Certifications Help Organizations and Clients

George Jackelen
Software Consultants, Inc.

As part of the United States government's request for proposal (RFP) process to acquire products and services, more emphasis is currently being placed on the past performance/experience proposal section. This article addresses another area the government (and other potential clients) should examine, especially for potential bidders with limited experience: organizational certification by certified, independent assessors based on internationally and nationally recognized standards and methodologies[1].

In a *Washington Technology* article [1], Michael Hardy describes how certifications help contractors to compete and thrive. This article expands this theme by describing how contractor certifications can help organizations improve, help clients choose contractors, and how certifications can be used to provide better services and products.

My definition of certification is:

> Being accredited by an external independent group certified by a standard's (to include methodologies) owner to evaluate organizations and to provide objective evidence to a nationally/internationally recognized group (for example, the American National Standards Institute – American Society for Quality National Accreditation Board) to issue formal certificates of approval.

Internal accreditation is not addressed because, in my opinion, they rarely provide independence to identify and document the existence of objective evidence and artifacts; indeed, I have witnessed data manipulation to provide an organization with the desired results. I do accept the importance of internal audits for the purpose of gap analysis to determine what is missing to fulfill compliance requirements.

Capacity and Experience

Before going into a discussion about certifications, I want to discuss the terms *capacity* and *experience*, which some people consider to be the same.

An organization's capacity—defined as "the potential or suitability for holding, storing, or accommodating" [2]—is not a reliable evaluation tool. Capacity does not always provide objective evidence that an organization can actually provide this capacity or really knows how to satisfy the requirements. Thus, an organization can have a capacity to do something without ever having experience doing that thing. Also, a stated capacity may only be due to one employee's capacity (who may leave the organization or may not work on the contract) or education (e.g., a person took a course on the topic, but has no application experience); rather than having several people with the capacity and/or having organizational documented and implemented procedures on how to provide a stated capacity. Thus, there may be no evidence to show a capacity was ever provided successfully by an organization.

"I have seen the distinction between capacity and experience applied to RFPs when a client wants organization/team experiences (reality) rather than capabilities (theory)."

An organization's experience—defined as "the act of living through an event or events" [3]—is more valuable to a client. Thus, a capacity is not the same as experience, nor should capacity have as much weight in an evaluation as experience. For example, advertisements say my car has the capacity to provide 30 miles per gallon (mpg); but, in the real world, I have no experience where my car had an actual performance measurement of 30 mpg or greater.

Thus, experience is better than capacity to determine if an organization can support a client. This is especially true if the client contacts the referenced clients, identified in the experience part of a proposal, for their view of how well the organization performed and/or implemented their processes and developed the needed product or service. This step is similar to verifying a future employee's references, experience, and education.

I have seen the distinction between capacity and experience applied to RFPs when a client wants organization/team experiences (reality) rather than capabilities (theory)[2]. I recognize that experience may not be a true reflection of an organization's present and future environment. Also, some organizations are too new or too small to have the needed experience. In these situations, an organization may not bid or a client may not have high confidence that an organization can deliver what a client expects.

A possible solution to this dilemma is for clients to examine an organization's certifications. I am ignoring employee certification since people can leave an organization and employee certifications do not show that an organization has implemented the principles of these certifications. However, I have seen RFPs requiring the proposed people who will work a contract to have specific certifications (e.g., related to information or computer security).

Independent Certifications

I recommend clients require a copy of each organizational certificate related to the RFP. Independent certifications (e.g., the International Organization for Standardization [ISO]) can help organizations and clients reduce the risk of having a lack of experience by showing clients the organization has a certified set of processes in place. Besides having processes in place, certifications are based on independently observed objective evidence showing that the processes are implemented as stated.

Why should clients believe that certification is a bridge between an organization's capacity and its lack of client-required experience? Since receiving an organizational certificate is not cheap and cannot normally be obtained in a few months, clients should recognize an organization for its willingness to expand resources so they can prove their processes are established and maintained, and are actually implemented. At the same time

(prior to being certified), auditors/certifiers spend a lot of time looking for objective evidence that organizations comply with the given standards and certification requirements. For a client, this means organizations must not only have processes in place, but must also prove these processes are implemented as stated.

