Why ISO27001 Certified Organizations Still Experience Data Leakage?

Harrison Stewart
Harrison Stewart Group
Germany
stewart@harrisonstewart.net

Journal of Digital Information Management

ABSTRACT: *The increases in mobile applications, IoT, and cloud technology have recently witnessed massive data leaks, ranging from personally identifiable information to corporate secrets. Despite numerous standards and frameworks, human errors that cause information security breaches have not yet been managed. This study contributes to the ISMS literature regarding the processing and operating of an ISMS concept based on the new comprehensive measures of information security management. The study uses exploratory surveys to determine significant differences in the fifty financial institutes. The study confirmed that the primary root cause of information security incidents is the interrelationship between humans and technology. The results of this study show that the NFC principle can assist in the enhancement and ability to monitor the performance of these interconnections compared to other recognized standalone ISMS standards.*

Subject Categories and Descriptors: D.4.6 Security and Protection H.2 DATABASE MANAGEMENT E.5 Security, integrity, and protection

General Terms: ISMSs, Reformed ISMS

Keywords: Information security management systems (ISMSs); Reformed ISMS; Human error related information security incident, Technology error related information security incident, Factors related information security incident

Received: 5 May 2022, Revised 22 July 2022, Accepted 29 July 2022

Review Metrics: Review Scale: 0-6, Review Score- 5.12, Inter-reviewer consistency 86.5%

DOI: 10.6025/jdim/2022/20/3/90-103

1. Introduction

The field of information security has developed various standards and frameworks governing how organizations should process information. These standards include the ISO2700* series and other specific policy standards to enhance data security and protection. Despite numerous international standards and frameworks, humans are still the weakest link in information security.

In previous work, Stewart (2017) proposed the NFC framework to demonstrate human and technology interrelationship in information security management and proposed various approaches to mitigate information security incidents. Their work has been cited in multiple information security research, and this paper evaluates the application of the NFC technique applied to information security incident management over 13 months within fifty ISO27001-certified financial organizations around Europe, Asia, Africa and the USA.

The Nine Five Circles (NFC) is an information security management system technique that enables organizations to make smarter decisions using data and analytics by combining human and technology factors. The NFC is "an information security framework that indicates the necessities for implementing operational and information security enhancements. It also emphasizes the measurement, the evaluation of organization information security management incidents (ISMI) performance and outsourcing, and enhancement of the interrelationship between technology and human factors."

As financial a. Likewise, every organization needs ISMSs that enable them to identify and manage assets to protect their critical assets. ISMSs can be seen as the interconnection of various factors, such as the human, technology (hardware, software), methods, policies, environment, and cultural factors, into a system that has been strategically and carefully implemented to tackle the current and future security threats. The process of an ISMS in our work is illustrated in Figure 1.

According to Stewart (2017), "the NFC, as illustrated in Figure 1, is designed to meet individual organization's requirement and is portable, simple and an improved starting point when compared to other principles and frameworks, such as the standard ISO27001 and ISO27002." Stewart (2017, 2018) argued that, even though both standards come with different distinct features, the ISO27001 lacks a distinction between the controls applicable to a particular organization and those that are not, while the ISO27002 prescribes a risk assessment to be performed but fails to provide the extent to which it should be applied. Stewart (2017) concluded that the standards are different, but they lack positive attributes when combined.

2. Past Studies

2.1. Information Security Management Systems

Information security standards are very much represented in the relevant literature (vonSolms, 1999; Hone and Eloff, 2002; Saint-Germain, 2005; von Solms,2005; Sahibudin et al., 2008). These standards' advantages lie in their character of providing guidelines for infrastructure. There is a belief that conformance to these standards is expected to give a competitive advantage. This assumption or expectation is also relevant in some governmental organizations. These standards have been developed through the experiences of driving innovative countries.

