

THE FACTS BEHIND RESILIENCY AUDITING

With the passage of Public Law 110-53, the topic of resiliency auditing gained national attention. Formally entitled “Implementing the Recommendations of the 9/11 Commission Act of 2007,” Title IX of this law calls for private sector organizations of all sizes to voluntarily submit to a resiliency audit. Not specified in this law is the standard that should be used as the basis for the audit. Several such standards exist including popular ones such as:

- National Fire Protection Association specification 1600 (NFPA 1600), and
- British Standard 25999 (BS 25999)

It is important to note that other standards exist that speak to the topic of resiliency and preparedness.¹ For example, the banking, healthcare, and the securities industries have regulations that address aspects of business continuity planning and resiliency. Other countries have issued specifications in this area, some of which are excellent! Many of these specifications are auditable, but not all. The driving difference between auditable and non-auditable standards has to do with the use of a specific verb. For a specification to be auditable it must use the verb “shall,” which means that the stated action is a *requirement*. Guidance documents use the verb “should” which indicates a recommendation, not a requirement². A lack of understanding of this usage of *shall* versus *should* terms has caused great confusion and even some gross misrepresentations of capabilities by firms promising to help firms “prepare for an audit.”

Auditing Principles

An audit is a systematic review which establishes adherence to and compliance with a pre-established standard. Various examination techniques are used by the auditor including document review, transaction sampling, interviews, and third party verification of claims. Professionally trained auditors are taught to use the “tell me, show me, prove to me” approach when conducting an examination.

The goal of any auditor is to verify compliance, not to discover non-compliance. If the auditor finds the organization to be in compliance with the principles of the base standard, then he or she will *certify* the audit and issue a *certificate of registration*. If there are minor issues that need to be addressed, the auditor will likely cite some “minor non-conformities” and issue a *conditional certificate of registration*. If significant problems are uncovered, then the auditor will record these as “major nonconformities” and no certificate will be issued. The fourth option available to an auditor is to issue an “observation.” These are usually comments about processes and procedures that fall outside the scope of the contracted audit.

¹ Go to <http://www.sloan.org/assets/files/olsiewski/frameworkforvoluntarypreparednessfinalreport.pdf> for a summary of the leading specifications in this area.

² Both NFPA 1600 and BS 25999 have *shall* specifications.

If You Would Like to View the Complete Article,
Become a Member of ICOR. It's easy and you'll have
access to this and other informative and valuable
presentations and articles.



THE ICOR
The International Consortium For Organizational Resilience

www.theicor.org