Diffusion and Adoption of Information Security Management Standards Across Countries and Industries

Deniz Tunçalp

EDITORIAL PREFACE

Diffusion and Adoption of Information Security Management Standards Across Countries and Industries

Deniz Tunçalp

Department of Management Engineering, Istanbul Technical University, Istanbul, Turkey

Information security management standards are usually overlooked in conventional information technology management literature. However, with the level of sophistication and popularity of volunteer management standards among organizations across the world, they represent a current and important global IT topic. As of 2013, there were 22,293 organizations in 105 countries and economies (Table 1) that were certified in information security management based on the International Organization for Standardization's (ISO's) Standard ISO 27001 (ISO, 2013). In this article, I wish to call the attention of the international researcher community to the ISO 27001 information security management standard and a number of potential research questions based on the empirical data reported by the ISO.

The ISO 27001 information security management standard can be considered as a technological artifact itself, covering systematic and instructional knowledge on how information security can be managed in organizations. It has been developed over various prior standards, first announced for certification in 2005 and revised in 2013. Organizations may adopt the ISO 27001 standard without pursuing certification as a global best practice or may voluntarily chose to get certified by an accredited auditor. Once certified, auditors keep visiting the certified organization at planned intervals, and the organization needs to show evidence to auditors that their information security management system is working and improving over time to keep their certification; otherwise, it is withdrawn and canceled.

Address correspondence to Deniz Tunçalp, Department of Management Engineering, Faculty of Management, Istanbul Technical University, Macka Cad. No: 1, 34357, Besiktas, Istanbul, Turkey. E-mail: tuncalp@itu.edu.tr

TABLE 1
Information Security Management Certifications Worldwide (2006–2013)

Year	2006	2007	2008	2009	2010	2011	2012	2013
Total	5,797	7,732	9,246	12,935	15,626	17,355	19,620	22,293
Africa	6	10	16	47	46	40	64	99
Central and South America	18	38	72	100	117	150	203	272
North America	79	112	212	322	329	435	552	712
Europe	1,064	1,432	2,172	3,563	4,800	5,289	6,379	7,950
East Asia and Pacific	4,210	5,550	5,807	7,394	8,788	9,665	10,422	10,748
Central and South Asia	383	519	839	1,303	1,328	1,497	1,668	2,061
Middle East	37	71	128	206	218	279	332	451

Source. ISO (2013).

DIFFUSION OF INFORMATION SECURITY MANAGEMENT STANDARDS

The most notable of voluntary management standards are ISO 9001 for quality management, ISO 14001 for environmental management, and ISO 27001 for information security management. As of 2013, there were 1,129,446 ISO 9001 and 301,647 ISO 14001 certifications but only 22,293 ISO 27001 certifications (ISO, 2013). While this may be due to the longer diffusion time of the ISO 9001 and ISO 14001 standards, the ISO 27001 information security management standard definitely has a slower rate of diffusion despite the increased awareness of information security and risk-related issues during the 2000s. After the first 6 years of their respective diffusion, ISO 9001 was adopted by 271,846 firms and ISO 14001 by 90,554 firms, whereas ISO 27001 was only taken up by only 17,509 firms globally (see Figure 1).

Theories to explain the nature, lifecycle, and the international diffusion of management standards bring a variety of perspectives and conceptualizations. These perspectives consider management standards as management technologies (Benner & Tushman, 2002; Nelson & Shaw, 2003) or social phenomena under institutional and political influence (Beck & Walgenbach, 2005; Brunsson & Jacobsson, 2000; Guler, Guillén, & MacPherson, 2002). Earlier literature reported that supply chains (Corbett, 2006), multinational corporations (Guler et al., 2002), and institutional expectations (Beck & Walgenbach, 2005) have significant influence in the adoption and the international diffusion of management standards. It has been also argued that the earlier diffusion of one management standard supports the diffusion of a newer management standard. The argument is that the diffusion of the first management standard creates a certification market in a country by establishing occupational roles for auditors, accreditation bodies, certification bodies, and registrant companies; creating professional norms for certification; and setting up institutional expectations for management standards, thus preparing the stage for diffusion of later management standards. For example, Corbett and Kirsch (2001) found strong correlation between existing ISO 9000 diffusion and the new ISO 14000 diffusion worldwide.

