Auditing the Preparedness Program

Periodic auditing may be required by regulation or customers. Assess capabilities to safeguard people, protect property, and minimize business interruption.

How capable is your preparedness program? Will it protect the lives of your employees if there is a fire or active shooter in your building? Will the recovery strategies in your business continuity plan enable you to continue priority operations when your building can’t be reoccupied? Will your communications plan enable you to quickly and effectively communicate with your customers and stakeholders as news of the incident is tweeted and blogged soon after emergency vehicles arrive?

Is your program compliant with the increasing number of federal, state, and local regulations? Are your major customers asking to review your business continuity plan to ensure it meets their requirements for a resilient supplier?

There are many misconceptions of what constitutes a preparedness program. Is it a disaster plan? Is it an emergency plan? Is it a business continuity plan? Is it a crisis management plan? A preparedness program is more than a plan or plans. It is a management program custom designed to safeguard your employees, protect your facilities, minimize business interruption, prevent environmental contamination, and protect your brand, image, and reputation.

The only way to determine whether your preparedness program meets the needs of your company is to conduct an audit.

What is an Audit?

The International Standards Organization (ISO) defines an audit as a “systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.”

The International Professional Practices Framework published by the Institute of Internal Auditors defines internal auditing as “an independent, objective assurance and consulting activity designed to add value and improve an organization’s operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.”

The most common type of audit is a “first party” audit, which is also known as a self-assessment. Your customers, a second party, may also audit your program. You may also engage a consultant—an independent third party—to audit your program. Regardless of who audits your program, audit standards should be followed and national or international standards should be used as the criteria.
Planning an Audit

When planning an audit, decide what you want to accomplish. Do you want to prepare for program certification such as the voluntary private sector preparedness program known as PS-Prep™? Do you want to know whether your program meets regulatory requirements? Does your program conform to international standards? Maybe you want to prepare for an audit by your most important customer.

The audit objectives will help to identify the criteria that will be used to evaluate your preparedness program. The criteria may be internal company standards, or you may choose to use standards such as NFPA 1600 “Standard on Disaster/Emergency Management and Business Continuity Programs” or ISO 22301 “Societal security - Business continuity management systems – Requirements.” These global standards provide comprehensive criteria for assessing a preparedness program.

If auditing to one of the global standards, the auditor(s) must be knowledgeable in the standard that will be used as well as the industry that will be audited. If program certification is the objective, then auditors from accredited certifying bodies must conduct the audit. Preparatory audits before certification may employ auditors who have successfully completed the approved courses required of the certifying bodies. Auditors should have subject matter expertise in emergency management and business continuity, demonstrated knowledge of your industry, and professional certification(s).

A dialog with a qualified auditor will help you determine the scope of the audit that will accomplish your objectives. Auditors must collect “evidence” to determine whether the audit criteria—the standard—has been met. Scope will include the components of the program that will be audited (e.g., emergency operations, business continuity, etc.); facilities that will be surveyed (e.g., a critical, or high-hazard facility); the persons with responsibility for aspects of the program who will be interviewed; and program documentation that will be reviewed.

A successful audit requires advance planning to ensure that representative evidence can be collected by the auditors. Planning should ensure that the following are available at the times specified in the audit schedule:

- Program plans (emergency response, business continuity, information technology disaster recovery, crisis management, crisis communications, risk assessments, business impact analyses, and prevention/mitigation strategies)
- Records of training, education, testing, drills, and exercises
- Access to facilities to become familiar with business operations, hazards, and assets at risk
- Persons who have a defined role in the program
- Senior management for an interview and to attend the audit’s closing conference

Auditing Elements of the Preparedness Program

The auditor must gather and evaluate sufficient evidence to determine whether the preparedness program conforms to the selected criteria. The following are elements of a preparedness program that should be evaluated by auditors. These elements are taken from NFPA 1600.

Program Management

The success of any program is dependent upon the commitment, direction, and support of senior management. A preparedness program is no different. Auditors should assess leadership of the program, the commitment of resources, and the support for continuous improvement of the program.
Auditors should assess the role of the person or persons responsible for development, implementation, and improvement of the program—the “program coordinator.” Does the coordinator(s) have the authority, knowledge, skills, and abilities to develop the program?

Program development requires the involvement of many persons with knowledge of the entity and its operations as well as subject matter expertise in the areas of emergency management and business continuity. Auditors should review the membership of the entity’s “program committee” to assess whether required input is provided. Auditors should also evaluate whether there is adequate input from external agencies such as fire, law enforcement, and medical as well as any partners, contractors, and vendors that may contribute resources to the program.

Auditors should also evaluate program objectives, budget, and schedules as well as records management and change management practices.

Numerous laws and regulations dictate requirements for a preparedness program. The auditor must be knowledgeable in the applicability of these requirements and should determine whether applicable requirements have been addressed in the program.

**Risk Assessment & Business Impact Analysis**

An understanding of the hazards, threats, and risks that could impact life safety, physical assets, business operations, the environment, and the entity’s brand, image, and reputation is a critical foundation of the preparedness program. Prevention and mitigation strategies, emergency operations plans, and business continuity plans must address identified hazards and threats.

