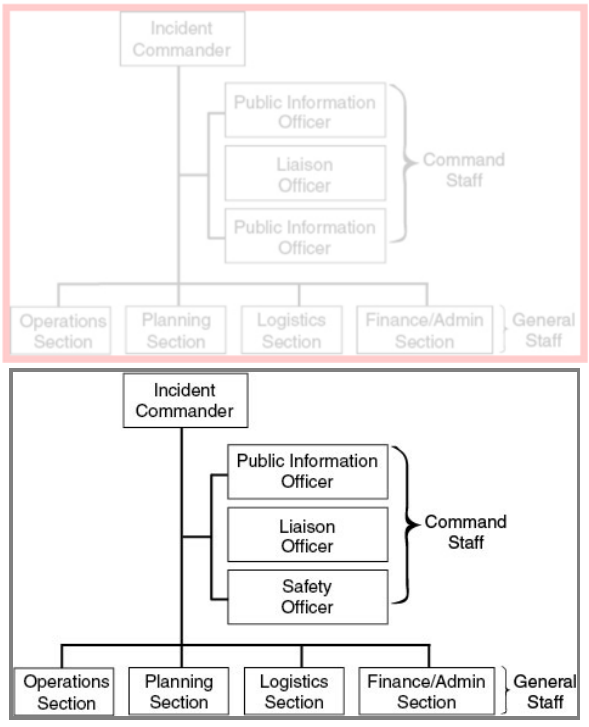
An incident management system (IMS) should be used to manage an incident. The system used varies among entities and among jurisdictions within entities. In minor incidents, IMS functions might be handled by one person: the incident commander or equivalent designee.

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.6.8.1 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.6.8.1 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.6.8.1 Diagram of Incident Command System.



Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:33:01 EDT 2018

Committee Statement

Committee Statement:	The committee is changing the figure to fix a typo where public information officer appeared twice.
Response Message:	

Second Revision No. 15-NFPA 1600-2018 [Section No. A.6.10]

A.6.10

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

(1) Strategies for disruption or loss of operational site, such as the following :

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

(b) Alternate site contracted through a commercial recovery vendor.

(c) Reciprocal agreement or mutual aid agreement with a similar entity.

(d) Dedicated alternate site built by the entity to support recovery.

(e) Mobile facility — Generally, a trailer or mobile home that has been equipped to support operational recovery. These can be owned or contracted for through a vendor.

(f) Remote access/work from home.

(g) Resources acquired at the time of disruption — This would be used for less time-sensitive operations.

(h) Customer service or product priority — Focuses operational capacity on specific high-value customers or high-profit products or services.

(i) Finished goods buyback.

(j) Utilized to recover already delivered inventory from other customers to meet the demands of customers who utilize “just in time.”

(k) Relocation of staff to a surviving site that has additional capacity.

(l) Stockpile critical equipment and inventory to be available at time of disaster.

(2) Third-party (i.e., vendor provided/extended enterprise) recovery strategy options, such as the following :

(a) Multiple sourcing — The entity buys the same or similar product or service from multiple vendors to prevent supply chain disruption should one of them experience a disruption.

(b) Alternate sourcing — To identify another source for a product or service should the current vendor experience a disruption.

(c) Service level agreement — Established service level agreements with the third party with penalties for nonperformance.

(d) Insource (do not outsource) — To identify internal resources that can provide service or product.

(3) Technical recovery alternatives, such as the following :

(a) Commercial vendor (hot site) — A variety of commercial vendors will provide a recovery environment for technology of all shapes and sizes. This eliminates the need to have redundant hardware/software within the entity’s own footprint.

(b) Resources acquired at time of disruption — This type of plan is used where the technology environment is small and easy to replace or not time sensitive to the survival of the entity.

(c) Quick-ship equipment — Established agreement with a vendor to provide specific technology on demand following a disruption.

(d) Dual data center with active/active — This strategy requires that the entity has access to two data center environments that are always fully operational and are either owned by the entity or leased where they can load balance time-sensitive applications between two geographic locations. If one center experiences a disruption, the surviving center takes the entire load without need for recovery and is capable of handling the entire load. These data centers must generally be within 50 network miles of each other to prevent network latency.

(e) Dual data center with active/passive — This strategy requires that the entity has access to two data center environments that are always fully operational and either owned by the entity or leased where they can split time-sensitive applications between the two geographic locations. The data that supports the applications in each center needs to be replicated to the other data center to facilitate recovery and to prevent significant data loss. If one center experiences a disruption, the applications operating in the disrupted data center are “restarted” at the surviving center that ~~is capable of handling~~ can handle the entire load. These data centers can be

geographically distant, even in different countries. The load from the impacted site is simply "switched over" to the surviving site. There is a minimal disruption during the transition and little data loss if the data is replicated between the centers.

(f) Outsourcing with a ~~service-level~~ service level agreement (e.g., cloud computing) — An entity can have some or all of this technology environment hosted in the "cloud." This would likely prevent the entity's operations and the technology environment from being impacted by the same disruption. The requirements for recovery of the technology environment are established with the cloud vendor.

(g) Stockpiled equipment — The entity could store the equipment needed for recovery ~~on site~~ on-site in their recovery location.

(h) Manual workarounds or alternate systems — The entity could use manual workarounds such as a manual call log or alternate systems such as spreadsheets instead of the general ledger system until the technology environment is recovered.

(4) Backup strategies for records, such as the following :

(a) Electronic storage — On media such as flash drives or external hard drives.

(b) Synchronous replication — Data is written onto data storage at two locations simultaneously.

(c) Asynchronous replication — Data is written onto data storage at two locations but with some degree of latency between writing on the production drive and writing on the backup drive.

(d) Electronic journaling — Activities that happen on one data store are captured on a journal as they are written. If a disruption occurs, you can recover up to the last good journal entry ~~off site~~ off-site at the time of the disruption.

(e) Standby database — A backup to the production database should the production database be corrupted or lost in a disruption.

(f) Electronic vaulting — A point-in-time backup stored on disk.

(g) Tape backup — A point-in-time backup stored on tape.

(h) Full backup — A point-in-time backup of everything on a data store.

(i) Differential backup — A point-in-time backup of everything on the data store that has changed since the last full backup was made.

(j) Incremental backup — A point-in-time backup of everything on the data store since the last time *any* type of backup was made.

(k) Salvage — An attempt to recover data from a device that has been damaged.

(5) Hard-copy storage, such as the following :

(a) Film — Pictures or video.

(b) Fiche — Old technology that allows large quantities of images to be stored in a small space.

(c) Photocopy — A copy of an original record stored ~~off site~~ off-site .

(d) Scan — A digital image of a record that can be stored ~~off site~~ off-site .

(e) Salvage — An attempt to restore damaged paper records following a disruption.

Plans should include or provide the following as needed to support the recovery:

(1) Facilities and equipment

(2) Technology infrastructure

(3) Telecommunications and data protection systems

(4) Distribution systems for essential goods

(5) Transportation systems, networks, and infrastructure

(6) Human resources

(7) Psychosocial services

(8) Health services

(9) Power, water, and HVAC

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

(1) Recovery of critical or time-sensitive personnel, systems, operations, records, and equipment

(2) Agreed-upon priorities for restoration and mitigation

(3) Length of downtime acceptable before restoration to a minimal level is required

(4) Minimal acceptable level of resources needed to provide for the restoration of facilities, processes, programs, services, 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 prevention and mitigation

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:45:06 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction.

Response Message:

Second Revision No. 16-NFPA 1600-2018 [Section No. A.6.10.1.2]

A.6.10.1.2

Plans for business continuity, continuity of operations, and continuity of government 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, continuity of government plans, and disaster recovery plans.

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Wed Mar 28 15:47:23 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction.
Response Message:

Second Revision No. 17-NFPA 1600-2018 [Section No. A.6.11.1]

A.6.11.1

Employee assistance and support might also be called human continuity, human impacts, workforce continuity, and 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. See Annex K, which supports emergency communications.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:49:20 EDT 2018

Committee Statement

Committee Statement: This is an editorial change to remove so forth.

Response Message:

Second Revision No. 18-NFPA 1600-2018 [Section No. A.6.11.1(2)]

A.6.11.1(2)

The entity should develop policies and procedures to store, retrieve, and control access to personal information when needed in an emergency ~~situation~~ , including the ability to facilitate notification to, and reunification of, family members.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:50:29 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction.

Response Message:

Second Revision No. 19-NFPA 1600-2018 [Section No. A.8.2]

A.9.2

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, and procedures; to train individuals; to practice using equipment; to validate alternate site readiness; and to practice utilization of interagency agreements. Exercise goals can include clarifying and training personnel in roles and responsibilities, improving coordination and communications, identifying gaps in resources, improving individual performance, and identifying opportunities for improvement.

A test or testing is a ~~unique and particular~~ type of exercise that incorporates an expectation of a pass or fail element within the established goal or objectives. Generally, one tests equipment and technology and exercises people and plans. Testing equipment and technology is either a pass or fail — it either works or it does not work. Exercising people and plans is not a pass or fail, although goals and objectives should be set that are either met or not met by the exercise. The purpose of exercising a person or a plan is to find out what does not work so the issue can be resolved before a problem occurs. Remember, if we knew it all worked, we would not need to test or exercise.

An exercise allows the entity 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 capabilities to respond to and recover from a real incident. 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 validate recently changed procedures

(2) Improve the coordination among various response entities, including, as appropriate, government officials and community support entities

(3) Validate the training for response (e.g., incident command, hazard recognition, protective actions, and communications) and recovery (e.g., crisis management, technology recovery, operational recovery, and recovery communications)

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

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

(6) Provide training and conditioning for team members and personnel in appropriate actions

(7) Practice established incident command structure, and practice response and recovery in a safe environment

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 15:53:13 EDT 2018

Committee Statement

Committee Statement: This is an editorial change for clarity within the standard.

Response Message:

Second Revision No. 20-NFPA 1600-2018 [Section No. A.8.3]

A.9.3

An exercise can involve invoking response and operational continuity procedures, or simulate response or operational continuity incidents, in which participants role-play ~~in order~~ to assess issues that could arise prior to a real invocation. Exercises can be announced in advance.

Exercises should include, but not be limited to, orientation seminars, drills, tabletop exercises, functional exercises, and full-scale exercises.

Orientation ~~*Seminar*~~ *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, such as an evacuation drill to test the ability to quickly and safely evacuate a facility. 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 and crisis management systems and operational recovery plans 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 exercise and evaluate the capabilities of the emergency management plan, the technology recovery plan, crisis management plan, and/or operational plan.

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Wed Mar 28 15:54:23 EDT 2018

Committee Statement

Committee Statement: This is an editorial change for clarity within the standard.
Response Message:

Second Revision No. 22-NFPA 1600-2018 [Section No. A.9.1]

A.7.1

The types of incidents to be recognized as having potential for major impact on the entity can be found through the risk assessment in 5.2.2.1 and 5.2.3, the business impact analysis (BIA) in 5.3.2, crisis communications and public information in Section 6.5, and incident management in Section 6.8.

Submitter Information Verification

Submitter Full Name: Michael Wixted
Committee:
Submittal Date: Wed Mar 28 16:01:38 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction based on sections moving due to first draft changes.
Response Message:

Second Revision No. 25-NFPA 1600-2018 [Chapter B]