Despite the extant literature and expectations, the existing diffusion of ISO 9000 and ISO 14000 has not really helped the ISO 27001 diffusion. Furthermore, it seems that the conditions and mechanisms described in the literature for diffusion and adoption of management standards
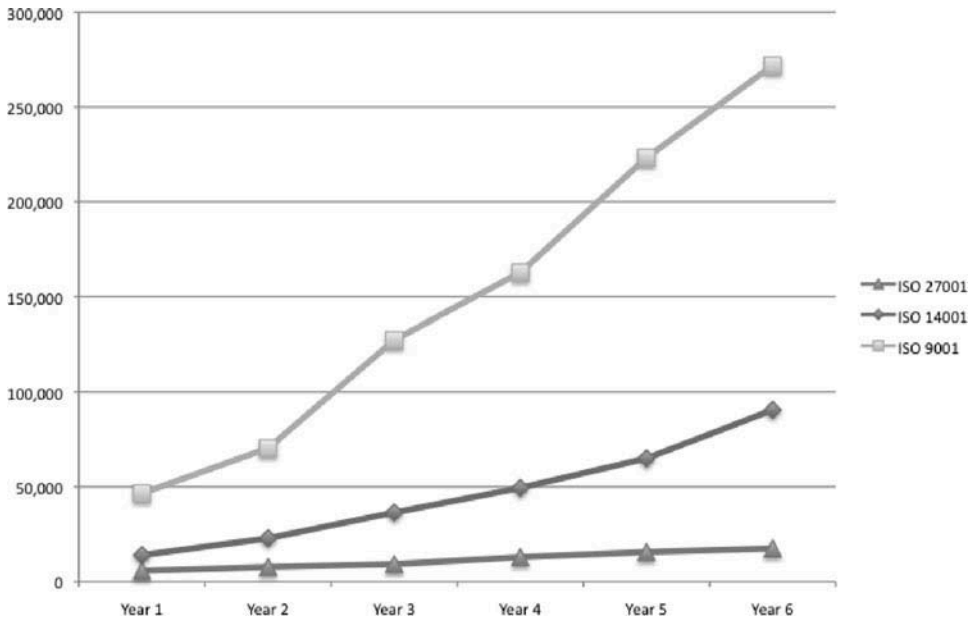
FIGURE 1 Early diffusion of voluntary management standards.

are not fulfilled or alternative mechanisms might be impeding the diffusion of information security management. Therefore, we need to know why information security management standard is not diffusing as fast as earlier standards, despite its popularity and significance. What mechanisms are impeding its growth, and why does diffusion of earlier standards not help its adoption?

EARLY ADOPTION OF INFORMATION SECURITY MANAGEMENT IN DIFFERENT COUNTRIES

When we look at the early diffusion pattern of ISO 27001 across the world, compared to other management standards, it shows an even more interesting phenomenon. For example, in its first years, 56% of ISO 27001 adopted companies were from three countries: Japan (40%), India (8%), and the United Kingdom (8%). This not only shows an uneven distribution among top adopting countries, but it also shows that adoption is much lower elsewhere. If we look at the global regions, it seems that ISO 27001 diffusion is underway mostly only in three regions: East Asia and Pacific, Europe, and Central and South Asia (see Figure 2). However, these relatively higher diffusion rates are much lower than early ISO 9001 and ISO 27001 diffusion in these regions (see Figure 3). Comparatively, in global regions with very low or limited ISO 27001 diffusion, ISO 9000 and ISO 14001 diffusion was much faster (see Figure 4).

