CASE STUDY

U.S. INTELLIGENCE AGENCY

The benefits of attaining ISO 9001, ISO 27001 and ISO 20000 certifications

Background

In an unprecedented accomplishment, one U.S. intelligence agency's Information Technology department simultaneously earned registration to ISO 9001, ISO 27001 and ISO 20000 in February, 2006. This is a first for any organization in the world. It took the agency just over three years to earn the three different certifications.

The agency's registration efforts were embolden by a consulting firm, the Institute for Quality Management Inc. (IQM) in Fairfax, Virginia. Dr. Thomas A. Mink founded IQM in 1992. According to the group's website, www.iqm.com, the organization's mission is to provide "client-tailored, success-focused, measurable business performance improvements." IQM has nearly 80 employees and has a niche in working with governmental organizations that need consultants with top-secret clearance.

"Integrated in the proper way, ISO 9001, ISO 20000, and ISO 27001 are a powerful combination. Together they ensure a robust world class management system... touching all critical areas of an organizational structure."

Customer needs

The intelligence agency implemented ISO Management System standards for a market advantage in the same manner a commercial client might, but the primary driver was better operational performance, said Monroe Ratchford, the IQM lead consultant for this effort. The agency wanted to improve day-to-day systems operations and leverage technology to ensure and protect the agency's mission by providing enterprise, corporate, dissemination and information services. This included the IT department, data centers, applications management, internet service management, printing and more.

The agency selected ISO 9001, ISO 27001 and ISO 20000 because of their relevancy to the agency's mission and the potential benefits from applying industry best practices and becoming more "process centric." These three standards help the agency standardize its processes and document configurations and adopt industry best practices so that processes are repeatable, documented, robust and executable.

One of the keys to success for this implementation was IQM's use of software tools to reduce cycle time, costs and defects. Using an ISO portal that addressed all three standards made the document control, auditing and Corrective Action Reports significantly more manageable. Also IQM's background in performance management, drove faster implementation and improved operational efficiencies.

Benefits

The primary benefit was discovering the performance management metrics that help the organization measure progress on meeting customer requirements. The organization had to make a cultural shift from measuring levels of effort to measuring how well the services were performing for the customer. Another benefit to using the management systems was that it forced employees to discuss substantive issues and to ask questions such as "So why didn't this work?" and "What are you doing to fix it?"

Ratchford said that "The beauty of ISO Management System standards is that it gives you that capacity to have those objective, actionable conversations, instead of just sad stories."

Most registered organizations believe that management systems improve their operations, but quantifying benefits can be difficult. Ratchford said the agency was able to put constructive numbers to the improvements. For example, they:

- Improved the creation of new accounts by reducing the cycle time from 14 days to 2 days.
- Reduced certification and accreditation cycle time from 365 days to 45 days.
- Improved continuity planning scores from 65 percent to over 75 percent.
- Helped the agency become one of the few government agencies cited for "what went right" in the White House report: "The Federal Response to Hurricane Katrina: Lessons Learned."
- Applied ISO 9001 and the IT Service Management (ISO 20000) standards' preventive clauses to the preventive maintenance on equipment so that trouble tickets and incidents that disrupt IT services were cut by 60 percent.
- Improved scheduling effectiveness for outage management from 80 percent to 95 percent.

Integrated in the proper way, ISO 9001, ISO 20000, and ISO 27001 are a powerful combination. Together they ensure a robust world class management system which provides the proper frame work for a holistic approach to information assurance and information security, touching all critical areas of an organizational structure.

ABOUT THE STANDARDS

ISO 9001:2000
ISO 9001 is an internationally recognized standard that defines the minimum requirements for an organization's business/quality management system. It can be used by any organization to establish, document and effectively implement a business management system that ensures customer expectations are identified and met.

ISO/IEC 20000:2005
ISO 20000 is the first worldwide standard specifically aimed at IT Service Management. It describes an integrated set of management processes for the effective delivery of services to the business and its customers. ISO/IEC 20000:2005 is aligned with and compliments the process approach defined within ITIL© from the Office of Government Commerce (OGC). It is sometimes called the quality management system for ITSM.

ISO/IEC 27001:2005
ISO 27001 is a standard setting out the requirements for an Information Security Management System. It helps identify, manage and minimize the range of threats to which information is regularly subjected.

BSI's role

The agency selected BSI as its third-party registrar as part of a competitive process. "We did market research on the registrars and created weighted criteria on what we considered to be an effective registrar for this agency," Ratchford said. "Then the government folks conducted an evaluation and selected the registrar that best served the government needs, and BSI came out on top."

"Very few registrars are capable of conducting training and certifying all three standards."

Ratchford said IQM has been in business long enough, with an unbroken string on operational results and perfect certifications that he is confident IQM can consult with clients to ensure they pass an audit. In selecting a registrar, the primary question was: How can an audit be turned into value for an organization that needs no market advantage? Or, to put it another way: What is the inherent value in a governmental agency earning registration?

"Each time the third party auditors came to the agency, to conduct continuing assessments, the auditors raised the bar in terms of depth of compliance, number of technicians interviewed, and levels of performance," Ratchford said of BSI. "Each time the bar gets raised, IQM consultants help the agency think through the next level of improvement, technicians to improve service, and better application of security controls. The agency finds this adds value and drives the agency in the direction of its vision."

"Very few registrars are capable of conducting training and certifying all three standards," he added.

THE SYSTEM

The intelligence agency's system is unique because of its mission – it has to integrate security into its processes every day, maintaining a continuity of operations or a resiliency under virtually any scenario.

"The agency has to ensure that their systems work even when catastrophic incidents happen," Ratchford said. "We know that that's a possible scenario, and we make preparing for that scenario part of our thinking every day. I think there's also a desire on behalf of the government to adopt industry best practices, so taxpayers get their money's worth."

Ratchford said, "Employees in the intelligence business are extremely good at security, but security folks do not necessarily speak in terms of processes … they speak in terms of compliance. With ISO 27001, you can address both process and integration compliance issues into the workflows of everyone," he said. "So, instead of having a shop with 10 people who police your security, you have a whole workforce using internal auditors to make sure they're addressing security requirements as an integrated aspect of their job."

Part of the challenge with this standard was finding ways to demonstrate to the auditors the agency's compliance with the standards without revealing classified information. With cooperation from BSI, unique ways were found to meet the security requirements and the ISO standard clauses.

The three ISO management system certifications are not an end but are the baseline for building the improvements necessary for the agency to succeed. ISO 9001 was used to build a baseline Quality Management System. ISO 20000 was used to integrate industry best practices, like ITIL and to drive better IT services. ISO 27001 was used to integrate Federal Laws, Department of Defense and Intelligence Community regulations into the processes executed every day. IQM believes this effort makes America a safer place, improves the U.S. Intelligence Agency's Information Services and gives the American taxpayers an impressive return on their tax dollars.

BSI Management Systems
12110 Sunset Hills Road, Suite 200
Reston, VA 20190-5902
USA
Tel: 1 800 862 4977
Fax: 1 703 437 9001
Email: inquiry.msamericas@bsi-global.com
www.bsiamericas.com

BSI Management Systems Canada
6205 Airport Road, Suite 102
Mississauga, ON
L4V 1E1
Canada
Tel: 1 800 862 6752
Fax: 416 620 9911
Email: inquiry.canada@bsi-global.com

BSI/USA/110/MS/0307/E