

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.

While it is true that any organization can conduct an audit, the value of this process is tied to the qualifications and standings of the organization conducting the inspection. A bookkeeper can audit a company's financial statements and issue an opinion on the accuracy and correctness of the documents; but unless the audit is conducted by a Certified Public Accountant the document has little standing in the business community.

The same is true of audits of other standards. A commonly audited standard, especially in the manufacturing industry, is the ISO 9001 quality management system specification. Here again, anyone can issue a certificate based on ISO 9001, but it has little standing unless granted by an organization which has itself met certain standards of review.

In the United States, the organization that oversees the qualification of companies that wish to grant audit certification is the ANSI/ASQ National Accreditation Board (ANAB).

Similar organizations exist around the world. For example in Canada, the organization performing this task is the Standards Council of Canada (SCC), while in Great Britain it is the United Kingdom Accreditation Service (UKAS), and in Japan there are two – the Japanese Accreditation Board (JAB) and the Japan Information Processing Development Corporation (JIPDEC).

Approximately fifty recognized accreditation boards are active in the world and all have agreed to a peer review process based in part on the standard ISO 19011. These organizations in turn review the qualifications of companies that apply to them for approval and *accreditation* as certifying bodies under the criteria listed in ISO 17021.

These certifying bodies (sometimes called registrars), are the organizations empowered by accreditation boards to grant internationally recognized certificates of registration. Because of a possible conflict of interest, these same organizations cannot offer consulting or pre-audit services to firms they plan to audit. Only consulting firms will offer pre-audit services. When considering a pre-audit service, closely examine the credentials of the organization offering the service. If they do not have a close affiliation with a certified body/registrar that grants certificates in one or more of the accepted standards – their ability to prepare a firm for an audit must be suspect.

Audit Alternatives

There are two alternatives to a full audit that are gaining in popularity. They are known as “first and second party attestations” (a.k.a. declaration). A first party attestation is a self assessment and a publicly issued declaration by a firm that it has conducted an internal review of its program and finds itself in line with that base standard.

A second party attestation is a review by an outside agent that is not a certifying body. This second party then issues a statement that the examined firm meets the criteria set as the base standard for the review. Second party declarations are popular with trading partners where a member of a supply chain will declare that one or more of its suppliers

meets the requirements set forth in a contract between the two organizations. The benefit of a second party declaration is that many other organizations that trade with the firm in question may accept the opinion of another firm as being “good enough.”

Many small and midsize businesses are looking at first and second party declarations as a way of avoiding the expense of a full third party audit which can approach \$10,000 or more. There seems to be growing support on the part of the Department of Homeland Security (DHS) for first and second party audits. This will become clearer as the new administration fills key positions at DHS and begins to dialog with the private sector on these issues.

Business Resiliency Audits

The goal of PL 110-53 is to lend support and guidance to a national goal of increased preparedness. Much work remains and some of the unresolved issues are controversial such as which standard will the United States endorse. In December of 2008, the Department of Homeland Security published in the Federal Register an announcement of a program they labeled PS Prep (for private sector preparedness).

DHS has invited comment on this document which “seeks recommendations from private sector stakeholders and the public at large regarding the private sector standards that DHS should adopt, both initially and over time” (73 FR at 79142). Importantly, publishing these guidelines in the Federal Register is a giant step towards making the published standard part of *administrative law*. As such, it is possible that the DHS specification will form the basis for legal opinions in this area, effectively circumventing any efforts to promote other recognized standards.

It should be noted that many of the interested parties tracking the actions of DHS in this area are concerned that the specification offered does not meet the general requirements of most private sector businesses, especially smaller ones.

The topic of business resiliency audits continues to be actively discussed and the pros and cons of various standards hotly debated. No one is sure where things will end up, but in the meantime, ICOR will continue to track developments and keep you informed.

Article written by Donald Byrne, ICOR Board Member and President of North River Solutions. Don can be reached at dbyrne@northriversolutions.com



THE ICOR
The International Consortium For Organizational Resilience

www.theicor.org