Annex B Self-Assessment for Conformity with *NFPA 1600*, ~~2016~~ 2019 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 and 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 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~~ 2019 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			
~~• 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 Performance Objectives. **4.3.1*** The entity shall establish performance objectives for the program in accordance with Chapter 4			
• and the elements in Chapters 5 through 10.			
4.3.2 The performance objectives shall address the results of the hazard identification,			
• risk assessment,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• and business impact analysis.			
4.3.3 Performance objectives shall be developed by the entity to address both short-term			
• and long-term needs.			
4.3.4* The entity shall define the terms *short-term*			
• and *long-term* .			
~~4.3~~ 4.4 Program Committee. **~~4.3.1*~~ 4.4.1** A program committee shall be established by the entity in accordance with its policy.			
~~4.3.2~~ 4.4.2 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~~ 4.4.3 * The program committee shall include the program coordinator			
• and others who have the expertise, the knowledge of the entity, and the capability to identify resources from all key functional areas within the entity			
• and shall solicit applicable external representation.			
~~4.4~~ 4.5 Program Administration. **~~4.4.1~~ 4.5.1** The entity shall have a documented program that includes the following: (1) Executive policy, including: vision, mission statement, roles, and responsibilities, and enabling authority			
~~• vision,~~			
~~• mission statement,~~			
~~• roles, and responsibilities,~~			
~~• and enabling authority~~			
(2)* Program scope, goals, performance objectives, and metrics for program evaluation			
~~• goals,~~			
~~• performance objectives,~~			
~~• and metrics for program evaluation~~			
(3)* Applicable authorities, legislation, regulations, and industry codes of practice as required by Section 4.6			
~~• legislation,~~			
~~• regulations,~~			
~~• and industry codes of practice as required by Section 4.5~~			
(4) Program budget and schedule, including milestones			
~~• and schedule,~~			
~~• including milestones~~			
(5) Program plans and procedures that include the following: (a) Anticipated cost			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
(b) Priority			
(c) Resources required			
(6) Records management practices as required by Section ~~4.7~~ 4.8			
(7) Management of change			
~~4.4.2~~ **4.5.2** The program shall include the requirements specified in Chapters 4 through ~~9~~ 10 , the scope of which shall be determined through an “all-hazards” approach and the risk assessment.			
~~4.4.3~~ **4.5.3** * 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~~ **4.6 Laws and Authorities.**			
~~4.5.1~~ **4.6.1** The program shall comply with:			
• applicable legislation,			
• policies,			
• regulatory requirements,			
• and directives.			
~~4.5.2~~ **4.6.2** The entity shall:			
• establish,			
• maintain,			
• and document procedure(s) to comply with:			
• applicable legislation,			
• policies,			
• regulatory requirements,			
• and directives.			
~~4.5.3*~~ **4.6.3*** The entity shall implement a strategy for addressing the need for revisions to:			
• legislation,			
• regulations,			
• directives,			
• policies,			
• and industry codes of practice.			
~~4.6~~ **4.7 Finance and Administration.**			
~~4.6.1~~ **4.7.1** The entity shall develop finance and administrative procedures to support the program:			
• before,			
• during,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• and after an incident.			
~~4.6.2*~~ 4.7.2* 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			
~~• 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			
~~• request,~~			
~~• receive,~~			
~~• manage,~~			
~~• and apply funds in a nonemergency environment and in emergency situations to ensure the timely delivery of assistance~~			
~~4.6.3~~ 4.7.3 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~~ 4.7.4 Finance and administrative procedures shall include the following: (1) Responsibilities for program finance authority, including reporting relationships to the program coordinator			
~~• 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			
~~• and accessing alternative funding sources~~			
(9) Managing budgeted and specially appropriated funds			
~~4.7*~~ 4.8* **Records Management.** ~~4.7.1~~ 4.8.1 The entity shall:			
• develop,			
• implement,			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
• and manage a records management program to ensure that records are available to the entity.			
~~4.7.2~~ **4.8.2** The program shall include the following: (1) Identification of records (hard copy or electronic) vital to continue the operations of the entity			
~~• (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 on-site or off-site			
~~• store,~~			
~~• retrieve,~~			
~~• and recover records on site or off site~~			
(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:			
~~• 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:			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• operations,			
• brand,			
• image,			
• 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			
~~• 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			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
(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 (rumors, false allegations, or accusations)			
(f) Kidnapping/hostage/extortion			
(g) ~~Acts of war~~ Geopolitical risks including acts of war, change in government, and political instability			
(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:~~ :(q) Supply chain constraint or failure			
~~(a)* Hardware,~~ (6) Technological:			
~~• software,~~			
~~•~~ (a)* Hardware, software, and network connectivity interruption, disruption, or failure			
~~• interruption,~~			
~~• disruption,~~			
~~• or failure~~			
(b)* Utility interruption, disruption, or failure			
~~• disruption,~~ (7) Economic/financial:			
~~• or failure~~ (a) Foreign currency exchange rate change			
(b) Economic recession			
(c) Boycott			
(d) Theft/fraud/malfeasance/impropriety/scandal involving currency, monetary instruments, goods, and intellectual property			
(8) Strategic:			
(a) Loss of senior executive			
(b) Failed acquisition/strategic initiative			
(9) Humanitarian issues			
5.2.2.2* The vulnerability of:			
• people,			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
• 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			
~~• facilities,~~			
~~• assets,~~			
~~• and critical infrastructure~~			
(7) Delivery of the entity's services			
(8) Supply chain			
(9) Environment			
(10)* Economic and financial conditions			
~~• and financial conditions~~			
(11) Legislated, regulatory, and contractual obligations			
~~• regulatory,~~			
~~• and contractual obligations~~			
(12) ~~Reputation of~~ Brand, image, and reputation			
~~• 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,			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
• 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			
~~• 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			
~~• 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 time frame 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.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
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			
~~• 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			
~~• 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.**~~			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
~~**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			
~~• 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			
~~• 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.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
6.2.3 The prevention strategy shall be based on the results of hazard identification			
• and risk assessment,			
• an analysis of impacts,			
• program constraints,			
• operational experience,			
• and cost-benefit analysis.			
6.2.4 The entity shall have a process to:			
• monitor the identified hazards			
• and adjust the level of preventive measures to be commensurate with the risk.			
6.3 Mitigation.			
6.3.1* The entity shall develop			
• and implement a mitigation strategy			
• that includes measures to be taken to limit or control the consequences,			
• extent,			
• or severity of an incident that cannot be prevented.			
6.3.2* The mitigation strategy shall be based on the results of hazard identification			
• and risk assessment,			
• an analysis of impacts,			
• program constraints,			
• operational experience,			
• and cost-benefit analysis.			
6.3.3 The mitigation strategy shall include interim			
• and long-term actions to reduce vulnerabilities.			
6.4 Crisis Management.			
6.4.1 The entity shall establish,			
• and maintain a crisis management capability to manage issues,			
• events,			
• or series of events,			
• that severely impact or have the potential to severely impact an entity's brand,			
• image,			
• reputation,			
• market share,			
• ability to do business,			
• or relationships with key stakeholders.			
6.4.2 The crisis management capability shall include assigned responsibilities and established processes to perform the following:			
(1) Engage senior leadership			
(2) Detect the signals, symptoms, incidents, events, or circumstances that portend an emerging crisis or have the potential to trigger a crisis			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
(3) Conduct a situation analysis			
(4) Declare a crisis, alert responsible persons, and activate crisis management plans should the current situation meet established criteria			
(5) Identify issues to be addressed by the responsible persons and senior leadership			
(7) Provide direction and support for the entity's facilities, operations, employees, customers, and others affected by or potentially affected by the crisis			
(8) Coordinate with the entity's crisis communication capability and provide strategic direction, authorize communications strategies, and communicate with stakeholders			
~~6.4~~ 6.5 Crisis Communications and Public Information.			
~~6.4.1*~~ 6.5.1* 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			
~~• including employees~~			
~~(2) External audiences,~~			
~~• including the media,~~			
~~• access~~			
• (2) External audiences, including the media, access and functional needs population, and other stakeholders			
~~• and other stakeholders~~			
~~6.4.2*~~ 6.5.2* 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			
~~• gathering,~~			
~~• monitoring,~~			
~~• and disseminating information~~			
(4) Procedures for developing and delivering coordinated messages			
~~• and delivering coordinated messages~~			
(5) Protocol to clear information for release			
~~6.5~~ 6.6 Warning, Notifications, and Communications.			
~~6.5.1*~~ 6.6.1* The entity shall determine its warning,			
• notification,			
• and communications needs.			
~~6.5.2*~~ 6.6.2* Warning,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• notification,			
• and communications systems shall be reliable,			
• redundant,			
• and interoperable.			
~~6.5.3*~~ 6.6.3* 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~~ 6.6.4 Procedures shall include issuing warnings through authorized agencies if required by law			
• as well as the use of ~~prescripted~~ pre-scripted information bulletins or templates.			
6.6.5* Information shall be disseminated through the media,			
• social media, ~~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~~ 6.7 **Operational Procedures.** ~~6.6.1~~ 6.7.1 The entity shall develop,			
• coordinate,			
• and implement operational procedures to support the program.			
~~6.6.2~~ 6.7.2 Procedures shall be established			
• and implemented			
• for response to			
• and recovery from the impacts of hazards identified in 5.2.2.			
~~6.6.3*~~ 6.7.3* 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~~ 6.7.4 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 ~~• and demobilization of resources~~			
~~6.6.5~~ 6.7.5 Procedures shall allow for concurrent activities of response,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• continuity,			
• recovery,			
• and mitigation.			
~~6.7~~ 6.8 **Incident Management.**			
~~6.7.1*~~ 6.8.1* The entity shall develop an incident management system to direct,			
• control,			
• and coordinate response,			
• continuity,			
• and recovery operations.			
~~6.7.1.1*~~ 6.8.1.1* **Emergency Operations Centers (EOCs).**			
~~6.7.1.1.1*~~ 6.8.1.1.1* The entity shall establish primary			
• and alternate EOCs capable of managing response,			
• continuity,			
• and recovery operations.			
~~6.7.1.1.2*~~ 6.8.1.1.2* The EOCs shall be permitted to be physical ~~or virtual.~~			
• or virtual.			
~~6.7.1.1.3~~ 6.8.1.1.3* On activation of an EOC, communications			
• and coordination shall be established between incident command ~~and the EOC~~ .			
• and the EOC			
~~6.7.2~~ 6.8.2 The incident management system shall describe specific entity roles,			
• titles,			
• and responsibilities for each incident management function.			
~~6.7.3*~~ 6.8.3* The entity shall establish procedures			
• and policies for coordinating prevention,			
• mitigation,			
• preparedness,			
• response,			
• continuity,			
• and recovery activities.			
~~6.7.4~~ 6.8.4 The entity shall coordinate the activities specified in ~~6.7.3~~ 6.8.3 with stakeholders.			
~~6.7.5~~ 6.8.5 Procedures shall include a situation analysis that incorporates ~~a damage~~ an assessment of the following for the purposes of activating emergency response/operations,			
• business continuity/continuity of operations,			
• crisis management,			
• and/or crisis communications plans and capabilities:			
(1) Casualties and the availability of required personnel resources			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
(2) Physical damage to property under the jurisdiction of the entity			
(3) Interruption or disruption of the entity's operations			
(4) Impacts to digital information and vital records			
(5) Actual or potential contamination of the environment			
(6) Actual or potential impacts to brand, image, reputation, market share, ability to do business, or relationships with key stakeholders			
~~• and a needs assessment to identify resources~~ (7) Resources needed to support response, continuity, and recovery activities.			
~~6.7.6*~~ **6.8.6** Emergency operations/response shall be guided by an incident action plan ~~or management by objectives.~~			
• or management by objectives.			
~~6.7.7~~ **6.8.7** Resource management shall include the following tasks: (1) Establishing processes for describing, taking inventory of, requesting, and tracking resources			
~~• taking inventory of,~~			
~~• requesting,~~			
~~• and tracking resources~~			
(2) Resource typing or categorizing by size, capacity, capability, and skill			
~~• capacity,~~			
~~• capability,~~			
~~• and skill~~			
~~(3) Mobilizing~~			
~~•~~ (3) Mobilizing and demobilizing resources in accordance with the established IMS			
(4) Conducting contingency planning for resource deficiencies			
~~6.7.8~~ **6.8.8** A current inventory of internal			
• and external resources shall be maintained.			
~~6.7.9~~ **6.8.9** Donations of human resources,			
• equipment,			
• material,			
• and facilities shall be managed.			
~~6.8~~ **6.9 Emergency Operations/Response Plan.** ~~6.8.1*~~ **6.9.1*** Emergency operations/response plans shall define responsibilities for carrying out specific actions in an emergency.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
~~6.8.2*~~ 6.9.2* The plan shall identify actions to be taken to protect people,			
• including people with disabilities			
• and ~~others~~ other access and functional needs,			
~~• and functional needs,~~			
• information,			
• property,			
• operations,			
• the environment,			
• and the entity.			
~~6.8.3*~~ 6.9.3* The plan shall identify actions for incident stabilization.			
~~6.8.4~~ 6.9.4 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 6.6			
~~• notifications,~~			
~~• and communication in accordance with Section 6.5~~			
(3) Crisis communication and public information in accordance with Section 6.5			
~~• and public information in accordance with Section 6.4~~			
(4) Resource management in accordance with ~~6.7.7~~ 6.8.7			
(5) Donation management in accordance with ~~6.7.9~~ 6.8.9			
~~6.9*~~ 6.10* **Continuity and Recovery.** ~~6.9.1~~ 6.10.1 **Continuity.** ~~6.9.1.1~~ 6.10.1.1 Continuity plans shall include strategies to continue critical			
• and time-sensitive processes and as identified in the BIA.			
~~6.9.1.2~~ 6.10.1.2 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			
~~• and responsibilities of the individuals implementing the continuity strategies~~			
(4) Procedures for activating the plan, including authority for plan activation			
~~• including authority for plan activation~~			
(5) Critical and time-sensitive technology, application systems, and information			
~~• and time-sensitive technology,~~			
~~• application systems,~~			
~~• and information~~			
(6) Security of information			
(7) Alternative work sites			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
(8) Workaround procedures			
(9) Vital records			
(10) Contact lists			
(11) Required personnel			
(12) Vendors and contractors supporting continuity			
~~• and contractors supporting continuity~~			
(13) Resources for continued operations			
(14) Mutual aid or partnership agreements			
~~• or partnership agreements~~			
(15) Activities to return critical and time-sensitive processes to the original state			
~~• and time-sensitive processes to the original state~~			
~~**6.9.1.3**~~ **6.10.1.3** Continuity plans shall be designed to meet the RTO			
• and RPO.			
~~**6.9.1.4**~~ **6.10.1.4** Continuity plans shall address supply chain disruption.			
~~**6.9.2**~~ **6.10.2** **Recovery.**			
~~**6.9.2.1**~~ **6.10.2.1** Recovery plans shall provide for restoration of processes,			
• technology,			
• information,			
• services,			
• resources,			
• facilities,			
• programs,			
• and infrastructure.			
~~**6.9.2.2**~~ **6.10.2.2** 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			
~~• 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			
~~• and time-sensitive processes,~~			

***NFPA 1600* Program Elements**	**Conforming**	**Nonconforming**	**Comments**
~~• technology,~~			
~~• systems,~~			
~~• applications,~~			
~~• and information~~			
(6) Roles and responsibilities of the individuals implementing the recovery strategies			
~~• 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			
~~• 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~~ 6.11 **Employee Assistance and Support.** ~~6.10.1~~ 6.11.1 * 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			
~~• including emergency contact outside the anticipated hazard area~~			
(3) Accounting for persons affected, displaced, or injured by the incident			
~~• displaced,~~			
~~• or injured by the incident~~			
(4) Temporary, short-term, or long-term housing and feeding and care of those displaced by an incident			
~~• 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			
~~• and physical well-being of individuals affected by the incident~~			
(6) Pre-incident and post-incident awareness			
~~• and post-incident awareness~~			
~~6.10.2~~ 6.11.2 The strategy shall be flexible for use in all incidents.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
~~6.10.3*~~ 6.11.3* The entity shall promote family preparedness education			
• and training for employees.			
Chapter 7 Execution.			
7.1* Incident Recognition.			
The entity shall establish,			
• and implement a process whereby all appropriate stakeholders have a common reference for the types of incidents that could adversely affect its people,			
• property,			
• operations,			
• or the environment,			
• and ensure it is appropriately referenced throughout the incident management process.			
7.2 Initial Reporting/Notification.			
The entity shall establish			
• and implement a process whereby all appropriate stakeholders can warn,			
• notify,			
• and report an incident that has potential to cause an adverse impact on its people,			
• property,			
• operations,			
• or the environment. *(See Section 6.6.)*			
7.3 Plan Activation and Incident Action Plan.			
7.3.1 The entity shall establish			
• and implement a process to assess the impact of the incident on its people,			
• property,			
• operations,			
• or the environment.			
7.3.2 The entity shall develop a time frame to activate appropriate planning as detailed in Sections 6.5, 6.9, and 6.10,			
• and coordinate activation when there is a declaration by public officials.			
7.4 Activate Incident Management System.			
7.4.1 The entity shall execute procedures from the documented plans in accordance with the following:			
(1) Section 6.5			
(2) Section 6.8			
(3) Section 6.9			
(4) Section 6.10			
7.4.2 The entity shall execute its incident management system			
• and activities in support of established objectives and tasks.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
7.4.3 On activation of an emergency operations center (EOC), communications			
• and coordination shall be established between incident command			
• and the EOC.			
7.5 Ongoing Incident Management and Communications. 7.5.1 The entity shall continually assess the impact of the incident on its people			
• property,			
• operations,			
• the environment.			
• and reevaluate/implement its action plan in accordance with established objectives			
• and tasks			
7.5.2 The entity shall implement the warning, notification, and communications systems to alert stakeholders who are potentially at risk from an actual			
• or impending incident.			
7.5.3 Based upon the extent of damage sustained to the entity, all necessary actions to invoke special authorities			
• and request assistance needed to deal with the situation shall be as described in Chapter 4.			
7.6 Documenting Incident Information, Decisions, and Actions. The entity shall establish			
• and implement a system for tracking incident information received,			
• decisions made,			
• resources deployed,			
• and actions taken during the incident.			
7.7* Incident Stabilization. The entity shall establish criteria for measuring when the incident has been stabilized. 7.7*			
7.8 Demobilize Resources and Termination. The entity shall execute a procedure to terminate the response.			
• and demobilize resources when the incident has been stabilized .			
Chapter ~~7~~ 8 Training and Education. ~~7.1*~~ **8.1* 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~~ **8.2 Goal of Curriculum.** The goal of the curriculum shall be to create awareness			
• and enhance the knowledge,			
• skills,			
• and abilities required to implement,			
• support,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• and maintain the program.			
~~7.3~~ 8.3 **Scope and Frequency of Instruction.** The scope of the curriculum			
• and the frequency of instruction shall be identified.			
~~7.4~~ 8.4 **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~~ 8.5 **Recordkeeping.** Records of training			
• and education shall be maintained as specified in Section 4.7.			
~~7.6~~ 8.6 **Regulatory and Program Requirements.** The curriculum shall comply with applicable regulatory			
• and program requirements.			
~~7.7*~~ 8.7* **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~~ 9 Exercises and Tests **~~8.1~~ 9.1 Program Evaluation.** ~~8.1.1~~ 9.1.1 The entity shall evaluate program plans,			
• procedures,			
• training,			
• and capabilities			
• and promote continuous improvement through periodic exercises			
• and tests.			
~~8.1.2~~ 9.1.2 The entity shall evaluate the program based on post-incident analyses,			
• lessons learned,			
• and operational performance in accordance with Chapter ~~9~~ 10 .			
9.1.3 Exercises .			
~~8.1.3~~ ~~Exercises~~ • and tests shall be documented.			
~~8.2*~~ 9.2* **Exercise and Test Methodology.** ~~8.2.1~~ 9.2.1 Exercises shall provide a standardized methodology to practice procedures			
• and interact with other entities (internal			
• and external) in a controlled setting.			
~~8.2.2~~ 9.2.2 Exercises shall be designed to assess the maturity of program plans,			
• procedures,			
• and strategies.			
~~8.2.3~~ 9.2.3 Tests shall be designed to demonstrate capabilities.			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
~~8.3*~~ 9.3* **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			
~~• property,~~			
~~• operations,~~			
~~• and the environment involved in the exercise or test~~			
(2) Evaluate the program			
(3) Identify planning and procedural deficiencies			
~~• and procedural deficiencies~~			
(4) Test or validate recently changed procedures or plans			
~~• or validate recently changed procedures~~			
~~• or plans~~			
(5) Clarify roles and responsibilities			
~~• and responsibilities~~			
(6) Obtain participant feedback and recommendations for program improvement			
~~• and recommendations for program improvement~~			
(7) Measure improvement compared to performance objectives			
(8)* Improve coordination between internal and external teams and entities			
~~• and entities~~			
(9) Validate training and education			
~~• and education~~			
(10) Increase awareness and understanding of hazards and the potential impact of hazards on the entity			
~~• 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			
~~• 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			
~~• assess,~~			
~~• and manage an incident~~			
(13) Practice the deployment of teams and resources to manage an incident			
~~• and resources to manage an incident~~			
(14) Improve individual performance			
~~8.4*~~ 9.4* **Exercise and Test Evaluation.**			
~~8.4.1~~ 9.4.1 Exercises shall evaluate program plans,			
• procedures,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• training,			
• and capabilities to identify opportunities for improvement.			
~~8.4.2~~ 9.4.2 Tests shall be evaluated as either pass or fail.			
~~8.5*~~ 9.5* **Frequency.** ~~8.5.1~~ 9.5.1 **Exercises.** • and tests shall be conducted on the frequency needed to establish			
• and maintain required capabilities.			
Chapter ~~9~~ 10 Program Maintenance and Improvement ~~9.1*~~ 10.1* **Program Reviews.** The entity shall maintain • and improve the program			
• by evaluating its policies,			
• program,			
• procedures,			
• and capabilities using performance objectives.			
~~9.1.1*~~ 10.1.1* The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive			
• and corrective action.			
~~9.1.2*~~ 10.1.2* 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~~ 10.1.3 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			
~~• and potential impacts~~			
(3) Resource availability or capability			
~~• or capability~~			
(4) Entity’s organization			
(5)* Funding changes			
(6) Infrastructure, including technology environment			
~~• including technology environment~~			
(7) Economic and geographic stability			
(8) Entity operations			
(9) Critical suppliers			
~~9.1.4~~ 10.1.4 Reviews shall include post-incident analyses,			
• reviews of lessons learned,			
• and reviews of program performance.			
~~9.1.5~~ 10.1.5 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~~ 10.1.6 Documentation,			
• records,			

NFPA 1600 Program Elements	Conforming	Nonconforming	Comments
• and reports shall be provided to management for review			
• and follow-up.			
~~9.2*~~ 10.2* **Corrective Action.** ~~9.2.1*~~ 10.2.1* The entity shall establish a corrective action process.			
~~9.2.2*~~ 10.2.2* The entity shall take corrective action on deficiencies identified.			
~~9.3~~ 10.3 **Continuous Improvement.** The entity shall effect continuous improvement of the program through the use of program reviews			
• and the corrective action process.			

