ISMS Certification in the United States

by Rebecca Herold, CISSP, CISM, CISA, FLMI

Significantly fewer United States-based organizations are pursuing formal ISMS certification than in many other countries. In this article, I share my discussions with 10 chief information security officers (CISOs) from U.S.-based organizations about whether they are going to pursue ISMS certification and why. I also share the feedback given to me from a U.S.-based ISMS certification preparer group.

Perspectives of U.S. CISOs

I spoke with CISOs from a wide range of industries of varying sizes, most with international presence. As Table 1 reveals, with the exception of one, they were not pursuing formal ISMS certification.

Industry	Number of Employees	International?	Have or Pursuing ISMS Certification?
Communications	80,000	Yes	No
Entertainment	150,000	Yes	No
Financial	115,000	Yes	No
Financial/Healthcare Insurer	20,000	Yes	No
Financial/Healthcare Insurer	28,000	Yes	No
Healthcare Insurer	3000	No	No
Manufacturing	8000	Yes	No
Manufacturing	200,000	Yes	No
Retail/Manufacturing	8000	Yes	No
Retail/Manufacturing	150,000	Yes	Yes

Table 1: ISMS certification plans.

Why Most U.S. Businesses Are Not Pursuing ISMS Certification

With one exception, all the CISOs I spoke with asked to remain anonymous. The following are some of their revealing reasons for not pursuing ISMS certification:

The CISO for a multinational communications organization indicated she has built her information security program around ISO/IEC 17799, and has found the concepts extremely valuable, but does not see the business value to invest the time and resources in pursuing formal ISMS certification.

The CISO for a multinational entertainment organization indicated she has many other higher-priority information security initiatives to address before considering whether to pursue ISMS certification.

Ben Rothke, CISSP, the Director of Security Technology Implementation for AXA Technology Services, a division of AXA, the world's largest financial services company, offered his personal opinions about ISMS certification. "I have found many U.S. organizations are quite keen to ISO27001. When performing security audits or reviews, many of these organizations are requesting that the consultants that perform them map the results around the 27001 framework. One of the main benefits is that this standard ISO framework enables the organization to have a common way to look at the output, rather than each consultancy organizing the results to their particular methodology. Most organizations do not necessarily require the consultants or firms to be qualified auditors or implementers, rather to simply map the output to the standard. This is primarily due to the dearth of qualified auditors and implementers, combined with the fact that many organizations don't even know that qualified auditors or implementers exist."

Over the past year, the CISO for a multinational financial/healthcare insurer has been seriously considering whether to pursue ISMS certification. However, she has made the decision to focus her resources and efforts to regulatory requirements instead; she can demonstrate business value for regulatory compliance, but she cannot for ISMS certification.

The CISO from a multinational financial/healthcare insurer organization indicated her organization was not planning to pursue ISMS certification because her organization is "in the crosshairs of many of the current big hitters for information security-related U.S. legislative mandates" in addition to not having the funds to undertake formal ISMS certification. However, she indicated that she uses ISO/IEC 17799 within her information security program, but is just not going to get formal certification.

The CISO from a non-international healthcare organization indicated that he was not pursuing formal ISMS certification because other projects have higher priority, the maturation of his relatively new information security program did not lend itself to ISMS certification yet, and there was no perceived value within his organization to obtain ISMS certification.

The CISO for a multinational manufacturing organization indicated that although he was aware of ISO/IEC 17799, he was not aware it was possible to obtain certification based upon the BS7799 standards, was not aware of the change to ISO/IEC 27001, and had never heard of ISMS certification before I spoke with him about these topics. However, after learning about the ability to certify, he did not see the business value in obtaining ISMS certification. His organization's current policies and standards are based on ISO/IEC 17799, and he is currently incorporating COBIT, ITIL, HIPAA, SOX, and various privacy and FDA laws and regulations requirements into the program.

The CISO for a multinational manufacturing organization indicated his organization does not pursue any formal certification unless it is required by law or as a condition to do business (for example, ISO 9000). The primary issue for his organization is funding and management perception of business value, which they do not see with ISMS certification.

The CISO for a multinational retail manufacturing organization indicated that she created the security program based upon ISO/IEC 17799, but that other priorities must be addressed before she even thinks about ISMS certification, if at all.

Why One Organization Did Obtain ISMS Certification

One of the multinational retail/manufacturing organizations indicated they have obtained formal certification in more than 20 of their locations outside of the U.S. The scope for these certifications was for their commercial infrastructure management systems and their SAP services.

The primary drivers for obtaining ISMS certification at these locations was for an overall better security program for their customer-facing business and customer requirements. Security is very important to this organization, and obtaining ISMS certification is one of several ways that they are able to demonstrate to their customers that they take security seriously.

Additionally, as a U.S.-based organization, they have found certification has helped them with customer credibility not only outside of but also within the U.S. "Without the existence of a viable accreditation program and the accompanying demand from U.S. customers, though," this organization believes that, "other regulatory and legal pressures push ISMS certification to be a lower priority in the U.S."

