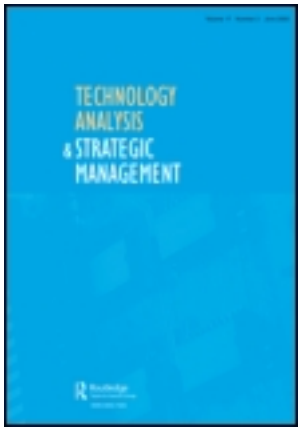

Technology Analysis & Strategic Management

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ctas20

Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study

Robert van Wessel [a], Xu Yang [b] & Henk J. de Vries [a]

[a] Rotterdam School of Management, Erasmus University, Rotterdam, The Netherlands

[b] Beijing University of Posts and Telecommunications, Beijing, People's Republic of China

Published online: 25 Aug 2011.

To cite this article: Robert van Wessel , Xu Yang & Henk J. de Vries (2011) Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study, Technology Analysis & Strategic Management, 23:8, 865-879, DOI: 10.1080/09537325.2011.604155

To link to this article: http://dx.doi.org/10.1080/09537325.2011.604155

Technology Analysis & Strategic Management
Vol. 23, No. 8, September 2011, 865–879

Routledge
Taylor & Francis Group

Implementing international standards for Information Security Management in China and Europe: a comparative multi-case study

Robert van Wessel[a]*, Xu Yang[b] and Henk J. de Vries[a]

[a]*Rotterdam School of Management, Erasmus University, Rotterdam, The Netherlands;* [b]*Beijing University of Posts and Telecommunications, Beijing, People's Republic of China*

The leading international standards for information security management, ISO/IEC 27001 and ISO/IEC 27002 originate from the UK, but are applied worldwide. This paper explores whether the processes of selection, implementation and use of these interrelated standards differ between China and Europe by studying cases of Chinese and European companies. Chinese companies face some additional problems with the standards but manage to get them successfully implemented in a short period of time. Main differences relate to governance and management of standard adoption. This study is innovative in the method used for standardisation research (comparative multi-case study), and the topic: implementation and impact of information security management standards.

Keywords: information security management; standard; ISO/IEC 27001; China; Europe

Introduction

Information is a key asset for organisations and therefore information systems should be well protected (ITGI 2001). Information security should assure the organisation's operations (Ezingeard and Birchall 2005). Standards for information security management specify the requirements and processes to enable a business to establish, implement, review and improve information security. Several standards exist including NIST SP 800 and COBIT (ISACA 2005). Since 2005, the international standards ISO/IEC 27001 and ISO/IEC 27002 are implemented all over the world. Certification based on ISO/IEC 27001 showed 40% increase in 2009, the global number of certified companies is 12,934; which can be compared with 1,064,785 for the quality management system standard ISO 9001 and 223,149 for the environmental management system standard ISO 14001. China has become the leading country for the older standards ISO 9001 and ISO 14001 (24% and 25% of the number of certificates). Japan is number one for ISO/IEC 27001 (43%), China has 459 certificates (4%) but an above-average growth (95%) (ISO 2010). Although the

*Corresponding author. Email: rwessel@rsm.nl

ISSN 0953-7325 print/ISSN 1465-3990 online

DOI: 10.1080/09537325.2011.604155
http://www.informaworld.com

technology used in organisations is identical, institutional and cultural settings may differ per country (Hofstede 1984). A key question is whether implementation of these standards differs per country, knowing that technology adoption may vary across different cultures, although the role of culture in affecting adoption has not been fully understood (Srite and Karahanna 2006; Zhang and Maruping 2008; Venkatesh and Zhang 2010). This paper explores whether selection, implementation and use (altogether referred to as adoption) of these interrelated standards differ between China and Europe.

Information security

Information security protects the interests of those relying on information and the systems and communications that deliver the information, from harm resulting from failures of confidentiality (ensuring that information is accessible only to those authorised to have access to it), integrity (safeguarding the accuracy, completeness and timeliness of information and processing methods) and availability (ensuring that authorised users have access to information and associated assets when required) (ITGI 2001). Few studies address implementation and impact of information security management systems (Kotulic and Clark 2004; Spears and Cole 2006). Jung, Han, and Lee (2001) and Yeh and Chang (2007) focus on specific topics such as security threats. Huang and Lee (2006) and Bojanc and Jerman-Blazic (2008) combine information security and organisational performance. Some studies originate from Chinese Taipei (Yeh and Chang 2007; Farn, Lin, and Lo 2008; Lai and Dai 2009) but publications from mainland China are notably absent except some in Chinese language (Wu, Wang, and Shangguan 2006; Shangguan and Xu 2008).

Technology adoption and culture

Often, research on organisational adoption of information systems uses the Technology Acceptance Model (TAM) (Davis 1989; Bagozzi 2007). The TAM suggests that perceived usefulness and perceived ease-of-use are the two most important factors in predicting an individual's acceptance of a new technology. The model is less suited for investigation of organisational-level acceptance of technologies as these adoption decisions are strategic level concerns (Lippert and Govindarajulu 2006).