Supplemental Information

File Name	Description	Approved
SR_25_section_B.docx	Revised Annex based on First Draft. For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 16:18:31 EDT 2018

Committee Statement

Committee Statement: The committee updated the self-assessment checklist based on First Draft changes to the parent sections. It is based on the content in the main body of the standard. This checklist provides the user the ability to test their conformity to NFPA 1600 and allows for the opportunity for a gap analysis.

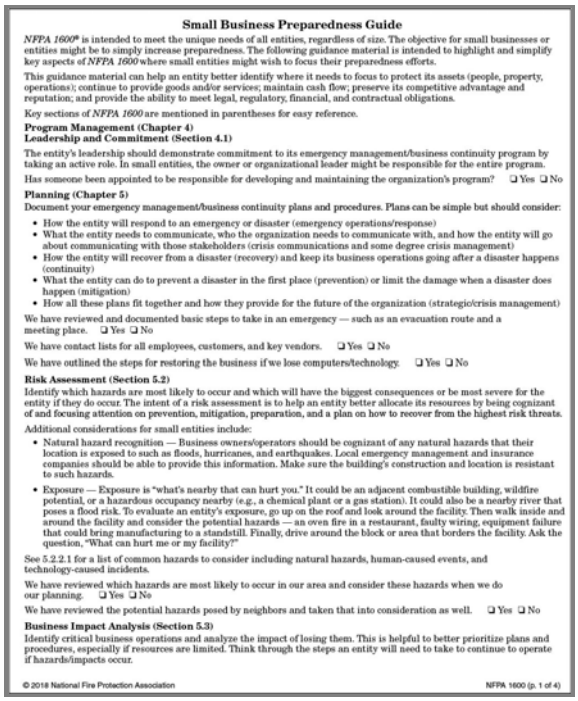
Response Message:

Second Revision No. 5-NFPA 1600-2018 [Section No. C.1]

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.

 NFPA 1600 (p. 1 of 4)

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

We have a copy of these planning documents off site. ❑ Yes ❑ No

Resource Needs Assessment (Section 5.4)

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

Additional considerations for small entities include:

- 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

- Plan ahead – The entity should anticipate the level of planning required for their situation by discussing operations, capabilities, and expectations with local emergency services agencies (fire, rescue, police, hazmat, etc.) and local emergency planning nonprofit organizations (local emergency planning committees, Red Cross, Salvation Army, and similar groups).

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

 NFPA 1600 (p. 2 of 4)

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 safety of employees and public, and 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., TV, radio, print, social websites). The same media can be used to help recover from a crisis. Preplanning 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 an 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 6.9)

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:

- Emergency numbers/alarms — Simple procedures such as knowing to call appropriate emergency numbers 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

Continuity and Recovery (Section 6.10)

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. ❑ Yes ❑ 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 10)

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://www1.mwcog.org/security/security/continuity/intro.asp]

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, as well as the OFB – EZ mobile app. This app includes several helpful planning tools, such as evaluation checklists to help business users understand their risks, and forms for users to enter and store important contact information for employees, key customers, suppliers, and vendors. In addition, it provides mitigation tips for protecting property from natural hazard events. (www.disastersafety.org/ibhs-business-protection)

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

The Red Cross web site (ReadyRating.org) includes emergency preparedness information, checklists, and tools to help with preparing for emergency and disasters.

- 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. ❑ Yes ❑ No

Training and Education (Chapter 8) and Exercises and Tests (Chapter 9)

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 10)

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://www1.mwcog.org/security/security/continuity/intro.asp]

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, as well as the OFB – EZ mobile app. This app includes several helpful planning tools, such as evaluation checklists to help business users understand their risks, and forms for users to enter and store important contact information for employees, key customers, suppliers, and vendors. In addition, it provides mitigation tips for protecting property from natural hazard events. (www.disastersafety.org/ibhs-business-protection)

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

The Red Cross web site (ReadyRating.org) includes emergency preparedness information, checklists, and tools to help with preparing for emergency and disasters.

 NFPA 1600 (p. 4 of 4)

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Wed Mar 28 14:26:26 EDT 2018

Committee Statement

Committee Statement: These are changes to align with sections added from the First Draft.

Response Message:

Second Revision No. 27-NFPA 1600-2018 [Chapter D]

Annex D Crosswalk Between *NFPA 1600* and DRII Professional Practices, CSA Z1600, and Federal Continuity Directive 1 & 2

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

D.1

Annex ~~E~~ D is a cross-reference to the requirements of *NFPA 1600* and Disaster Recovery Institute International's *Professional Practices for Business Continuity ~~Practitioners~~ Management* ; CSA Z1600, *Emergency ~~Management and Business~~ Continuity ~~Programs~~ Management Program* ; and Federal Continuity ~~Directive~~ Directives 1 & 2 . *[See Table D.1(a) through Table D.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 D.1(a) Cross-Reference of *NFPA 1600* to DRII *Professional Practices for Business Continuity Management*

***NFPA 1600* (~~2016~~ 2019) Chapter/Section**	**DRII *Professional Practices for Business Continuity ~~Practitioners (2012)~~ Management* ~~(2012)~~ (2017) Subject Area**
Chapter 4 Program Management	
4.1 Leadership and Commitment	1. ~~Project~~ Program Initiation and Management
4.2 Program Coordinator	1. ~~Project~~ Program Initiation and Management
4.3 Performance Objectives	1. Program Initiation and Management
~~4.3~~ 4.4 Program Committee	1. ~~Project~~ Program Initiation and Management
~~4.4~~ 4.5 Program Administration	1. ~~Project~~ Program Initiation and Management
~~4.5~~ 4.6 Laws and Authorities	1. Program Initiation and Management 3. Business Impact Analysis 9. Crisis Communications 10. Coordinating with External Agencies
~~4.6~~ 4.7 Finance and Administration	1. ~~Project~~ Program Initiation and Management
~~4.7~~ 4.8 Records Management	3. Business Impact Analysis
Chapter 5 Planning	
5.1 Planning and Design Process	2. Risk ~~Evaluation and Control~~ Assessment 3. Business Impact Analysis 4. Business Continuity Strategies 5. ~~Emergency Preparedness and~~ Incident Response 6. ~~Business Continuity~~ Plan Development and Implementation
5.2 Risk Assessment	2. Risk ~~Evaluation and Control~~ Assessment
5.3 Business Impact Analysis	3. Business Impact Analysis
5.4 Resource Needs Assessment	1. Program Initiation and Management 2. Risk ~~Evaluation and Control~~ Assessment 3. Business Impact Analysis 5. ~~Emergency~~ Incident 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~~ 5. Incident Response ~~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

***NFPA 1600* (~~2016~~ 2019) Chapter/Section**	**DRII *Professional Practices for Business Continuity ~~Practitioners (2012)~~ Management* ~~(2012)~~ (2017) Subject Area**
	~~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~~ Assessment 5. ~~Emergency~~ Incident Response ~~and Operations~~
6.3 Mitigation	2. Risk ~~Evaluation and Control~~ Assessment 5. ~~Emergency~~ Incident Response ~~and Operations~~ ~~9. Crisis Communications~~
6.4 Crisis Management	5. Incident Response 6. Plan Development and Implementation 10. Coordination with External Agencies
~~6.4~~ 6.5 Crisis Communications and Public Information	5. ~~Emergency~~ Incident Response ~~and Operations~~ 6. ~~Business Continuity~~ Plan Development and Implementation 9. Crisis Communications 10. Coordination with External Agencies
~~6.5~~ 6.6 Warning, Notifications, and Communications	5. ~~Emergency Preparedness and~~ Incident Response 9. Crisis Communications
6.7 Operational Procedures	5. Incident Response 6. Plan Development and Implementation 9. Crisis Communications
6.8 Incident Management	5. Incident Response 6. Plan Development and Implementation
6.9 Emergency Operations/Response Plan	5. Incident Response 6. Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, ~~Audit~~ Assessment and Maintenance ~~9. Crisis Communications~~ ~~10. Coordinating with External Agencies~~
~~6.6 Operational Procedures~~ 6.10 Continuity and Recovery	~~5. Emergency Preparedness and Response~~ 4. Business Continuity Strategies 6. ~~Business Continuity~~ Plan Development and Implementation 7. Awareness and Training Program 8. Business Continuity Plan Exercise, ~~Audit~~ Assessment and Maintenance 9. Crisis Communications
~~6.7 Incident Management~~ 6.11 Employee Assistance and Support	~~5. Emergency Preparedness and Response~~ 6. ~~Business Continuity~~ Plan Development and Implementation 9. Crisis Communications

NFPA 1600 (~~2016~~ 2019) Chapter/Section	DRII *Professional Practices for Business Continuity ~~Practitioners (2012)~~ Management* (~~2012~~) (2017) Subject Area
	10. Coordinating with External Agencies
Chapter 7 Execution	
~~6.8 Emergency Operations/Response Plan~~ 7.1 Program Reviews	5. ~~Emergency Preparedness and Response~~ Incident Response 8. Business Continuity Plan Exercise, Assessment and Maintenance
7.2 Incident Reporting/Notification	
7.3 Plan Activation and Incident Action Plan	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~~ 7.4 Activate Incident Plan	~~4. Business Continuity Strategies~~ 6. ~~Business Continuity~~ Plan Development and Implementation ~~7. Awareness and Training Program~~ ~~8. Business Continuity Plan Exercise, Audit and Maintenance~~
7.5 Ongoing Incident Management and Communications	~~9. Crisis Communications~~ 5. Incident Response
~~6.10 Employee Assistance and Support~~ 7.6 Documenting Incident Information, Decisions, and Actions	5. ~~Emergency Preparedness and~~ Incident Response ~~6. Business Continuity Plan Development and Implementation~~
7.7 Incident Stabilization	~~7. Awareness and Training Program~~ 5. Incident Response
7.8 Demobilize Resources and Termination	8. Business Continuity Plan Exercise, ~~Audit~~ Assessment and Maintenance ~~9. Crisis Communications~~ ~~10. Coordinating with External Agencies~~
Chapter ~~7~~ 8 Training and Education	~~8. Business Continuity Plan Exercise, Audit and Maintenance~~
~~7.1~~ 8.1 Training and Education Curriculum	7. Awareness and Training Programs
~~7.2~~ 8.2 Goal of the Curriculum	7. Awareness and Training Programs 8. Business Continuity Plan Exercise, Assessment and Maintenance
~~7.3~~ 8.3 Scope and Frequency of Instruction	~~5. Emergency Preparedness and Response~~ 8. Business Continuity Plan Exercise, Assessment and Maintenance
~~7.4~~ 8.4 Incident Management System Training	~~5. Emergency Preparedness and Response~~ ~~10. Coordination with External Agencies~~
~~7.5~~ 8.5 Recordkeeping	
~~7.6~~ 8.6 Regulatory and Program Requirements	~~10. Coordination with External Agencies~~
~~7.7~~ 8.7 Public Education	
Chapter ~~8~~ 9 Exercises and Tests	~~5. Emergency Preparedness and Response~~

NFPA 1600 (~~2016~~ 2019) Chapter/Section	DRII *Professional Practices for Business Continuity ~~Practitioners (2012)~~ Management* (~~2012~~) (2017) Subject Area
9.1 Program Evaluation ~~8.1 Program Evaluation~~	8. Business Continuity Plan Exercise, ~~Audit~~ Assessment and Maintenance ~~10. Coordination with External Agencies~~
~~8.2~~ 9.2 Exercise and Test Methodology	8. Business Continuity Plan Exercise, Assessment and Maintenance
~~8.3~~ 9.3 Design of Exercises and Tests	8. Business Continuity Plan Exercise, Assessment and Maintenance
~~8.4~~ 9.4 Exercise and Test Evaluation	8. Business Continuity Plan Exercise, Assessment and Maintenance
~~8.5~~ 9.5 Frequency	8. Business Continuity Plan Exercise, Assessment and Maintenance 10. Coordination with External Agencies
Chapter ~~9~~ 10 Program Maintenance and Improvement	~~5. Emergency Preparedness and Response~~
10.1 Program Reviews	~~6.~~ 8. Business Continuity Plan Exercise, Assessment ~~Development~~ and ~~Implementation~~ Maintenance ~~7. Awareness and Training Program~~
10.2 Corrective Action ~~9.1 Program Reviews~~ ~~9.2 Corrective Action~~	8. Business Continuity Plan Exercise, ~~Audit~~ Assessment and Maintenance 9. Crisis Communications ~~9. Crisis Communications~~ ~~10. Coordinating with External Agencies~~
~~9.3~~ 10.3 Continuous Improvement	8. Business Continuity Plan Exercise, Assessment and Maintenance

DRII: DRI International, Inc.