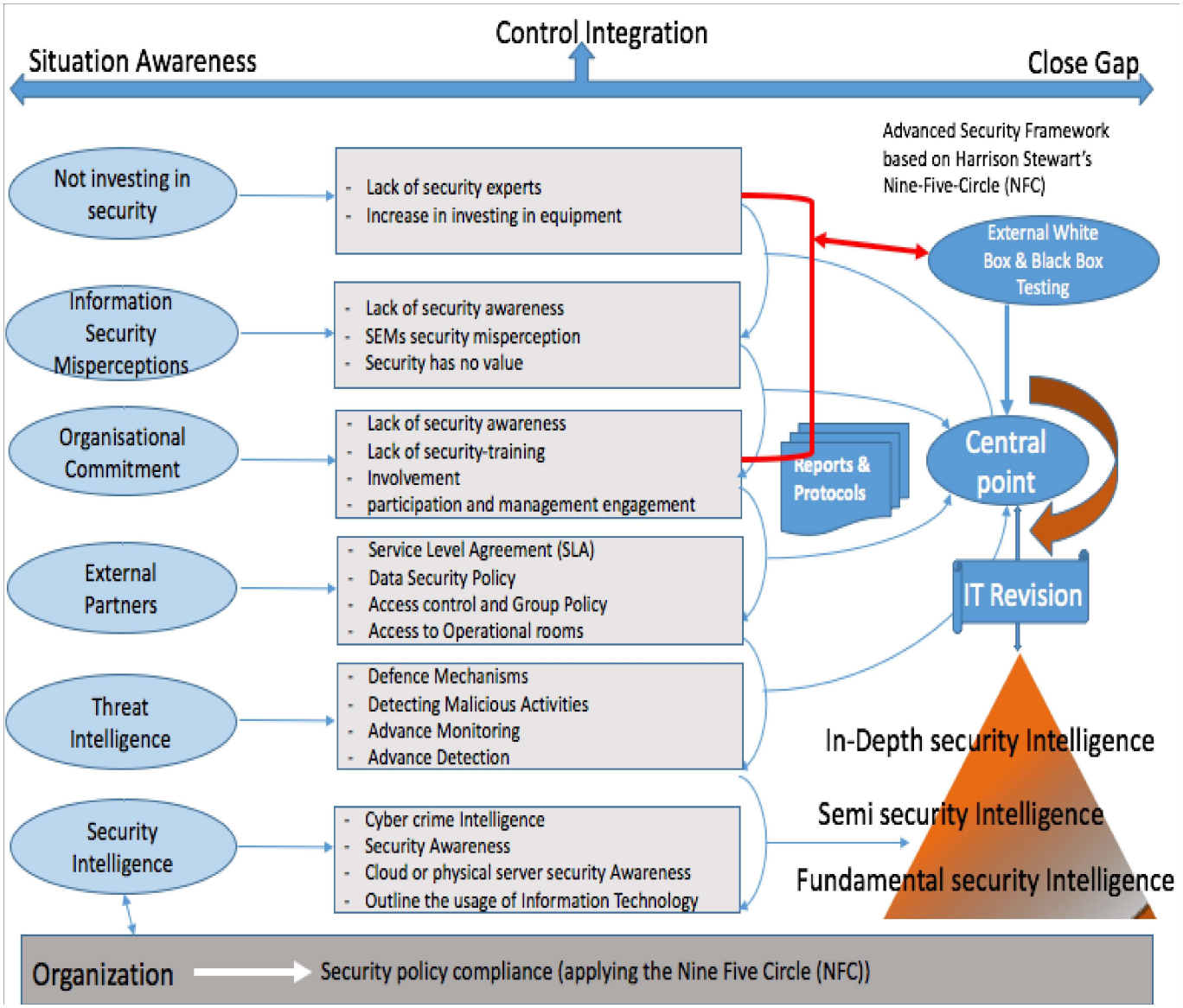


Figure 1. The Process of Information Security in the NFC concept

The role of information security management standards

Various information security management systems standards and guidelines are already in place to address the concept and the prerequisites for information security management systems. These standards and guidelines aim to ensure the security of an organization's information assets regarding confidentiality, integrity and availability. A moderately substantial number of frameworks, standards and guidelines with data assurance exercises have been established and published in the open literature. All these are being supported by legislation and regulations to promote the concepts of information security and privacy on national bases (AS/NZS, 2006; NIST, 2006; OECD, 2002) as well as globally (ISO/IEC, 2005). Another worldwide exertion has been made using the IT Governance Institute and Information Systems Audit and Control Association's Control Objectives for Information and Related Technology (COBIT)(COBIT, 2000). The standards and guidelines provide nonexclusive guidance and frameworks, not solutions for managing information security. They rely on the organization's risk assessment to determine how they should be implemented and require a policy baseline without providing specifications for compliance with the standard (Hone and Eloff, 2002). Standards and guidelines lack legitimate support regarding the proper practices to choose.

2.2. Organization Measures

Jouini et al. (2014), Loch et al. (1992), and Stewart (2017) divided organization threats into internal and external threats. Jouini et al. (2014) and Stewart (2017) took this further by classifying the threats into a human, environmental, and technological threats. According to Stewart (2017), the human aspects of information security in the NFC context are insider and external partners' threats. Neumann (1999, p. 160) stated that an insider is someone who has been permitted to access or use a particular system or facility. Anderson et al. (2000 p. 21) also argued that an insider is always malicious, and Stewart (2017) added that external partners increase the organization's threats and should be addressed effectively.

Despite all the standards available today and other ISMS s proposed by various researchers, the rate of cybercrime is still increasing because researchers and governmental institutes have made organizations believe that being compliant with one of the standards available brings with it a level of security protection. Nevertheless, Stewart (2017) argued that an ISMS could not simply be seen as a standard. Still, it should be seen as a systematic approach to managing sensitive information to protect it. This indicates that compliance with one of the ISMS standards does not convey security because securing information today is far beyond compliance with standards, installing a simple firewall, or outsourcing security from a third party.

