American Journal of Industrial and Business Management, 2022, 12, 934-954
https://www.scirp.org/journal/ajibm
ISSN Online: 2164-5175
ISSN Print: 2164-5167

Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding

Syed Asad Abbas Bokhari[1], Shahid Manzoor[2]

[1]Center of Security Convergence & e-Governance, Inha University, Incheon, Korea
[2]Graduate School of Business Administration, Ajou University, Suwon, Republic of Korea
Email: *asad.bokhari@inha.edu, shahidahmadkhan@ajou.ac.kr

How to cite this paper: Bokhari, S. A. A., & Manzoor, S. (2022). Impact of Information Security Management System on Firm Financial Performance: Perspective of Corporate Reputation and Branding. *American Journal of Industrial and Business Management, 12,* 934-954.
https://doi.org/10.4236/ajibm.2022.125048

Received: April 25, 2022
Accepted: May 23, 2022
Published: May 26, 2022

Abstract

The immense organizational emphasis on information technology (IT), combined with the growing impact of information security issues, has inflated information security to the top list of management's priorities. The ISO 27001 standard defines the requirements for an effective information security management system (ISMS). However, the implementation of ISMS not only maximizes firm performance directly, but it can also have a significant impact in different contexts. We investigated whether ISMS implementation can benefit organizations financially by contributing to corporate reputation and branding in this study. With samples from 171 Pakistani firms, we examined firm performance after ISMS ISO 27001 certification. Compatible with our expectations, we discovered strong evidence that ISMS implementation benefited certified firms in terms of high corporate reputation, brand and branding, and financial performance.

Keywords

Information Security Management System (ISMS), ISO 27001, Corporate Reputation, Brand and Branding, Firm Performance

1. Introduction

Information security management system (ISMS) has emerged as a contentious topic not only in information security but also in information management (Eloff & Von Solms, 2000; Susanto et al., 2011). Contemporary manufacturing, financial, and services providing institutions are integrating intrinsic diverse work-

force, physical assets, and process management with governance strategies and objectives for providing a competitive advantage for their business, as well as investing significant resources in developing and operating information systems to support the preceding operation. Firms increase overall productivity by sharing information through such informatization, but there are adverse effects that occur simultaneously, such as provoking a new criminal activity consisting of information being retrogressed from initially planned objectives or implications (Chang, 2013). Firms often created technical information security mechanisms in the early stages to address the negative impacts of digitization, but their focus is increasingly shifting to management security considering the features of contemporary information breaches. They are constructing information assurance systems comprised of five information protection organizational activities, notably, policy and organizational formation, controlling risks, implementation of programs, and follow-up control, to provide an organization with adequate in-depth information protection systems (Eloff & Von Solms, 2000).

Elevated information security violation situations, including phishing, incursion, and identity theft, have drawn massive attention and emphasized the importance of information security as an administrative problem (Hsu et al., 2016). According to a recent study, overall costs experienced in a single security event have gotten increasingly serious, encompassing direct monetary loss such as operating damages or unfavourable equity market responses (Goel & Shawky, 2009), reputational harm, and professional liability. ISO 27001 is a benchmark that has been produced and implemented by businesses all over the globe to help including Pakistan with the implementation of information security management (Mastoi et al., 2021). This standard was initially published in 1995, and it was amended again in 2005. ISO 27001 is a guideline that outlines a set of principles for implementing a suitable information security management system. ISO 27001 has become the most generally accepted standard for information systems globally. Provided concerns raised about information leakage, accredited of compliance to the ISO 27001 criterion may serve as an excellent presentation, to the community, indicating the manager's assessment of information systems or positive mindset toward information security management. It also demonstrates that an organization's information management adheres to a global standard, making it more credible and reputable.

Numerous academics discovered that the implementation of information security management system has a direct positive impact on firm performance such as operational performance (Hsu et al., 2016), financial performance (Chang, 2013; Wu et al., 2021), productivity performance (Velasco et al., 2018), and performance in IT skills and infrastructure (Tewamba et al., 2019), but only a few scholars have investigated the indirect impact of IT capabilities (Kamdjoug et al., 2018) between information security management system and firm performance. Continuing prior research, this study aims at whether the implementation of ISO 27001 certification advantages a firm in terms of financial performance indirectly

by mediating the role of corporate reputation (Iwu-Egwuonwu, 2010) and brand and branding (Rastogi & von Solms, 2012). We believe that the association between the information security management system (ISO 27001) and firm financial performance depends on contextual or situational factors (Bokhari et al., 2021) so we will investigate the mediating role of corporate reputation and brand and branding between the two constructs among manufacturing, financial, and services firms in Pakistan.

The following is how this paper is structured. Section 2 examines current ISMS literature as well as earlier research on the performance of certification uptake in general. We next construct our theories because of this debate and develop our hypothesis. Section 3 discusses the research methodology, and Section 4 discusses the empirical results. Section 5 concludes with contributions, limitations, and future research directions.

2. Literature Review and Hypothesis Development

2.1. Information Security Management System (ISMS ISO 27001)

Firms are increasingly depending on information security management systems (ISMS) to achieve a competitive advantage in different industries. Information technology has progressed to rely on industrial capacity, and information resources have become a valuable economic resource (Lele & Lihua, 2016). Different sectors have progressively gained the advantage of digital technologies for business efficiency and consolidation; nonetheless, assaults on enterprise information systems are growing more common and diversified (Hung et al., 2019). Invisible vulnerabilities in information security might grow more visible over time, affecting a firm's progress (Moghe et al., 2014; Wu et al., 2021). Inadequate business information security management systems cannot protect against data breaches and can result in damaged property; hence, information security has steadily been a cause of concern (Dao et al., 2017). Existing insurance financing techniques cannot effectively address the specific elements of information security substantial risk of geography, intensity, and perception. In this regard, the ISO 27001 protocol defines a legitimate and functional institutional foundation for the information security sector and is thus a key access point in business information security management (Peng et al., 2019).

The information security management system (ISO-27001) standard's criteria serve to strengthen organizational efficiency and financial growth. Besides that, implementing an ISMS infrastructure can boost consumer confidence, organizational reputation, brand image, and economic growth of the firm (Mukundan & Sai, 2014). According to ISMS ISO 27001 criteria, organizations must ensure that their information security policy and corporate strategy are aligned and that the information security framework is embedded into the business operations (Neubauer et al., 2008). These standards involve not only establishing the functional structure, obligations, and authority of information security management experts but also developing appropriate risk-control strategies and producing ne-

cessary adaptation statements. Concomitantly, these methods allow businesses to reduce computer malware assaults (Calder, 2017). Such enhancements increase consumer loyalty, decrease the cost of information security protocols, and foster a perfect correlation and collaboration among firms (Meixner & Buettner, 2012; Sato et al., 2010).