Table D.1(b) Cross-Reference of ~~*NFPA 1600–13*~~ *NFPA 1600* to CSA ~~Z1600–14~~ Z1600, *Emergency and Continuity Management Program*

NFPA 1600(~~2013~~) (2019) Chapter/Section	CSA ~~Z1600-14~~ Z1600-17 , *Emergency ~~Management~~ and ~~Business~~ Continuity Management Programs* (2017) 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 Performance Objectives	4.4.3 Goals, Objectives, and Performance Measures
~~4.3~~ 4.4 Program Committee	4.3 Program Committee
~~4.4~~ 4.5 Program Administration	4.4 Program Administration
~~4.5~~ 4.6 Laws and Authorities	4.5 Compliance with Laws and Authorities
~~4.6~~ 4.7 Finance and Administration	4.6 Financial Management
~~4.7~~ 4.8 Records Management	4.4.6 Records Management
Chapter 5 Planning	**5 Planning**
5.1 Planning and Design Process	5.1 Planning Process

NFPA 1600 ~~(2013)~~ (2019) Chapter/Section	CSA ~~Z1600-14~~ Z1600-17 , *Emergency ~~Management~~ and ~~Business~~ Continuity Management Programs* (2017) Chapter/Section
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 Supporting Resources for RTO 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
6.2 Prevention	5.5.2 Prevention 6.1.2 Prevention
6.3 Mitigation	5.5.3 Mitigation 6.1.3 Mitigation
6.4 Crisis Management	~~6.1.2 Prevention~~ 5.1.2 (part of the planning process) ~~6.1.3 Mitigation~~ 6.2.4 (described in the response plan)
~~6.4~~ 6.5 Crisis Communications and Public Information	~~5.5.8~~ 6.2.2 Communications Assessment ~~6.2.5.2 Communications Assessment~~ 6.2.5.3 Communication Systems ~~6.2.5.4 Communication Procedures~~ 6.2.5.7 Emergency Information ~~6.2.5.6 Emergency Communication and Warning Capability~~ 6.2.5.8 Crisis Information ~~6.2.5.7 Emergency Information~~ 6.3.6 Emergency Information ~~6.2.5.8 Crisis Information~~ ~~6.3.5 Communications~~ ~~6.3.6 Emergency Information~~
~~6.5~~ 6.6 Warning, Notifications, and Communications	6.2.5 Communication and Warning ~~6.2.5.6 Emergency Communication and Warning Capability~~
~~6.6~~ 6.7 Operational Procedures	6.3.1 Operational Procedures
~~6.7~~ 6.8 Incident Management	~~6.5~~ 6.2.3 Incident Management System
~~6.8~~ 6.9 Emergency Operations/Response Plan	5.5.5 Response 6.2.4 Response Plan 6.3 Response
~~6.9 Business~~ 6.10 Continuity and Recovery	~~6.10 Business~~ 5.5.6 Continuity ~~5.5.6 Continuity~~ 5.5.7 Recovery ~~6.2.6 Continuity~~ 6.2.6 Continuity ~~6.3.3 Continuity~~ 6.3.3 Continuity ~~5.5.7 Recovery~~ 6.4 Recovery ~~6.4 Recovery~~ ~~6.4.1 Recovery Procedures~~ ~~6.4.2 Recovery Assessment~~
~~6.10~~ 6.11 Employee Assistance and Support	—

NFPA 1600 ~~(2013)~~ (2019) Chapter/Section	CSA ~~Z1600-14~~ Z1600-17 , *Emergency ~~Management~~ and ~~Business~~ Continuity Management Programs* (2017) Chapter/Section
Chapter 7 Execution	
7.1 Incident Recognition	
7.2 Initial Reporting/Notification	
7.3 Plan Activation and Incident Action Plan	
7.4 Activate Incident Management Plan	
7.5 Ongoing Incident Management and Communications	
7.6 Documenting Incident Information, Decisions, and Actions	
7.7 Incident Stabilization	
7.8 Demobilize Resources and Termination	
Chapter ~~7~~ 8 Training and Education	5.5.9 Training and Education 6.2.8 Training
~~7.1~~ 8.1 Curriculum	6.2.8.2 (competency-based curriculum)
~~7.2~~ 8.2 Goal of the Curriculum	—
~~7.3~~ 8.3 Scope and Frequency of Instruction	6.2.8.3 (frequency and scope of training)
~~7.4~~ 8.4 Incident Management System Training	—
~~7.5~~ 8.5 Recordkeeping	6.2.8.4 (maintain training records)
~~7.6~~ 8.6 Regulatory and Program Requirements (pertaining to training curriculum)	4.5 Compliance with ~~Laws~~ laws and ~~Authorities~~ authorities (pertaining to overall program)
~~7.7~~ 8.7 Public Education	6.2.5.5 Public Awareness and Education 6.3.7 Public Awareness
Chapter 8 9 Exercises and Tests	**7 Program Evaluation**
~~8.1~~ 9.1 Program Evaluation	7.1 Evaluation
~~8.2~~ 9.2 Exercise and Test Methodology	—
~~8.3~~ 9.3 Design of Exercises and Tests	—
~~8.4~~ 9.4 Exercise and Test Evaluation	7.2 Exercises and Tests ~~7.2.1 Exercises~~ ~~7.2.2 Tests~~
~~8.5~~ 9.5 Frequency	—
Chapter 9 10 Program Maintenance and Improvement	**8 Management Review**
~~9.1~~ 10.1 Program Reviews	7.3 Audit and Review ~~8~~ 8.1 Senior Management Review ~~8.1 Senior Management Review~~ ~~7.3 Audit and Review~~
~~9.2~~ 10.2 Corrective Action	7.4 Corrective Action
~~9.3~~ 10.3 Continuous Improvement	8.2 Continual Improvement

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

NFPA 1600 (~~2016~~ 2019) Chapter/Section	Federal Continuity Directive ~~1~~ (FCD) 1 (2017) Chapter/Section
Chapter 4 Program Management	**~~8 Program Management~~ IV. Policy and Background**
4.1 Leadership and Commitment	~~9 Elements of a Viable Continuity Capability (9.b Orders of Succession and 9.c Delegations of Authority)~~ IV. A. Policy ~~12~~ v. Roles and Responsibilities (assigned responsibilities are outlined in ~~NSPD-51/HSPD-20 and the NCPIP~~ PPD-40)
4.2 Program Coordinator	~~9 Elements of a Viable Continuity Capability (9.g Human Resources)~~ V. Roles and Responsibilities
4.3 Performance Objectives	Annex A: Program, Management, Plans, and Procedures
~~4.3~~ 4.4 Program Committee	— VI. Federal Executive Level Continuity Coordination Meetings
~~4.4~~ 4.5 Program Administration	~~8 Program Management~~ V. Roles and Responsibilities, B. Continuity Program Manager (Continuity Manager)
~~4.5~~ 4.6 Laws and Authorities	— Annex O: Authorities and Resources
~~4.6~~ 4.7 Finance and Administration	— Annex A: Program Management, Plans, and Procedures; Requirements and Criteria for Program Management, Plans, and Procedures, para 5
~~4.7~~ 4.8 Records Management	~~9 Elements of a Viable Continuity Capability (9.f~~ Annex F: Essential Records Management~~)~~
Chapter 5 Planning	**~~8~~ IV. Policy and Background, Annex A: Program Management, Plans, and Procedures**
5.1 Planning and Design Process	Annex A: Program Management, Plans, and Procedures
5.2 Risk Assessment	~~8 Program Management (Risk Management)~~ VI. Risk Management and Analysis (FCD-2)
5.3 Business Impact Analysis	~~9 Elements of a Viable Continuity Capability (9.a Essential Functions)~~ Annex B: Essential Functions (FCD-1), Annex C: Business Process Analysis (FCD-2), Annex D: Business Impact Analysis (FCD-2)
5.4 Resource Needs Assessment	— Annex C: Business Process Analysis (FCD-2), Annex D: Business Impact Analysis (FCD-2)
5.5 Performance Objectives	— VIII. Readiness Reporting System
Chapter 6 Implementation	**~~11~~ Annex L: Continuity Plan Operational Phases and Implementation**
6.1 Common Plan Requirements	~~8~~ Annex A: Program Management ~~(Annex A Program Plans and Procedures)~~ , Plans, and Procedures
6.2 Prevention	— VI. Risk Management and Analysis, para A
6.3 Mitigation	— VI. Risk Management and Analysis, para A
6.4 Crisis Management	
~~6.4~~ 6.5 Crisis Communications and Public Information	~~9 Elements of a Viable Continuity Capability (9.e Continuity Communications)~~ Annex E: Communications and Information Systems
~~6.5~~ 6.6 Warning, Notifications, and Communications	Annex E: Communications and Information Systems
~~6.6~~ 6.7 Operational Procedures	~~8 Program Management (Annex A Program Plans and Procedures)~~ Annex L: Continuity Operational Phases and Implementation
~~6.7~~ 6.8 Incident Management	—
~~6.8~~ 6.9 Emergency Operations/Response Plan	—

***NFPA 1600* (~~2016~~ 2019) Chapter/Section**	**Federal Continuity Directive ~~1~~ (FCD) 1 (2017) Chapter/Section**
~~6.9~~ 6.10 Business Continuity and Recovery	~~8 Program Management (Annex A Program Plans and Procedures)~~ Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase ~~9 Elements of a Viable Continuity Capability (9.j Reconstitution)~~ Annex J: Reconstitution
~~6.10~~ 6.11 Employee Assistance and Support	~~9 Elements of a Viable Continuity Capability (9.g Human Resources)~~ Annex H: Human Resources
Chapter 7 Execution	**Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase**
7.1 Program Reviews	
7.2 Incident Reporting/Notification	Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase
7.3 Plan Activation and Incident Action Plan	Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase
7.4 Activate Incident Plan	Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase
7.5 Ongoing Incident Management and Communications	Annex L: Continuity Operational Phases and Implementation, Continuity Operations Phase
7.6 Documenting Incident Information, Decisions, and Actions	
7.7 Incident Stabilization	
7.8 Demobilize Resources and Termination	
Chapter ~~7~~ 8 Training and Education	**~~9 Elements of a Viable Continuity Capability (9.h Tests, Training, and Exercises)~~ Annex K: Test, Training, and Exercise Program**
~~7.1~~ 8.1 Curriculum	
~~7.2~~ 8.2 Goal of Curriculum	
~~7.3~~ 8.3 Scope and Frequency of Instruction	Annex K: Test, Training, and Exercise Program, para Training
~~7.4~~ 8.4 Incident Management System Training	
~~7.5~~ 8.5 Recordkeeping	Annex F: Essential Records Management
~~7.6~~ 8.6 Regulatory and Program Requirements	Annex F: Essential Records Management
~~7.7~~ 8.7 Public Education	
Chapter ~~8~~ 9 Exercises and Tests	**~~9 Elements of a Viable Continuity Capability (9.h Tests, Training, and Exercises)~~ Annex K: Test, Training, and Exercise Program, para Testing**
~~8.1~~ 9.1 Program Evaluation	
~~8.2~~ 9.2 Exercise and Test Methodology	Annex K: Test, Training, and Exercise Program
~~8.3~~ 9.3 Design of Exercises and Tests	Annex K: Test, Training, and Exercise Program
~~8.4~~ 9.4 Exercise and Test Evaluation	Annex K: Test, Training, and Exercise Program
~~8.5~~ 9.5 Frequency	Annex K: Test, Training, and Exercise Program, para Testing, para Exercises

NFPA 1600 (~~2016~~ 2019) Chapter/Section	Federal Continuity Directive ~~1~~ (FCD) 1 (2017) Chapter/Section
Chapter ~~9~~ 10 Program Maintenance and Improvement	**~~11 Continuity Plan Operational Phases and Implementation~~ Annex A: Program Management, Plans, and Procedures**
~~9.1~~ 10.1 Program Reviews	Annex A: Program Management, Plans, and Procedures, para 1.b
~~9.2~~ 10.2 Corrective Action	
~~9.3~~ 10.3 Continuous Improvement	
—	~~9 Elements of a Viable Continuity Capability (9.d Continuity Facilities)~~ Annex G: Alternate Locations
—	~~9 Elements of a Viable Continuity Capability (9.i Devolution of Control and Direction)~~ Annex I: Devolution
—	~~10~~ X. Coordination with State, Local, Tribal, ~~State,~~ and Territorial~~, Local~~ Governments ~~and the~~ , Non-Governmental Organizations, and Private Sector Critical Infrastructure Owners and Operators

Supplemental Information

File Name	Description	Approved
SR_27_section_Annex_D.docx	Annex D--for staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Thu Mar 29 13:10:04 EDT 2018

Committee Statement

Committee Statement: The committee has updated the cross-walks to meet the latest 2017 editions of DRII, CSA and FCD. These changes are also to correlate with revisions made during the First Draft. They also encompass changes to the 2017 edition of Z1600. It also matches changes to the parent sections of 1600 from the first draft. The standard allows you to marry the requirements of other documents to NFPA 1600.

Response Message:

Public Comment No. 6-NFPA 1600-2017 [Chapter D]

Second Revision No. 30-NFPA 1600-2018 [Chapter E]

Annex E *NFPA 1600*, ~~2016~~ 2019 Edition, as an MSS

This annex is not a part of the requirements of this NFPA document ~~but is included for informational purposes only.~~ unless specifically adopted by the jurisdiction.

E.1 Introduction.

Information in this annex is intended to be adopted by the entity at its discretion, replacing Chapters 1 through ~~9~~ 10 . 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~~ 10 and becoming the full requirements of the standard. A management system (MS) 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 (MSS) for implementation and maintenance of the program.

This annex was created using ~~the~~ Annex SL.9 of *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~~ 10 of *NFPA 1600* are provided in brackets. Paragraphs without a cross-reference are part of the ISO identical text for ~~management system standards (MSS)~~ MSS , common ~~management system (MS)~~ MS terms, and core definitions from ~~the~~ Annex SL, Appendix 2 of *ISO/IEC Directives, Part 1, Consolidated ISO Supplement~~, 2014, Annex SL Appendix 2~~ .

E.2 Scope. [Chapter 1]

E.2.1 Scope.

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

E.2.2 Purpose.

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

E.2.3 Application.

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

E.3 Normative References. [Chapter 2]

E.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]

E.3.2 NFPA Publications. (Reserved)

[2.2]

E.3.3 Other Publications.

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

E.3.4 References for Extracts in Mandatory Sections. (Reserved)

[2.4]

E.4 Terms and Definitions. [Chapter 3]

E.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]

E.4.2 NFPA Official Definitions. [3.2]

E.4.2.1 Approved.

Acceptable to the authority having jurisdiction. [3.2.1]

E.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]

E.4.2.3 Shall.

Indicates a mandatory requirement. [3.2.3]

E.4.2.4 Should.

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

E.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~~ Non-mandatory 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~~ Manual 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]

E.4.3 General Definitions. [3.3]

E.4.3.1 Access and Functional Needs.

Persons requiring special accommodations because of health, social, economic, or language challenges. [3.3.1]

E.4.3.2 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. [3.3.2]

E.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 continuity and recovery strategies~~, recovery~~ and plans~~, and continuity of operations~~ . [3.3.3]

E.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~~ can identify time-critical functions, recovery priorities, dependencies, and interdependencies so that recovery time objectives can be established and approved. [3.3.4]

E.4.3.5 Capability.

The ability to perform required actions. [3.3.5]

E.4.3.6 Competence.

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

E.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]

E.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]

E.4.3.9 Crisis.

An issue, event, or series of events with potential for strategic implications that severely impacts or has the potential to severely impact an entity's operations, brand, image, reputation, market share, ability to do business, or relationships with key stakeholders. A crisis might or might not be initiated or triggered by an incident, and requires sustained input at a strategic level to minimize its impact on the entity. [3.3.9]

E.4.3.10 Crisis Management.

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

E.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]

E.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]

E.4.3.13 Entity.

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

E.4.3.14 Exercise.

A process to assess, train, practice, and improve performance in an ~~organization~~ entity . [3.3.14]

E.4.3.15 Incident.

An event that has the potential to cause interruption, disruption, loss, emergency, ~~crisis,~~ disaster, or catastrophe, and can escalate into a crisis . [3.3.15]

E.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]

E.4.3.17 Incident Management System (IMS).

The combination of facilities, equipment, personnel, procedures, and communications operating within a common organizational ~~structureand~~ structure and designed to aid in the management of resources during incidents. [3.3.17]

E.4.3.18 Interoperability.

The ability of diverse personnel, systems, and ~~organizations~~ entities to work together seamlessly. [3.3.18]

E.4.3.19 Mitigation.

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

E.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]

E.4.3.21 Preparedness.

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

E.4.3.22 Prevention.

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

E.4.3.23 Recovery.

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

E.4.3.24 Resiliency.

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. [3.3.24]

E.4.3.25 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]

E.4.3.26 Response.

Immediate and ongoing activities, tasks, programs, and systems to manage the effects of an incident that threatens life, property, operations, an entity, or the environment. [3.3.26]

E.4.3.27 Risk Assessment.

The process of ~~hazard identification~~ identifying threats and hazards to life, property, operations, the environment, and entities , and the analysis of probabilities, vulnerabilities, and impacts. [3.3.27]

E.4.3.28 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]

E.4.3.29 Social Media.

Forms of electronic communication (such as web sites) through which people create online communities to share information, ideas, and personal messages. [3.3.29]

E.4.3.30 Supply Chain.

A network of individuals, ~~organizations~~ entities , activities, information, resources, and technology involved in creating and delivering a product or service from supplier to end user. [3.3.30]

E.4.3.31 Test.

Procedure for evaluation with a pass or fail result. [3.3.31]

E.4.3.32 Vital Records.

Information critical to the continued operation or survival of an entity. [3.3.32]

E.4.4 ISO Terms and Definitions.

For the purposes of this document, the following terms and definitions apply.

E.4.4.1 Organization.