Our work is based on the NFC framework (Stewart, 2017). It involves various security activities with a common strategy to provide an optimal protection level for 25 out of 50 selected organizations. The NFC focuses on the design, identification, and mitigation of potential factors causing an overall hindrance to security-related policy compliance within an organization. This should enable us to get a rigid solution for the 25 organizations in our work. Every potential factor that generates any hindrance in one of these 25 organizations is a cause of variation that we will address using the NFC; this is unlike other frameworks, where standards are designed for a specific focus. According to Stewart (2017), "the ISO27001 is for building an IS foundation in an organization, the ISO 27002 is for the control implementation, and the ISO 27005 is for carrying out a risk assessment and risk treatment, whereas the NFC enhances all the standards above by combining all these with a dynamic compliance process standard that involves: A) situation regulation, B) controlling the integration, and C) closing the gaps".

3. Methodology

The methodology adopted for this study draws on the NFC approach, along with t-tests (O'Mahony, 1986), to test our hypotheses. The contribution of our work is two-fold, the systematization of literature and the evaluation of ISO27001 and the NFC-ISMS along with pen testing and survey of 50 ISO27001-certified banking sectors in Europe, Asia, Africa and the USA. We also adopted the representative sample approach to interview the employees to generalize the results of our study outcome confidently.

3.1. Overview

We propose a comprehensive NFC-ISMS to represent ISMS deployments and their approach to enhance data security. Figure 2 is an example of an NFC-ISMS connected with six potential vital factors that hinder information security management success. The process involves segmenting each factor into its respective topology, as shown in Figure 2. The NFC steadiness is depicted using the central point, which holds all the constraints grouped into attributes and potential vital factors. The key factors and the central point are encapsulated in the control integration and close gaps dynamic illustrated in Figure 2. Overall, six main components: Security intelligence (A), Cyber threat intelligence (B), External partners (C), Organizational commitment (D), Information security misperception (E) and Lack of security investment (F), are all located in the situation awareness circle.

3.2. Security Properties

The security properties have three categories: situation awareness, integration control, and gap closure. Attack vectors are the six constraints used to circumvent the security of each of the organizations in this work. Situational awareness defines the problem and its possible causes. The integration control is the controlling and evaluation phase; the gap closure involves the actions needed to ensure that the entire process is completed satisfactorily and that the process follows the standards embodied in the organization's IS policy.

The NFC cycle, illustrated in Figure 2, emphasizes the prevention of error recurrence by utilizing the NFC to enhance the IS effectively. The experiment is conducted in a controlled environment based on objective experiments and accurate measurements to ensure that the data are valid and unbiased. Each factor in our work is analyzed and prioritized by measuring the impacts against the probability during each lifecycle. The minimum number of rotations is five times in each lifecycle, which can then be repeated based on the entity's needs to stabilize the process. The process of stabilization is often called the SDCA (standardize-do-check-action) cycle. According to Ishikawa (1985), "Failure to revise standards and regulations is proof that no one is seriously using them."

3.3. Chronological Development of NFC-ISMS

The concept of the Nine Five Circle was initially developed by Harrison Stewart (Stewart, 2017). It is often referred to as "NFC" or "Harrison-NFC." Our current research process-based approach to management systems is derived from his work. His holistic and process -based approach to the financial sector is still in the initial phase. Still, it is being embraced in many economic sectors around the globe after the introduction of the General Data Protection Regulation (GDPR) in 2018. Although the NFC was initially viewed as relevant only to a financial line environment, the concepts have since been successfully applied to many other industries. The NFC is illustrated in Figure 2.

3.4. Data Collection

To increase the awareness of the organization leaders about security in their environment and to help us with our research. A data policy agreement was signed stating that the data collected would be utilized only for this study and would not be imparted to any third party. Our pilot testing during the initial phase consisted of 95 questions, and there were 73 questions in the final version due to a change of focus based on the pilot feedback. During the pilot testing, a selected group of employees tried the 95 questions under test and provided feedback before fully deploying the final questions. All answers were stored in

