The Importance of Conducting Maturity Assessments for your Business Continuity Management Program
Business Continuity Management (BCM) is the framework developed by an organization to identify their risk of exposure to internal and external threats and to ensure business continuity is maintained across their organization. According to Disaster Recovery International\(^1\), Business Continuity Planning is “The strategic and tactical capability of the organization to plan for and respond to incidents and business disruptions in order to continue business operations at an acceptable predefined level.”

Ultimately, the goal of BCM is to provide organizations with the ability to efficiently and effectively respond to threats such as supply chain disruptions, natural disasters or cyber/data breaches, and protect the business interests of the organization.

**Driving Maturity in Business Continuity Management Programs**

Today, many organizations are seeking formal accreditation and certification for their Business Continuity Management programs. In 2007, the U.S Department of Homeland Security (DHS) and the Federal Emergency Management Agency (FEMA) established and implemented the voluntary private sector preparedness accreditation and certification program, PS-Prep™. This program is designed to help private sector and not-for-profit organizations institute a comprehensive business continuity management system that addresses business continuity, organizational resilience, emergency and disaster management. PS-Prep™ incorporates three key industry standards and offers organizations the opportunity to develop and maintain certification to comply with nationally recognized and respected approaches to resilience and preparedness. The first step in determining readiness is to identify the standard to which organizations should become certified in preparation for a PS-Prep third party audit. The three standards are:

- ISO 22301:2012: Societal security – Business continuity management systems

Aon Global Risk Consulting has developed a *BCM Maturity Assessment Workbook* which is based on two of the recognized industry standards (NFPA 1600 and ISO 22301) that enable organizations to implement an assessment benchmark against best practices. The workbook consists of a menu of requirements/benchmark/comparisons and a best practice compliance aggregation dashboard founded upon recognized standards, including National Fire Protection Association (NFPA) 1600 - “Standard on Disaster / Emergency Management and Business Continuity Programs” and 2013 and ISO 22301: Societal Security – Business Continuity Management Systems, 2012.

*Note: The BCM Maturity Assessment is designed to determine whether the applicable best practice processes have been followed as part of the preparedness plan. It is not intended to validate the viability or effectiveness of the plan. Beyond these standards, there are other codes and standards that address the technical aspects of planning, such as evacuation and sheltering in place etc. that need to be considered as part of business continuity plan development, depending on specific organizational requirements.*

---

\(^1\) Disaster Recovery International is the leading nonprofit that helps organizations around the world prepare for and recover from disasters by providing education, accreditation, and thought leadership in business continuity and related fields.
ISO and NFPA Standards, and How They Drive Structured Preparedness

ISO (International Organization for Standardization) is a worldwide federation comprised of national standards bodies. International Standards are typically prepared by technical committees. The ISO standard, ISO 22301, "Societal security -- Preparedness and Continuity Management Systems -- Requirements", specifies requirements for setting up and managing an effective Business Continuity Management System (BCMS). ISO 22301 specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your business recovers from disruptive incidents. ISO 22301 is recognized in most countries as the main business continuity standard or framework.

The National Fire Protection Association (NFPA), a United States trade association which includes international members, creates and maintains private, copyrighted, standards and codes for usage and adoption by local governments. NFPA 1600 is the “Standard on Disaster/Emergency Management and Business Continuity Programs”, prepared by the Technical Committee on Emergency Management and Business Continuity. NFPA 1600 covers the development, implementation, assessment, and maintenance of programs for prevention, mitigation, preparedness, response, continuity, and recovery. NFPA 1600 is a widely accepted and instituted standard in the Western Hemisphere and has been endorsed by the 9/11 Commission and adopted by the U.S. Department of Homeland Security as a best practice. It has also received designation and certification as an anti-terrorism technology under the SAFETY Act, and.

ISO and NFPA: Business Continuity Management Specifics

While there are certainly differences between the two standards, it is widely accepted that at least 90% of the requirements are similar.

According to ISO 22301, “A business continuity management system emphasizes the importance of

- Understanding continuity and preparedness needs, as well as the necessity for establishing business continuity management policy and objectives.
- Implementing and operating controls and measures for managing an organization’s overall continuity risks.
- Monitoring and reviewing the performance and effectiveness of the business continuity management system.
- Continual improvement based on objective measurements.”

ISO 22301 recommends formal internal audits while NFPA 1600 emphasizes program maintenance and improvement.
According to ISO 22301, “The organization shall conduct internal audits at planned intervals to provide information on whether the Business Continuity Management System (BCMS)

a) Conforms to
   1) The organization’s own requirements for its BCMS,
   2) The requirements of this International Standard, and

b) Is effectively implemented and maintained.

The organization shall

- Plan, establish, implement and maintain (an) audit program(s), including the frequency, methods,
- Define responsibilities, planning requirements and reporting. The audit program(s) shall take into consideration the importance of the processes concerned and the results of previous audits,
- Define the audit criteria and scope for each audit,
- Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process,
- Ensure that the results of the audits are reported to relevant management, and
- Retain documented information as evidence of the implementation of the audit program and the audit results.