Person or group of people that has its own functions with responsibilities, authorities, and relationships to achieve its objectives (E.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.

E.4.4.2 Interested Party (Preferred Term) Stakeholder (Admitted Term).

Person or *organization* (E.4.4.1) that can affect, be affected by, or perceive itself to be affected by a decision or activity.

E.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.

E.4.4.4 Management System.

Set of interrelated or interacting elements of an *entity* (E.4.4.1) to establish *policies* (E.4.4.7), and *objectives* (E.4.4.8), and *processes* (E.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~~ an 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.

E.4.4.5 Top Management.

Person or group of people who directs and controls an *organization* (E.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* (E.4.4.4) covers only part of an entity, then top management refers to those who direct and control that part of the entity.

E.4.4.6 Effectiveness.

Extent to which planned activities are realized and planned results achieved.

E.4.4.7 Policy.

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

E.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* (E.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~~ the program objective, or by the use of other words with similar meaning (e.g., aim, goal, or target).

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

E.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.

E.4.4.10 Competence.

Ability to apply knowledge and skills to achieve intended results.

E.4.4.11 Documented Information.

Information required to be controlled and maintained by an entity (E.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* (E.4.4.4), including related *processes* (E.4.4.12)

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

(3) Evidence of results (records)

E.4.4.12 Process.

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

E.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* (E.4.4.10), products (including services), systems or (E.4.4.1).

E.4.4.14 Outsource (Verb).

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

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

E.4.4.15 Monitoring.

Determining the status of a system, a process (E.4.4.12), or an activity.

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

E.4.4.16 Measurement.

Process (E.4.4.12) to determine a value.

E.4.4.17 Audit.

Systematic, independent, and documented *process* (E.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.

E.4.4.18 Conformity.

Fulfillment of a *requirement* (E.4.4.3).

E.4.4.19 Nonconformity.

Non-fulfillment of a *requirement* (E.4.4.3).

E.4.4.20 Corrective Action.

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

E.4.4.21 Continual Improvement.

Recurring activity to enhance *performance* (E.4.4.13).

E.5 Context of the Entity.

Global SR-1

E.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~~crisis/disaster/emergency management and business continuity/continuity of operations continuity management system.

E.5.2 Understanding the Needs and Expectations of Interested Parties.

The entity shall determine:

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

(2) The relevant requirements of these interested parties.

E.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/~~ continuity, emergency, and crisis 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~~ F.1

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

The scope shall be available as documented information.

E.5.4 ~~Disaster/~~ Continuity, Emergency, and Crisis Management ~~and Business Continuity/Continuity of Operations~~ Management System.

The entity shall, establish, implement, maintain and continually improve a ~~disaster/~~ continuity, emergency, and crisis 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.

E.5.5 Laws and Authorities. **[~~4.5~~ 4.6]**

E.5.5.1

The program shall comply with applicable legislation, policies, regulatory requirements, and directives. [~~4.5.1~~ 4.6.1]

E.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~~ 4.6.2]

E.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~~ 4.6.3]

E.6 Leadership.

Detail SR-29

E.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~~program by:

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

(2) Ensuring the integration of the ~~disaster/~~continuity, emergency, and crisis 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~~program are available

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

(5) Ensuring that the ~~disaster/emergency management and business continuity/continuity of operations management system~~program 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~~program

(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.~~

E.6.2 Leadership and Commitment. **[4.1]**

E.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]

E.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

[4.1.2]

E.6.2.3

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

E.6.3 Policy.

Top management shall establish ~~a disaster/emergency management and business continuity/continuity of operations~~ the program 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~~ the program objectives

(3) Includes a commitment to satisfy applicable requirements

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

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

(1) Be available as documented information

(2) Be communicated within the entity

(3) Be available to interested parties, as appropriate

E.6.3.1 Program Administration. [~~4.4~~ 4.5]

E.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 E.5.5

(4) Program budget and schedule, including milestones

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

(a) Anticipated cost

(b) Priority

(c) Resources required

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

(7) Management of change

[4.5.1]

E.6.3.1.2

The program shall include the requirements specified in Sections E.5 to E.12, the scope of which shall be determined through an “all-hazards” approach, and the risk assessment. [~~4.4.2~~ 4.5.2]

E.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~~ 4.5.3]

E.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/~~ continuity, emergency, and crisis 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~~ program to top management

E.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]

E.6.4.2 Performance Objectives. [~~5.5~~ 4.3]

E.6.4.2.1

The entity shall establish performance objectives for the program in accordance with Section E.5 and the elements in Sections E.7 through E.12. [~~5.5.1~~ 4.3.1]

E.6.4.2.2

The performance objectives shall address the results of the hazard identification, risk assessment, and business impact analysis. [~~5.5.2~~ 4.3.2]

E.6.4.2.3

Performance objectives shall be developed by the entity to address both short-term and long-term needs. [~~5.5.3~~ 4.3.3]

E.6.4.2.4

The entity shall define the terms *short term* and *long term*. [~~5.5.4~~ 4.3.4]

E.6.4.3 Program Committee. [~~4.3~~ 4.4]

E.6.4.3.1

A program committee shall be established by the entity in accordance with its policy. [~~4.3.1~~ 4.4.1]

E.6.4.3.2

The program committee shall provide input, ~~and/~~ or assist in the coordination of the preparation, development, implementation, evaluation, and maintenance of the program. [~~4.3.2~~ 4.4.2]

E.6.4.3.3

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~~ . [~~4.3.3~~ 4.4.3]

E.6.4.3.4

The program committee shall solicit applicable external representation. [4.4.4]

E.7 Planning. [Chapter 5]

E.7.1 Actions to Address Risks and Opportunities.

When planning for the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program , 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~~ program 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~~ program processes

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

E.7.2 ~~Disaster/~~ Continuity, Emergency, and Crisis Management ~~and Business Continuity/Continuity of Operations~~ Objectives and Planning to Achieve Them.

E.7.2.1

The entity shall establish ~~disaster/emergency management and business continuity/continuity of operations~~ the program objectives at relevant functions and levels.

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

(1) Be consistent with the ~~disaster/emergency management and business continuity/continuity of operations~~ program 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/~~ continuity, emergency, and crisis management ~~and business continuity/continuity of operations~~ objectives.

When planning how to achieve its ~~disaster/~~ continuity, emergency, and crisis 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

~~**E.7.2.2** Performance Objectives. [5.5]~~

~~**E.7.2.2.1**~~

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

~~**E.7.2.2.2**~~

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

~~**E.7.2.2.3**~~

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

~~**E.7.2.2.4**~~

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

E.7.3 Planning and Design Process. [5.1]

E.7.3.1

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

E.7.3.2

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

E.7.3.3

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

E.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]

E.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]

E.7.3.6

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

E.7.4 Risk Assessment. [5.2]

E.7.4.1

The entity shall conduct a risk assessment. [5.2.1]

E.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]

E.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

[5.2.2.1]

E.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]

E.7.4.3

The entity shall conduct an analysis of the impact of the hazards identified in E.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

[5.2.3]

E.7.4.4

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

E.7.4.5

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

E.7.4.6

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

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

E.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]

E.7.5.1.1

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

E.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

[5.3.1.2]

E.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 E.7.5.1.2

[5.3.2]

E.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]

E.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]

E.7.5.4

The BIA identify gaps between the RTOs and RPOs and demonstrated capabilities. [5.3.4]

E.7.5.5

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

E.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]

E.8 Support.

E.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~~ program .

E.8.1.1 Resource Needs Assessment. [5.4]

E.8.1.1.1

The entity shall conduct a resource needs assessment based on the hazards identified in E.7.4 and the business impact analysis in E.7.5. [5.4.1]

E.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

[5.4.2]

E.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]

E.8.1.1.4

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

E.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]

E.8.1.2 Resource Management.

E.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

[6.8.7]

E.8.1.2.2

A current inventory of internal and external resources shall be maintained. [~~6.7.8~~ 6.8.8]

E.8.1.2.3

Donations of human resources, equipment, material, and facilities shall be managed. [~~6.7.9~~ 6.8.9]

E.8.1.3 Finance and Administration. [~~4.6~~ 4.7]

E.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~~ 4.7.1]

E.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

[4.7.2]

E.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~~ 4.7.3]

E.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

[4.7.4]

E.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~~ the program's 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.

E.8.2.1 Training. [Chapter ~~7~~ 8]

E.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~~ 8.1]

E.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~~ 8.2]

E.8.2.1.3 Scope and Frequency of Instruction.

The scope of the curriculum and the frequency of instruction shall be identified. [~~7.3~~ 8.3]

E.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~~ 8.4]

E.8.2.1.5 Recordkeeping.

Records of training and education shall be maintained as specified in Section E.8.5.5. [~~7.5~~ 8.5]

E.8.2.1.6 Regulatory and Program Requirements.

The curriculum shall comply with applicable regulatory and program requirements. [~~7.6~~ 8.6]

E.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

[8.7]

E.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~~ The program policy

(2) Their contribution to the effectiveness of the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program , including the benefits of improved ~~disaster/~~ continuity, emergency, and crisis 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~~ program requirements

E.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~~ program , including:

(1) On what it will communicate

(2) What to communicate

(3) With whom to communicate

(4) How to communicate

E.8.4.1 Crisis Management. [6.4]

E.8.4.1.1

The entity shall establish and maintain a crisis management capability to manage issues, events, or series of events, that severely impact or have the potential to severely impact an entity's brand, image, reputation, market share, ability to do business, or relationships with key stakeholders. [6.4.1]

E.8.4.1.2

The crisis management capability shall include assigned responsibilities and established processes to perform the following:

(1) Engage senior leadership

(2) Detect the signals, symptoms, incidents, events, or circumstances that portend an emerging crisis or have the potential to trigger a crisis

(3) Conduct a situation analysis

(4) Declare a crisis, alert responsible persons, and activate crisis management plans should the current situation meet established criteria

(5) Identify issues to be addressed by the responsible persons and senior leadership

(6) Develop strategies to mitigate the potential impacts of identified issues

(7) Provide direction and support for the entity's facilities, operations, employees, customers, and others affected by or potentially affected by the crisis

(8) Coordinate with the entity's crisis communication capability and provide strategic direction, authorize communications strategies, and communicate with stakeholders

[6.4.2]

E.8.4.2 Crisis Communications and Public Information. [~~6.4~~ 6.5]

E.8.4.2.1

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

(1) Internal audiences, including employees

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

[6.5.1]

E.8.4.2.2

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

(1) Central contact facility or communications hub

(2) Physical or virtual information center

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

(4) Procedures for developing and delivering coordinated messages

(5) Protocol to clear information for release

[6.5.2]

E.8.4.3 Warning, Notifications, and Communications. [~~6.5~~ 6.6]

E.8.4.3.1

The entity shall determine its warning, notification, and communications needs. [~~6.5.1~~ 6.6.1]

E.8.4.3.2

Warning, notification, and communications systems shall be reliable, redundant, and interoperable. [~~6.5.2~~ 6.6.2]

E.8.4.3.3

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~~ 6.6.3]

E.8.4.3.4

Procedures shall include issuing warnings through authorized agencies if required by law as well as the use of ~~prescripted~~ pre-scripted information bulletins or templates. [~~6.5.4~~ 6.6.4]

E.8.5 Documented Information.

E.8.5.1 General.

The entity's ~~disaster/~~ continuity, emergency, and crisis 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~~ program .

Note: The extent of documented information for a ~~disaster/~~ continuity, emergency, and crisis 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

E.8.5.2 Common Plan Requirements. [6.1]

E.8.5.2.1

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

E.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]

E.8.5.2.3

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

E.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]

E.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

E.8.5.4 Control of Documented Information.

Documented information required by the ~~disaster/~~ continuity, emergency, and crisis 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

Documented information of external origin determined by the entity to be necessary for the planning and operation of the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program shall be identified, as appropriate, and controlled.

Note: Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

E.8.5.5 Records Management. [~~4.7~~ 4.8]

E.8.5.5.1

The entity shall develop, implement, and manage a records management program to ensure that records are available to the entity. [~~4.7.1~~ 4.8.1].

E.8.5.5.2

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 [4.7.2]

[4.8.2]

E.9 Operation.

E.9.1 Operational Planning and Control.

E.9.1.1

The entity shall plan, implement and control the processes and to meet requirements, and to implement the actions determined in E.7.1, by:

(1) Establishing criteria for the processes

(2) Implementing the control of the processes in accordance with the criteria

(3) Keeping documented information to the extent necessary to have confidence that the processes have been carried out as planned

The entity shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The entity shall ensure outsourced processes are controlled.

E.9.2 Prevention. [6.2]

E.9.2.1

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

E.9.2.2

The prevention strategy shall ~~be based and shall~~ be kept current using the information collection and intelligence techniques. [6.2.2]

E.9.2.3

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. [6.2.3]

E.9.2.4

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

E.9.3 Mitigation. [6.3]

E.9.3.1

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. [6.3.1]

E.9.3.2

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. [6.3.2]

E.9.3.3

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

E.9.4 Operational Procedures. [~~6.6~~ 6.7]

E.9.4.1

The entity shall develop, coordinate, and implement operational procedures to support the program. [~~6.6.1~~ 6.7.1]

E.9.4.2

Procedures shall be established and implemented for response to and recovery from the impacts of hazards identified in E.7.5. [~~6.6.2~~ 6.7.2]

E.9.4.3

Procedures shall provide for life safety, property conservation, incident stabilization, continuity, and protection of the environment under the jurisdiction of the entity. [~~6.6.3~~ 6.7.3]

E.9.4.4

Procedures shall include the following: [~~6.6.4~~]

(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

[6.7.4]

E.9.4.5

Procedures shall allow for concurrent activities of response, continuity, recovery, and mitigation. [~~6.6.5~~ 6.7.5]

E.9.5 Incident Management. [~~6.7~~ 6.8]

E.9.5.1

The entity shall develop an incident management system to direct, control, and coordinate response, continuity, and recovery operations. [~~6.7.1~~ 6.8.1]

E.9.5.1.1 Emergency Operations Centers (EOCs). [~~6.7.1.1~~ 6.8.1.1]

E.9.5.1.1.1

The entity shall establish primary and alternate EOCs capable of managing response, continuity, and recovery operations. [~~6.7.1.1.1~~ 6.8.1.1.1]

E.9.5.1.1.2

The EOCs shall be permitted to be physical or virtual. [~~6.7.1.1.2~~ 6.8.1.1.2]

E.9.5.1.1.3

On activation of EOC, communications and coordination shall be established between incident command and the EOC. [~~6.7.1.1.3~~ 6.8.1.1.3]

E.9.5.2

The incident management system shall describe specific organizational roles, titles, and responsibilities for each incident management function. [~~6.7.2~~ 6.8.2]

E.9.5.3

The entity shall establish procedures and policies for coordinating prevention, mitigation, preparedness, response, continuity, and recovery activities. [~~6.7.3~~ 6.8.3]

E.9.5.4

The entity shall coordinate the activities specified in 6.8.3 with stakeholders. [~~6.7.4~~ 6.8.4]

E.9.5.5

Procedures shall include a situation analysis that incorporates ~~a damage~~ an assessment of the following for the purposes of activating emergency response/operations, business continuity/continuity of operations, crisis management, and ~~a needs assessment to identify~~ /or crisis communications plans and capabilities: ~~resources to support activities. [6.7.5]~~

(1) Casualties and the availability of required personnel resources

(2) Physical damage to property under the jurisdiction of the entity

(3) Interruption or disruption of the entity's operations

(4) Impacts to digital information and vital records

(5) Actual or potential contamination of the environment

(6) Actual or potential impacts to brand, image, reputation, market share, ability to do business, or relationships with key stakeholders

(7) Resources needed to support response, continuity, and recovery activities

[6.8.5]

E.9.5.6

Emergency operations/response shall be guided by an incident action plan or management by objectives. [~~6.7.6~~ 6.8.6]

E.9.6 Emergency Operations/Response Plan. [~~6.8~~ 6.9]

E.9.6.1

Emergency operations/response plans shall define responsibilities for carrying out specific actions in an emergency. [~~6.8.1~~ 6.9.1]

E.9.6.2

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. [~~6.8.2~~ 6.9.2]

E.9.6.3

The plan shall identify actions for incident stabilization. [~~6.8.3~~ 6.9.3]

E.9.6.4

The plan shall include the following: ~~[6.8.4]~~

(1) Protective actions for life safety in accordance with ~~6.8.2~~ 6.9.2

(2) Warning, notifications, and communication in accordance with Section ~~6.5~~ 6.6

(3) Crisis communication and public information in accordance with Section ~~6.4~~ 6.5

(4) Resource management in accordance with ~~6.7.7~~ 6.8.7

(5) Donation management in accordance with ~~6.7.9~~ 6.8.9

[6.9.4]

E.9.7 Continuity and Recovery. [~~6.9~~ 6.10]

E.9.7.1 Continuity [~~6.9.1~~ 6.10.1]

E.9.7.1.1 Continuity Plans.