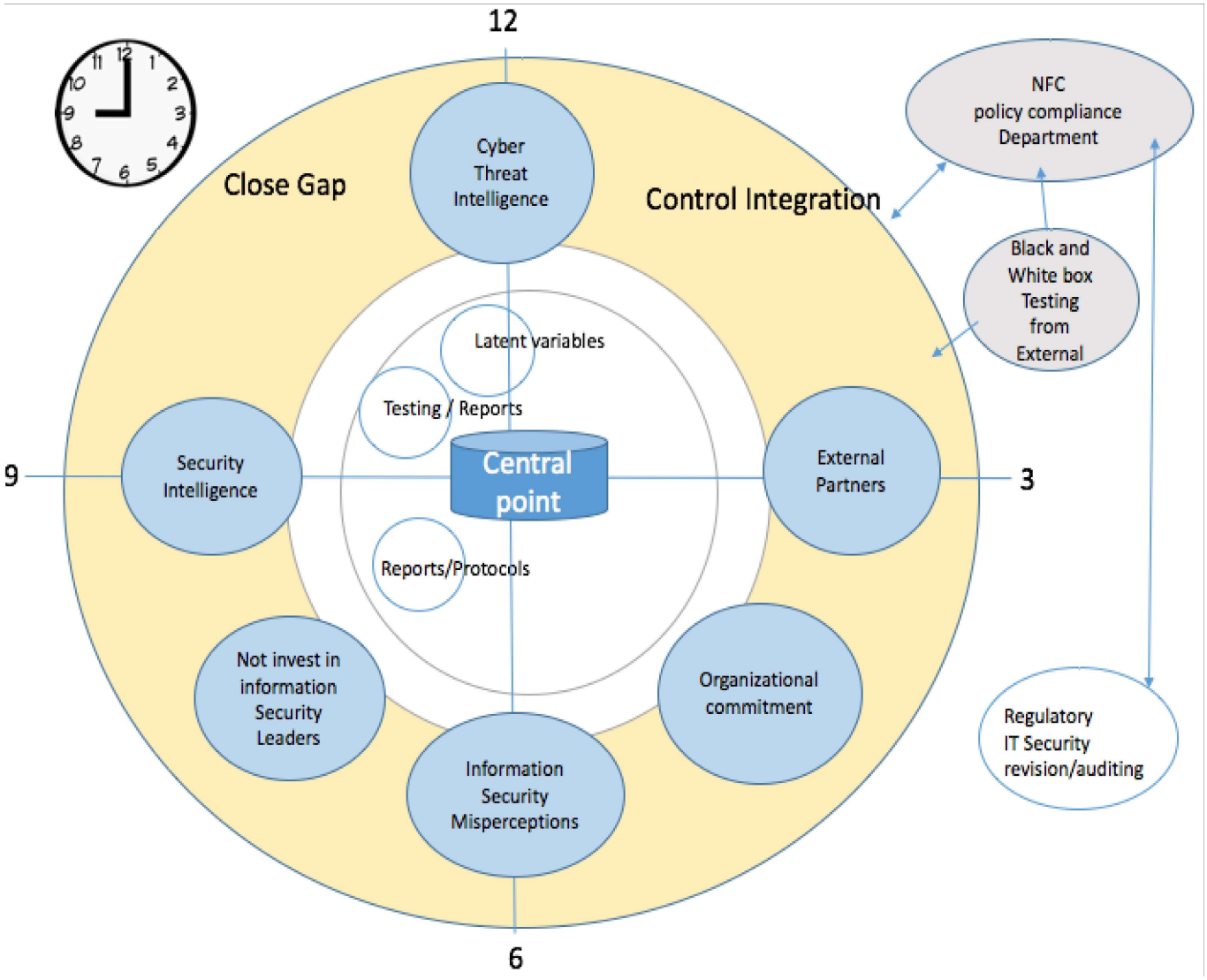


Figure 2. The NFC Process of Information Security

Source: Stewart, H. (2017). "Emerald: Information Security Management Systems

a secured MySQL database for further analysis. All surveyed questions are related to an item illustrated in Table 1. Data analysis was conducted with the SPSS. Questionnaires were performed using the Cetbix situation awareness platform. The results discussed in this work are based on the responses of 457 CEOs, CFOs, CIOs, CISOs, CSOs, VPs, directors of IT, security experts, and employees in all the selected countries.

3.5. Findings and Discussions

The NFC risk assessment graph illustrated in Figure 3 shows the total number of factors in all the organizations that hinder ISMS strategies. It can be seen that there has been a significant increase in the number of issues in Security Awareness, followed by Cyber Threat Intelligence, External partners, Commitment, Leadership, Security Misperception, and Security Investment.

Given the organisation's size, most had no Chief Information Security Officer and only one person within the security function. This shows the potentially insufficient for various security activities. The CISO's responsibilities are not fully aligned with the RACI matrix. An information security steering committee is not established. Executive management is not actively involved in reviewing the information security strategy and ensuring that security risks are mitigated—insufficient awareness around information security policies. Information security roadmap is not built based on their current risks/threats.