The audit program, including any schedule, shall be based on the results of risk assessments of the organization’s activities, and the results of previous audits. The audit procedures shall cover the scope, frequency, methodologies and competencies, as well as the responsibilities and requirements for conducting audits and reporting results. The management responsible for the area being audited shall ensure that any necessary corrections and corrective actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

NFPA 1600 states that “The entity shall effect continuous improvement of the program through the use of program reviews and the corrective action process.” NFPA recommends that:

- The entity shall maintain and improve the program by evaluating its policies, program, procedures, and capabilities using performance objectives,
- The entity shall improve effectiveness of the program through evaluation of the implementation of changes resulting from preventive and corrective action,
- Evaluations be conducted on a regularly scheduled basis and when the situation changes to challenge the effectiveness of the existing program,
- The program shall be re-evaluated when a change in any of the following impacts the entity’s program:
  - Regulations
  - Hazards and potential impacts
  - Resource and availability or capability
  - Entity’s organization
  - Infrastructure, including technology environment
– Economic and geographic stability
– Entity operations

- Reviews shall include post-incident analysis, reviews of lessons learned, and reviews of program performance,
- The entity shall maintain records of its reviews and evaluations,
- Documentation, records, and reports shall be provided to management for review and follow-up,
- The entity shall establish a corrective action program,
- The entity shall take corrective action on deficiencies identified

Putting the Standards to Work to Develop an Effective BCM Approach

An effective Business Continuity Management Program should define the risks or threats that could impact business operations and exercise the controls in place to determine whether or not those risks are acceptable. Given the fact that change is a constant in the modern business environment, it is extremely important to perform regularly scheduled audits. A business continuity management audit is a formalized method for evaluating how business continuity processes are being managed. The goal of an audit is to determine whether the program/plan has been developed and is managed according to industry best practices, identify weaknesses, and provide recommendations for business continuity plan improvements, as/if warranted. Why apply valuable time, resources and expense of developing a business continuity plan to simply let it become outdated?

While business continuity program audits can be time consuming, up-front and proactive planning can help drive efficiencies and expedite the process of keeping the plan current with organizational needs. An effective business continuity audit requires a structured audit framework and access to a qualified staff or external consultants to generate high-quality results.

Audit activities of a BCM program may include but are not limited to the following:

- Interviewing key stakeholders and participants in the program,
- Reviewing plan development documents including Business Impact Analysis and Risk Assessments,
- Reviewing individual Business Continuity Planning and Disaster Recovery plans by ensuring that they are complete, accurate, and up to date,
- Verifying current state of recovery strategies
- Verifying Recovery Time Objectives and Recovery Point Objectives,
- Examining training materials, procedures, and guidelines,
- Reviewing communication/notification protocols between management, staff and external stakeholders,
- Reviewing plan exercise results and exercise criteria
- Reviewing contractor and service provider contingencies
- Verifying senior management sign-off responsibility and accountability
The bottom line is, if you have a Business Continuity Management Program in place, you need to be confident that your investment in business continuity planning will respond effectively in the event of a disaster. A viable plan should not only protect your organization’s interests, but should also take into account the extent of a company’s responsibilities to other entities and be cognizant of supply chain exposures. It is critical that measures are developed and implemented to track your risks, and assure that management is regularly informed of and ready to assess and improve the organization’s preparedness and continuity capabilities in the event of a disaster.

Aon’s Business Continuity Management Services has the expertise and resources necessary to provide an unbiased evaluation of your Business Continuity Management Program’s maturity to assure it conforms to current accepted standards and best practices.

References:

- ISO 22301:2012: Societal security -- Business continuity management systems
- Disaster Recovery International
- FEMA
Contact Information

**Kieran Stack**  
Managing Director  
Business Continuity Management  
312.381.4778  
kieran.stack@aon.com

**James Pinzari**  
Director  
Business Continuity Management  
781.878.3546  
james.pinzari@aon.com

**Greg Cybulski**  
Associate Director  
Business Continuity Management  
973.463.6075  
greg.cybulski@aon.com

**Carey Loukides**  
Senior Consultant  
Business Continuity Management  
603.557.4754  
carey.loukides@aon.com
About Aon

Aon plc (NYSE:AON) is the leading global provider of risk management, insurance and reinsurance brokerage, and human resources solutions and outsourcing services. Through its more than 66,000 colleagues worldwide, Aon unites to empower results for clients in over 120 countries via innovative and effective risk and people solutions and through industry-leading global resources and technical expertise. Aon has been named repeatedly as the world’s best broker, best insurance intermediary, best reinsurance intermediary, best captives manager, and best employee benefits consulting firm by multiple industry sources. Visit aon.com for more information on Aon and aon.com/manchesterunited to learn about Aon’s global partnership with Manchester United.