The continuity plan shall include recovery strategies to continue critical and time-sensitive processes and provide the supporting technology that supports these processes as identified in the business impact analysis BIA. [~~6.9.1.1~~ 6.10.1.1]

E.9.7.1.2

Continuity plans shall identify and document the following: ~~[6.9.1.2]~~

(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

[6.10.1.2]

E.9.7.1.3

Continuity plans shall be designed to meet the RTO and RPO. [~~6.9.1.3~~ 6.10.1.3]

E.9.7.1.4

Continuity plans shall address supply chain disruption. [~~6.9.1.4~~ 6.10.1.4]

E.9.7.2 Recovery. [~~6.9.2~~ 6.10.2]

E.9.7.2.1

Recovery plans shall provide for restoration of processes, technology, information, services, resources, facilities, programs, and infrastructure. [~~6.9.2.1~~ 6.10.2.1]

E.9.7.2.2

Recovery plans shall document the following: ~~[6.9.2.2]~~

(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 ~~preincident~~ pre-incident controls

[6.10.2.2]

E.9.8 Employee Assistance and Support. [~~6.10~~ 6.11]

E.9.8.1

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

(1) Communications procedures

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

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

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

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

(6) Pre-incident and post-incident awareness

[6.11.1]

E.9.8.2

The strategy shall be flexible for use in all incidents. [~~6.10.2~~ 6.11.2]

E.9.8.3

The entity shall promote family preparedness education and training for employees. [~~6.10.3~~ 6.11.3]

E.10 Performance Evaluation.

Global SR-1

E.10.1 Monitoring, Measurement, Analysis, and Evaluation.

The entity shall determine:

(1) What needs to be monitored and measured

(2) The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results

(3) When the monitoring and measuring shall be performed

(4) When the results from of monitoring and measurement shall be analyzed and evaluated

The organization shall retain appropriate documented information as evidence of the results.

The entity shall evaluate the ~~disaster/emergency management and business continuity/continuity of operations~~ program performance and the effectiveness of the ~~disaster/emergency management and business continuity/continuity of operations~~ crisis/disaster/emergency management and business continuity/continuity of operations management system.

E.10.2 Internal Audit.

E.10.2.1

The entity shall conduct internal audits at planned intervals to provide information on whether the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program :

(1) Conforms to the following :

(a) The entity's own requirements for its ~~disaster/~~ continuity, emergency, and crisis management ~~and business continuity/continuity of operations~~ management system

(b) The requirements of this International Standard

(2) Is effectively implemented and maintained

E.10.2.2

The entity shall:

(1) Plan, establish, implement and maintain an audit program(s,) including the frequency, methods, responsibilities, planning requirements and reporting, which shall take into consideration the importance of the processes concerned and the results of previous audits

(2) Define the audit criteria and scope for each audit

(3) Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process

(4) Ensure that the results of the audits are reported to relevant management

(5) Retain documented information as evidence of the implementation of the audit program and the audit results

E.10.3 Management Review.

E.10.3.1

Top management shall review the entity's ~~disaster/~~ continuity, emergency, and crisis management ~~and business continuity/continuity of operations~~ management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

E.10.3.2

The management review shall include consideration of:

(1) The status of actions from previous management reviews

(2) Changes in external and internal issues that are relevant to the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program

(3) Information on the ~~disaster/emergency management and business continuity/continuity of operations~~ program performance, including trends in:

(a) Nonconformities and corrective actions

(b) Monitoring and measurement results

(c) Audit results

(4) Opportunities for continual improvement

E.10.3.3

The outputs of the management review shall include decisions related to continual improvement opportunities and any need for changes to the ~~disaster/~~ continuity, emergency, and crisis management ~~and business continuity/continuity of operations~~ management system.

E.10.3.4

The entity shall retain documented information as evidence of the results of management reviews.

E.10.4 Exercises and Tests. [Chapter ~~8~~ 9]

E.10.4.1 Program Evaluation. [~~8.1~~ 9.1]

E.10.4.1.1

The entity shall evaluate program plans, procedures, training, and capabilities and promote continuous improvement through periodic exercises and tests. [~~8.1.1~~ 9.1.1]

E.10.4.1.2

The entity shall evaluate the program based on post-incident analyses, lessons learned, and operational performance in accordance with Chapter 10. [~~8.1.2~~ 9.1.2]

E.10.4.1.3

Exercises and tests shall be documented. [~~8.1.3~~ 9.1.3]

E.10.4.2 Exercise and Test Methodology. [~~8.2*~~ 9.2*]

E.10.4.2.1

Exercises shall provide a standardized methodology to practice procedures and interact with other entities (internal and external) in a controlled setting. [~~8.2.1~~ 9.2.1]

E.10.4.2.2

Exercises shall be designed to assess the maturity of program plans, procedures, and strategies. [~~8.2.2~~ 9.2.2]

E.10.4.2.3

Tests shall be designed to demonstrate capabilities. [~~8.2.3~~ 9.2.3]

E.10.4.3 Design of Exercises and Tests. [8.3*]

E.10.4.3.1

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, entities, 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

E.10.4.4 Exercise and Test Evaluation. [~~8.4*~~ 9.4*]

E.10.4.4.1

Exercises shall evaluate program plans, procedures, training, and capabilities to identify opportunities for improvement. [~~8.4.1~~ 9.4.1]

E.10.4.4.2

Tests shall be evaluated as either pass or fail. [~~8.4.2~~ 9.4.2]

E.10.4.5 Frequency. [~~8.5~~ 9.5]

E.10.4.5.1

Exercises and tests shall be conducted on the frequency needed to establish and maintain required capabilities. [~~8.5.1~~ 9.5.1]

E.11 Execution. [Chapter 7]

E.11.1 Incident Recognition.

The entity shall establish and implement a process whereby all appropriate stakeholders have a common reference for the types of incidents that could adversely affect its people, property, operations, or the environment, and ensure it is appropriately referenced throughout the incident management process. [7.1]

E.11.2 Initial Reporting/Notification.

The entity shall establish and implement a process whereby all appropriate stakeholders can warn, notify, and report an incident that has potential to cause an adverse impact on its people, property, operations, or the environment. *(See Section 6.6 .)* [7.2]

E.11.3 Plan Activation and Incident Action Plan. [7.3]

E.11.3.1

The entity shall establish and implement a process to assess the impact of the incident on its people, property, operations, or the environment. [7.3.1]

E.11.3.2

The entity shall develop a time frame to activate appropriate planning as detailed in Sections 6.5 , 6.9 , and 6.10 , and coordinate activation when there is a declaration by public officials. [7.3.2]

E.11.4 Activate Incident Management System. [7.4]

E.11.4.1

The entity shall execute procedures from the documented plans in accordance with the following:

(1) Section 6.5

(2) Section 6.8

(3) Section 6.9

(4) Section 6.10

[7.4.1]

E.11.4.2

The entity shall execute its incident management system and activities in support of established objectives and tasks. [7.4.2]

E.11.4.3

On activation of an emergency operations center (EOC), communications and coordination shall be established between incident command and the EOC. [7.4.3]

E.11.5 Ongoing Incident Management and Communications. [7.5]

E.11.5.1

The entity shall continually assess the impact of the incident on its people, property, operations, and the environment, and reevaluate/implement its action plan in accordance with established objectives and tasks. [7.5.1]

E.11.5.2

The entity shall implement the warning, notification, and communications systems to alert stakeholders who are potentially at risk from an actual or impending incident. [7.5.2]

E.11.5.3

Based upon the extent of damage sustained to the entity, all necessary actions to invoke special authorities and request assistance needed to deal with the situation shall be as described in Chapter 4 . [7.5.3]

E.11.5.4 Documenting Incident Information, Decisions, and Actions.

The entity shall establish and implement a system for tracking incident information received, decisions made, resources deployed, and actions taken during the incident. [7.6]

E.11.5.5 Incident Stabilization.

The entity shall establish criteria for measuring when the incident has been stabilized. [7.7]

E.11.5.6 Demobilize Resources and Termination.

The entity shall execute a procedure to terminate the response and demobilize resources when the incident has been stabilized. [7.8]

E.12 Improvement. [Chapter ~~9~~ 10]

E.12.1 Nonconformity and Corrective Action.

When a nonconformity occurs, the entity shall:

(1) React to the nonconformity, and as applicable:

(a) Take action to control and correct it

(b) Deal with the consequences

(2) Evaluate the need for action to eliminate the causes of order that it does not recur or occur elsewhere, by:

(a) Reviewing the nonconformity

(b) Determining the causes of nonconformities

(c) Determining if similar nonconformities exist, or could potentially occur

(3) Implement any action needed

(4) Review the effectiveness of any corrective action taken

(5) Make changes to the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program , if necessary

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The entity shall retain documented information as evidence of:

(1) The nature of the nonconformities and any subsequent actions taken

(2) The results of any corrective action

E.12.1.1

The entity shall maintain and improve the program by evaluating its policies, program, procedures, and capabilities using performance objectives. [~~9.1~~ 10.1]

E.12.1.1.1

The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action. [~~9.1.1~~ 10.1.1]

E.12.1.1.2

Evaluations shall be conducted on a regularly scheduled basis, and when the situation changes to challenge the effectiveness of the existing program. [~~9.1.2~~ 10.1.2]

E.12.1.1.3

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

(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

[10.1.3]

E.12.1.1.4

Reviews shall include post-incident analyses, reviews of lessons learned, and reviews of program performance. [~~9.1.4~~ 10.1.4]

E.12.1.1.5

The entity shall maintain records of its reviews and evaluations, in accordance with the records management practices developed under Section E.8.5.5. [~~9.1.5~~ 10.1.5]

E.12.1.1.6

Documentation, records, and reports shall be provided to management for review and follow-up. [~~9.1.6~~ 10.1.6]

E.12.1.2 Corrective Action. [~~9.2~~ 10.2]

E.12.1.2.1

The entity shall establish a corrective action process. [~~9.2.1~~ 10.2.1]

E.12.1.2.2

The entity shall take corrective action on deficiencies identified. [~~9.2.2~~ 10.2.2]

E.12.2 Continual Improvement.

The entity shall continually improve the suitability, adequacy, and effectiveness of the ~~disaster/emergency management and business continuity/continuity of operations management system~~ program .

E.12.3 Continuous Improvement.

The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process. [~~9.3~~ 10.3]

Supplemental Information

File Name	Description	Approved
SR_30_section_Annex_E.docx	Annex changes. For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:04:20 EDT 2018

Committee Statement

Committee Statement: The committee is updating the annex based on changes made during the First Draft.

Response Message:

Second Revision No. 31-NFPA 1600-2018 [Section No. F.1]

Global SR-1

F.1 Development.

An internal assessment of the development, implementation, and progress made in ~~an emergency management and business continuity/continuity of operations~~a crisis/disaster/emergency management and business continuity/continuity of operations program is an important part of an entity's growth and success. The entity should consider the benefits of developing a documented method to conduct an assessment similar to the example provided in ~~Annex B~~B.1 that also tracks the program's continuous improvement and progress. This can be done through a "maturity model" or other form of internal metrics the entity has adopted and committed to monitoring for tracking progress through a defined time period. By quantifying progress through a scalable method, the entity can also benefit by documenting its efforts when responding to an internal or external audit process. This form of continuous improvement allows the entity to set goals (short term through long term), track progress, and eliminate waste in cost and effort while monitoring present state through future state. This also helps in justifying expenses and substantiating the need for capital, personnel, and other process components that can help to improve implementation of ~~an emergency management and business continuity/continuity of operations program~~a crisis/disaster/emergency management and business continuity/continuity of operations. Internal metrics can be monitored over a defined time period (e.g., semiannual or annual) and cross-compared with other divisions, departments, or sectors of the entity.

A specific method of applying a self-assessment and maturity model can include the following:

(1) Defining the key concepts of the maturity model

(2) Defining the elements of each concept

(3) Providing the guidelines and minimum requirements for each element

(4) Defining a method for the entity to conduct a scoring process to record its compliance with the model

(5) Implementing a method to distribute the model, train the participants, gather results, and prepare a summary to all interested parties

Best practices, lessons learned, and other criteria discovered during the assessment can be shared throughout, resulting in process improvement for the entire entity.

There are multiple approaches to evaluating the maturity of ~~an emergency management and business continuity/continuity of operations~~a crisis/disaster/emergency management and business continuity/continuity of operations program, and multiple models have been published. Consideration should be given to providing guidelines and minimum requirements for each item being evaluated by the entity, so that the assessment is applied accurately and effectively. Regardless of the approach selected, a continued focus on a quantifiable process and its use throughout all levels of the entity will provide maximum benefits for the entity.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:19:20 EDT 2018

Committee Statement

Committee Statement: This is an editorial change to reference the correct section.

Response Message:

Second Revision No. 32-NFPA 1600-2018 [Section No. F.2]

~~**F.2** Examples of Maturity Models.~~

~~**F.2.1**~~

~~**Capability Maturity Model (CMM)®.** CMM, which was developed at Carnegie Mellon University, is a model in which the term *maturity* relates to the degree of formality and optimization of processes. Originally created for use in software development, the model has been adopted by other disciplines. The five maturity levels are Initial (ad hoc), Repeatable, Defined, Managed, and Optimizing.~~

~~**F.2.2**~~

~~**Organizational Project Management Maturity Model (OPM3).** OPM3 was published by the Project Management Institute (PMI) as a way to understand project management processes. One version is an American National Standard (ANSI/PMI 08-004-2008). Within a life cycle of assessment-improvement-reassessment, there are three interlocking elements: Knowledge (learn about best practices); Assessment (identify current capabilities and areas for improvement); and Improvement (take steps to achieve performance improvement goals).~~

~~**F.2.3**~~

~~The Business Continuity Maturity Model® (BCMM®) is a free open access tool created to assist entities of all sizes perform self-assessments and assist in improving their ability to recover from a disruption. It provides a consistent, objective means for evaluating an entity's state of preparedness, including evaluation criteria in eight critical competencies across six maturity levels. The six levels are Self-Governed, Departmental, Cooperative, Standards Compliant, Integrated, and Synergistic. These competencies address business continuity program considerations including, but not limited to, the traditional areas of business recovery, security management, incident management, and technology recovery.~~

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:20:46 EDT 2018

Committee Statement

Committee Statement: Per the NFPA Manual of Style (MOS), NFPA Standards cannot contain trade names or identify individual products.

Response Message:

Second Revision No. 33-NFPA 1600-2018 [Chapter G]

Annex G APELL

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

Global SR-1

G.1

Awareness and Preparedness for Emergencies at the Local Level (APELL) consists of a series of programs first developed in 1988 under the leadership of the United Nations Environmental Programme (UNEP) with the cooperation of multiple entities, including the U.S. EPA, in response to the Union Carbide gas leak in Bhopal, India, in December 1984. APELL is a multistakeholder dialogue tool that ~~establishes~~is intended to establish adequate coordination and communication in situations in where the public might be affected by accidents and disasters. The most recent edition of the APELL Handbook was issued at the end of 2015.

The APELL program was successfully used to implement *NFPA 1600*, a standard developed to define a program for the integration of crisis/disaster/emergency management and business continuity/continuity of operations, and applicable to the private, public, and not-for-profit sectors.

The APELL program for technological hazards was implemented in 1996 in Bahia Blanca, Argentina, a city located in the southeast of the province of Buenos Aires, by the Atlantic Ocean. The city, with a population of over 300,000, is an important seaport whose harbor reaches a depth of 40 ft (12 m). The name Bahía Blanca, which means “White Bay,” comes from the typical color of the salt covering the soil surrounding the shores.