Furthermore, centralized asset inventory, including key attributes such as CIA, was not developed in the context of risk management. Business and corporate applications are not linked to specific hosting infrastructure. Security risk assessment methodology/process and standardized ranking criteria are not defined. Application categorization based on the criticality of data in terms of CIA has not been performed following a formal risk assessment methodology jointly with the business owners. Most of the organization's high-level assessments do not identify specific risks or impacted assets. The data inserted onto their current security tools are not cross-checked with business owners. A risk register is not developed, including identified security risks and impacted assets. In the context of data protection, a list of confidential data is not maintained in an inventory. Exact locations and repositories hosting Personally Identifiable Information (PII) and other personal information are not identified.

A list of applications processing PII, along with the locations where data resides, is not defined as part of the records of processing activities. Clean Desk / Clear Screen

Related Items	Questions
Security Awareness	Q1-Q7
Malware Prevention	Q8-Q11
Logs management	Q12-Q17
Event Management and Security Information	Q18-Q22
Threat Intelligence	Q23-Q27
Fraud & Anomaly Detection	Q28-Q33
Directories management	Q34-Q40
User Account and roles management	Q41-Q47
Authentication	Q48-Q51
Grained Entitlements	Q52-Q55
Data Encryption	Q56-Q60
Database Monitoring	Q61-Q67
Cloud Providers and SaaS	Q68-Q73

The size of each organization ranged between 100 – 2000 employees as shown in table 2.

Table 1. Questionnaire and Related Items

No	Sector	No. of Vulnerable Systems	Country	ISMS Implemented
1	Bank	235	Germany	ISO27001
2	Bank	171	Germany	ISO27001
3	Bank	272	Germany	ISO27001
4	Bank	181	Germany	ISO27001
5	Bank	551	Germany	ISO27001
6	Bank	1131	Germany	ISO27001
7	Bank	173	Germany	ISO27001
8	Bank	210	Germany	ISO27001
9	Bank	100	United Kingdom	ISO27001
10	Bank	189	United Kingdom	ISO27001
11	Bank	1219	United Kingdom	ISO27001
12	Bank	2101	United Kingdom	ISO27001
15	Bank	367	United Kingdom	ISO27001
16	Bank	109	United Kingdom	ISO27001
17	Bank	89	France	ISO27001
18	Bank	1001	France	ISO27001
19	Bank	67	France	ISO27001
20	Bank	99	France	ISO27001
21	Bank	891	France	ISO27001
22	Bank	212	France	ISO27001
23	Bank	151	France	ISO27001
24	Bank	501	France	ISO27001
25	Bank	231	Netherland	ISO27001
26	Bank	704	Netherland	ISO27001
27	Bank	645	Netherland	ISO27001
28	Bank	357	Netherland	ISO27001
29	Bank	453	Netherland	ISO27001
30	Bank	785	Netherland	ISO27001
31	Bank	921	Netherland	ISO27001
32	Bank	436	South Africa	ISO27001
33	Bank	675	USA	ISO27001
34	Bank	553	USA	ISO27001
35	Bank	811	USA	ISO27001
36	Bank	232	USA	ISO27001
37	Bank	2342	USA	ISO27001
38	Bank	4501	Australia	ISO27001
39	Bank	2411	Australia	ISO27001
40	Bank	1965	Australia	ISO27001
41	Bank	1201	Australia	ISO27001
42	Bank	511	Japan	ISO27001
43	Bank	333	China	ISO27001
44	Bank	973	China	ISO27001
45	Bank	453	Russia	ISO27001
46	Bank	332	Switzerland	ISO27001
47	Bank	211	Switzerland	ISO27001
48	Bank	101	Belgium	ISO27001
49	Bank	91	Belgium	ISO27001
50	Bank	573	Switzerland	ISO27001

Table 2. Organizations and number of vulnerable systems detected after the pen testing