In contrast, the deployment of an ISO 27001 infrastructure assists businesses in reducing superfluous expenses. Losses incurred by information security vulnerabilities can occasionally be passed on to customers (Han et al., 2017); hence, ensuring information security can give a pricing advantage for a product and service (Wu & Tsai, 2018). Furthermore, the ISMS framework ISO 27001 provides necessary steps to fulfill the criteria of information transmission performance and information document folder accessibility. Such approaches eliminate updated information management expenses and open the door to growth and profitability (Sharma & Dash, 2012). Jannah et al. (2020) discovered that firms may obtain financial benefits after achieving the ISO 9001 certification in an examination of the influence of Quality management systems on enterprise performance. Likewise, several investigations have demonstrated that implementing ISO 14001 accreditation may increase a company's financial performance by causing an attractive economic market reaction (He et al., 2015). Consequently, firms who obtain ISMS certification ISO 27001 ought to anticipate increasing their financial profitability and economic growth, supporting the study's first hypothesis:

Hypothesis 1: *Higher implementation of ISMS ISO* 27001 *in firms has a positive impact on financial performance*

2.2. ISMS ISO 27001, Corporate Reputation, and Firm Financial Performance

Corporate reputation has sparked the interest of academics from a variety of fields (Barnett et al., 2006; Chun, 2005). It is also attracting considerable corporate and information security attention (Nechai et al., 2020). It is undeniable that reputations are rarely addressed unless they are jeopardized. Nevertheless, it is also an issue of definition in part. It is difficult to dispute those corporate reputations are underexplored nowadays. The developments of the previous several years have undoubtedly brought corporate reputations into the mainstream (Arshad et al., 2012).

As people become more conscious about the role of business in society, executives need to deploy ISMS ISO 27001 to fulfill the requirements of various stakeholders in terms of information security management. As firms operate within a framework of diverse stakeholders who can impact it explicitly or implicitly, corporate executives' ability to address social norms is a crucial tool in developing positive connections between the firm numerous stakeholders. From a resource-based viewpoint, implementing ISMS ISO 27001 program allows firms to demonstrate that they are socially responsible and responsive to the concerns of

their stakeholders (Campbell, 2007). Failure to satisfy the needs of different stakeholders can cause support withdrawals, which can harm the organization's brand image and economic survival. This means that numerous stakeholders contribute to the formation of corporate reputation (Fombrun et al., 2015), which in turn results in economic advantages (Iwu-Egwuonwu, 2010). According to Bakar et al. (2015), when firms participate in information security programs ISO 27001 and include them in their annual reports, their corporate reputation improves. These organizations are perceived to have strong corporate values and intangible resources, which might be translated positively in a variety of ways, including attracting more customers, generating investment interest, recruiting the best talent, inspiring employees, bolstering work satisfaction, producing more positive publicity, and accepting positive remarks from financial experts (Laufer & Coombs, 2006).

The majority of modern financial, commerce, services, and commercial enterprises have their smartphone application to target the mass of prospective clients who place online purchases over the phone. Nevertheless, most typical data security solutions are inadequate for mobile applications, and the danger of data leakage is larger than with a computer (Nechai et al., 2020). Despite the use of encryption, John Atkinson demonstrated that smartphone apps can mistakenly disseminate personal information through wireless networks (Atkinson et al., 2018). If an enterprise has an application but does not have an appropriate information security system in place, it may lead to severe difficulties with private information and, consequently, a negative impact on the corporate reputation. Previous studies have shown that one of the most serious threats to information security originates from inside a corporation. Employees' lack of information security skills or understanding of information security policies is major factor in security breaches (Alqahtani, 2017). Many privacy violations continue to be caused by unintentional, purposeful, or malicious human factors, resulting in economic or reputational damage (Ki-Aries & Faily, 2017). Designing an information security policy, adopting ISO 27001, and atomizing procedures with the use of specialized software not only decreases the hazards connected with undetected weaknesses but also improves the operational team's knowledge of the current issue, and increases corporate reputation (Nechai et al., 2020).

Despite prior studies offering a mathematical basis for information security managers to balance the costs and benefits of investment, it is challenging to apply in enterprises (Hausken, 2006). This is primarily because the advantages of information security investment are ambiguous and invisible. Traditionally, information security investments are made neither for income growth nor cost mitigation (Baskerville, 1991). Companies devote resources to information security to deter security threats, and the optimal solution is typical "nothing happens" (Menon & Siponen, 2020) but they are more interested to gain long-term intangible assets such as corporate reputation (Gwebu et al., 2018). The reputation of a corporation is an intangible asset that is difficult for opponents to rep-

licate and maybe effectively transformed into a competitive advantage. The yearly publishing of corporate social responsibility reports by large corporations demonstrates the importance of corporate reputation in their success. Scholars also have discovered that corporate reputations are beneficial to attracting excellent employees and investment on advantageous terms, as well as providing negotiating advantages in general across a variety of stakeholder relationships (Lee & Roh, 2012). These competitive advantages convert corporate reputation into firms' financial performance (Barney, 2001). Following these theories and research, we set our hypothesis as:

***Hypothesis* 2**: *Higher implementation of ISMS ISO* 27001 *in firms has a positive impact on Corporate Reputation*

***Hypothesis* 3**: *Firms with higher corporate reputation enjoy have higher financial performance*

***Hypothesis* 4**: *Corporate Reputation mediates the relationship between ISMS Implementation and financial performance*

2.3. ISMS ISO 27001, Brand and Branding, and Firm Financial Performance

Information security systems are utilized to protect important information from malicious users via electronic means in technological communication. Information security researchers have underlined the necessity for executives to protect information resources from cyber-attacks and security breaches, despite the overwhelming use of information security systems in organizations (Smith et al., 2010). Meanwhile, unauthorized personnel can acquire access to their organization's secret information due to information security flaws. Lack of significance, poor accessibility, inadequate training, and ineffective security are all identified as information system flaws. These characteristics can prohibit a company from achieving its objectives, affect the brand name negatively, and offer high-quality services to stakeholders. In the current competitive environment, corporate governance amplifies public pressure for corporations' integrity in terms of information reporting to meet stakeholders' aspirations. Corporations that do business with a massive public aspect commit to advancing commercial operations that benefit the community in commercial, societal, and environmental ways to create a positive brand image in the society (Martínez et al., 2014). It is found by (He & Lai, 2014) that corporations can achieve their brand and branding by acting in a socially responsible way toward all stakeholders.