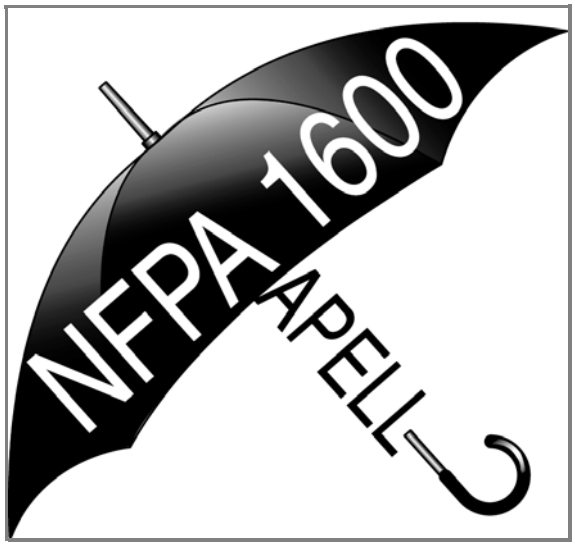
The need for the APELL program in Bahia Blanca is reinforced by a review of the number and amounts of hazardous chemicals produced each year. The industrial complex is made up of three types of industry:

(1) Petroleum industry, with an installed capacity of 4 million tons a year, producing ethanol, petrol, naphtha, GLP, fuel oil, gas oil, gasoline, asphalt, and kerosene

(2) Petrochemical industry, with an installed capacity of 3.4 million tons a year, producing ethylene, VCM, PVC, polyethylene, urea, and pure ammonia

(3) Chemical industry, with an installed capacity of 350,000 tons a year, producing chlorine and caustic soda

Figure G.1 Relationship of APELL to *NFPA 1600*.



Due to the success of implementing APELL and *NFPA 1600(see Figure G.1)* in Bahia Blanca, Argentina, the ~~Local Emergency Planning Committee~~local emergency planning committee (LEPC) in Lake County, Indiana has adopted the same integrated approach to enhance the interaction among industries, local government, and the public as required under the Superfund Amendments and Reauthorization Act (SARA), Title III. Lake County is located on the southern shore of Lake Michigan and has a heavy industrial concentration of steel, oil, and chemicals, a similar set of hazards as faced by Bahia Blanca. The LEPC is recommending a county ordinance to ensure implementation. Other counties in Indiana are exploring the advantages of using the APELL/*NFPA 1600* approach.

The APELL process is being practiced in other places within the United States and worldwide. The National Association of SARA Title III Program Officials (NASTTPO) has encouraged the use of the *APELL Handbook* as a guide for local emergency planning committees. The newest version of the handbook, issued in October 2015, emphasizes the use of metrics based upon gap analysis of capabilities to support strategic planning by communities as they seek to improve their preparedness and resilience capabilities. The gap analysis approach is equally applicable to entities seeking to improve their preparedness and planning capabilities under this standard and will assist managers in the performance

of the activities outlined in Chapter 7.

A key aspect of the gap analysis is the concept of a “vision of success.” Put simply, this concept is designed to have communities thinking long range in terms of the preparedness and capabilities outcomes they would like to achieve. It is an aspirational view of the future that helps to drive strategic planning and short-term progress. The same concept can be used by entities following this standard to promote and measure continuous improvement.

APELL process implementation consists of the following ten elements:

(1) Element 1 — Identify Participants and Establish Their Roles

(2) Element 2 — Evaluate Risks

(3) Element 3 — Review Existing Capabilities and Emergency Plans — Identify Gaps

(4) Element 4 — Create the Vision of Success

(5) Element 5 — Making Progress Toward the Vision of Success

(6) Element 6 — Make Changes in Existing Emergency Plans and Integrate into Overall Community Preparedness Plan

(7) Element 7 — Obtain Endorsement from Government Authorities

(8) Element 8 — Implement Community Preparedness Plans Through Communicating, Educating, and Training Community Members

(9) Element 9 — Establish Procedures for Periodic Testing, Review, and Updating of the Plans

(10) Element 10 — Maintain APELL Through Continuous Improvement

Each of these elements is illustrated through examples and desired outcomes in the *APELL Handbook*.

The APELL process informs the community about the risks to which they are exposed and educates the community on how to react to accidents/disasters. The program promotes the coordination among representatives from the industry, local-level institutions, and the public. The APELL process includes the preparation of an integrated community preparedness plan, including preparing the community for early warnings of emergencies.

Other APELL programs have been produced for mining, port areas, multihazards, transportation, and tourism ~~and~~. The latest edition of the *APELL Handbook* and these other documents are available at the “Global APELL Platform” web page~~.~~: apell.eecentre.org.

Supplemental Information

File Name	Description	Approved
SR_33_section_Annex_G.docx	Revised Annex. For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:25:24 EDT 2018

Committee Statement

Committee Statement: These are editorial changes necessary to correct grammatical errors and better clarify the intended reference to the APELL Handbook.

Response Message:

Second Revision No. 34-NFPA 1600-2018 [Section No. I.1]

I.1 General.

Responsibility for preparedness is a whole-community approach that rests on the shoulders of many stakeholders, from persons with disabilities and other access and functional needs to community emergency response personnel and the community supply chain that supports this population during times of peace and emergencies (i.e., Meals on Wheels, food providers, volunteers, public health, NGOs, infrastructure service providers, and commercial entities). Each segment of the community, has a role in prevention, mitigation, response, continuity, and recovery that can be addressed in a holistic manner as long as ~~people~~ persons with disabilities and other access and functional needs are identified in advance.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:39:05 EDT 2018

Committee Statement

Committee Statement: The terminology is being changed to be compliant with ADA requirements and section 508.

Response Message:

Second Revision No. 35-NFPA 1600-2018 [Section No. I.4]

I.4 The Role of Emergency Management and EOCs.

Emergency management departments can be prepared to support people with disabilities and other access and functional needs by engaging in outreach strategies at local levels with nonprofit and nongovernmental entities to understand the access and functional needs supply chain of services and provide preparedness education to ~~NPOs and other services~~ other providers.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:43:07 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to align with the scope of the standard and associated annex.

Response Message:

Second Revision No. 36-NFPA 1600-2018 [Section No. I.9.2]

I.9.2 Additional Documents.

American Red Cross at redcross.org, *search:* disaster safety for people with disabilities.

Cal OES Access & Functional Needs at caloes.ca.gov, *search:* access, functional, needs.

Centers for Disease Control and Prevention at cdc.gov, *search:* emergency preparedness for older adults.

Developing a Disaster Ready Organization — Inclusion Research Institute at inclusionresearch.org, *search:* inclusion research institute.

Disaster Resources for People with Disabilities, Disability-related Organizations and Emergency Managers at jik.com, *search:* disaster preparedness.

Emergency Response for People Who Have Access and Functional Needs — St. Petersburg College at spcollege.edu, *search:* national terrorism preparedness institute.

Employers' Guide to Including Employees with Disabilities in Emergency Evacuation Plans — Job Accommodation Network at askjan.org, *search:* emergency evacuation plans — job accommodation network.

Evacuation and Transportation Planning Toolkit for People with Functional Needs — CA EMA at nusura.com, *search:* understanding evacuation and transportation of people.

FEMA's Functional Needs Support Services Guidance at phe.gov, *search:* preparedness, planning, functional, needs.

Guidance on Planning for Integration of Functional Needs Support Services in General Population Shelters at fema.gov, *search:* guidance, planning, functional needs, population, shelters.

Individuals with Access and Functional Needs at Ready.gov, *search:* individuals with disabilities.

Individuals with Access and Functional Needs — FEMA at ready.gov, *search:* access, functional, needs.

National Council on Disability at ncd.gov, *search:* emergency management.

National Organization on Disability at nod.org, *search:* emergency preparedness initiative.

National Resource Center on Advancing Emergency Preparedness for Culturally Diverse Communities at diversitypreparedness.org.

North Carolina Institute for Public Health at unc.edu, *search:* assisting persons with disabilities during an emergency.

Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures at eeoc.gov, *search:* emergency evacuation.

People with Disabilities and Other Access and Functional Needs — FEMA at fema.gov, *search:* disabilities, access, functional needs.

Project Safe EV-AC Evacuation and Accommodation of People with Disabilities at preventionweb.net/English, *search:* evacuation, accommodation, people, disabilities.

U.S. Department of Health and Human Services, Civil Rights at hhs.gov, *search:* emergency preparedness.

U.S. Department of Labor, Office of Disability Employment Policy at dol.gov, *search:* emergency preparedness and people with disabilities.

U.S. Department of Transportation at transportation.gov, *search:* emergency preparedness and individuals with disabilities.

U.S. Office of Personnel Management at opm.gov, *search:* disability employment.

~~Assisting Persons with Disabilities during an Emergency: http://cphp.sph.unc.edu~~

~~CDC Releases Older Adult Preparedness Portal: http://www.cdc.gov~~

~~Community Planning Toolkit for State Emergency Preparedness Managers: http://www.hhs.gov/~~

~~Developing a Disaster Ready Organization — Inclusion Research Institute: http://www.inclusionresearch.org/~~

~~Disability Preparedness Resource Center — DHS: http://www.disabilitypreparedness.gov/~~

~~Disability.gov — Emergency Preparedness: https://www.disability.gov/~~

~~DisabilityPreparedness.gov: http://www.disabilityresources.org/~~

~~Disaster Preparedness for People with Disabilities: http://www.disabilityresources.org/~~

~~Disaster Resources for People with Disabilities, Disability-related Organizations and Emergency Managers: http://www.jik.com/~~

~~Emergency Management National Council on Disability: http://www.ncd.gov/policy/emergency_management~~

~~Emergency Preparedness — Disability.gov: http://www.disability.gov/emergency_preparedness~~

~~Emergency Preparedness and Individuals with Disabilities — U.S. DOT: http://www.dotcr.ost.dot.gov/asp/emergencyprep.asp~~

~~Emergency Preparedness and People with Disabilities — U.S. DOL Office of Disability Employment Policy: http://www.dol.gov/odep/programs/emergency.htm~~

~~Emergency Preparedness Initiative — National Organization on Disability: http://nod.org~~

~~Emergency Preparedness Resources for those with Special Needs — Wisconsin Board for People with Developmental Disabilities: http://www.wibpdd.org/disasterpreperation/index.cfm~~

~~Emergency Response for People Who Have Access and Functional Needs — St. Petersburg College: http://terrorism.spcollege.edu/~~

~~Employers' Guide to Including Employees with Disabilities in Emergency Evacuation Plans — Job Accommodation Network: http://www.jan.wvu.edu/media/emergency.html~~

~~Evacuation and Transportation Planning Toolkit for People with Functional Needs — CA EMA: http://www.nusura.com/media/projects/Cal_EMA_Toolkit/resources5.html~~

~~Evacuation Documents — ORNL CSEPP Protective Action Toolkit: http://emc.ornl.gov/CSEPPweb/data/html/Evacuation_Documents.html~~

~~Evacuation Preparedness Guide — Resources and References — Center for Disability Issues and the Health Professions: http://www.cdihp.org/evacuation/resources.html~~

~~Federal Employment of People with Disabilities — Reasonable Accommodation: http://www.opm.gov/disability/~~

~~Inclusion Research Institute — Developing a Disaster Ready Organization: http://inclusionresearch.org/OL/~~

~~Inclusive Preparedness Center for People with Disabilities: http://www.inclusivepreparedness.org/~~

~~Inclusive Preparedness Center: http://www.inclusivepreparedness.org/~~

~~Individuals with Access and Functional NeedsReady.gov: http://www.ready.gov/~~

~~Meeting the Needs of Vulnerable Populations Equity in Emergency Response: http://www.apctoolkits.com/~~

~~National Dissemination Center for Children with Disabilities: http://nichcy.org/~~

~~National Organization on Disability: http://www.nod.org/~~

~~National Resource Center on Advancing Emergency Preparedness for Culturally Diverse Communities: http://www.diversitypreparedness.org/~~

~~Obtaining and Using Employee Medical Information as Part of Emergency Evacuation Procedures: http://www.eeoc.gov/~~

~~People with Disabilities and Other Access and Functional Needs — FEMA: http://www.fema.gov/plan/prepare/specialplans.shtm~~

~~PrepareNow.org — Supporting Special Needs and Vulnerable Populations in Disaster: http://www.preparenow.org/prepare.html~~

~~Project Safe EV-AC Evacuation and Accommodation of People with Disabilities: http://evac.icdi.wvu.edu/library/~~

~~Resources on Emergency Evacuation and Disaster Preparedness — U.S. Access Board: http://www.access-board.gov/evac.htm~~

~~Safe Escape — Emergency Preparedness for Children with Health Care Needs and Disabilities: http://www.escapesafe.org/~~

~~http://www.ready.gov/individuals-access-functional-needs~~

~~http://www.fema.gov/pdf/about/odic/fnss_guidance.pdf~~

~~http://m.fema.gov/individuals-access-functional-needs~~

~~http://www.phe.gov/Preparedness/planning/abc/Pages/funcitonal-needs.aspx~~

~~http://www.calema.ca.gov/ChiefofStaff/Pages/Access-and-Functional-Needs.aspx~~

~~http://community.fema.gov/connect.ti/ACCESS_COP/groupHome~~

~~http://www.domesticpreparedness.com/Industry/Private_Sector/Community_Resilience_%26_Functional_Needs/~~

Supplemental Information

File Name	Description	Approved
SR_36_section_I.9.2.docx	For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 11:46:26 EDT 2018

Committee Statement

Committee Statement: The committee has updated all references found in the Annex. They have also removed duplicate references and checked availability of resources based on the Second Draft meeting. In addition the committee has revised the hyperlinks provided so that the user can now go to the main domain page and search for the topic. This helps prevent broken links appearing in the standard.

Response Message:

Second Revision No. 39-NFPA 1600-2018 [Section No. K.1]

K.1 Introduction.

The material in this annex is based on the National Institute of Standards and Technology (NIST) and Fire Protection Research Foundation research and documents: *Developing Emergency Communication Strategies for Buildings,* by E. Kuligowski, S. Gwynne, K. Butler, B. Hoskins, and C. Sandler; *General Guidance on Emergency Communication Strategies for Buildings, 2nd Edition,* by E. Kuligowski and H. Omori; ~~and~~ *Outdoor Siren Systems: A review of technology, usage, and public response during emergencies*, by E. Kuligowski and K. Wakeman~~.~~ , and *A Review of Public Response to Short Message Alerts under Imminent Threat* , by E. Kuligowski and J. Doermann.

The purpose of this annex is to provide information and guidance on emergency communication strategies to emergency managers, emergency personnel, first responders, government agencies, the media, businesses, and other entities responsible for alerting and warning the public in the response phase of hazards and disasters. This guidance is based on multiple reviews of literature sources from a variety of social science and engineering disciplines.

First, the annex discusses the differences between alerts and warnings, followed by an overview of emergency communication technology and/or approaches. The annex ends with a presentation of guidance on emergency communication strategies, including general guidance on coordination and preplanning, alerts, and warnings.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 12:10:12 EDT 2018

Committee Statement

Committee Statement: The committee added a reference relating to guidance added on short message alerts.

Response Message:

Second Revision No. 40-NFPA 1600-2018 [Section No. K.3.3]

K.3.3 Wireless Emergency Alerts (WEAs).

WEA is a nationwide program across the United States whereby emergency alerts (currently restricted to 90 characters in length) are sent to individual mobile devices by “authorized government alerting authorities.” An individual can receive these alerts directly to his or her mobile device without the need to download an app or subscribe to a particular service. There are three main types of alerts that can be disseminated through this system: alerts for extreme weather, AMBER alerts (i.e., urgent bulletins alerting individuals about child-abduction cases), and Presidential Alerts during a national emergency. WEA messages are always accompanied by a special tone and vibration, which are both repeated twice as the message is first displayed on the mobile device. In addition to emergency managers, the National Weather Service is considered an “authorized government alerting authority” and can send WEA messages for tsunami, tornado, and flash floods, and hurricanes, typhoons, dust storms, and extreme wind. The WEA messages are sent to individuals based upon their geographical location (i.e., WEAs are broadcast from area cell towers to mobile devices in the area), their type of device (i.e., it needs to be a WEA-capable phone), and their wireless carrier (i.e., the carrier must participate in the program). This is an opt-out program, in that if individuals do not wish to receive WEAs, they can opt out of the system via settings on their mobile devices.