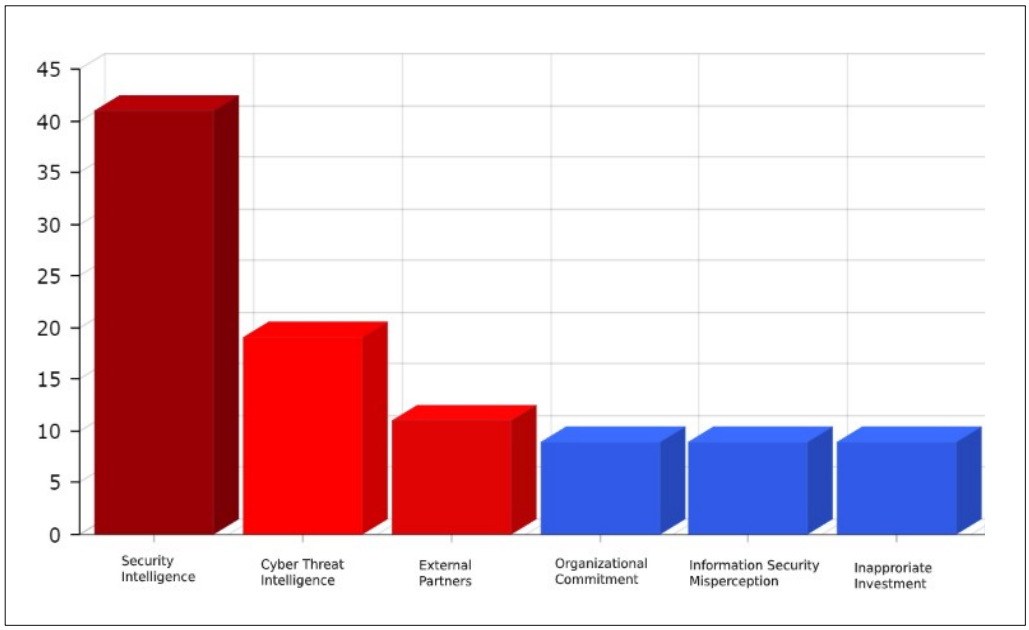


Figure 3. The NFC Process of Information Security

Policy is not defined. Removable Media (USBs) are enabled by default and used with no encryption. The Transparent Data Encryption (TDE) feature is not implemented to protect data stored in DBs. Privacy Enhancing Technologies (PETs) such as sanitization and masking technologies are not implemented. The secure disposal and decommissioning process are not defined or documented.

All organizations in our work had issues with user management and awareness. For example, the user lifecycle management processes, such as access review, are not fully documented. Core applications used for business operations are not integrated with Active Directory (AD), which makes tracking users' rights challenging. Privileged accounts used to manage Linux platforms, such as root, are not traceable. Several generic accounts were noted in different AD groups. Numerous standard user accounts (10+) are granted local admin privileges. A formalized process does not govern the usage of administrative charges. Local password policies are not enforced on some applications. For instance, some organizations were using four characters long for some critical applications. Specific training on information security policies is not provided to IT personnel.

We also realized their infrastructure weakness. For example, a VLAN topology scheme with description and functionality is not designed. The process of rules validation is not documented. I just wanted to inform you that a formal flow matrix is not meant. Due to a lack of documentation, the effectiveness of network segmentation could not be assessed. There is no regular and documented network equipment patch management process. There is no specific security hardening applied to network components. The IDS/IPS solution is not implemented (enabled) to detect/block malicious attacks. Network Admission Control or Switch Port security is not implemented. Access to public file-sharing platforms is enabled, which could be misused to exfiltrate data. Network Access Control (NAC) is not implemented. An endpoint compliance check is not performed.

Critical remote activities (e.g. admin operation on a server) are not logged or monitored. Application security was also a concern; the process is not yet enforced, and there is no business-oriented risk analysis systematically performed at the beginning of projects. Security reviews at the end of the design phase and acceptance are not fulfilled. Source code reviews for in-house developed applications are not conducted. Secure coding standards in line with security best practices such as OWASP are not defined. Security training is not provided to application developers. PII and financial information are not anonymized or pseudonymized. Applications testing performed by the development team utilize real/original data. Customers' related information is archived on a web app. Users access the application over HTTP and submit their credentials. Incident response-specific roles and responsibilities are not defined and documented.

Detailed incident root-cause analysis is not consistently conducted. The CISO and other operational teams are not trained to use a defined incident response service or to handle information security incidents. Cyber threat simulations or tabletop exercises are not regularly conducted. No process is defined around reviewing security incidents, and lessons learned are not identified or captured in a centralized repository. Information / Cyber security is not considered for IT and organization-wide crisis management processes. Recovery Time (RTO) and Recovery Point (RPO) for applications are not defined.

Last but not least, the list of initiatives compiled did not address all the key risks and issues identified from the audits and self-assessments. There is no local security operational dashboard. No security management dashboard has been developed, including security posture, main risks, security incidents and action plans. A consolidated list of local regulations impacting cyber security is not maintained. Application level (L7) security testing is not conducted. Application servers logs are not shipped to a centralized repository for review & monitoring. IPS/IDS solution is not implemented to block/detect suspicious security events. Intrusive penetrating tests are not conducted regularly and according to specific testing schedules. The researchers realized that the approved budget was underestimated or too low to acquire or enhance various security controls. All the banks in our work were informed about our findings and illustrated in table 3.