Information systems (IS) research has addressed the importance of national culture in understanding technology adoption (Srite and Karahanna 2006). Hofstede's (1984) cultural dimensions have been extensively applied to assess the effects of national culture in various economic and behavioural contexts (Sondergaard 1994). China differs from European and North American countries in terms of power distance, individualism, and long-term orientation. Recent papers on technology adoption and competitive advantage in China (Qi et al. 2009; Tian et al. 2010) do not address cultural aspects and/or differences with the West, empirical IS studies related to human and organisation aspects in China are scarce (Chen 2010). Martinsons and Westwood (1997) found that organisational co-ordination and control of IS are achieved using reliance on informal information, implicit and indirect communications, and centralised decision making. Other studies about China addressed knowledge management (Burrows, Drummond, and Martinsons 2005), e-commerce (Martinsons 2008), or IT-enabled organisational change (Martinsons, Davison, and Martinsons 2009) and suggest that national culture can affect how people actually use IS. Tong and Mitra (2009) found five key Chinese cultural characteristics: hierarchy-consciousness, fear of losing face, a sense of modesty, keeping own knowledge implicit, and preference for face-to-face communication.

Standards for information security management

The ISO/IEC 27000 series of standards published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) are intended to assist organisations of all types and sizes to implement and operate an Information Security Management System (ISMS). The series provides best practice recommendations on information security management, risks and controls. ISO/IEC 27001 specifies requirements for establishing, implementing, operating, reviewing and improving an ISMS using a 'Plan-Do-Check-Act' approach: Plan: create security policy and accompanying procedures and controls; subsequently prepare a scope statement of applicability, justifying why certain controls were not selected, if applicable; Do: implement policy, procedures and controls; Check: determine process performance and report the outcome to management; Act: take appropriate actions to improve the risk profile. Meeting ISO/IEC 27001 requirements can be demonstrated by a certificate. The largest numbers of certificates have been issued to organisations in Japan (5508), India (1240), UK (946), Chinese Taipei (934), Spain (483), and China (459) (ISO 2010). The accompanying standard ISO/IEC 27002 provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance for ISO/IEC 27001. These can be tailored to specific risks and needs of an organisation. ISO/IEC 27002 can be implemented independently. Controls include policies, practices, procedures, organisational structures and software functions. ISO/IEC 27002's 11 sections address security policy; organising information security; asset management; human resource security; physical and environmental security; communications and operations management; access control; information systems acquisition; development and maintenance; business continuity management; compliance; and information security incident management. These two international standards originate from the British Standard BS 7799:1995.

Organisations implement ISO/IEC 27001 and/or ISO 27002 to have a better position at the market by, for instance, increased confidence and thus acceptability for customers, assurance of services, for marketing reasons or to meet legal requirements (Fenz et al. 2007; Neubauer, Ekelhart, and Fenz 2008). Implementation increases staff awareness of information security, mitigates threats, and provides better data and privacy protection (Ezingeard and Birchall 2005; Karabacak and Sogukpinar 2006; Neubauer, Ekelhart, and Fenz 2008). In this paper we will investigate whether these standards, rooted in Europe, are selected, implemented and used differently in China.

Research design

We need case study research, as there is little previous research on ISMS implementation in China, let alone comparisons with Europeans counterparts (Benbasat, Goldstein, and Mead 1987; Yin 2009). We have selected Chinese and European companies and sought for variety in size, sectors, and private versus (semi)public. Case companies should have implemented at least 80% of the ISO/IEC 27001 or ISO/IEC 27002 requirements, and the time horizon between initial implementation and current use should be approximately three years.

Pre-field procedures of the case study protocol included sending an introduction letter to potential case companies and a check by phone whether potential interviewees have the necessary knowledge about adoption of ISO/IEC 27001/2 in their company. Interviewees included typically the (Chief) Information Security Officer and Information Security specialists. The researchers also asked whether the company had relevant data about standards adoption and its impact available. Per trip one company was visited. Semi-structured interviews were carried out and recorded. Simultaneously the interviewer wrote down the responses. The first author carried out the European

Table 1. Profile of the case companies

Case	Sector	Type	Country	Number of interviewees	Size	Certification
1	Telecommunication	Commercial	CN	2: General manager, staff member information management	Very large	Enterprise-wide
2	Computing services	Commercial	CN	2: Director services, engineer information management	Large	Enterprise-wide
3	E-business	Public	CN	2: General manager payments deputy manager technology	Large	Enterprise-wide
4	Telecommunication	Commercial	CN	2: Technical engineer, staff member equipment maintenance	Large	Single department
5	Software/outsourcing	Commercial	CN	3: Director and staff member of quality management department, IT manager	Large	Enterprise-wide
6	Software/outsourcing	Commercial	CN	4: Director, information security manager, quality staff	Large	Enterprise-wide
7	Financial services	Commercial	NL	5: Strategic and operational managers of the information security department	Very large	Some departments
8	Computing services	Commercial	NL	2: Information security officer, operational security manager	Very large	Some departments
9	Financial services	Commercial	NL	2: Information security manager and officer	Very large	Some departments
10	Telecommunication	Commercial	NL	2: Information security manager and officer	Very large	Some departments
11	Purchasing	Public	UK	1: Information security officer	Large	Enterprise-wide
12	Software industry	Commercial	UK	2: IT manager, information security officer	SME	Enterprise-wide