Another organizational factor—an important cost-benefit determination for an organization—is deciding what part of the organization is to be certified (i.e., the whole organization or an organizational subset). Can an organization afford to wait for a payback that may not appear for months after certification? For a client, certification may be with an organizational subset that is not proposed to participate on a contract or is only providing minor contract support.

Therefore, organizations need to make a decision about their need for certifications, what certifications they want to achieve, what part of the organization to certify, and their willingness to pay the cost. Organizations must also be aware that the cost to be certified does not end with certification. For ISO and the Software Engineering Institute (SEI), for instance, achieving certification is not a *be all and end all*. ISO and SEI require periodic recertification to assure the certification standards and organizational processes are maintained and the processes are implemented. To an organization, achieving certification and recertification may be a key to future contracts, especially for RFPs requiring particular certificates.

For clients, this means certification is not a lifelong *license to brag* based on a one-time evaluation of an organization. As a result, clients need to know when an organization was last certified and the certificate's duration.

What Certifications Will Meet an Organization's Needs?

Given what I've just explained, what certificates should an organization apply for and what certificates should a client look for? The answer depends on an organization's goals and objectives—and what a client is looking for to ensure the right organization is picked to execute a contract[3].

Table 1 provides examples of four major international standards that provide recognized certifications, and examples of how these standards relate. The first qualification (ISO 27000) should be strongly considered by clients and organizations since sensitive data security (e.g., payroll or personnel records) is critical to most clients and organizations. In addition, this certification is important for its guidance on providing physical and procedural protection of data, physical equipment, people, and the operational environment.

The second qualification (ISO 9001) is arguably *the standard that set the standard* for the other qualifications. The third qualification (ISO 20000) is not known by many organizations, but it expands ISO 9001 by addressing IT's involvement with business needs and strategy. Several ISO 20000 requirements relate to ISO 27000 and ISO 9001. As a result, achieving ISO 20000 certification helps an organization to also achieve ISO 9001 and ISO 27000 certification. ISO 20000 certification can also help organizations with CMMI® appraisals.

> *"... organizations need to make a decision about their need for certifications, what certifications they want to achieve, what part of the organization to certify, and their willingness to pay the cost."*

Table 1 also shows some of the similarities between the three international standards and an internationally accepted methodology/model (CMMI) to improve quality.

Certifications

Due to similarities with certification, this article addresses only the following standards because they are internationally well-known in assisting organizations to improve their quality, efficiency, and effectiveness (other standards could be added):

- **ISO 27000:2005, IT – Security Techniques – Information Security Management.** Provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System (ISMS).
- **ISO 9001:2000, Quality Management Systems – Requirements.** Intended for use in any organization which designs, develops, manufactures, installs, and/or services any product or provides any form of service. It identifies the requirements an organization needs to fulfill to achieve customer satisfaction through consistent products and services meeting client expectations. It includes a need for continual (i.e., planned) improvement of a Quality Management System.
- **ISO 20000:2005, IT – Service Management.** Promotes the adoption of an integrated process approach to effectively deliver management services to meet business and client requirements. Its process improvement can be managed through the CMMI approach.
- **CMMI.** A methodology enabling organizations to identify the maturity level achieved by their processes, and to design and implement a continuous improvement plan to raise their process maturity level to one appropriate for their business objectives.

Using the Standards and Methodology

For this article, these standards relate to organizational-level quality (e.g., what is best for an organization or its sub-organizations), not just lifecycle processes (e.g., what is required to perform requirements analysis, design, or testing). For instance, lifecycle processes normally minimize top management's business goals and objectives whereas organizational-level requirements (the three mentioned ISO standards) emphasize business needs, goals, and objectives. In my opinion, CMMI ties together organizational-level and lifecycle processes.

Organizational requirements recognize the need for owners and key decision makers to decide if requirements are cost-effective, an organizational need, etc. For example, people normally recognize the need for alternate backup sites to protect an organization from collapse due to a disaster at a key organization location. However, at the organizational level, management may determine having one or more backup sites is too expensive since clients are unwilling to share in the cost, or the organization's business base is too diverse in functionality and/or geographic location to have back-up sites. Thus, an organization must formally identify the risks it is willing to accept even when attempting to be certified.