Current U.S. Organizations with ISMS Certification

How do the industries of the CISOs I spoke with align with the industries of the U.S. organizations that have obtained ISMS certification? I found only 27 unique U.S.-based organizations that are currently registered as having obtained formal ISMS certification. See Table 2 for the industries within which these organizations belong. This statistic does not include the one organization I spoke with that obtained certifications within their non-U.S. locations.

Industry	Number of ISMS Certifications in U.S.
Financial and Computer Processing Outsourcer	5
Manufacturing	5
Technology and Information Security Consulting	3
Financial Services	3
Software Development	3
Banking	3
Construction and Engineering	1
Pharmaceuticals	1
Digital Certificate Registration	1
Education	1
Legal Services	1

Table 2: Current U.S. ISMS certifications.

Based upon these factors and conversations I've had with several other information security practitioners at various conferences and professional meetings, it appears that the U.S.-based organizations that are most likely to seek formal ISMS certification are those in the outsourcing, manufacturing, consulting, financial services, software development, and banking industries. Based upon my own experience, I see a trend in outsourcers pursuing ISMS certification to make it more efficient for them to validate their security programs to their business partners.

An ISMS Certification Preparer's Perspective

Hotskills, Inc., based out of St. Paul, Minnesota, has participated in ISMS certifications for organizations based within the U.S. as well as outside the U.S. Tom Carlson with Hotskills indicates that the motivations for organizations to obtain ISMS certification differ. However, he has found the primary reason to be market differentiation, and the secondary is for regulatory compliance. Carlson also indicated that he believes the industries that are most likely to pursue ISMS certification are those that are heavily regulated, such as banking and finance, because of the third-party external validation and the inherent regulatory umbrella. According to Carlson, "It is a defensibility and efficiency issue."

A huge roadblock for an organization to obtain ISMS certification is to properly establish the scope of the certification. Carlson indicates, "Registration scope is one of the most misunderstood parts of the certification process. Most organizations do not scope wisely and bite off more than they can chew, resulting in project failure, or more than makes sense, which results in a waste of resources."

Many of the U.S. organizations I've spoken with that are aware of ISMS certification mistakenly believe that the certification must cover their entire organization. Raising the awareness and understanding of the need to properly establish the scope for the ISMS certification, which will typically be a subset of the organization, and often a very small subset at that, would likely lead to more U.S. organizations pursuing ISMS certification.

It is also important for U.S. organizations to realize there is not a typical timeframe within which ISMS certification can be accomplished; it depends upon a great number of factors and the scope of the certification. Some organizations could obtain ISMS certification within a few weeks, and for others, it could take well over a year.

Carlson described a hypothetical ISMS certification process and the factors involved. "A bank data center certification may be done as a result of both regulatory compliance and market differentiation motivators. The time, resources, and level of effort are totally dependent on the organization's information security program maturity. For example, some of the issues involved from my perspective as a certification preparer are:

> Do I have to spend a lot of time in tutorial mode or is everybody a CISSP?
>
> Will the organization dedicate a full-time person to shadow me and absorb knowledge transfer or will I spend a significant amount of time waiting for the client to respond?

"Experience has shown that a typical project will run from 6 to 12 months depending upon the answers to the questions above. I have run the gamut from a 2-week project to a 14-month project."

Many more U.S. organizations might pursue ISMS certification if they were more aware of the scope issues, the resources and effort involved, and the benefits for obtaining ISMS certification.

Five Things to Know

Carlson provided the following five things he believes are most important for an organization to know when considering ISMS certification:

> You can build a defensible information security program, based upon the concepts of ISO27001 and ISMS, without going the extra mile of obtaining certification.
>
> Although ISO27001 certification requires an ISMS, an ISMS does not require ISO27001. An ISMS can be built around, or include, other standards such as COBIT.
>
> Choose a scope that makes sense. Don't set yourself up for failure.
>
> Realize that creating and certifying an ISMS is a process, not a product; your organization will be required to participate in the creation and maintenance.
>
> Cross certification is the coming trend. There is wonderful synergy between ISO27001 (ISMS) and ISO9001 (TQM) as well as ISO20000 (ITIL).

Benefits for Pursuing ISMS Certification

It is important to consider that the documentation created as a result of pursuing a formal ISMS certification will demonstrate due diligence to any regulators or outside auditors that are reviewing the adequacy of your organization's information security program. The CISOs I spoke with often indicated their regulatory requirements showed business value and the ISMS certification did not. Organizations need to realize that ISMS certification actually can be quite valuable in supporting regulatory compliance requirements.

I have performed many business partner information security reviews, and those who had already obtained ISMS certification not only saved themselves much time and effort when answering my questions but also saved me much time by having sufficient readily-available third-party validated documentation about their information security practices. ISMS certification can ease and facilitate business partner due diligence information security program reviews.

When an information security incident occurs, having ISMS certification will help demonstrate you took every possible precaution and had appropriate safeguards implemented to try to prevent the incident from occurring; it demonstrates your standard practice of due care as validated by an independent third party. The business value of ISMS certification will be clearer as organizations understand more completely what is involved with ISMS certification.