4. Field Work

The banks were divided into Group A and B. The Group A banks were asked to mitigate their vulnerability with their

Findings	Causes
Security Awareness	• Lack of security awareness-training • Human factors • Use of obsolete operating systems from critical tasks • Lack of BYOD policies • Limited visibility on the cloud security • Security breaches are not detected • Absence of compliance administrative Directives and/or roles. • Hindrance of leaders' conduct • Lack of security intelligence and threat intelligence
Data protection	• No USB restrictions
	• Lack of overall overview of responsibility • Network complexity • Lack of IPS and SIEM • Lack of network access control of LAN connection • Lack of backup policy compliant
IS Organization and governance, Risk Management	• Lack of administrative leaders and Support • Organizational disengagement • Lack of key security metrics and measures • Exhausting procedures and too many Rules (ISO27001). • Staff not conforming to compliance. • ISMS projects not completed. • Absence of training. • Absence of administrative leaders. • Absence of compliance department
Infrastructure security	• Insufficient workstation hardening • Lack of hard drive encryption • Complex filtering rules and complex network architecture
Monitor, Measure, Audit and Control	• Lack of KPI and vulnerable management system • Heterogeneous emergency password • Usage of invalid SSL certificates • Legacy domains

Table 3. Findings And Causes

current risk assessment tools in combination with the ISO. In contrast, the Group B banks were asked to mitigate their vulnerabilities by applying the NFC-ISMS as in the work of Stewart (2017) with the help of the researchers. We evaluated how each group performed between March and June 2019.

4.1. GROUP B

The instructions and recommendations to Group B were based on the NFC. This involved the three dynamics of the NFC, namely; A) Situation Awareness; B) controlling integration, and C) closing gaps.

4.1.1. Situation Awareness

The first step in the NFC principle is to identify the type of governance that will fit the business domain and then list any related controls. At this point, the organization's management board and security team need to understand their regulatory environment and conduct research on information security issues. This will enable them to identify all sources of governance applicable to their business domain. Utilizing the NINE-Five-Circle principle will enable organizations to harmonize their information security management framework. Assuming that the Bank and the Fintech organizations have plans to add credit cards to their services, they need to comply with other information security standards, such as the PCI DSS. Additionally, assuming the FinTech company decides to utilize a third-party service in light of budget constraints, they must comply with partner stands. These were intended to affect their security posture significantly, and the aim was then to compare the outcome with Group A. A conceptual framework was established based on our data analysis and outcomes. Our work is based on the NINE-Five-Circle principle that the governance establishment needs to follow, as illustrated in figure 4:

(1) Right Metrics

Our model consists of operation, organizing, budgeting, time frame, management and reporting procedures. All these factors ensure the appropriate usage of information effectively in the business units, by regulations and to provide strategic outcomes. From our analysis and findings, the proposed metric consists of the following:

a. End to end: All members should understand how their efforts contribute to the results. All members need to have a broad understanding of input and output procedures and the efficiency of the drivers.

b. Balance: Here, we propose that organizations should incorporate the measurement of their viability and productivity. Using the scorecards will enable organizations to quantify progression status and the adequacy of educational programs, occasionally on an alternate cadence than the execution reporting.

(2) Right Configuration

Due to employees not complying with organization rules and regulations, the lack of organization handbooks, the lack of clear rules and regu-lations, lack of IS training, lack of managerial direction, absence of compliance departments and the disregarding of essential strategies, it is vital for the organizations to utilize a method, e.g. a breakdown chart, to define the level of roles and obligations, and to report channels and correspondences to close any gap that may exist between operation substances and the governance system being applied. Meetings and reviews need to be held occasionally. This means top senior managers must effectively make decisions and address those attributes.

(3) Right People

At this phase, issues like; ill management, employee errors, lack of IS knowledge sharing, poor, or lack of, IS training, keeping relevant information to themselves, selfishness, lack of commitment, lack of security awareness, security infringement(s) not reported, disregarding essential strategies and lack of bringing own devices (BYOD) policies need to be addressed efficiently. Here, governing bodies should challenge and question standards at any time, and a responsibility assessment metric should be established to enable an operational team to establish joint decisions frequently.