The mentioned standards allow an

® CMMI is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Items	ISO 27000:2005	ISO 9001:2000	ISO 20000:2005	CMMI
Planning	1 Scope 1.2 Application	1 Scope 1.2 Application		Process Area (PA) Project Planning
Quality Management	4 Information Security Management System 4.2 Establishing and Managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and Operate the ISMS 4.2.3 Monitor and Review the ISMS 4.2.4 Maintain and Improve the ISMS	4 Quality Management System 8.2.3 Monitoring and Measurement of Processes 8.2.4 Monitoring and Measurement of Product	5 Planning and Implementing New or Changed Services	PA – Requirements Development PA – Integrated Project Management Specific Practices 3.1 – 3.5 PA – Project Monitoring and Control (PMC) General Practice (GP) 2.8 Monitor and Control the Process PA – Measurement and Analysis (MA) GP 3.1 Establish a Defined Process GP 3.2 Collect Improvement Information
Quality Plan, and Maintenance of Documents and Records	4.3 Documentation Requirements 4.3.2 Control of Documents 4.3.3 Control of Records	4.2 Documentation Requirements 4.2.2 Quality Manual 4.2.3 Control of Documents 4.2.4 Control of Records	3.2 Documentation 4.1 Planning Service Management (Plan)	PA – Process and Product Quality Assurance (PPQA) PA – Configuration Management GP 2.6 Manage Configurations
Audits	6 Internal ISMS Audits	8.2.2 Internal Audit		PA – PPQA
Process Improvement	8 ISMS Improvement 8.1 Continual Improvement	8.5 Improvement 8.5.1 Continual Improvement	4.4 Continual Improvement	PA – MA PA – PMC GP 2.2 Plan the Process
Reviews	7 Management Review of the ISMS 7.2 Review Input 7.3 Review Output	5.6 Management Review 5.6.2 Review Input 5.6.3 Review Output	4.3 Monitoring, Measuring, and Reviewing	PA – Decision Analysis and Resolution GP 2.9 – Objectively Evaluate Adherence GP 2.10 – Review Status with Higher Level Management

Table 1: *Sample Relationship Showing Similarities Between the Four Standards*

organization to tailor the implementation of the standards to match how an organization operates. For instance, ISO 9001 allows clauses to be deleted if an organization does not implement a clause (e.g., clause 7.3, Design and Development, if an organization does not design or develop products).

But how does an organization receive authorized certification? Is this process of any benefit to potential clients?

The Process to Receive Certification

Each standards development group has its own certification process and there are many Internet sites discussing the processes to receive independent certification. Some requirements are the existence of objective evaluations and a history (e.g., at least three months) of artifacts (proof) to show organizational processes are implemented. Another requirement is for the organizational processes to comply with an authorized standard. Most organizations should be able to ensure this requirement is being satisfied through an objective gap analysis (internal audit) of their processes versus a given standard. Many organizations—even if they have effective, efficient processes in place—find they lack objective artifacts showing a continuous and objective use of the processes stated within a given standard.

Conclusion

The identified standards have publicly assessable databases with information about what organizations are currently certified. However, clients must be aware that status posting may take weeks to be stored into a database or for an organization to receive a formal certificate. Because of this, clients must determine the cut-off date for an active certificate (e.g., the certificate must be valid on the date proposals are due, so many calendar days after a proposal is due, or at the time of the contract award). Another option, if an organization's certificate has yet to be posted, is for a client to allow an organization to provide a copy of its certification packet to indicate the certification results. In this case, the RFP needs to state that if an official certificate is being processed that the entire certification packet must be included in the proposal so a client can identify the auditor's recommendation for approval. In this situation, I recommend that the RFP also states that an official certificate must be provided upon contract award.