These numbers show that there might be an anomaly in information security management compared to earlier standards. Is this anomaly caused by the differences between countries
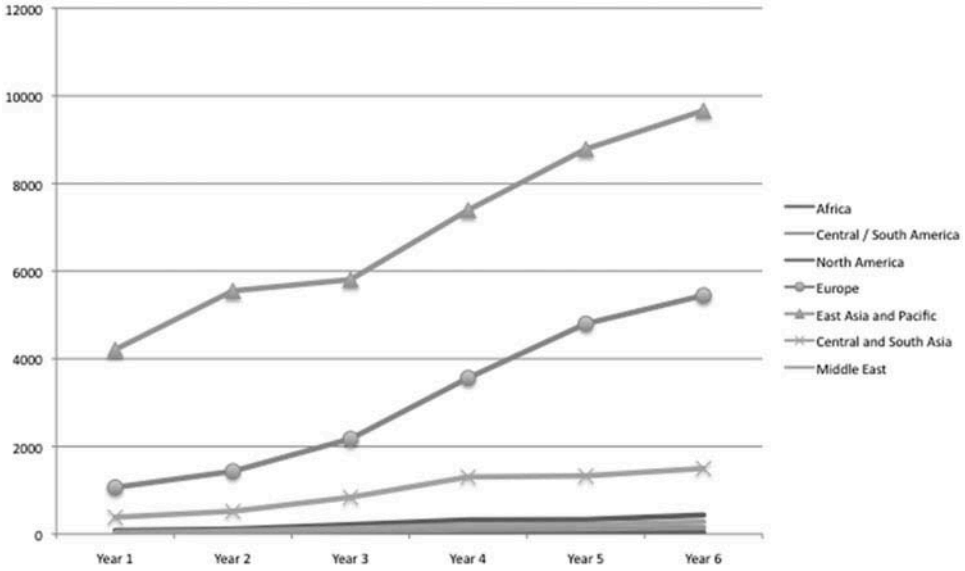
FIGURE 2 Diffusion of information security management standards in global regions.
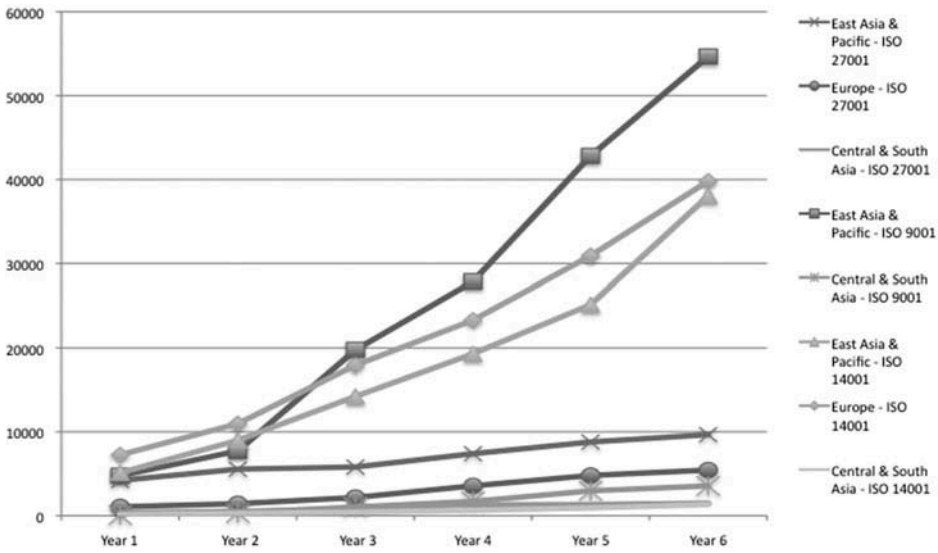

FIGURE 3 Diffusion of other management standards in global regions with relatively high ISO 27001 diffusion.
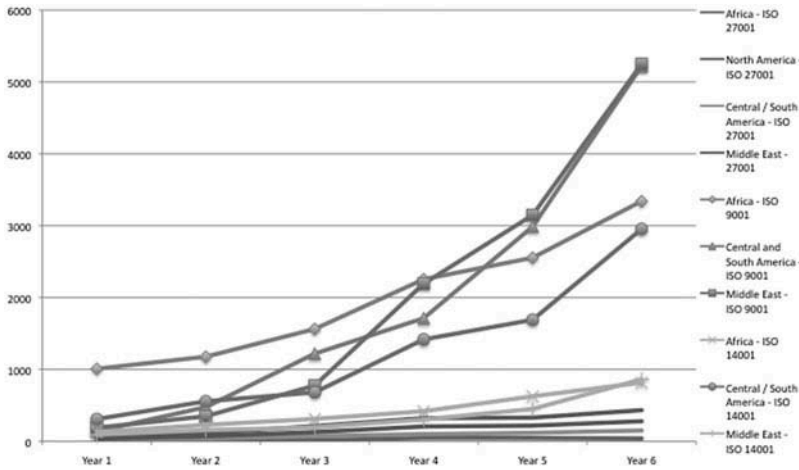
www.m

FIGURE 4 Diffusion of other management standards in global regions
with relatively low ISO 27001 diffusion.

in terms of Internet diffusion or by the semantic distance of these countries from the United
Kingdom, the inventor of all three standards? How does culture impact diffusion? Do coun-
tries with a lower level of diffusion have a different cultural understanding of risk and security?
We need studies that show why and how information security management diffusion has
been very different from the diffusion of quality management and environmental management.
Institutional, political, cultural, or technical explanations are needed as to why information
security management is widely accepted in certain countries yet other countries remain highly
reluctant.