Although this may take years to develop a great brand name, it only takes a fraction to tarnish the positive picture by instilling explicitly unfavorable impressions. The ability of information security perceptions to enhance branding, or insecurity perceptions to destruct a brand, is becoming more widely recognized. Nothing, in today's economic and political atmosphere, could harm a brand more than portrayed impressions of insecurity, such as high rates of malicious crimes, the threat of cyber-attacks, or the risk of important information

leakage. Under certain circumstances, nevertheless, we can observe how deliberate promotion of information security, as well as measures to disguise, minimize, or diminish the effect of insecure qualities, can emerge as significant brand and branding using the information security management system ISO 27001 (Coaffee & Van Ham, 2008). A brand is a combination of physical and intellectual characteristics used to generate awareness and recognition, as well as the reputation of goods, services, company, place, or entity. When a corporation achieves a strong brand image through brand awareness, demand's equilibrium price falls, allowing corporations to raise prices and boost profits (Sammut-Bonnici, 2014).

Since the 1960s, numerous scholars have been studying the evolution of branding and how firms might attain brand identity and branding (Choong et al., 2017; Farquhar, 1994; Hampf & Lindberg-Repo, 2011; Holt & Holt, 2004; Kitchin, 2003; Marquardt et al., 1965; Moore & Reid, 2008) and influence of brand and branding on firms' financial performance (Homburg et al., 2010; Park et al., 2013). Previous researchers argued that a brand is first and foremost a relationship among all-important relationships within branding, involving profound emotional connections and loyalty (Kapferer, 2008), it can be viewed as relationship partners, and highlighting how brands are dynamic, realistic, and personalized can help to validate this viewpoint (Fournier, 1998), a company's internal function as a brand creator must be emphasized more, with a focusing on enhancing personnel and staff behavior and attitudes (De Chernatony, 1999), the concept of CSR has become popular not only in all line of industries but also for all corporations to achieve brand and branding (Kitchin, 2003), and firms can achieve high brand and branding by applying information security as their socially responsible obligation and publishing it in their annual reports to share with all relevant stakeholders (Coaffee & Van Ham, 2008).

An information security system is described as corporate policies in connection to the accomplishment of corporate ethics, which encompasses corporate commitments and obligations to society (Yaeger et al., 2015). Information security, according to (Tipton & Krause, 2007), is an extension of corporate ethics and organizational morality that must not only comply with legal requirements but also respond to public influence and social expectations. Consequently, an information security system can assist an organization to achieve brand and branding by addressing corporate ethics principles to protect the interests of all stakeholders. Numerous studies also suggest that ensuring information security is the same as investing in a socially responsible commitment, leading to an improvement in firm profitability (Kamdjoug et al., 2018; Ki-Aries & Faily, 2017; Rastogi & von Solms, 2012; Tewamba et al., 2019). Lai et al. (2010) examine the impact of socially responsible behavior on brand success in B2B marketplaces. According to scholars, socially responsible behavior has a beneficial impact on brand and branding performance.

In summary, the literature reveals that the information security system, brand

and branding, and firm performance have a positive relationship. Based on previous literature, we can propose the following testable hypotheses on the existence of a causal relationship between the information security systems, brand and branding, and firm financial performance:

***Hypothesis* 5**: *Higher implementation of ISMS ISO* 27001 *in firms has a positive impact on brand and branding*

***Hypothesis* 6**: *Firms with high brand and branding have higher firm performance*

***Hypothesis* 7**: *High brand and branding mediate the relationship between ISMS ISO* 27001 *and firm performance.*

3. Research Methodology

We describe our data sample and measure information security system, corporate governance, brand and branding, and firm performance in this section. We particularly gathered a list of organizations with and without an information security infrastructure in place. We examine how firms with information security systems are correlated with firm performance and how corporate governance and branding mediate this relationship by comparing firm performance between these two categories.

3.1. Data Collection

The main purposes of this study are to investigate how information security systems are employed and their effects on corporate financial performance. To collect the data, a systematic questionnaire was constructed and utilized. The questionnaire's objective was to examine the aspects of an organization that is influenced by information security implementation. This questionnaire was e-mailed to 600 major companies in Pakistan that have implemented and utilized information security systems. Each organization's head of the IT department was called (by phone or in-person) to provide information about various areas of the study. A total of 190 completed surveys were received. Nineteen of them were disposed of because they were deemed invalid. Eventually, 171 surveys from Pakistani businesses are included in the data. The questionnaire is split into four sections and has twenty multiple-choice questions. Each section contains five questions that are assessed on a 5-point Likert scale ranging from 1 (very low) to 5 (extremely high). When we assessed responding and non-responding companies across numerous parameters, we found no significant differences (firm age, firm size, and industry as shown in Table 1).

3.2. Measures of Variables

3.2.1. Information Security System

Our first sample comprised a list of Pakistani enterprises holding ISMS certifications. We chose this developing nation since much prior research examined the influence of ISMS certification on organizations' monetary and non-monetary

Table 1. Demographic Characteristics firm wise.

Characteristics	N	%
Firm Industry		
Manufacturing	23	14
Banking/Financial	52	30
Accounting Services	68	40
Information Technology	28	16
Firm Age		
01 - 15 years	102	60
16 - 30 years	48	28
>30	21	12
Firm Size		
01 - 1000	98	57
1001 - 5000	46	27
>5000	27	16

performance in developed countries (Hsu et al., 2016). It should be noted that the name of the ISO 27001 certificate registrant may represent a manufacturing, financial, services, or information technology firm or a corporate body. Following that, we compiled a list of control firms that had no prior experience with ISMS certification. We started by compiling a list of all candidate control firms from Compustat. The match was then done for businesses in the same industry based on pre-certification performance and company size.

3.2.2. Corporate Reputation

Despite some doubts regarding the "Fortune reputation index's" validity (Fryxell & Wang, 1994), it remains the most extensively used indicator of corporate reputation (McGuire et al., 1990). 8 criteria were considered for this investigation. The ratings were then averaged for each organization to provide an overall reputation index, which functioned as a proxy for overall corporate reputation. The 8-item questionnaire was distributed to manufacturing, financial, services, and information technology businesses to validate the measure of corporate reputation. The quota was determined by two age factors as well as gender. On a five-point Likert scale ranging from "I disagree strongly" (=1) to "I agree strongly" (=5), each respondent was asked to identify their degree of agreement or disagreement (Bokhari & Aftab, 2022). Following data collection, negatively characterized components were reverse coded, and descriptive statistics were generated for all items on the scale. Items with adjusted item-total correlations less than 0.5 did not contribute substantially to measuring the corporate reputation concept and were thus deleted, leaving a 5-item questionnaire.