interviews using their national language (English and Dutch), the second author did the Chinese interviews. Some Chinese companies did not allow tape recording but an assistant wrote down the answers. The common semi-structured questionnaire contained closed general questions and more specific open questions on selection, implementation, use and impact of the standards. The questionnaire was based on earlier in-depth case studies on adoption of standards including ISO/IEC 27002 (van Wessel 2010). In several closed questions interviewees had to provide a score at a Likert scale (showing, for instance, the extremes 'bottom-up' and 'top-down' for implementation) and then they were asked to explain their score. Additional sources of data included project plans, project reports, presentations, policy documents, memoranda and leaflets to make data triangulation possible. The transcript was processed, preferable within 24 h, and subsequently sent to respondent(s) for validation and approval. Data in Chinese language have been translated into English. Following Miles and Huberman (1994), data have been displayed in a matrix showing per box the essence of an answer per question per case. This facilitated cross-case analysis. First, per question the answers were compared across China and the West providing an initial view. Subsequently this initial result was complemented and refined based on the detailed answers provided by the interviewees. Finally, the findings per question have been combined to draw a general picture of differences and similarities between Chinese and European cases.

Case company descriptions and findings

Twelve companies were visited and 29 members of staff were interviewed (Table 1). Individual interviews lasted between one and four hours with an average of 90 min. The four-hour interview concerned case study 11. All companies adopted ISO/IEC 27002, some of them gained the ISO/IEC 27001-certificate enterprise-wide, whereas others limited certification to one or more departments. The Chinese companies were located in the greater Beijing area. Paper length requirements compelled us to select the most informative case descriptions, so we skipped cases nine and 10.

Company 1

Company 1 is a mobile communications operator in the provincial market and employs over 10,000 FTEs (full time equivalent). The company has a two-tier structure: the corporate (provincial) level and municipal subsidiaries. The information security team includes three FTEs at the provincial level and 22 FTEs at the municipal level. The Information Security function is part of the IT Department, with some specialised sections in the Network Department and the Management Information Department.

The Management Information Department at corporate level decided to implement ISO/IEC 27001 to secure the company's competitive advantage during its shift from mobile communications service provider to mobile information service provider. Objectives were to enhance the risk profile, information systems quality, and businesses continuity. But according one of the interviewees 'regulatory pressures become more and more important, such as SMS SPAM control and customer's privacy'. The Management Information Department managed the implementation. Implementation was carried out gradually at the corporate level, starting with some major information systems such as Business and Management Support Systems. An American IT firm assisted internal staff to implement the standard. 'There is a lack of clear and applicable instructions in the standard. A good consultant is needed as it is a tough job to implement it on your own'. Next, all municipal companies had to implement the standard based on the corporate specification.

During implementation, knowledge on information security and ISO/IEC 27001 has been disseminated through several channels such as short message services (SMS), the company portal and awareness posters. The interviewee said proudly: 'We can really say that information security is everywhere in our company, it brought us high awareness and this made it much easier to push the implementation'. Since there are automated interfaces between the information systems of the case company and its partners/suppliers, the company requested them to meet the controls specified in ISO/IEC 27001 as well.

Company 2

Company 2 provides professional information security products, services and solutions to its customers. It has over 550 employees in its Beijing headquarters and more than 30 branches all over China. Approximately 30 staff spend part of their time on information security. The information security function is organised in the Information Management Department.

Adoption objectives are to protect the interest of the clients and the company, and to strengthen the company's brand. The president of the company, the Information Management Department and the Professional Services Department have all been involved in the selection process. 'It was a semi-formal process and the president finally decided. Then all departments were informed and the Information Management Department carried out implementation'. Information security being their core business, this company is the only one that implemented ISO/IEC 27001/2 all by itself. It used a gradual top-down approach, by first piloting it in a number of their IT products and systems, such as the web application firewall, and then applying it to the whole enterprise. ISO/IEC 27001 has enhanced customer, employee and IT staff satisfaction because the company can prove its professional ability. ISO/IEC 27001/2 has helped to turn the company from a reactive, incident driven mode to a proactive one. For example, customers complain far less on available issues as these are solved before these would actually occur.

Company 3

The state-owned company operates full-range e-commerce and e-government platforms for governmental institutions, trade associations and millions of domestic companies. It has 500 employees. The technology department employs over 10 information security FTEs.