INFORMATION SECURITY MANAGEMENT IN DIFFERENT INDUSTRIES

It is expected that the IT industry is the most likely adopter of information security manage-
ment certifications across the world. This claim is also supported by data (Table 2). The ISO
(2013) reports 5.059 certifications in the IT industry across the world. However, adoption and
non-adoption across other industries need further explanation. For example, how can we explain
the recent popularity of information security management in the construction industry? On the
other hand, industries that are traditionally very advanced in risk management and certification,
such as aerospace and aviation, are lagging behind others in terms of information security man-
agement. By the same token, strong industries, such as metal products and other manufacturing,
seem to keep a distance from information security management, despite their relatively large foot-
print worldwide. The underlying mechanisms for such wide differences in adoption rates need to
be understood and explained.

TABLE 2
Global Top 10 Industries - Information Security Management (2006–2013)

	2006	*2007*	*2008*	*2009*	*2010*	*2011*	*2012*	*2013*
Information technology	890	1.236	1.152	2.086	3.217	3.588	4.558	5.059
Other services	189	204	228	380	579	564	755	849
Construction	55	17	12	127	266	350	409	396
Transportation and communication	60	70	63	170	184	241	288	322
Electrical and optical equipment	38	58	50	135	221	280	342	289
Wholesale and retail trade	12	38	26	93	164	214	215	224
Engineering services	25	33	48	173	122	126	189	211
Health and social work	14	10	61	102	102	145	201	201
Public administration	23	33	79	181	79	106	155	192
Financial intermediation and real estate	47	54	68	148	185	113	138	169

Source. ISO (2013).

CONCLUSION

This article discusses the diffusion of information security management standards at a macro and global level. At the organizational level of analysis, there might be many other issues to study. Currently, very little is known about how information security management practices are applied across the world, how it is adopted by organizations in different industries, the way it is implemented in tandem with various other information technologies, and their impact and value in organizations. We need to theorize and empirically validate what cultural, institutional, and organizational mechanisms can explain the practice of information security management around the world.

REFERENCES

Beck, M., & Walgenbach, P. (2005). Technical efficiency or adaptation to institutionalized expectations? The adoption of ISO 9000 standards in the German mechanical engineering industry. *Organization Studies*, *26*(6), 841–866. doi:10.1177/0170840605054599

Benner, M. J., & Tushman, M. (2002). Process management and technological innovation: A longitudinal study of the photography and paint industries. *Administrative Science Quarterly*, *47*(4), 676–706. doi:10.2307/3094913

Brunsson, N., & Jacobsson, B. (2000). *A world of standards*. Oxford, UK: Oxford University Press.

Corbett, C. J. (2006). Global diffusion of ISO 9000 certification through supply chains. *Manufacturing and Service Operations Management*, *8*(4), 330–350.

Corbett, C. J., & Kirsch, D. A. (2001). International diffusion of ISO 14000 certification. *Production and Operations Management*, *10*(3), 327–342. doi:10.1111/j.1937-5956.2001.tb00378.x

Guler, I., Guillén, M. F., & MacPherson, J. M. (2002). Global competition, institutions, and the diffusion of organizational practices: The international spread of ISO 9000 quality certificates. *Administrative Science Quarterly*, *47*, 207–232. doi:10.2307/3094804

International Organization for Standardization (ISO). (2013). *The ISO survey of certifications*. Retrieved from http://www.iso.org/iso/home/standards/certification/iso-survey.htm.

Nelson, M., & Shaw, M. (2003). *The adoption and diffusion of interorganizational system standards and process innovations*. Management Information Systems Quarterly (MISQ) Special Issue Workshop, Seattle, WA.

AUTHOR NOTE

Deniz Tunçalp *is Assistant Professor of Management at Istanbul Technical University in Turkey. His research interests include technology, organization studies, and qualitative research methods. He has studied organizational adaptation to technological change in different organizational situations at different levels of analysis. His research has appeared in such journals as* Operations Research *and* Journal of Organizational Ethnography.