Whether a database or a certificate copy is used, clients need to be aware that some organizations exaggerate the certification results. Commonly, an organization's subset may be certified, but an organization indicates the certification is at the organizational level covering all organizational subsets. To overcome this problem,

Coming Events

February 2-4

Soldier Technology U.S. 2009
Arlington, VA
www.wbr.co.uk/soldiertechnologyusa/

February 3-5

3rd Annual Lean and Six Sigma for Process Excellence in IT and Software Development Conference
San Francisco, CA
www.wcbf.com/quality/5089/

February 8-11

16th Annual Network and Distributed System Security Symposium
San Diego, CA
www.isoc.org/ndss09/

February 10-12

USAF Test and Evaluations Days 2009
Albuquerque, NM
www.aiaa.org/content.cfm?pageid=230&lumeetingid=2104

February 25-26

AFCEA Homeland Security Conference
Washington, D.C.
www.afcea.org/events/homeland/landing.asp

April 20-23

21st Annual Systems and Software Technology Conference
Salt Lake City, UT
www.sstc-online.org

Coming Events: Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.

certificates and certification databases clearly state what part of an organization is certified. As a result, clients need to go beyond just accepting the word of organizations. Clients need organizations to provide objective evidence (e.g., copy the certificate) or have the client verify an organization's certification statement based on certification databases.

Is this proof of certification worth it? Clients can use certifications to establish the chances that an organization or subset can deliver the needed product or services on time, within cost, and at the needed quality level. When an organization provides proof of performance and a copy of its certificate, this provides a client with a degree of confidence that the organization can satisfy the client's needs.

However, an important reminder for clients is that the existence of a certificate does not mean an organization will actually use what is said within a certificate. As a result, clients need to contractually receive the plans, processes, steps, etc., used to receive an organization's certificate(s), and organizations must receive client approval for modifications to these plans, etc.

Having performed independent verification and validation (IV&V) for more than 12 years, I have seen organizations win contracts based in part on certifications (e.g., having a CMMI Level 5), but they do not implement these features during a contract. In this situation, I blame the client for not verifying the implementation of what was promised or clearly implied in the proposal. For example, I have seen a major, well-known organization's CMMI Level 5 subset (which was stated in their proposal and contract) not be penalized for failure to use promised standards. Thus, the client promoted the importance of cost and schedule over quality.

Therefore, a client can use an organizational certificate to show an organization has implemented documented processes (that were based on known standards). However, it is up to the client to sometimes require an organization to use the certified processes for a given contract.

Also, certification does not guarantee successful implementation of quality processes or delivery of quality products or services. What certifications do provide is objective evidence that a certified independent group has examined artifacts showing that an organization has implemented processes to satisfy stated standards.◆

References

1. Hardy, Michael. "Get your ducks in a row." Washington Technology. Vol. 23, No. 2. 11 Feb. 2008 <www.washingtontechnology.com/print/23_02/32228-1.html>.
2. "Capacity." Merriam-Webster Online Dictionary. Merriam-Webster Online. 2008 <www.merriam-webster.com/dictionary/capacity>.
3. "Experience." Webster's New World Dictionary.

Notes

1. Since the author is not a government employee, he is not providing guidance currently used by the government to assist in making better selections based on the RFP process.
2. The U.S. government uses RFPs to ask organizations to provide a proposal addressing the issues provided in the model contract and statement of work (SOW). The resulting proposals determine what organization(s) wins a contract to provide the SOW-stated needs. Within the RFP, the government identifies the evaluation criteria (e.g., understanding of the problem, past performance, technical and/or management approach, and cost) and the priority or weight of each criterion.
3. The standards I cite do not provide detailed requirements (e.g., what level of software testing is required). They are at a high level to address what organizations need to implement to ensure quality processes, products, or services, without disrupting an organization's goals, objectives, and level of acceptable risks.

About the Author

George Jackelen is currently working with Software Consultants, Inc. as a principal consultant. Since 1996, he has provided IV&V support to various federal agencies and in Colorado and California. Prior to that, Jackelen spent 10 years in quality assurance and 20 years in the USAF in various computer jobs. He also assisted the ISO, the IEEE, and the Project Management Institute in developing standards.

Software Consultants, Inc.
4601 President's DR
STE 240
Lanham, MD 20706
E-mail: georgej@scigrp.com