Auditors knowledgeable in the process of hazard identification, vulnerability analysis, and impacts analysis should carefully review the risk assessment. Look for foreseeable hazards that have not been considered or those whose potential impacts have been discounted. Failure to identify foreseeable hazards with potentially significant impacts will undermine all other elements of the program.

The business impact analysis (BIA) gathers information for development of the business continuity plan. Prioritization of business operations, determination of maximum downtimes, and identification of the resources required for continuity and recovery strategies must be accomplished during the BIA. Auditors must review the BIA, validate assumptions that are the basis of the BIA, and then evaluate whether continuity and recovery strategies accurately reflect the priorities, recovery time objectives, and availability of resources.

**Prevention & Mitigation**

Auditors should use the risk assessment and BIA documentation to assess whether opportunities for loss prevention and hazard mitigation were identified. Auditors must also review prevention and mitigation strategies, which identify how risks will be managed. Those with responsibility for risk management, safety, security, environmental protection, operations, and facilities management should be interviewed by auditors as strategies are assessed.

**Resource Management**

A preparedness program is no different than any other program. It requires numerous resources—funding, people, expert knowledge, training, facilities, equipment, materials, technology, information, and intelligence. The auditor must assess whether the entity has conducted a needs assessment to identify required resources—based on the hazards identified and the response and recovery plans that are developed. The auditor must also evaluate whether the entity has considered the quantity, capabilities, limitations, and response time of required resources as well as any liabilities associated with their use.
Alerting, Communications & Warning
Alerting of team members and public emergency services as quickly as possible; warning of persons at risk; and the ability of teams to communicate must be assessed by the auditor. The reliability of systems and the testing of protocols and procedures that dictate when and how systems are used should be reviewed.

Emergency Operations/Response
The auditor’s review of the emergency operations or response plan should determine whether procedures for foreseeable hazards or threats identified during the risk assessment have been included. Actions to protect life safety (e.g., evacuation, shelter-in-place, and lockdown), property conservation, incident stabilization, and protection of the environment should be reviewed. The auditor should identify whether team members have sufficient staffing, training, equipment and other resources to safely fulfill their functions and comply with regulations.

Business Continuity & Information Technology Disaster Recovery Planning (IT DRP)
Auditing the business continuity plan and IT DRP must determine whether business continuity and recovery strategies can maintain or restore critical or time-sensitive functions and processes within the time frame determined during the business impact analysis. The auditor must also assess whether the personnel, procedures, and resource requirements required to execute continuity strategies are or will be available when needed. Vital records identification, backup, protection, and recovery capabilities must also be assessed. Records of tests of continuity and recovery strategies must also be reviewed to determine whether strategies can be executed.

Crisis Communications
Crisis communications is more than interfacing with the news media. Communications with stakeholders is essential to protect brand, image, and reputation. Auditors must review crisis communications plans to determine whether internal audiences (e.g., employees, management, board, etc.) and external audiences (e.g., customers, regulators, government officials, etc.) have been identified. Auditors should assess whether plans include communications strategies, pre-scripted templates, and technologies to communicate customized messages to each audience during and following an incident. Strategies should be developed for the types of hazards or threats identified during the risk assessment.

Training, Education, Testing & Exercises
Without training, drills, testing, and exercises, the program will be nothing more than paper. Personnel must be trained; drills such as evacuation drills must be conducted; strategies, systems and equipment must be tested; and exercises must evaluate capabilities.

The auditor should review the training curriculum to identify what training is required and when it should be provided for employees; response, continuity, and communications teams; and those with responsibility for leadership and incident management. Then the auditor must review training records to determine whether required training has been conducted.

After-action reports from testing and exercises should provide a picture of the implementation of the program. Auditors should assess whether the testing and exercise program is adequately assessing the program and whether action items are capturing opportunities for program improvement.

Program Improvement
Change is constant, and the preparedness program must keep pace with changes. Policies, procedures, and capabilities must be evaluated through periodic reviews using the program’s
performance objectives as criteria. The auditor should assess the metrics used for program review; whether periodic reviews are conducted; and whether corrective action is pursued until completion.

**Reporting Audit Findings & Recommendations**

At the completion of the audit, a closing conference should be held to discuss preliminary findings, identify incomplete or missing information; address information gaps or conflicting information; and confirm reporting requirements.

The audit report should include a statement of conformity to voluntary standards or compliance with regulations and entity requirements. Findings should be accurately reported along with recommendations to improve the program. An action plan for program improvement that prioritizes action can be very helpful to spur action.

**Resources for Risk Assessment, Prevention, Deterrence & Plan Development**

Links to many resources to help you develop, implement and evaluate your organization’s preparedness program can be found on the “[Links to Program Resources](#)” page (“Resources” menu) of Preparedness, LLC’s website. Be sure to check out the program self-assessment checklist based on [NFPA 1600](#).

---

**About Preparedness, LLC**

Preparedness, LLC is a client-focused risk consulting company. Our mission is to safeguard people, protect property, minimize business interruption, and protect an entity’s image and reputation. Our vision is to thoroughly understand each client’s business and become a long-term, trusted advisor.

If you have questions, or need assistance with the development, implementation, or evaluation of your preparedness program, please contact us.

**Subscribe to Preparedness Bulletins**

[Click here](#) and sign up for our Preparedness Bulletins. You can unsubscribe at any time.