Being a monopolist, the company lacks external drivers for implementation and has no commercial needs for certification. However, the national e-commerce platform needs confidentiality, integrity and availability of the information systems. They wanted to resolve issues related to Access Control, Communications and Operations management and Business Continuity Management. It is the only Chinese case company that did not implement all ISO/IEC 27002's sections but it intends to implement the remaining sections in the near future. The implementation was initiated by the technical department and carried out by internal staff and external consultants. It took a relatively long time but resulted in a professional ISMS. Certification was a spin-off rather than a key objective from the start.

Company 4

Company 4 is another provincial telecommunications operator, with about 5000 employees. The ISMS scope is limited to the Internet Data Centre services. There are no dedicated employees for the information security function, but over 10 staff spend part of their time on it.

This company adopted ISO/IEC 27001/2 to obtain competitive advantage. It integrated information security management in its existing integrated management system based on ISO 9001, ISO 14001, and GB/T 28001 (occupational health and safety management). These standards share the same general requirements, document structure, and management principles such as the 'Plan-Do-Check-Act'-cycle. As one of the interviews mentioned: 'this helped us to rationalise the management in these areas resulting in more protection and fewer losses'. Implementation was carried out top-down by the department that previously had implemented the other management system standards. This experience facilitated the process but implementation was still considered as complex because of the technical expertise needed. Consultants supported implementation, carried out risk assessments and drafted policy documents. Implementation has had a positive impact on the availability of IT systems, service quality, business continuity and customer satisfaction but interviewees could not provide evidence for financial benefits. The company won the Information Security Award of the state in 2008 after its ISO/IEC 27001 implementation.

Company 5

Company 5 is one of China's top IT outsourcing companies. Its main services are Application Development and Maintenance and IT consulting. The company has branches in Beijing, Xi'an, Shanghai and Tokyo and more than 1200 employees. A dozen of employees spend a part of their time on information security.

Regarding the main driver for implementation, the IT manager said: 'As soon as Japanese clients arrive here, the first thing asked is about our ISO/IEC 27001 certificate. When they know we have it, everything goes well then, it seems there is no need to check it again'. The Quality Management Department lead the implementation team. All divisions and department managers were involved. The big bang and top-down implementation covered all business units in China and abroad. The IT manager explained 'The Quality Management Department selects the standard, and we (IT team) accept'. The company also used elements from other standards, such as BS 25999 (business continuity) and ISO/IEC 13335 (IT security), to complement their ISMS. The interviewee of the quality management department said, 'We had to refer to these and other standards for more instructions'. A consultant provided assistance. Before, this company had tried to meet security needs related to the customer requirements case by case. Adoption of ISO/IEC 27001/2 resulted in better understanding and co-operation. 'Now they often consult my team for information security issues and so we can meet the customer's needs better', the IT manager said.

Company 6

Company 6 also provides IT outsourcing services including application development, and production testing. It is one of the few companies in the world that has obtained certification on the highest level of the Capability Maturity Model, an American process control approach for software development. Its Chinese, Canadian, Japanese and US branches deliver high quality IT services to Fortune 500 customers. Its around 3300 employees include 12 FTE in the Security and Compliance Department.

Enterprise-wide certification was required to meet customer requirements. Implementation was relatively easy since the company was already familiar with information security and with the implementation of other management system standards. A consultancy firm was hired first but did not deliver what was required. Subsequently the Security and Compliance team finished the job successfully. The director of the Security and Compliance Department told that they had to

balance conflicting interests between the requirements set by the standard and the business 'by means of postponing, re-assessing, and forced decision-making, depending on the situation'. The project team struggled during the implementation period with the issue how to meet the controls 'as there were no clear criteria to tell what statement would meet the requirements of the standard'. Nevertheless, they developed a quantitative assessment model and a specialised information system to collect and process information security related performance data. The director continued: 'This showed us that a significant improvement was found between the branches or departments with and without the implemented standard. The performance of the branches or departments with the implementation was much better than the others without it'. Performance data included customer satisfaction, Return on Investment and Payback Period of the implementation project.

Company 7

This Dutch financial services provider has a large domestic footprint and an international network for private and business clients. It employs over 30,000 FTE including 60 FTE at the information security department.

The company adopted ISO/IEC 27002 to increase the overall quality level, reduce costs and get a common language. External drivers were complying with legal requirements, meeting regulatory pressures, and building trust with customers. Only two departments gained ISO/IEC 27001 certification, to enhance local competitive advantage or to meet requirements for specific services. ISO/IEC 27002 has been implemented gradually with the corporate information security department supervising a bottom-up approach. Before ISO/IEC 27001/2 adoption, a number of information security management policies had been implemented already (e.g. for access control and encryption). Policies based on ISO/IEC 27002 were added and existing ones were aligned, 'retrofitted' as one of the interviewees called this. 'In doing so it makes life easier to deal with third parties on information security, as you talk the same language'.

Another interviewee: 'The Business is not really interested in information security policies. They just want to know what to do and how to implement the necessary policies. They also would like to know the level of compliance and to understand the level of risk they are exposed to and then implement the required controls'. Many controls have been implemented by others than the information security organisation, for example, the clean desk policy by the business departments, staff screening by HR, and data encryption by IT vendors. ISO/IEC 27001/2 is perceived as an enabler for Internet banking as it makes transactions more secure.

Company 8

This large provider of Information and Communication Technology services employs over 14,000 FTEs worldwide. Approximately 20 staff is involved in information security management, not counting Security Consultants that work at the clients premises.

The company obtained ISO/IEC 27001 certification as required by a customer. Initially there was staff resistance (more procedures, more instructions, etc.) but now most staff are proud of what they have achieved. Improvements include fewer incidents, clarity on accountabilities, processes and procedures that run far more smoothly, fewer escalations, and increased level of quality thinking. Certification as such does not bring any competitive advantage other than staying in business.

The information security function in this company is structured according to a federal model. Business Units have large autonomy to make decisions on implementation of the information

security policies. The central security organisation only requires BUs to have an information security policy and to carry our risk analyses. Every BU has to decide which elements from the standard they need, using a risk assessment template created by the central security organisation. They decide whether a risk is acceptable or not, based on business drivers and cost/benefit ratio. If they accept the risk they have to sign off and provide the rationale to higher management. Otherwise they subsequently implement the required security controls. They remain fully responsible and accountable.

Implementation of ISO/IEC 27001/2 was carried out as part of the normal activities of 10 FTE operational security officers and assisted by consultants for foreign locations that lacked local expertise, combining a top down decision with a gradual bottom-up approach. Of all 12 case companies, they were the least pleased with the standards, chapters 4 to 8 of ISO/IEC 27001 are fine from a process perspective. However the annex, and especially ISO/IEC 27002 has far too much detail, and more importantly, is even sometimes inconsistent and has overlap with other controls. (. . .) It is about risk management, not about implementing the 133 controls (. . .) The standard says: 'implement measures that are in line with the company culture' but it lacks any guidance here as well.

Company 11

The company is an executive UK Government procurement agency of around 300 FTEs. Two FTEs work on information security at the corporate level and four FTEs spend a part of their time on it at a departmental level.

Government required the company to comply with the standard from the outset. Additionally, the internal driver was to improve the security quality of the services. A project team was formed consisting of eight staff members, one from each department, including the IT department, and an external consultant. As part of the project, they ran a mandatory training program for all employees. 'If you try to implement it as "an IT thing" then it is a useless exercise. You have to have the co-operation and trust of your staff and other departments'. The whole implementation went really well, they managed to get certified in 11 months.

Satisfaction of customers on IT delivery and support improved much but satisfaction of IT and information security staff is lower as they feel restricted in their freedom. ISO/IEC 27001 is seen as a business enabler, it resulted in the ability to provide high quality secure services outside their inner purchasing and supply area.

Company 12

The company is one of the leading providers of claims solutions in the UK for the automotive insurance. It employs around 100 FTE. Information security and Business Continuity Management requirements are part of the contracts between the company and its customers.

Two major information systems outages had triggered adoption. Adoption should increase quality and lower costs. External drivers included ensuring compliance with customers' requirements, competitive advantage, improving brand image, and meeting legal requirements and regulatory pressures. Senior management wanted certification to mark achievements. Implementation was carried out as a big bang, from top down and took nine months. Initially, ISO/IEC 27001 adoption was an IT effort driven by the IT director. It took a while for senior management to realise that without their proactive support it would not be successful.

Nobody was familiar with the standard so implementation was difficult. The information security officer further explains 'Some areas of the Business have picked it up quite well and it has become part of their day to day operations. Others you still need to nudge them a few times for them to realise that they have to think about it in everything they do'. The business units became more aware of the risks they face including the risks that suppliers bring to the business. Most importantly, ISO/IEC 27001 improved customer confidence in the companies' ability to service them properly.

Cross case analysis

In this section, case findings are discussed with a focus on the implementation phase. First governance arrangements for adoption and management attitude are examined and then the reasons for adoption and other key elements are dealt with.

Governance and management

Van Wessel (2010) demonstrated the importance of governance and management for effective adoption of standards. Governance is 'Specifying the decision rights and accountability framework to encourage desirable behaviour in the selection, implementation and use of standards within an organisation', management 'The decision-making efforts associated with planning, organising, controlling, and directing the selection, implementation and use of standards within an organisation'.

One of the most visible governance elements is the organisational set-up of the information security function. Most European case companies had a centralised governance structure. The Chinese companies had a less centralised structure and opted for a 'federal' set-up, allowing the individual units to maintain certain powers and aspects of sovereignty, in combination with power for the strategic information security group at corporate level. In both China and the West, IT, Risk Management or Compliance departments at corporate level managed implementation.

The general attitude of business and IT management towards ISO/IEC 27001/2 implementation is very positive in China; in Europe it is marginally positive for business management and mildly positive to very positive for IT management. Top management in China regards information security as a key element to differentiate the company from its competitors and prepare for future business. In China, endorsement by business and top management is typically higher than in the European companies. Chinese top management decides but they first ask the IT department to prepare a proposal and arrange meetings with all stakeholders to balance business needs and IT needs. In Europe, the power balance between the business and IT departments differs per company.

Reasons for adoption

Almost all companies had internal and external drivers for adopting the standards. Internal drivers are related to quality, cost reduction and to avoid incidents. All Chinese companies indicated competitive advantage as a main external driver. In contrast, European companies mention regulatory pressures and two companies also pressure from customers. The companies are early adopters but some European market segments, such as IT Services, are more mature and then the certificate does not distinguish the company from its competitors anymore, it is a prerequisite for staying in business. China has less legal and regulatory pressures. The two smaller Europe companies articulated more external than internal drivers for adoption.

Implementation method

In China, a big bang and top-down approach was the default way of implementation. Then commitment from senior management is a prerequisite and the necessary resources can be allocated easily. The process of adopting ISO/IEC 27001/2 ranged from *ad-hoc* decisions to using formal processes executed by a specific department. The adoption process in China was more formal compared to Europe.

In Europe, findings suggest the preferred implementation combines central top-down activities (setting strategic objectives, policies and guidelines) with local bottom-up initiatives. In the large companies, a gradual implementation process seemed to be more effective than a big bang approach; in the small companies the big-bang approach was successful.

Mostly, implementation is perceived to be complex and therefore consultants are invited to support internal staff. In China and the UK, all projects were funded by dedicated project budgets from IT, business or quality assurance departments and were completed within one year. In three Dutch companies, implementations were carried out as part of business as usual activities and typically took much longer.

Challenges

For the Chinese companies the biggest challenge was to meet business demands and at the same time comply with the requirements in the standard. All relevant stakeholders are involved but top management decides. In Europe, the business and its management show less interest, main challenge is to convince management of the need of information security and engage staff. Current information security issues convince them.

The standards lack instructions or best-practice examples on implementation, and guidance on how to tailor the standard to the company situation. This problem is more or less countered with the introduction of a number of complementary standards in the ISO/IEC 27000 series, such as ISO/IEC 27003:2010 'Information security management system implementation guidance'. All Chinese and most Western companies perceived implementation as expensive, compared to other IT-expenses. Costs of consultancy, staff-training, IT resources and certification ranged from €50 to €150 K.

Experiences

Successful ISO/IEC 27001/2 adoption is business-driven and subsequently embedded as 'business as usual'. Business departments determine needs for information security by identifying areas of weakness in risk assessments. Subsequently they implement those controls that really add value, by using a risk/benefit trade-off. Commitment and endorsement at senior management level is a prerequisite. Adequate communications and approaches improve the efficiency of the implementation, especially the communications between the IT department and the business departments and also the co-ordination between the implementation team and the information security management board. Moreover, the better employees are aware of information security, the more support from the business departments.

In particular in China, experiences gained with other management system standards, notably ISO 9001 and ISO 14001 contributed much to the successful adoption of ISO/IEC 27001/2. Several European case companies achieved successful ISO/IEC 27002 implementations by asking their business units to follow a few basic requirements and let themselves decide on the remaining ones based on cost/benefit ratio.

All companies managed to meet their initial objectives. They got a professional ISMS, which resulted in an improved risk profile, a better understanding and cooperation among staff, and an increase in customer satisfaction. Just one case company was not really pleased with the result and explained it also had to use other standards to make the system really work.

Discussion

The TAM model on technology adoption (Davis 1989) contains two core constructs 'perceived usefulness' and 'perceived ease of use'. Although the standards originate from the UK and address more than technology alone, they are perceived as useful both in China and the West. The Chinese seem to face a bit more difficulty in using the standard and this seems to be related to their inclination to implement all controls whereas European companies feel freer to focus on the most relevant controls. Just one cultural characteristic on co-ordination and control of IS found by Martinsons and Westwood (1997) and Tong and Mitra (2009) constituted an importance difference between standard implementation in China and Europe: the Chinese cases showed more centralised decision making and hierarchy-consciousness.

Our case companies were early adopters having internal next to external motivation for adoption. ISO 9001 experience shows that then benefits can be expected (Sampaio, Saraiva and Rodrigues 2009) but after a certain period, smaller organisations also implement the standard, certification is no longer distinctive and certification becomes less attractive for the remaining companies (Franceschini, Galetto, and Cecconi 2006). Late adopters no longer gain financial benefits from adoption (Benner and Veloso 2007). In some countries, the number of ISO 9001 certificates is stabilising or even in decline (Australia, USA) but it is rapidly growing in China and other countries where companies exporting to (in particular) Europe need the certificate to signal reliability. Then the motivation is 'license to export' rather than internal improvements with the danger of decline of the value of certificates. This may be informative for the future of ISO 27001 and then the role of external consultants in the implementation may further increase while the involvement of own staff, both from business and IT departments, may decrease as will do the distinctive value of certification and the internal benefits.

Conclusions

Studying Chinese and European case companies revealed commonalities and differences in ISO/IEC 27001/2 adoption. Main difference is that the Chinese see implementation as a strategic asset; therefore, top-management pursues it. They nevertheless involve both the IT and business departments and do this in a balanced way. Companies in Europe showed a diverse way how governance and management of implementation are shaped, whereas employees and operational management are more empowered. In Europe, therefore, the TAM factors perceived usefulness and perceived ease of use and more important for successful adoption. In line with Hofstede (1984) Chinese employees expect managers to lead and are less comfortable with delegation of discretionary decisions than employees from lower power distance cultures such as the Netherlands (Adler 1991, 146–78). However, some argue that traditional contrasts between countries may not always be the dominant force as this could be influenced by organisational and globalisation effects, which complement or even counteract cultural and societal effects (Mueller, 1994). International standards are manifestations of globalisation, and indeed we found more similarities than differences in implementation despite the fact that this standard has British roots. Nevertheless, the Chinese faced additional difficulty in implementation, firstly because in general

some terminology is difficult to translate as no exact Chinese word exists to match it, secondly because of the requirements themselves, and thirdly because they are more inclined to take the standard too literally whereas the Europeans feel more free to add and ignore elements. Though it fits their culture, the Chinese are not accustomed to the concepts laid down in international management system standards, and therefore, it is an advantage if they can build on experiences with ISO 9001 or ISO 14001 implementation. Despite these difficulties, the Chinese pursue top down implementation and manage to do this successfully in a short period of time.

Acknowledgements

The authors should like to thank BSI British Standards and the Ministry of Education of The People's Republic of China for making this research possible.

Notes on contributors

Robert M. van Wessel holds a Master in Electrical Engineering from Twente University and a PhD in Business Administration from Tilburg University (Department of Information Systems and Management). He is associated with Rotterdam School of Management, Erasmus University. Robert's research interests relate to the interaction and alignment of Business and Information Technology and include Business Performance and the Value of IT, Portfolio Management, IT Governance, Information Security Management and IT Standardisation and Standards.

Xu Yang holds a PhD in Management Science and Engineering, was visiting scholar of Rotterdam School of Management (RSM), Erasmus University in 2009, and now works as an Associate Professor and Director of Laboratory Center of the School of Economics & Management, Beijing University of Posts & Telecommunications (BUPT). The main research field includes Information management and Informationisation, IT project management and Risk Management, and Standardisation.

Henk J. de Vries is associate professor of standardisation at the Rotterdam School of Management, Erasmus University, Department of Management of Technology and Innovation. His research and teaching concern standardisation from a business point of view. Previous positions included different jobs at the Dutch national standardisation institute NEN. Henk is president of the European Academy for Standardisation EURAS and special advisor to the International Federation of Standards Users IFAN. He is (co-)author of more than 250 publications in the field of standardisation.

References

Adler, N. 1991. *International dimensions of organizational behaviour*. 2nd edition. Boston: PWS-Kent Publishing Co.

Bagozzi, R.P. 2007. The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems* 8, no. 4: 244–54.

Benbasat, I., D.K. Goldstein, and M. Mead. 1987. The case research strategy in studies of information systems. *MIS Quarterly* 11, no. 3: 369–86.

Benner, M.J., and F.M. Veloso. 2008. ISO 9000 practices and financial performance: A technology coherence perspective. *Journal of Operations Management* 26, no. 5: 611–29.

Bojanc, R., and B. Jerman-Blazic. 2008. An economic modelling approach to information security risk management. *International Journal of Information Management* 28, no. 5: 413–22.

Burrows, G.R., D.L. Drummond, and M.G. Martinsons. 2005. Knowledge management in China. *Communications of the ACM* 48, no. 4: 73–6.

Chen, L. 2010. Business-IT alignment maturity of companies in China. *Information & Management* 47, no. 1: 9–16.

Davis, F.D. 1989. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly* 13, no. 3: 319–40.

Ezingeard, J.N., and D. Birchall. Information security standards: Adoption drivers – what drives organisations to seek accreditation? The case of BS 7799–2: 2002, *Security management, integrity, and internal control in information systems, Book series: International federation for information processing, vol. 193*, ed. Paul Dowland, Steve Furnell, Bhavani Thuraisingham and X. Sean Wang, 1–20, Joint Working Conference on Security Management, Integrity, and Internal Control in Information Systems, George Mason University Fairfax, VA.

Farn, K.-J., S.-K. Lin, and C.-C. Lo. 2008. A study on e-Taiwan information system security classification and implementation. *Computer Standards & Interfaces* 30, nos. 1–2: 1–7.

Fenz, S., G. Goluch, and A. Ekelhart. 2007. Information security fortification by ontological mapping of the ISO/IEC 27001 standard, *13th Pacific Rim International Symposium on Dependable Computing, Proceedings*, 17–19 December, 381–388. Melbourne, Australia.

Franceschini, F., M. Galetto, and P. Cecconi. 2006. A worldwide analysis of ISO 9000 diffusion – considerations and future development. *Benchmarking: An International Journal* 13, no. 4: 523–41.

Hofstede, G. 1984. Cultural and management development. *Asian Pacific Journal of Management* 1, no. 1.

Huang, S.-H., and C.-L. Lee. 2006. Balancing performance measures for information security management. A balanced scorecard framework. *Industrial Management and Data Systems* 106, no. 2: 242–55.

ISACA. 2005. *Information security harmonisation. Classification of global guidance.* Illinois, USA: Information Systems Audit and Control Association.

ISO. 2010. *The ISO survey of certifications 2009.* Geneva: ISO Central Secretariat.

ITGI. 2001. *Information security governance: Guidance for boards of directors and executive management.* IL, USA: IT Governance Institute – Information Systems Audit and Control Foundation.

Jung, B., I. Han, and S. Lee. 2001. Security threats to Internet: A Korean multi-industry investigation. *Information and Management* 38, no. 8: 487–98.

Karabacak, B., and I. Sogukpinar. 2006. A quantitative method for ISO 17799 gap analysis. *Computers & Security* 25, no. 6: 413–9.

Kotulic, A.G., and J.G. Clark. 2004. Why there aren't more information security research studies. *Information & Management* 41, no. 5: 597–607.

Lai, Y.-P., and R.-H. Dai. 2009. The implementation guidance for practicing network isolation by referring to ISO-17799 standard. *Computer Standards & Interfaces* 31, no. 4: 748–56.

Lippert, S.K., and C.G. Govindarajulu. 2006. Technological, organizational, and environmental antecedents to web services adoption. *Communications of the IIMA* 6, no. 1: 146–58.

Martinsons, M.G. 2008. Relationship-based e-commerce: Theory and evidence from China. *Information Systems Journal* 18, no. 4: 331–55.

Martinsons, M.G., and R. Westwood. 1997. Management information systems in the Chinese business culture: An explanatory theory. *Information & Management* 32, no. 5: 215–28.

Martinsons, M.G., R.M. Davison, and V. Martinsons. 2009. How culture influences IT-enabled organizational change and information systems. *Communications of the ACM* 52, no. 4: 118–23.

Miles, M.B., and A.M. Huberman. 1994. *Qualitative data analysis.* 2nd edition. Thousand Oaks, CA: Sage.

Mueller, F. 1994. Societal effect, organizational effect and globalization. *Organization Studies* 15, no. 3: 407–28.

Neubauer, T., A. Ekelhart, and S. Fenz. 2008. Interactive selection of ISO 27001 controls under multiple objectives, Proceedings of the IFIP TC 11/23rd International Information Security Conference, 477–491, 2008. 23rd International Information Security Conference held at the 20th World Computer.

Qi, J., L. Li, Y. Li, and H. Shu. 2009. An extension of technology acceptance model analysis of the adoption of mobile data services in China. *Systems Research and Behavioral Science* 26, no. 3: 391–407.

Sampaio, P., P. Saraiva, and Guimaraes Rodrigues. 2009. ISO 9001 certification research: Questions, answers and approaches. *International Journal of Quality & Reliability Management* 26, no. 1: 38–58.

Shangguan, X., and Y. Xu. 2008. Research on information security management standards of abroad and domestic. *Information Technology & Standardization*, (In Chinese.) 5: 12–6.

Sondergaard, M. 1994. Research note: Hofstede's consequences: A study of reviews, citations and replications. *Organizational Studies* 15, no. 3: 447–56.

Spears, J.L., and R.J. Cole. 2006. A preliminary investigation of the impact of the Sarbanes–Oxley Act on information security, *Proceedings of the 39th Hawaii International Conference on System Sciences.*

Srite, M., and E. Karahanna. 2006. The role of espoused national cultural values in technology acceptance. *MIS Quarterly* 30, no. 3.

Tian, J., K. Wang, Y. Chen, and B. Johansson. 2010. From IT deployment capabilities to competitive advantage: An exploratory study in China. *Information Systems Frontiers* 12: 239–55.

Tong, J., and A. Mitra. 2009. Chinese cultural influences on knowledge management practice. *Journal of Knowledge Management* 13, no. 2: 49–62.

Venkatesh, V., and X. Zhang. 2010. Unified theory of acceptance and use of technology: US vs. China. *Journal of Global Information Technology Management* 13, no. 1.

Wu, Z., L. Wang, and X. Shangguan. 2006. Summary and development analysis on information security management standards of China. *Netinfo Security*, (In Chinese) 6: 17–9.

Yeh, Q.-J., and A.J.-T. Chang. 2007. Threats and countermeasures for information system security: A cross-industry study. *Information & Management* 44, no. 5: 480–91.

Yin, R.K. 2009. *Case study research: Design and methods*. Applied Social Research Methods Series: p. 4. th ed. XVI, 219. Thousand Oaks, CA: Sage.

Zhang, X., and L.M. Maruping. 2008. Household technology adoption in a global marketplace: Incorporating the role of espoused cultural values. *Information Systems Frontiers* 10, no. 4.