3.2.3. Brand and Branding

As evident from the literature review, 15 characteristics that contribute to brand

and branding efficacy have been discovered. The settings are altered based on the kind of respondent. The brand and branding effectiveness score of information security is calculated based on the evaluations given by respondents on these characteristics. The mean of the evaluations supplied by the various stakeholders is computed on a five-point Likert scale ranging from (1) " strongly disagree " to (5) "strongly agree". The mean score of the brand and branding effectiveness ratings of information security computed from the perspective of participating organizations was then used to generate the final ranking.

3.2.4. Firm Financial Performance

As indicated in our hypothesis, we regarded ROA as a measure of firm performance. As indicated in Hypothesis 1, we predicted organizations that implemented information security systems to have superior firm financial performance through sales growth. Consequently, the first measure we employed was Return on Assets (ROA), which was determined as operating income divided by total assets. ROA has been utilized to measure firm performance widely in previous research (McGuire et al., 1990).

3.2.5. Control Variables

Firm age and size were used as control variables in this study.

3.3. Methodology

To test our hypothesis, we conducted a comparative analysis of the ROA and ROE of organizations with and without an information security management system. Our statistical analyses were based on the null hypothesis that the profitability of certified companies differed from that of noncertified enterprises. We utilized SmartPLS SEM to investigate our hypotheses and analyze the results following (Bokhari & Myeong, 2022). The research framework proposed for this study is given in **Figure 1**.

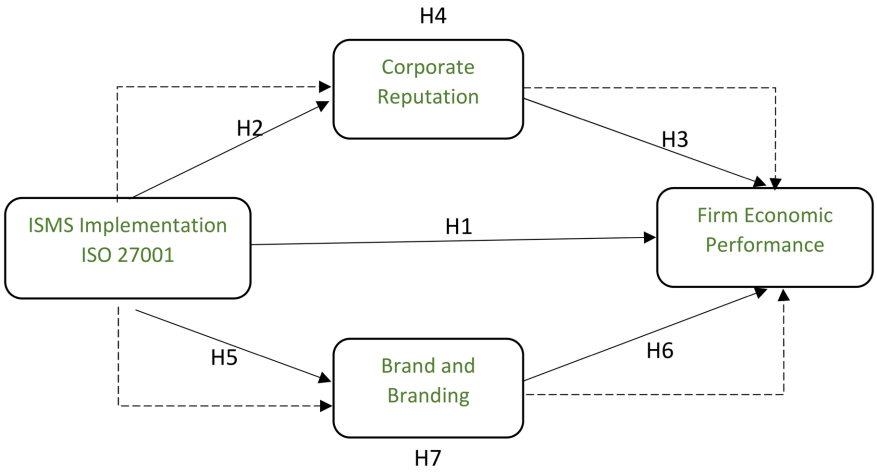

Figure 1. Research framework for ISMS, corporate reputation, brand and branding, and firm performance.

4. Results Interpretation

To test the hypothesized relationships between the implementation of ISMS, corporate reputation, brand and branding, and firm performance, a model was constructed on a logical theoretical base. For the analysis, PLS software version 3 and SPSS version 21 were utilized. The first step was to examine the measurement model's reliability and validity. The hypotheses were then tested using a structural equation model.

4.1. Construct Reliability and Validity

The internal consistency and discriminant validity of the measurement models were assessed to place them to the test in Table 2. Internal consistency is signified by composite reliability (CR) and convergent validity. The outcomes of the CR tests indicate that all components have values greater than the generally accepted criterion of 0.7 (Abdillah & Hartono, 2015). The convergent reliability analysis looked at CR, factor loadings, and AVE. First, it was observed that all the components have statistically significant loadings. This finding suggests that all items associated with their respective components validate the assumed correlation between the indicators and the components. Second, in all study constructs, the average variance extracted (AVE) indicators surpassed the cut-off point of 0.50 (Abdillah & Hartono, 2015). Thereby, referring to all the convergent validity standards, it demonstrated that the equipped measures could be applied.

The discriminant validity test determines how much the constructs vary from one another. To demonstrate discriminant validity, the construct's AVE should be higher than the variation explained by that construct and the other components in the framework (e.g., the symmetrical correlation between related components) (Abdillah & Hartono, 2015). This criterion was compiled by all constructs in this study; in specific, the diagonal values (AVEs) are higher than the non-diagonal aspects in the respective columns in Table 2. In short, the model evaluations revealed strong evidence of validity and reliability for the concepts' operationalization.

4.2. Testing Direct Effects

The mean values, standard deviations, and correlation matrices for ISMS implementation, corporate reputation, brand and branding, and firm financial performance are presented in Table 3. The matrices demonstrate a significant correlation between the independent variables (ISMS implementation, corporate reputation, brand, and branding) and the dependent variable (i.e., firm financial performance). These findings illustrate and support the authors' aspirations for the interdependence of ISMS implementation, corporate reputation, brand and branding, and firm performance. All correlation coefficients were in the expected directions, suggesting that hypotheses such as ISMS implementation being positively related to firm performance ($r = 0.735$, $p < 0.01$), corporate repu-

tation (r = 0.708, $p < 0.01$), and brand and branding (r = 0.587, $p < 0.01$) should be tested further (Bokhari & Myeong, 2022; Tewamba et al., 2019).

Table 2. Reliability and validity test.

Variables	Items	Factor Loadings	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Information Security Management System	Determination of internal and external factors relevant to ISMS	0.766	0.737	0.726	0.721	0.706
	The scope of ISMS 270001 documented	0.749				
	Established information security policy that is appropriate	0.814				
	Roles within the ISMS clearly defined and communicated	0.800				
	The ISMS adequately resourced	0.697				
	The information security risk assessment process repeatable	0.744				
	A program to ensure the ISMS achieves its outcomes	0.797				
	There is an information security risk treatment process to select appropriate risk treatment options	0.723				
Corporate Reputation	My company produces quality products	0.932	0.953	0.956	0.962	0.759
	My company uses high caliber adverts	0.916				
	My company sponsors many activities	0.701				
	My company is always willing to welcome visitors to tour the factory	0.868				
	My company is a long-established company	0.828				
	My company carry out a lot of advertising	0.901				
	My company offer a variety of well-known products	0.891				
	The employees of my company are well trained	0.910				
Brand and Branding	The brand of my company prefers to be true to them	0.777	0.859	0.911	0.902	0.569
	Authenticity of the brand of the company means aesthetic	0.821				
	Products of the brand of the company are made genuine and honesty	0.854				
	The authenticity is considered as prestige of the brand	0.768				
	Authenticity of the brand of the company means reliable	0.814				
	The brand of the company needs to note friendly environment	0.904				
	The brand of the company explains the morality	0.739				
	Advertising of the brand of my company sometimes is too exaggerated	0.858				

Table 3. Descriptive, correlation, mean, min & max values, and standard deviation.

	N	Min Value	Max Value	Mean	SD	Age	Size	FP	ISMS	CR	BB
Age	171	6	34	1.4386	0.4977	1					
Size	171	146	7229	1.3509	0.4787	0.264**	1				
FP	171	5.19	18.1	12.2982	3.6940	0.229**	0.179*	1			
ISMS	171	3.88	4.63	4.0288	0.7798	−0.035**	0.273**	0.735**	1		
CR	171	3.76	5.0	3.8901	0.8438	0.049	0.203**	0.708**	0.882**	1	
BB	171	3.75	4.5	3.8919	0.7052	−0.054	−0.130	0.587**	0.903**	0.926**	1

**Correlation is significant at the 0.01 level (2-tailed). *Correlation is significant at the 0.05 level (2-tailed).

Table 4 displays the statistical findings of univariate analysis of variance using robust standard errors. While there are three or more categories and only one predictor variables and one outcome variable, the one-way ANOVA is employed. Since there are three independent variables, the univariate analysis of variance is advanced to the two-way ANOVA. The interactivity between the predictor factors, as well as the overall impacts of the variables, must be investigated in this approach. previous scholars advised avoiding employing more than three independent variables due to complexity.

The Type I error rate might be distorted if the normality and homoscedasticity presumptions are violated. The Type I error (alpha rate) is usually suggested at 0.05. This indicates that if a findings are significant statistically, there must be less than a 5% possibility that a Type I error occurred. When traditional parametric statistics are applied to assess non-normally distributed or heteroscedastic data, the actual risk of committing a Type I error could be significantly greater (or lesser) than the p value produced (Erceg-Hurn & Mirosevich, 2008). The potency of standard parametric statistics can be significantly reduced when the assumption of homogeneity or homogeneity of variance are violated. In that case, a slight deviation from normality reduces the impact of the t test from 0.28 to 0.96 (Erceg-Hurn & Mirosevich, 2008). Table 4 displays the values of robust std. error where minimum value is 0.307, greater than 0.28, and maximum value is 0.928, lesser than 0.96, which indicates our assumptions are true and p-values signify that correlations are significant.

According to the findings in Table 5, ISMS implementation had a positive and statistically significant direct influence on firm financial performance, with a path coefficient (β = 0.663; t value = 10.659; p = 0.000). This finding demonstrated that hypothesis 1 is strongly supported. As projected, Hypothesis 2 found a strong association between ISMS implementation and corporate reputation, with a path coefficient (β = 0.934; t value = 106.755; p = 0.000). With a path coefficient (β = 1.044; t-value = 4.125; p = 0.000), Hypothesis 3 supported the proposed relationship between corporate reputation and firm financial performance with a path coefficient. The positive impact of ISMS implementation on

brand and branding was hypothesized in hypothesis 5, and findings confirmed a strong positive association between the two constructs with a path coefficient (β = 0.924; t-value = 105.627; p = 0.000), indicating that H5 is supported. Finally, hypothesis 5 predicted a strong correlation between brand and branding and firm financial performance. The findings strongly support our proposition, with a path coefficient (β = 0.752; t-value = 4.998; p = 0.000) significantly supporting H5. To investigate the variance of the latent variables, the framework evaluated the squared multiple correlation (R^2) coefficient for latent constructs. Table 5 displays the squared multiple correlations (R^2) result, suggesting that the presumed model described statistically significant variance for the dependent constructs (Tewamba et al., 2019).

4.3. Mediating Effect

The significant study of the indirect impact and total effect path coefficients from the bootstrapping procedure (with 450 tests, 5000 subsamples, and no significant changes) was shown in Table 6. The findings revealed that corporate reputation plays an important role in mediating the relationship between ISMS implementation and firm performance, as evidenced by a path coefficient (Beta value = 0.975; t value = 4.123; p = 0.000), hence supporting suggested H4 strongly. Further, the final hypothesis 7 identified that brand and branding have a significant mediating relationship between ISMS implementation and firm performance, with a path coefficient (Beta value = 0.695; t value = 4.879; p = 0.00), therefore, H7 is significantly supported. A summary of the findings of the total direct and indirect relationships is given in Table 5.

Table 4. Parameter estimates with robust standard errors.

Dependent Variable: FP						
Parameter	B	Robust Std. Error[a]	T	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Intercept	−21.110	2.653	−7.957	0.000	−26.349	−15.872
Age	1.117	0.307	3.639	0.000	0.511	1.723
Size	0.580	0.350	1.655	0.100	−0.112	1.272
ISMS	9.432	0.928	10.165	0.000	7.600	11.264
CR	3.424	0.366	9.357	0.000	2.702	4.147
BB	5.217	0.554	9.418	0.000	6.310	4.123

a. HC3 method

Descriptive Statistics

Dependent Variable: FP

Mean	SD	N
12.2982	3.69402	171

Table 5. Framework testing for ISMS, corporate reputation, branding, and firm performance.

	Original Sample (O)	T Statistics (|O/STDEV|)	*p* Values
Age -> FP	0.168	3.256	0.001
Size -> FP	−0.042	0.862	0.029
ISMS -> FP	0.663	10.659	0.000
ISMS -> CR	0.934	106.755	0.000
ISMS -> BB	0.924	105.627	0.000
CR -> FP	1.044	4.125	0.000
BB -> FP	0.752	4.998	0.000
ISMS -> CR -> FP	0.975	4.123	0.000
ISMS -> BB -> FP	0.695	4.879	0.000
Model Summary			
R	R square	Adjusted R Square	Std. Error of the Estimate
0.839[a]	0.703	0.694	2.04244

[a]Predictors: (Constant), Size, BB, Age, ISMS, CR; **Correlation is significant at the 0.01 level (2-tailed).

Table 6. A summary of the findings.

H1	Higher implementation of ISMS ISO 27001 in firms has a positive impact on firm performance	Supported
H2	Higher implementation of ISMS ISO 27001 in firms has a positive impact on corporate reputation	Supported
H3	Firms with a high corporation reputation have higher firm performance	Supported
H4	High corporate reputation mediates the relationship between implementation of ISMS ISO 27001 and firm performance.	Supported
H5	Higher implementation of ISMS ISO 27001 in firms has a positive impact on brand and branding	Supported
H6	Firms with high brand and branding have higher firm performance	Supported
H7	High brand and branding mediate the relationship between implementation of ISMS ISO 27001 and firm performance.	Supported

5. Discussions, Implications, and Conclusions

5.1. Discussions

This study was able to produce results that have implications for both social science research and information security management in the Pakistani environment by using a multiple regression model to investigate hypotheses of information security system, corporate reputation, branding, and information security system. This research concluded that ISMS had a significant impact on corporate reputation, brand and branding, and firm profitability in organizations.

Furthermore, corporate reputation, brand, and branding have a favorable correlation with firm performance. Finally, company reputation and branding considerably mediate the relationship between the information security systems and firm performance. Several scholars have concluded that strengthening information security entails considering human behavior and increasing stakeholders' intention to continue with the organization due to its reputation and branding, both of which contribute to the firm's economic growth. This demonstrates that strengthening the information security system allows for boosting the reputation and branding, and consequently firm profitability. Most respondents operate in the banking, information technology, and telecommunications industries, and information security is considered one of the greatest and most crucial components of their success. Information security measures are already highly developed in our environment, particularly in the banking, information technology, and telecommunications sectors. Their perception of the significance of ISMS in a firm is reflected in our findings. Consequently, every firm should develop an information security system since it has a substantial impact on its reputation, branding, and financial performance.

5.2. Implications

The major recommendation is to implement an ISMS or to comply with an existing ISMS that is based on ISO 27001 standards. The findings demonstrated the need of focusing on the constant improvement of the maturity level of the vulnerability management process, as this improvement will support a high-quality information security management system. This suggestion will include global standards at different levels of the organization.

On the level of the executives, it is mostly a matter of handling policy concerns and supporting ISMS adoption. It is essential to empower the information security manager to influence the selection and specifications of vendor services, as well as to suggest content components for liability insurance. Furthermore, it is crucial to frequently communicate the net advantages of an ISMS in the organization and pave the way for strategy implementation in an information security management system integration. Finally, it must provide the security manager with enough autonomy, so that he or she can respond to the board of governance rather than the Executive or CIO. This would make it easier for him to collect data for security purposes and execute alternative approaches.

At the level of the manager of information security, operations must be completed daily, and security expenditures must be rationalized. In general, he plays a vital role in areas such as counseling, assistance, communication, orientation, and alerts. He has the authority to act immediately on all or a portion of the company's information security. He must formulate strategies for information security issues, develop, or oversee the implementation of these strategies, put the contingency planning strategy into action, mitigate the threat of information security, learn how to manage uncertainty, and learn the several departments of the organization. and evaluate the return on investment in information security.

5.3. Conclusion

Fundamentally, the information security management system, which includes people, processes, and information technology systems, is a comprehensive method through which a business protects its information security through a risk assessment. The key issue in Pakistan is the lack of comprehension regarding the establishment of corporate information asset security management since damages are substantial, even if their intensity is low for certain executives who favor therapeutic approaches. The assessment of performance is crucial for an organization and each of its functions. Consequently, it is critical to identify the factors that permit measuring the success of the information security department and its contribution to overall firm performance.

Nevertheless, the respondents' reluctance to cooperate hampered our efforts. Conversely, this may have helped us enhance our framework. In absolute agreement with Pakistani enterprises, we should have precisely presented the ideas of administrative competence and corporate reputation. This will allow leaders to invest in the security of their information assets more swiftly by using more significant manifest factors. This study concentrates on certain administrators on the significance of information security management systems.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Abdillah, W., & Hartono, J. (2015). Partial Least Square (PLS): Alternatif Structural Equation Modeling (SEM) Dalam Penelitian Bisnis. *Yogyakarta: Penerbit Andi, 22,* 103-150.

Alqahtani, F. H. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science, 124,* 691-697. https://doi.org/10.1016/j.procs.2017.12.206

Arshad, R., Othman, S., & Othman, R. (2012). Islamic Corporate Social Responsibility, Corporate Reputation and Performance. *International Journal of Economics and Management Engineering, 6,* 643-647.

Atkinson, J. S., Mitchell, J. E., Rio, M., & Matich, G. (2018). Your WiFi Is Leaking: What Do Your Mobile Apps Gossip about You? *Future Generation Computer Systems, 80,* 546-557. https://doi.org/10.1016/j.future.2016.05.030

Bakar, Z. A., Yaacob, N. A., & Udin, Z. M. (2015). The Effect of Business Continuity Management Factors on Organizational Performance: A Conceptual Framework. *International Journal of Economics and Financial Issues, 5,* 128-134.

Barnett, M. L., Jermier, J. M., & Lafferty, B. A. (2006). Corporate Reputation: The Definitional Landscape. *Corporate Reputation Review, 9,* 26-38. https://doi.org/10.1057/palgrave.crr.1550012

Barney, J. B. (2001). Resource-Based Theories of Competitive Advantage: A Ten-Year Retrospective on the Resource-Based View. *Journal of Management, 27,* 643-650. https://doi.org/10.1177/014920630102700602

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Infor-

mation Systems Security. *European Journal of Information Systems, 1,* 121-130. https://doi.org/10.1057/ejis.1991.20

Bokhari, S. A. A., & Aftab, M. (2022). Personality Traits and Social Loafing among Employees Working in Teams at Small and Medium Enterprises: A Cultural Perspective Data from Emerging Economies. *Data in Brief, 42,* Article ID: 108085. https://doi.org/10.1016/j.dib.2022.108085

Bokhari, S. A. A., & Myeong, S. (2022). Use of Artificial Intelligence in Smart Cities for Smart Decision-Making: A Social Innovation Perspective. *Sustainability*, *14*, Article No. 620. https://doi.org/10.3390/su14020620

Bokhari, S. A. A., Aftab, M., & Shahid, M. (2021). Political Instability and Inward Foreign Direct Investment: The Perspective of Government Corruption from an Emerging Economy. *Industry Promotion Research, 6,* 69-81.

Calder, A. (2017). *Nine Steps to Success*: *An ISO 27001 Implementation Overview*. IT Governance Ltd. https://doi.org/10.2307/j.ctt1wn0skw

Campbell, J. L. (2007). Why Would Corporations Behave in Socially Responsible Ways? An Institutional Theory of Corporate Social Responsibility. *Academy of Management Review*, *32*, 946-967. https://doi.org/10.5465/amr.2007.25275684

Chang, H. (2013). Is ISMS for Financial Organizations Effective on Their Business? *Mathematical and Computer Modelling, 58,* 79-84. https://doi.org/10.1016/j.mcm.2012.07.018

Choong, P., Hutton, E., Richardson, P. S., & Rinaldo, V. (2017). Protecting the Brand: Evaluating the Cost of Security Breach from a Marketer's Perspective. *Journal of Marketing Development and Competitiveness, 11,* 59-68.

Chun, R. (2005). Corporate Reputation: Meaning and Measurement. *International Journal of Management Reviews, 7,* 91-109. https://doi.org/10.1111/j.1468-2370.2005.00109.x

Coaffee, J., & Van Ham, P. (2008). 'Security Branding': The Role of Security in Marketing the City, Region or State. *Place Branding and Public Diplomacy, 4,* 191-195. https://doi.org/10.1057/pb.2008.11

Dao, T. K., Tapanainen, T. J., Nguyen, H. T. T., Nguyen, T. H., & Nguyen, N. D. (2017). Information Safety, Corporate Image, and Intention to Use Online Services: Evidence from Travel Industry in Vietnam. In *23rd Americas Conference on Information Systems (AMCIS 2017): A Tradition of Innovation* (pp. 147-156). Association for Information Systems.

De Chernatony, L. (1999). Brand Management through Narrowing the Gap between Brand Identity and Brand Reputation. *Journal of Marketing Management, 15,* 157-179. https://doi.org/10.1362/026725799784870432

Eloff, M. M., & Von Solms, S. H. (2000). Information Security Management: An Approach to Combine Process Certification and Product Evaluation. *Computers & Security, 19,* 698-709. https://doi.org/10.1016/S0167-4048(00)08019-6

Erceg-Hurn, D. M., & Mirosevich, V. M. (2008). Modern Robust Statistical Methods: An Easy Way to Maximize the Accuracy and Power of Your Research. *American Psychologist, 63,* 591-601. https://doi.org/10.1037/0003-066X.63.7.591

Farquhar, P. H. (1994). Strategic Challenges for Branding. *Marketing Management, 3,* 8-15.

Fombrun, C. J., Ponzi, L. J., & Newburry, W. (2015). Stakeholder Tracking and Analysis: The RepTrak® System for Measuring Corporate Reputation. *Corporate Reputation Review, 18,* 3-24. https://doi.org/10.1057/crr.2014.21

Fournier, S. (1998). Consumers and Their Brands: Developing Relationship Theory in

Consumer Research. *Journal of Consumer Research, 24,* 343-373. https://doi.org/10.1086/209515

Fryxell, G. E., & Wang, J. (1994). The Fortune Corporate Reputation Index: Reputation for What? *Journal of Management, 20,* 1-14. https://doi.org/10.1177/014920639402000101

Goel, S., & Shawky, H. A. (2009). Estimating the Market Impact of Security Breach Announcements on Firm Values. *Information & Management, 46,* 404-410. https://doi.org/10.1016/j.im.2009.06.005

Gwebu, K. L., Wang, J., & Wang, L. (2018). The Role of Corporate Reputation and Crisis Response Strategies in Data Breach Management. *Journal of Management Information Systems, 35,* 683-714. https://doi.org/10.1080/07421222.2018.1451962

Hampf, A., & Lindberg-Repo, K. (2011). *Branding: The Past, Present, and Future: A Study of the Evolution and Future of Branding*. Hanken School of Economics.

Han, J., Kim, Y. J., & Kim, H. (2017). An Integrative Model of Information Security Policy Compliance with Psychological Contract: Examining a Bilateral Perspective. *Computers & Security, 66,* 52-65. https://doi.org/10.1016/j.cose.2016.12.016

Hausken, K. (2006). Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. *Information Systems Frontiers, 8,* 338-349. https://doi.org/10.1007/s10796-006-9011-6

He, W., Liu, C., Lu, J., & Cao, J. (2015). Impacts of ISO 14001 Adoption on Firm Performance: Evidence from China. *China Economic Review, 32,* 43-56. https://doi.org/10.1016/j.chieco.2014.11.008

He, Y., & Lai, K. K. (2014). The Effect of Corporate Social Responsibility on Brand Loyalty: The Mediating Role of Brand Image. *Total Quality Management & Business Excellence, 25,* 249-263. https://doi.org/10.1080/14783363.2012.661138

Holt, D. B., & Holt, D. B. (2004). *How Brands Become Icons: The Principles of Cultural Branding*. Harvard Business Press.

Homburg, C., Klarmann, M., & Schmitt, J. (2010). Brand Awareness in Business Markets: When Is It Related to Firm Performance? *International Journal of Research in Marketing, 27,* 201-212. https://doi.org/10.1016/j.ijresmar.2010.03.004

Hsu, C., Wang, T., & Lu, A. (2016). The Impact of ISO 27001 Certification on Firm Performance. In *2016 49th Hawaii International Conference on System Sciences (HICSS)* (pp. 4842-4848). IEEE. https://doi.org/10.1109/HICSS.2016.600

Hung, W. H., Chang, I. C., Chen, Y., & Ho, Y. L. (2019). Aligning 4C strategy with Social Network Applications for CRM Performance. *Journal of Global Information Management (JGIM), 27,* 93-110. https://doi.org/10.4018/JGIM.2019010105

Iwu-Egwuonwu, R. C. (2010). Corporate Reputation & Firm Performance: Empiricial Literature Evidence. *International Journal of Business and Management, 6,* 197-206. https://doi.org/10.2139/ssrn.1659595

Jannah, M., Fahlevi, M., Paulina, J., Nugroho, B. S., Purwanto, A., Subarkah, M. A., Kurniati, E., Wibowo, T. S., Kalbuana, K. N., & Cahyono, Y. (2020). Effect of ISO 9001, ISO 45001 and ISO 14000 toward Financial Performance of Indonesian Manufacturing. *Systematic Reviews in Pharmacy, 11,* 894-902.

Kamdjoug, J. R. K., Tewamba, H. J. N., & Wamba, S. F. (2018). IT Capabilities, Firm Performance and the Mediating Role of ISRM: A Case Study from a Developing Country. *Business Process Management Journal, 25,* 476-494. https://www.emerald.com/insight/content/doi/10.1108/BPMJ-11-2017-0297/full/html

Kapferer, J. N. (2008). *The New Strategic Brand Management: Creating and Sustaining Brand Equity Long Term*. Kogan Page Publishers.

Ki-Aries, D., & Faily, S. (2017). Persona-Centred Information Security Awareness. *Computers & Security, 70,* 663-674. https://doi.org/10.1016/j.cose.2017.08.001

Kitchin, T. (2003). Corporate Social Responsibility: A Brand Explanation. *Journal of Brand Management, 10,* 312-326. https://doi.org/10.1057/palgrave.bm.2540127

Lai, C. S., Chiu, C. J., Yang, C. F., & Pai, D. C. (2010). The Effects of Corporate Social Responsibility on Brand Performance: The Mediating Effect of Industrial Brand Equity and Corporate Reputation. *Journal of Business Ethics, 95,* 457-469. https://doi.org/10.1007/s10551-010-0433-1

Laufer, D., & Coombs, W. T. (2006). How Should a Company Respond to a Product Harm Crisis? The Role of Corporate Reputation and Consumer-Based Cues. *Business Horizons, 49,* 379-385. https://doi.org/10.1016/j.bushor.2006.01.002

Lee, J., & Roh, J. J. (2012). Revisiting Corporate Reputation and Firm Performance Link. *Benchmarking: An International Journal, 19,* 649-664. https://doi.org/10.1108/14635771211258061

Lele, Q., & Lihua, K. (2016). Technical Framework Design of Safety Production Information Management Platform for Chemical Industrial Parks Based on Cloud Computing and the Internet of Things. *International Journal of Grid and Distributed Computing, 9,* 299-314. https://doi.org/10.14257/ijgdc.2016.9.6.28

Marquardt, R., Makens, J., & Larzelere, H. (1965). Measuring the Utility Added by Branding and Grading. *Journal of Marketing Research, 2,* 45-50. https://doi.org/10.1177/002224376500200106

Martínez, P., Pérez, A., & Del Bosque, I. R. (2014). CSR Influence on Hotel Brand Image and Loyalty. *Academia Revista Latinoamericana de Administración, 27,* 267-283. https://doi.org/10.1108/ARLA-12-2013-0190

Mastoi, R. B., Khan, Z., Mastoi, S. et al. (2021). ISO Certifications in Pakistan: Patterns & Application. *International Journal of Management, 12,* 403-415.

McGuire, J. B., Schneeweis, T., & Branch, B. (1990). Perceptions of Firm Quality: A Cause or Result of Firm Performance. *Journal of Management, 16,* 167-180. https://doi.org/10.1177/014920639001600112

Meixner, F., & Buettner, R. (2012). Trust as an Integral Part for Success of Cloud Computing. In *ICIW 2012 Proceedings* (pp. 207-214).

Menon, N. M., & Siponen, M. T. (2020). Executives' Commitment to Information Security: Interaction between the Preferred Subordinate Influence Approach (PSIA) and Proposal Characteristics. *ACM SIGMIS Database: The DATABASE for Advances in Information Systems, 51,* 36-53. https://doi.org/10.1145/3400043.3400047

Moghe, P., Gehani, N., & Smith, P. T. (2014). *Enterprise Information Asset Protection through Insider Attack Specification, Monitoring and Mitigation.* US8880893B2.

Moore, K., & Reid, S. (2008). The Birth of Brand: 4000 Years of Branding. *Business History, 50,* 419-432. https://doi.org/10.1080/00076790802106299

Mukundan, N., & Sai, L. P. (2014). Perceived Information Security of Internal Users in Indian IT Services Industry. *Information Technology and Management, 15,* 1-8. https://doi.org/10.1007/s10799-013-0156-y

Nechai, A., Pavlova, E., Batova, T., & Petrov, V. (2020). Implementation of Information Security System in Service and Trade. *IOP Conference Series: Materials Science and Engineering, 940,* Article ID: 012048. https://doi.org/10.1088/1757-899X/940/1/012048

Neubauer, T., Ekelhart, A., & Fenz, S. (2008). Interactive Selection of ISO 27001 Controls

under Multiple Objectives. In *IFIP International Information Security Conference* (pp. 477-491).

Park, C. W., Eisingerich, A. B., Pol, G., & Park, J. W. (2013). The Role of Brand Logos in Firm Performance. *Journal of Business Research, 66,* 180-187. https://doi.org/10.1016/j.jbusres.2012.07.011

Peng, J., Quan, J., & Peng, L. (2019). It Application Maturity, Management Institutional Capability and Process Management Capability. *Journal of Organizational and End User Computing (JOEUC), 31,* 61-85. https://doi.org/10.4018/JOEUC.2019010104

Rastogi, R., & von Solms, R. (2012). Information Security Service Branding—Beyond Information Security Awareness. *Systemics, Cybernetics and Informatics, 10,* 54-59.

Sammut-Bonnici, T. (2014). Brand and Branding. *Wiley Encyclopedia of Management*. https://doi.org/10.1002/9781118785317.weom120161

Sato, H., Kanai, A., & Tanimoto, S. (2010). A Cloud Trust Model in a Security Aware Cloud. In *2010 10th IEEE/IPSJ International Symposium on Applications and the Internet* (pp. 121-124). IEEE. https://doi.org/10.1109/SAINT.2010.13

Sharma, N., & Dash, P. K. (2012). Effectiveness of ISO 27001, as an Information Security Management System: An Analytical Study of Financial Aspects. *Far East Journal of Psychology and Business, 9,* 42-55.

Smith, S., Winchester, D., Bunker, D., & Jamieson, R. (2010). Circuits of Power: A Study of Mandated Compliance to an Information Systems Security "De Jure" Standard in a Government Organization. *MIS Quarterly, 34,* 463-486. https://doi.org/10.2307/25750687

Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical Computer Sciences IJECSIJENS, 11,* 23-29.

Tewamba, H. N., Kamdjoug, J. R. K., Bitjoka, G. B., Wamba, S. F., & Bahanag, N. N. M. (2019). Effects of Information Security Management Systems on Firm Performance. *American Journal of Operations Management and Information Systems, 4,* 99-108. https://doi.org/10.11648/j.ajomis.20190403.15

Tipton, H. F., & Krause, M. (2007). *Information Security Management Handbook*. CRC Press. https://doi.org/10.1201/9781439833032

Velasco, J., Ullauri, R., Pilicita, L., Jácome, B., Saa, P., & Moscoso-Zea, O. (2018). Benefits of Implementing an ISMS According to the ISO 27001 Standard in the Ecuadorian Manufacturing Industry. In *2018 International Conference on Information Systems and Computer Science (INCISCOS)* (pp. 294-300). IEEE. https://doi.org/10.1109/INCISCOS.2018.00049

Wu, C. H., & Tsai, S. B. (2018). Using DEMATEL-Based ANP Model to Measure the Successful Factors of E-Commerce. In *Intelligent Systems: Concepts, Methodologies, Tools, and Applications* (pp. 1122-1138). IGI Global. https://doi.org/10.4018/978-1-5225-5643-5.ch047

Wu, W., Shi, K., Wu, C. H., & Liu, J. (2021). Research on the Impact of Information Security Certification and Concealment on Financial Performance: Impact of ISO 27001 and Concealment on Performance. *Journal of Global Information Management (JGIM), 30,* 1-16. https://doi.org/10.4018/JGIM.20220701.oa2

Yaeger, M. L. et al. (2015). *Information Security: Obligations and Expectations.* Schulte Roth & Zabel.