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 12:12:58 EDT 2018

Committee Statement

Committee Statement: This is an editorial correction to clarify that WEA relates to United States specific guidance. Also, the committee is aware that the 90 character length may change in the near future and in order to prevent the next edition of the standard being incorrect added “currently”.

Response Message:

Second Revision No. 41-NFPA 1600-2018 [Section No. K.4.2.2]

K.4.2.2 ~~Wireless Mobile Alerts and~~ "Short Messages Alerts" ~~Sent via Social Media Platforms for Alerting~~ .

~~Guidance will be provided on the following items:~~

- ~~Message content and order of content~~
- ~~Message language (e.g., 6th grade reading level is appropriate)~~
- ~~The development of multilingual messages~~
- ~~Factors that influence public message retransmission (and in turn, message saliency)~~
- ~~The appropriate use of links, maps, geolocation information, graphics, and videos~~
- ~~The dissemination of messages by credible sources (and those sources perceived as credible might be different for different audiences)~~

The following guidance is provided for the creation of short message alerts (i.e., alert messages with specific character restrictions) for populations under imminent threat.

Include the following content within the short message alert:

(1) Source of the message

(2) Type of hazard and its consequences

(3) Location of the hazard

(4) Timeline of the hazard

(5) Actions that should be taken by the receiving public

List the message source at the beginning of the short message alert. Messages are more successful in prompting safe and effective public response if the source of the message is perceived as credible by the receiving public.

Use clear language. Reduce, and if possible, remove abbreviations, acronyms, and jargon. Clearly spell out all words, including the source of the message and timeline information (e.g., time zones). When identifying hazard or safe zones, use terminology that is familiar to the receiving public.

Communicate the seriousness of the event, the consequences of the risk if the receiver does not act, and the specific actions that should be taken in response to the event.

Craft the messages using imperative- or instructional-style voice, especially when relaying the protective action(s) that should be taken by the receiving public.

Supplemental Information

File Name	Description	Approved
1600_SR-41_K.4.2.2-legislative_changes.docx	For staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 12:14:23 EDT 2018

Committee Statement

Committee This annex item provides information on how short message alerts can be created in manner

Statement:	more effective for public response.
Response Message:	

Second Revision No. 43-NFPA 1600-2018 [Chapter L]

Annex M Informational References

M.1 Referenced Publications.

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

M.1.1 NFPA Publications.

National Fire Protection Association, 1 Batterymarch Park, Quincy, MA 02169-7471.

NFPA 72®, *National Fire Alarm and Signaling Code*, ~~2016~~ 2019 edition.

NFPA 1026, *Standard for Incident Management Personnel Professional Qualifications*, 2018 edition.

NFPA 1561, *Standard on Emergency Services Incident Management System and Command Safety*, 2014 edition.

NFPA 1600, *Handbook: Emergency Management and Continuity Programs*, ~~2016~~ 2019 edition.

NFPA 1616, *Standard on Mass Evacuation, Sheltering, and Re-entry Programs*, 2017 edition.

M.1.2 Other Publications.

M.1.2.1 ASTM Publications.

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

ASTM ~~WK16252~~ E2640 , *Standard Guide for Resource Management in Emergency Management and Homeland Security*~~.~~ , 2010.

M.1.2.2 CSA Publications.

Canadian Standards Association, 178 Rexdale Boulevard, Toronto, ON, Canada M9W 1R3.

CSA Z1600, *Emergency Management and Business Continuity Programs*, ~~second~~ 2017 edition~~, 2014~~ .

M.1.2.3 DHS Publications.

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

NIMS DHS ICS-300, *Intermediate ICS for Expanding Incidents*, ~~2008.~~ 2011.

M.1.2.4 DRII Publications.

DRI International, 119 West 23rd Street, Suite 704, New York, NY 10011.

DRII International Glossary for Resiliency~~, https://drii.org.glossary.php 10/13/2014~~ .

Professional Practices for Business Continuity Practitioners, 2012.

M.1.2.5 ISO Publications.

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

~~*ISO/IEC Directives, Part 1, Consolidated ISO Supplement* , 2014.~~

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

~~ANSI/ASSE/ISO *Guide 73, Vocabulary for Risk Management,* 2011.~~

~~Draft ISO Guide 83, *High Level Structure and Identical Text for Management System Standards and Common Core Management System Terms and Definitions.*~~

ISO/TC 223, *Societal security*.

ISO 22300, *Societal security — Terminology,* 2012.

ISO 22301, *Societal security — Business continuity management systems — Requirements,* 2012.

ISO 22311, *Societal security — Video-surveillance — Export interoperability,* 2012.

ISO 22313, *Societal security — Business continuity management systems — Guidance,* 2012.

ISO 22320, *Societal security — Emergency management — Requirements for incident response,*~~2012.~~ 2011.

ISO 22398, *Societal security — Guidelines for exercises,* 2013.

ISO/PAS 22399, *Societal security — Guideline for incident preparedness and operational continuity management,* 2007.

ANSI/ASSE/ISO 31000, *Risk Management Principles and Guidelines,* 2011.

ANSI/ASSE/ISO *Guide 73, Vocabulary for Risk Management* , 2009.

ISO/IEC Directives, Part 1, Consolidated ISO Supplement, 2014.

~~ANSI/ASSE/ISO~~ ANSI/IEC/ISO 31010, *Risk Assessment Techniques,* 2011.

~~**M.1.2.6** U.S. Department of Homeland Security.~~

~~U.S. Department of Homeland Security Exercise and Evaluation Program (HSEEP), Washington, DC.~~

~~https://hseep.dhs.gov/pages/1001_HSEEP7.aspx~~

M.1.2.6 Other Publications.

APPELL Handbook, ~~United Nations Environmental Programme (UNEP).~~ available on the Global APELL Platform.

~~*Continuity Guidance Circular 1 (CGC 1)* , July, 2013. The U. S. Federal Emergency Management Agency (FEMA).~~

~~web page.~~

The CIA World Factbook, a handbook of economic, political, and geographic intelligence. (http://foia.cia.gov) (Excellent source of country information, including background information on countries not limited to geography, demographics, disaster, economy, political, transportation, and military information. The online version is updated continuously, while the print version is published every year.)

Kuligowski, E. D., S. M. V. Gwynne, K. M. Butler, B. L. Hoskins, and C. R. Sandler. 2012. *Developing Emergency Communication Strategies for Buildings*. NIST Technical Note 1733, National Institute of Standards and Technology: Gaithersburg, MD.

Kuligowski, E. D. and H. Omori. 2014. *General Guidance on Emergency Communication Strategies for Buildings, 2nd Edition*. NIST Technical Note 1827, National Institute of Standards and Technology: Gaithersburg, MD.

Kuligowski, E. D. and Wakeman, K. ~~(2017).~~ 2017 . *Outdoor Siren Systems: A review of technology, usage, and public response during emergencies*. NIST Technical Note 1950, National Institute of Standards and Technology: Gaithersburg, MD. Metropolitan Washington Council of Governments Small Business Preparedness: http://www1.mwcog.org/security/security/continuity/intro.asp

Kuligowski, E.D., and Doermann, J. 2018. *A Review of Public Response to Short Message Alerts under Imminent Threat* . NIST Technical Note 1982, National Institute of Standards and Technology: Gaithersburg, MD.

Open for Business EZ® — Business Continuity Planning, The Insurance Institute for Business and Home Safety.

~~http://disastersafety.org/wp-content/uploads/OFB-EZ_Toolkit_IBHS.pdf~~

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

~~*Training* , July 1996.~~ The U.S. Federal Emergency Management Agency (FEMA~~).~~), *Continuity Guidance Circular 1 (CGC 1)* , July 2013.

The U.S. Federal Emergency Management Agency (FEMA), *Training,* July 1996.

~~http://www.fema.gov/plan/prepare/specialplans.shtm~~

M.2 Informational References.

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

M.2.1 NFPA Publications. (Reserved)

M.2.2 ARMA Publications.

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

ANSI/ARMA 5, *Vital Records: Identifying, Managing, and Recovering Business-Critical Records* , 2010.

ARMA TR-22, *Glossary of Records and Information Management Terms* , 4th Edition, 2012.

M.2.3 Other Publications.

The American Red Cross Community Disaster Education ~~provides~~ at redcross.org. Provide s information organized for home and family, workplace and employees, and school and students. ~~See http://www.redcross.org/surveys/capss/cde~~ *Search:* community disaster education.

~~The U.S. Federal Emergency Management Agency Community Emergency Response Team (CERT) program provides information on disaster preparedness, fire safety, disaster medical operations, light search and rescue, disaster psychology, and terrorism. See: https://www.citizencorps.gov/cert/~~

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

~~ANSI/ARMA 5-2010, ARMA TR22–2012, *Vital Records: Identifying, Managing, and Recovering Business-Critical Records* , ARMA International, 2012.~~

~~ARMA TR 22-2012, *Glossary of Records and Information Management Terms, 4th Edition* , ARMA International, 2012.~~

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

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

~~*Contingency Planning Guide for Information Technology (IT) Systems* , National Institute of Standards and Technology, NIST Special Publication 800-34, http://csrc.nist.gov/publications/nistpubs/800-rev1/sp800-34-rev1_errata-Nov11-2010.pdf~~

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

Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology, Special Publication 800-50, ~~http://csrc.nist.gov/publications/nistpubs/800-50 /NIST-SP800-50.pdf.~~ at NIST.gov. *Search:* building an information technology security awareness.

Contingency Planning Guide for Information Technology (IT) Systems, ~~Security Handbook: A Guide for Managers~~ , National Institute of Standards and Technology, ~~SP 800-100, http://csrc.nist.gov/publications /nistpubs/800-100/SP800-100-Mar07-2007.pdf.~~ NIST Special Publication 800-34, at NIST.gov. *Search:* contingency planning at computer security resource center.

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

Developing Effective Standard Operating Procedures for Fire and EMS Departments, FEMA, 1999, at usfa.fema.gov. *Search:* developing effective standard operating procedures.

Generally Accepted Principles and Practices for Securing Information Technology Systems, National Institute of Standards and Technology, SP 800-14, NIST.gov. *Search:* principles and practices for securing information technology systems. ~~http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf.~~

Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities, Recommendations of the National Institute of Standards and Technology , Special Publication 800-84, at NIST.gov. *Search:* guide to test, training, and exercise programs for IT plans and capabilities.

Hiles, Andrew. *Business Continuity Management: Global Best Practices, Fourth Edition,* Rothstein Publishing, 2014.

Information Security Handbook: A Guide for Managers, National Institute of Standards and Technology, SP 800-100, at NIST.gov. *Search:* information security handbook: a guide for managers.

An Introduction to Computer Security: The NIST Handbook, National Institute of Standards and Technology, SP 800-12, ~~http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf.~~ at NIST.gov. *Search:* an introduction to computer security.

~~*Business Continuity Management: Global Best Practices, Fourth Edition* , by Andrew Hiles, Rothstein Publishing, 2014.~~

~~Congressional Research Service~~ Moore, L.K. , “Emergency Communications: The Emergency Alert System (EAS) and All-Hazard Warnings”: Congressional Research Service, 2009. ~~http://www.nws.noaa.gov/os/dissemination/nws_eas.shtml~~

National Incident Management System (NIMS). NIMS Resource Center, at FEMA.gov. *Search:* national incident management system.

Risk Management Guide for Information Technology Systems , National Institute of Standards and Technology, SP 800-30, at NIST.gov. *Search:* risk management guide for information technology systems.

The U.S. Federal Emergency Management Agency Community Emergency Response Team (CERT) program at ready.gov. Provides information on disaster preparedness, fire safety, disaster medical operations, light search and rescue, disaster psychology, and terrorism. *Search:* citizen corps.

M.2.4 Internet References.

Digital Librarian (www.digital-librarian.com)

Infomine (http://infomine.ucr.edu)

Internet Public Library (http://www.ipl.org)

Open Directory (http://www.dmoz.org

The WWW virtual library (http://vlib.org)

InfoPlease Countries of the World (www.infoplease.com/countries.html) *(See also under InfoPlease General Information.)*

This source, as well as similar sources, such as the BBC Country Reports, uses *The CIA World Factbook* as a source for its information.

Congressional Research Service, "Emergency Communications: The Emergency Alert System (EAS) and All-Hazard Warnings": http://www.nws.noaa.gov/os/dissemination/nws_eas.shtml

Crisis Communications Plan Template (Canadian Centre for Emergency Preparedness) http://www.ceep.ca/results.html?cx=016947605165415316345%3Alfdhstamyrc&q=Communications Plan Template&sa=Search&cof=FORID%3A11&siteurl=www.ceepca%2Fresources.html&ref=www.ceep.ca&2&ss=4575k930885j31 &siteurl= at ceep.ca. *Search:* crisis communications plan template.

Digital Librarian. *Search:* digital librarian — writing, speaking, and consulting with a focus on technology.

Disaster Research Center, University of Delaware: http://www.udel.edu/DRC/ , at udel.edu. *Search:* disaster research center.

Disaster Recovery Planning, University of Toronto, at utoronto.ca. *Search:* business continuity planning.

Emergency Management Assessment Program (EMAP): http://www.emaponline.org/ , at emap.org. *Search:* emergency management assessment program.

Emergency Management Competencies: http:// , at training.fema.gov. /EMIWeb /edu/EMCompetencies.asp *Search:* emergency management competencies.

Emergency Management Institute (FEMA) IS-120 Introduction: http://training.fema.gov

Emergency Management Institute homepage (FEMA): http:// , at training.fema.gov/ . *Search:* emergency management institute.

Emergency Program Manager: Knowledge, Skills, and Abilities: http:// , at training.fema.gov/EMIWeb /edu/EmergProgMgr.doc . *Search:* emergency program manager.

Enterprise Preparedness (International Center for Enterprise Preparedness): , at intercep http://www .nyu.edu/intercep . *Search:* international center for enterprise preparedness.

EPA Risk Assessment Portal: http://www.epa.gov/risk/ , at epa.gov. *Search:* risk assessment.

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

Hazard Mitigation Planning (FEMA): http://www.fema.gov/plan/mitplanning/index.shtm , at fema.gov. *Search:* hazard mitigation planning

Homeland Security Exercise and Security Evaluation Program: https://hseep.dhs.gov/pages /1001_HSEEP7.aspx , at fema.gov. *Search:* homeland security exercise and evaluation program.

ICS All-Hazard Core Competencies (FEMA): http://www.fema.gov/library/viewRecord.do?id=2948 , at fema.gov. *Search:* ICS all-hazard core competencies.

Infomine. *Search:* infomine — UCR library.

InfoPlease, Countries of the World. *Search:* infoplease general information.

International Standards Organization (ISO): http://www.iso.org , at iso.org. Search: international organization for standardization.

Internet Public Library. *Search:* ipl2: information you can trust.

Management Institute (FEMA) IS-120 Introduction, at training.fema.gov. *Search:* emergency management institute IS-120 introduction

Mitigation Best Practices Search (FEMA): http://www.fema.gov/mitigationbp/index.jsp , at fema.gov. *Search:* mitigation best practices portfolio.

Natural Hazards Center, University of Colorado: ~~www.colorado.edu/hazards/~~ , at colorado.edu. *Search:* natural hazards center.

New York State Department of Health (EMS) EMS Mutual Aid Planning Guidelines: ~~http://www.health.ny.gov/professionals/ems/policy/89-02.htm~~ , at health.ny.gov. *Search:* EMS mutual aid planning guidelines.

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

Records Managers (National Archives): ~~http://www.archives.gov/records-mgmt/~~ , at archives.gov. *Search:* records managers.

Risk Management Standard (Australia): ~~http://infostore.~~ , at saiglobal.com~~/store/getpage.aspx?path=/publishing/shop/promotions/AS_NZS_ISO_31000:2009_Risk_Management_Principles_and_guidelines.htm&site=RM~~ . *Search:* risk management standard.

WWW virtual library. *Search:* WWW virtual library.

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

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

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

Supplemental Information

File Name	Description	Approved
SR_43_section_Annex_M.docx	Annex L now Annex M--for staff use	

Submitter Information Verification

Submitter Full Name: Michael Wixted

Committee:

Submittal Date: Tue Apr 03 14:33:36 EDT 2018

Committee Statement

Committee Statement: The committee has added references based on changes per the MOS and also fixed the domain address issue by only referring to the main webpage.

Response Message: