Journal of Accounting, Finance, Economics, and Social Sciences
Vol 6, No 1, January – June 2021, pp. 9-17
Received: Jan 2021 | Revised: Mar 2021 | Accepted: Jun 2021
DOI: https://doi.org/10.62458/jafess.160224.6(1)9-17

Information Security Management Systems - Evolving Landscape & ISO 27001: An Empirical Study

Anil K. Makhija*

ABSTRACT

Information technology has become an integral part of all business activities. Managing information security has been a key aspect in ensuring that increased information security risks (due to reliance on IT) are managed effectively. The reliance on digital and technology platforms has increased even further due to pandemic driven changes. This has led to higher information security risk exposure of organizations and their employees and their customers. Organizations use various frameworks to design and implement information security management systems, with ISO 27001 standard being the leading framework. Past researches in ISMS and leveraging ISO 27001 have had limitation of single country focus, Further there is limited research on relevance of ISO 27001 in evolving paradigm of computing shift. This global research presents an empirical study, based on inputs from industry practitioners, reflecting the key drivers for ISO 27001 implementation and certification, investigates pattern in those drivers based on size of the organization and examines the relevance of ISO 27001 both as framework and / or certification in the evolving scenario of cloud. Findings of the research indicate that the top reason for ISO 27001 implementation and certification is "compliance", followed by "business value", "competitive edge", and "breach reduction" in that order. Findings also indicate that focus on information security is increasing and ISO 27001 implementation provides an effective ISMS and ISO 27001 certification helps organizations in improving their trustworthiness in keeping information secure.

Keywords: Information system, security, management system, information technology

INTRODUCTION

Technology has helped businesses improve their operational efficiencies and effectiveness and it has also created global business opportunities for them. Businesses are operating across the globe in a hyper-connected world, thanks to technological advances. Information is thus crossing boundaries across the systems, organizations, and geographies. The focus on keeping information secure has also increased. Part of this increased focus can be attributed to increased awareness and a significant part is due to increases in fraud and damages that happen as a result of information security breaches. Focus of industry has been to create frameworks that will help keeping information secure, implementing them, and getting an independent validation of their information security practices through a certification, such as ISO 27001. Reliance on technology has increased in pandemic times and there have been increase in instances of information security breaches. Corporate managers are therefore focused on providing assurances to their customers that in this time of increased information security threat, they do have effective mechanisms to keep information safe and secure. This research investigates the relevance and effectiveness of ISO 27001, both as a framework as well as certification, in the context of increased digital reliance and shift to cloud, as perceived by practitioners, clients of information technology service providers, and information security auditors. Practitioners, clients of information technology service providers, and information security auditors were interviewed through a survey questionnaire. They were interviewed about main drivers for implementing ISO 27001 and ISO 27001 certification, shift in focus on information security, and effectiveness of ISO 27001 as a framework and as a certification. Rest of this document provides background on shifting focus in information security domain, evolution of ISO 27001, research on ISO 27001 and its limitations leading to formulation of research objective, followed by research methodology, analysis and conclusion including recommendation to ISO body.

* Anil K. Makhija, MBA. Associate Professor, CamEd Business School
Email: anil@cam-ed.com

LITERATURE REVIEW

Increased reliance on technology and cloud shift

Information Technology revolution has accelerated in recent times, due to rapid technological advances. It has created a society in which most of the organizations, are digital and connected over the internet. Technology pervasiveness has led to creation of new business models and is leading to their ongoing refinements. Technology has also helped increase efficiency of operations, reduce the cost of operations, and helped increase the levels of customer engagement (Şahin & Topal, 2018).

Rapid advances in processing technologies and storage technologies have made computing resources cheaper and more powerful. This development has further enabled a new paradigm known as cloud computing. Cloud computing has lowered the digital entry barrier even for the smaller organizations, due to pay-as-you-go model, resulting in more widespread adoption of technologies and making technology an integral part of every business (Avram, 2014).

Cloud computing has many advantages but it does create some additional security challenges. Cloud computing requires data to be stored outside the enterprise, and hence creates need for additional information security measures in addition to the traditional measures to minimize data breaches that can happen due to security vulnerabilities (Kumar et al., 2018).

Information security risks & ISMS

These technological advances have also made organizations more vulnerable to various types of information security threats. Threats emanate from both internal sources as well as external sources, and the resulting security breaches cause both financial and reputation damages. Many a times, these breaches also reduce the revenue growth rate of the organizations. The need to focus on information security is higher than ever before. Even novice attacker with lesser technical ability are in a position to launch attacks easily (Freeman, 2007; Jouini et al., 2014).

Initial approaches to information security issues were to deal with them in purely technical context. However, the information security threats are now emanating from multiple channels. This new landscape of threats creates a need to address information security issues more in the context of an overall management system and not just technical context (Soomro et al., 2016).

Information assets of organizations need to be protected by using a systemic approach. It shall involve a set of policies, processes, people and associated controls to manage and protect organization's information and its customer's information. Such management systems are called Information Security Management System. Such information security management systems or ISMS help organizations protect their information assets in holistic manner. If designed and implemented properly, such systems enable managing information security risks at enterprise level.

Information Security Management System shall be based on core principles of CIA or Confidentiality, Integrity and Availability. Confidentiality implies that the information is not disclosed or made available to individuals, entities or processes unless they are authorized to receive it. Integrity implies information assets are protected from unauthorized changes so that they are reliable and correct and complete. Availability implies that authorized users have access to the information assets when they need. Information security requirements, around CIA, are input to an information security management system (ISMS). ISMS produces a set of information security outcomes that meet the requirements and expectations that are taken by it as inputs. These outputs are accomplished through a set of actions and procedures, which are governed by policies, processes and controls. (Asosheh et al., 2013).

Information Security Management Systems (ISMS) need to take a holistic approach towards managing information security. Model of information security needs to be more of value-based compliance model and not just control-based compliance model. Users' involvement and participation in the design and implementation of information security controls, combined with incorporation of user's feedback in improving ISMS are key foundations of a value-based compliance approach (Hedström et al., 2011).

Managing information security requires due diligence to know the risks and manage them to protect company's information assets. Thorough due diligence is an important first step in identifying the information security risks. An effective system of information security controls shall be implemented to manage the information security risks identified through due diligence. Organizations need to ensure that both the design and the implementation of information security controls is effective. Regular monitoring and reviews help assess the controls design and controls implementation (operating) effectiveness. Information security controls shall be improved, both from the design perspective and from the implementation approach perspective, in alignment with continuous improvement philosophy. Information security is everyone's responsibility within an organization. Overall company policy and direction for information security shall be set by Board of Directors. They should also ensure that adequate resources are provided for and are available for implementation of information security practices. Board's direction on information security shall be enforced by senior management and they shall provide additional support as necessary. All units and functions within the organization shall make information security practices as part of their day-to-day work. Effective implementation of information security practices requires involvement of all levels of the organization. This approach creates a comprehensive framework for an information security management system (ISMS) (Humphreys, 2008).

There is no denying to the fact that lack of an effective information security management system increases probability of security breach. Security breaches affect both bottom line of businesses and also may lead to brand switching. There is direct financial implication as well of information security breaches. The 2013 information security breach at Target, which involved release of millions of customers credit card and debit card information, eventually required Target to pay $10 million to settle the resulting class-action lawsuit. In addition to this $ 10 million, target revamped its information security practices that costed Target $ 162 million. Target saw a drop of 5.3% in sales and a drop of 46% in profit in Q4 of 2013, following the information security breach. Such security breaches create perception issues not just about the company that experiences the breach but about the industry in general (Jeong et al., 2018).

Evolution of ISO 27001

Over the last 30 years, many industry standards have been rolled out to help IT Governance. Most of them contain elements to help organizations address IT security and Information Security. The most popular ones related to information security are ISO 27001, BS7799, PCI-DSS, ITIL and COBIT (Susanto et al., 2012).

In early 1990s, UK government launched an initiative to document the information security best practices and make them available to industry. This led to creation of BS 7799-1 in 1995 and release of BS 7799-2 (titled ISMS Specifications) in 1997. A certification scheme was also developed to be used along with BS 7799-2. In year 2000, BS 7799-1 (Code of practice for information security management) was approved for publication as ISO/IEC 17799. BS 7799-2 was published as ISO/IEC 27001, the flagship of ISO/IEC 2700x family. ISO/IEC 17799 was later renumbered as ISO/IEC 27002 in 2006. Further, all other standard in ISO/IEC 2700x family provide support and guidance for implementation of ISO/IEC 27001. ISO/IEC 27001 processes are based on the Plan-Do-Check-Act (PDCA) model (Humphreys, 2011).

ISO 27001 is one of the key standards in the domain of information security. ISO 27001 standard was first published in 2005. This standard describes the requirements that must be fulfilled by an ISMS. ISO 27002 standard provides the implementation guidelines for implementing the practices detailed in ISO 27001. ISO 27001 standard details out the requirements for planning, implementing, operating, continuously monitoring and improving the ISMS, in alignment with the PDCA approach (Figure 1)

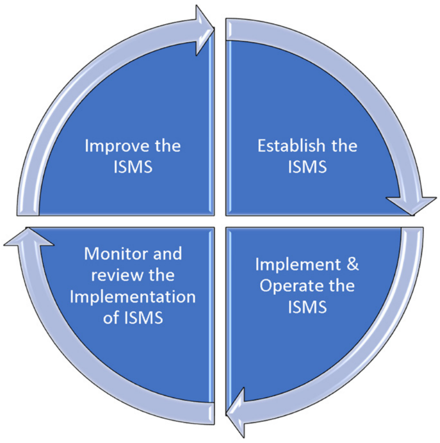
Improve the ISMS
Establish the ISMS
Monitor and review the Implementation of ISMS
Implement & Operate the ISMS

Figure 1

The various steps involved in this approach of ISO 27001 driven ISMS can be detailed out as following:

- Establish the ISMS
  - ◊ Identify the information assets
  - ◊ Identify the security requirements of all the information assets
  - ◊ Assess the information security risks
  - ◊ Identify and design the relevant controls needed to manage the information security risks

- Implement and Operate the ISMS
  - ◊ Implement the designed controls
  - ◊ Manage the operations

- Monitor and Review the implementation of ISMS
  - ◊ Monitor the implementation of ISMS controls
  - ◊ Review and assess the performance of ISMS, covering both the design of controls and the implementation of the controls

- Improve the ISMS
  - ◊ Initiate correction, corrective action and preventive action in case of non-compliance
  - ◊ Re-design the controls as necessary

Implementing an ISMS in alignment with ISO 27001 standard requires defining the coverage and scope of ISMS. The next step involves identification and assessment of risks, followed by defining necessary information security control objectives and control activities/measures. The annexure A of the ISO 27001 standard lists total of 39 control objectives and 134 control measures necessary for implementation of ISO 27001. ISO 27001 standard also highlights the need of adequate training in order to implement the information security controls. The standard also highlights that creating awareness about the need of those information security controls is also an important component of overall implementation plan. ISO 27001 Standard requires continuous monitoring with the defined procedures to measure compliance and improve the efficiency and effectiveness of the ISMS continuously. The standard also details out ISMS documentation requirements, the responsibilities of the top management, and the need of internal auditing as part of effective implementation. Few researchers have also suggested that implementing ISO 27001 in an integrated approach along with ISO 9001 would lead to efficient implementation (Disterer, 2013; Wang & Tsai, 2009).

ISO 27001 Drivers, Benefits, and Challenges

According to an analysis of ISO 27001 Global Report (Woollven, 2018), which was based on interviews of 128 ISMS implementation professionals around the world,

Top five drivers for ISO 27001 implementation:

- Improving information security posture
- Gain in competitive advantage
- Legal and regulatory compliance
- Alignment with information security best practices
- GDPR compliance

Top five benefits of ISO 27001 implementation:

- Improved information security
- Improvement in internal processes
- Higher levels of information security awareness
- Better company image
- New business opportunities.

Main challenges in ISO 27001 implementation:

- Lower staff awareness
- Lack of competence and expertise
- Lack of understanding about the requirements of the standard
- Budgetary constraints
- Not conducting information security risk assessment

ISO 27001 implementation landscape status summary as per the respondents is as follows:

- More than 72% of the respondents acknowledged that their customers have enquired about ISO 27001 status in last 12 months, with 40% mentioning that it was a regular contracting and tendering requirement.
- Majority of the respondents (61%) put the duration of ISO 27001 implementation project in 6 to 12 months range.
- Approximately 52% of the respondents pegged Implementation cost (excluding certification fee) in $ 6,600 to $ 26,500 range.
- Approximately 50% of overall respondents mentioned that ISO 27001 certification journey is an investment that is fully justified by its benefits.
- Majority of respondents (83%) mentioned that they have implemented incident response and business continuity management programs to respond to and recover from cyber- attacks.

Research on ISO 27001 and their limitations

A research, based on empirical study of 111 organizations, listed on NYSE and NASDAQ, over a period of 10 years, indicates that there was positive stock market reaction to the announcement of an organization achieving ISO 27001 certification. It reflects that market places significant value upon the organizational commitment to information security. Further, there have been researches that indicate that smaller organizations, categorized as smaller based on market capitalization, experience greater positive abnormal returns than larger firms, in response to their ISO 27001 announcements. Hence the overall benefit of ISO 27001 is higher for the smaller organizations, compared to the larger organizations. This empirical study also indicates that quantum of positive return is higher for the ISO 27001 announcements made after 2013, reflecting increased focus on information security. This research identifies the limitation that the empirical study was conducted with single country focus (Deane et al., 2019).

Cost of information security and investment in information security practices has been under a significant scrutiny. Combinatorial optimization of KPIs of efficiency and effectiveness were proposed as an approach towards evaluating investment in information security programs (Boehmer, 2009). Studies have also indicated that the time it takes to implement information security practices, such as those related to ISO 27001 framework, takes time. This cycle time from starting the journey of implementing information security management system (ISMS) to becoming certification ready makes it challenging to get this agenda as a top priority item on senior management table (Everett, 2011). Research on barriers to implementing ISO 27001 identified that adoption of ISO 27001 has been slow. This slow adoption has been attributed to approach being complex and costly to many organizations, especially small organizations (Gillies, 2011). Another research, though with a limited geographic scope identified the lack of availability of skilled resources and high market demand of such resources as reason for lower adoption of ISO 27001,

suggesting that barriers are more due to capability constraints and not due to limited business value perspective (Alshitri & Abanumy, 2014). Researchers have also indicated that implementing information security management system is difficult due to lack of documentation and recommended leveraging security requirements engineering to support ISO 27001 (Beckers et al.,2012).

A study on benefits of ISO 27001 in American and European companies did not find any evidence on benefit of ISO 27001 on the financial and stock performance of the organizations. This study concluded that ISO 27001 is seen more as a compliance requirement / obligation instead of competitive advantage (Hsu et al., 2016). However, in recent times, with the shift towards cloud computing and improvements done in ISO 27001 implementation practices, it is something that shall be evaluated again in the current context.

A study on effect of data breach announcements on customer behavior indicated 32.45% decrease in customer spending over a period of 7 months and customer migrated to non-breached channel post the data breach announcement. The study identifies the need to address the customers/perception of data vulnerability. The study identifies the importance of trust building initiatives post any information security breach (Janakiraman et al., 2018).

A recent study identifies that there is lack of specific guidelines for required security behavior in widely adopted standards, including ISO 27001, and that causes difficulties in effective implementation of ISO 27001 and realization of full business benefits that ISO 27001 can provide (Topa & Karyda, 2019).

RESEARCH OBJECTIVES

Covid-19 pandemic has created a need for organizations to digitalize their service delivery and stakeholder relationship management models. This has led to further increase in the technology risks faced by organizations. Organizations, especially SMEs, need to increase their focus on managing technology risks. Organizations shall utilize publicly available frameworks to understand information risks and associated mitigation controls (Lanz & Sussman, 2020).

Information security risks have increased in general with time, and even further due to increased technology reliance due to digital shift in pandemic times. This research aims to correlate the emerging need to address the information security risks with the industry leading information security certification of ISO 27001. This research aims to focus on gathering sample data from multiple countries across the globe, to address the limitations of single country focus highlighted in the previous researches. Data has been gathered from Information Technology, Information Security Professionals and from Consumers of Information Services (client organizations) and analyzes and evaluates following aspects:

(1) What are the top drivers for the organizations across the globe to implement Information Security Management Systems?

(2) Is there any shift/pattern in the drivers (for implementing ISMS) depending on the size (measured in terms of headcount or role or both) of the organization?

(3) Is ISO 27001 Certification perceived as an effective framework and/or certification to manage information security risks, especially in the context of shift towards cloud computing?

METHODOLOGY

This research aims to get an industry perceptive (from the practitioners and the auditors) about the top business reasons or drivers which are causing organizations to implement information security management systems, especially in alignment with ISO 27001 practices and guidelines. This research will also establish if there is a pattern or trend in the drivers based on the role of respondents (role group) in the organization. The research will also find out how relevant ISO 27001 certification is perceived in the context of computing now-a-days predominantly shifting to cloud.

A survey questionnaire was designed to understand the following dimensions:

- Number of security incidents/breaches – whether they are increasing or decreasing or no change
- Demand/Requirements for ISO 27001 from clients- whether they are asking for it or now
- Does ISO 27001 certification help in creating a positive image for the organization in its ability to manage information security risks
- Does ISO 27001 certification journey help in establishing an effective Information Security Management System
- Top business drivers / reasons for organizations to pursue ISO 27001 implementation and certification journey

Information Technology and Services companies and outsourcing services providers, client organizations outsourcing their development and maintenance activities, auditing companies that are involved ISO 27001 gap assessment and certification (Certifying Bodies – CBs) are in the scope of the survey. In service provider organizations, professionals working in delivery and operations function, sales and business development functions, and information security implementation team were reached out. In client organizations, persons primarily involved with vendor management function and delivery recipient teams were reached out. In certifying bodies, lead auditors involved in gap assessment and ISO 27001 certification were reached out. Survey responses were captured during on-call interview for around 88% of the respondents. Remaining provided their responses offline at a later date after getting an overview of the questionnaire and context.

From a total of 120 persons that were reached out, 102 provided their responses to the survey questionnaire. Remaining did not respond to the survey, citing a diverse set of reasons. Table 1 demonstrates the coverage of multiple roles and teams that responded to the survey questionnaire.

Table 1: Role / Team Distribution – Survey Respondents

Role / Team	# Responses	% Responses
Information Security Auditor	21	20.6%
Other	4	3.9%
Client Teams	26	25.5%
Service Provider Teams	51	50.0%
Total	102	100.0%

RESULTS ANALYSIS

Analysis of survey responses indicates that “compliance reasons” are the biggest driver for ISO 27001 implementation and certification, with a total of 78.4% indicating it as one of the reasons for their ISO 27001 implementation and certification journey. The second important driver for ISO 27001 implementation and certification is “business value”. The relative ranking of “compliance reasons” being the topmost, followed by “business value”, followed by “competitive edge” followed by “breach reduction” is same across all the roles that responded to the survey and same across different categories of the organization size. The details of these trends and respective numbers are shown in Table 2 and Table 3.

Table 2: Drivers for ISO 27001 Implementation/ Certification – Role Wise Summary

Drivers for ISO 27001 Implementation / Certification				
	Compliance	Competitive	Breach	Business
Role	Reasons	Edge	Reduction	Value
Client Teams	73.1%	11.5%	3.8%	38.5%
Information Security Auditor	71.4%	61.9%	38.1%	76.2%
Other	75.0%	25.0%	0.0%	0.0%
Service Provider Teams	84.3%	15.7%	19.6%	49.0%
Total	78.4%	24.5%	18.6%	50.0%

Table 3: Drivers for ISO 27001 Implementation/ Certification – Organization Size (Headcount) Wise Summary

Drivers for ISO 27001 Implementation / Certification				
Organization Size- Headcount	Compliance	Competitive	Breach	Business
	Reasons	Edge	Reduction	Value
10,000 or more	72.5%	25.0%	20.0%	57.5%
2000 to less than 10,000	83.3%	25.0%	18.8%	50.0%
500 to less than 2,000	66.7%	22.2%	11.1%	22.2%
Less than 500	100.0%	20.0%	20.0%	40.0%
Total	78.4%	24.5%	18.6%	50.0%

There is a clear agreement on increasing focus on information security. Overall, 89.2% of the survey respondents mentioned that the focus on information security is increasing (59.8%) or is significantly increasing (29.4%). Further, 75.5% of the survey respondents agreed (53.9%) or strongly agreed (21.6%) that ISO 27001 implementation and certification helps in managing information security risks effectively. A total of 64.7% survey respondents agreed (46.1%) or strongly agreed (18.6%) that ISO 27001 certification helps improve trustworthiness of organization in managing information security risks. The details of these trends and respective numbers are shown in Table 4, Table 5 and Table 6.

Table 4: Focus on Information Security – Role Wise Summary

Focus on Information Security				
				Significantly
Role / Team	Decreasing	No Change	Increasing	Increasing
Client Teams	0.0%	11.5%	88.5%	0.0%
Information Security Auditor	0.0%	4.8%	38.1%	57.1%
Other	25.0%	25.0%	50.0%	0.0%
Service Provider Teams	0.0%	9.8%	54.9%	35.3%
Total	1.0%	9.8%	59.8%	29.4%

Table 5: Perceived effectiveness of ISO 27001 in managing Information Security Risks – Role Wise Summary

ISO 27001 Helps in Managing Information Security Risks				
		Neither agree,		Strongly
Role / Team	Disagree	nor disagree	Agree	Agree
Client Teams	7.7%	23.1%	69.2%	0.0%
Information Security Auditor	4.8%	0.0%	33.3%	61.9%
Other	50.0%	50.0%	0.0%	0.0%
Service Provider Teams	5.9%	17.6%	58.8%	17.6%
Total	7.8%	16.7%	53.9%	21.6%

Table 6: Perceived Trustworthiness of ISO 27001 in managing Information Security Risks– Role Wise Summary

ISO 27001 Certification increases Trustworthiness of organization in Managing Information Security Risks				
		Neither agree,		Strongly
Role / Team	Disagree	nor disagree	Agree	Agree
Client Teams	15.4%	30.8%	53.8%	0.0%
Information Security Auditor	4.8%	9.5%	33.3%	52.4%
Other	25.0%	50.0%	25.0%	0.0%
Service Provider Teams	9.8%	25.5%	49.0%	15.7%
Total	10.8%	24.5%	46.1%	18.6%

CONCLUSION

Information security is an important focus area for the organizations. With globalization, lot of organizations have been outsourcing their work to a third-party provider (outsourcing service provider). Information security is one of the key concerns when the work is outsourced or even otherwise. Service provider organizations are expected to keep information of their clients (and of their customers) safe and secure. Many clients have been asking their service provider to demonstrate that they have an effective Information Security Management System (ISMS) in place and many a times, they are directly asking for ISO 27001 certification. Many service provider organizations also believe that having an ISO 27001 certification helps them gain a competitive edge and also provides them business value. This has resulted in many organizations (service providers) implementing ISO 27001 practices and creating an Information Security Management System (ISMS) derived from ISO 27001 framework and then going for an ISO 27001 certification provided by independent certifying bodies (CBs). “Compliance reasons” are believed to be the topmost driver for implementing ISO 27001, followed by “business value”, followed by “competitive edge”, followed by “breach reduction”. This rank order of business driver is similar irrespective of the role of respondents and size of the organization.

Research indicates that focus on information security is increasing. One of the interesting finding from the research was that while the client organizations (service recipients) and provider organizations (service providers) were mostly tending to suggest that focus on information security is increasing, majority of information security auditors were of the opinion that the focus on information security is significantly increasing.

On whether ISO 27001 implementation and certification provides an effective Information Security Management System (ISMS), there was high level of agreement (with a total of 75.5%). On whether ISO 27001 implementation/certification increases trustworthiness of the organization in managing information security risks, there was agreement on that too (with a total of 64.7%), though this number was lesser than ability of ISO 27001 to provide an effective ISMS. Raw data was analyzed statistically to see if this difference was statistically significant. However, this was not significantly different.

It can be concluded based on the research that ISO 27001 implementation and certification provides an effective information security management system (ISMS). ISO 27001 is considered relevant, even in the current changing trend of cloud computing by professionals both in provider organizations as well as recipient organizations, and also by information security audit professionals. Compliance is the topmost driver, followed by business value in terms of implementing ISO 27001 and its certification.

From an action standpoint, ISO (International Organization for Standardization) as well as certifying bodies need to evaluate as to how they can better articulate and socialize the “business value” of ISO 27001 for the organizations as current perception is more of compliance benefits.

Limitations & Future Research Suggestions

One of the limitations of this research was that survey respondents in the research from service provider organization consisting of both delivery personnel (those responsible for creation and maintenance of software / services) as well as sales and business development personnel (who are more of client touch points) were categorized into a common pool of “service provider teams”. In future research, it would be recommended to categorize them into separate pools since it was observed that both these set of personnel had difference in their opinion and ratings and hence researching them into separate pools could provide additional insights.

An additional limiting factor for the research was that Latin America was the least represented geography in the survey respondents. Participation from all other continents namely APAC, EMEA, North America & Canada was consistent.

REFERENCES

Alshitri, K. I., & Abanumy, A. N. (2014). Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia. 2014 International Conference on Information Science & Applications (ICISA). doi:10.1109/icisa.2014.6847396

Asosheh, A., Hajinazari, P., & Khodkari, H. (2013). A practical implementation of ISMS. 7th International Conference on e-Commerce in Developing Countries: with Focus on e- Security. doi:10.1109/ecdc.2013.6556730

Avram, M. G. (2014). Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective. *Procedia Technology,* 12, 529–534. doi:10.1016/j.protcy.2013.12.525

Beckers, K., Fassbender, S., Heisel, M., & Schmidt, H. (2012). Using Security Requirements Engineering Approaches to Support ISO 27001 Information Security Management Systems Development and Documentation. 2012 Seventh International Conference on Availability, Reliability and Security. doi:10.1109/ares.2012.35

Boehmer, W. (2009). Cost-Benefit Trade-Off Analysis of an ISMS Based on ISO 27001.2009 International Conference on Availability, Reliability and Security. doi:10. 1109/ares.2009. 128

Deane, J. K., Goldberg, D. M., Rakes, T. R., & Rees, L. P. (2019). The effect of information security certification announcements on the market value of the firm. *Information Technology and Management*. doi:10.1007/s10799-018-00297-3

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security,* 04(02), 92–100. doi:10.4236/jis.2013.42011

Everett, C. (2011). Is ISO 27001 worth it? Computer Fraud & Security, 2011(1), 5–7. doi:10.1016/s1361-3723(11)70005-7

Freeman, E. H. (2007). Holistic Information Security: ISO 27001 and Due Care. *Information Systems Security,* 16(5), 291–294. doi:10.1080/10658980701746478

Gillies, A. (2011). Improving the quality of information security management systems with ISO27000. *The TQM Journal,* 23(4), 367–376. doi:10.1108/17542731111139455

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. P. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems,* 20(4), 373–384. doi:10.1016/j.jsis.2011.06.001

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. 2016 49th Hawaii International Conference on System Sciences (HICSS). doi:10.1109/hicss.2016.600

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report,* 13(4), 247–255. doi:10.1016/j.istr.2008.10.010

Humphreys, E. (2011). Information security management system standards. *Datenschutz Und Datensicherheit - DuD,* 35(1), 7–11. doi:10.1007/s11623-011-0004-3

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The Effect of a Data Breach Announcement on Customer Behavior: Evidence from a Multichannel Retailer. *Journal of Marketing,* 82(2), 85–105. doi:10.1509/jm.16.0124

Jeong, C. Y., Lee, S.-Y. T., & Jee-Hae. (2018). Information Security Breaches and IT Security Investments: Impacts on Competitors. Information & Management. doi:10.1016/j.im. 2018.11.003

Jouini, M., Rabai, L. B. A., & Aissa, A. B. (2014). Classification of Security Threats in Information Systems. *Procedia Computer Science,*32,489–496. doi:10.1016/j.procs.2014.05.452

Kumar, P. R., Raj, P. H., & Jelciana, P. (2018). Exploring Data Security Issues and Solutions in Cloud Computing. *Procedia Computer Science, 125*, 691–697. doi:10.1016/j.procs.2017.12.089

Lanz, J., & Sussman, B. I. (2020). Information Security Program Management in a COVID-19 World. *The CPA Journal, 90*(6), 28–35

ŞAHİN, H., TOPAL, B. (2018). Impact of Information Technology on Business Performance: Integrated Structural Equation Modeling and Artificial Neural Network Approach. *Scientia Iranica,* 25(3), 1272-1280. doi: 10.24200/sci.2018.20526

Shojaie, B., Federrath, H., & Saberi, I. (2015). The Effects of Cultural Dimensions on the Development of an ISMS Based on the ISO 27001. 2015 10th International Conference on Availability, Reliability and Security. doi:10.1109/ares.2015.25

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management, 36*(2), 215–225. doi:10.1016/j.ijinfomgt.2015.11.009

Topa, I., & Karyda, M. (2019). From theory to practice: guidelines for enhancing information security management. Information and Computer Security. doi:10.1108/ics-09-2018-0108

Wang, C.-H., & Tsai, D.-R. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. 43rd Annual 2009 International Carnahan Conference on Security Technology. doi:10.1109/ccst.2009.5335527

Woollven, C., (2018). ISO 27001 Global Report 2018: top 3 key takeaways - IT Governance UK Blog. [online] IT Governance UK Blog. Available at: <https://www.itgovernance.co.uk/blog/iso-27001-global-report-2018-top-3-key- takeaways> [Accessed 5 March 2021].