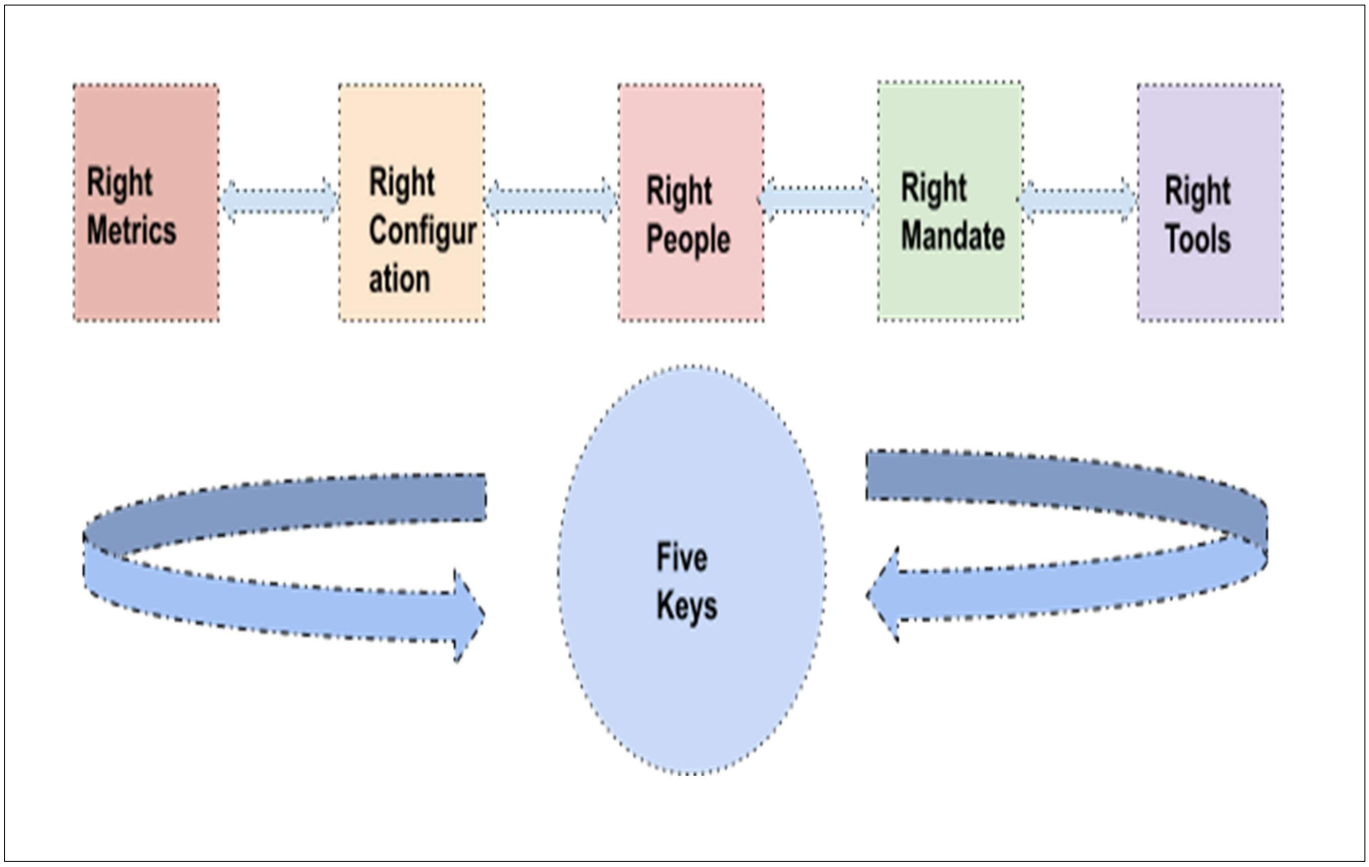
(4) Right Tools

This stage of the NINE-Five-Circle principle requires the right tools to monitor and detect staff activities. For example, they are accessing violations such as; malicious and viral software, monitoring unauthorized websites, and using a tool to monitor and approve the downloading of internet programs and email attachments. Furthermore, other tools to enable effective procedures need to be considered. An example is to enable the organization to assemble and enhance awareness of performance. In our work, we propose a “bolt-on tool” that will enable leaders to picture Service Level Agreement (SLA) performances and have an in-depth view to analyze leading causes.

(5) Right Mandate

Here, the right mandate needs to be established to address the punishment of culprit(s), poor, or lack of, security-related guidelines and the lack of security compliance regulations. The governance team should react proactively to any situation by monitoring and measuring delivery progress. This is vital for organizations that consolidate procedures and policies and operate globally. The leaders should survey all resolved obstructions and adjust various procedures into a single cognizant fund plan. Apart from the primary five keys; Right Metrics, Right Configuration, Right People, Right Tools and the Right Mandate, our principle pivot consists of the following guidelines that the organizations should consider, as shown in figure 5:

(i) Assign a certified leader: The compliance project should be assigned to a certified leader who has essential abilities. There are several certifications that organizations could look for when deciding on a competent leader, such as the CISM, CISSP, Lead ISO 27001 certificate, or the CISA.



(1) Right Metrics:

Figure 4. The NFC 5-Key steps

(ii) Communication/Commitment/Collaboration: These are not part of the significant five keys; however, since employees react to change critically, it is essential to make all changes transparent by answering employee queries and explaining why change is needed. Collaboration is characterized as working together with a specific end goal to accomplish an objective. Collaboration comes with participation, commitment and teamwork. It is a procedure in which at least two people, groups or organizations, cooperate to achieve shared objectives. Collaboration in information security management enables experts to gather, coordinate, group, disseminate, and share information security know-how with other experts and coworkers. Ahmad et al. (2012) highlighted the impact of collaboration and communication in information security management. Collaboration involves documentation and scheduling events and can be seen as proposing, submitting, reviewing, commenting and improving knowledge (Feledi et al., 2013).

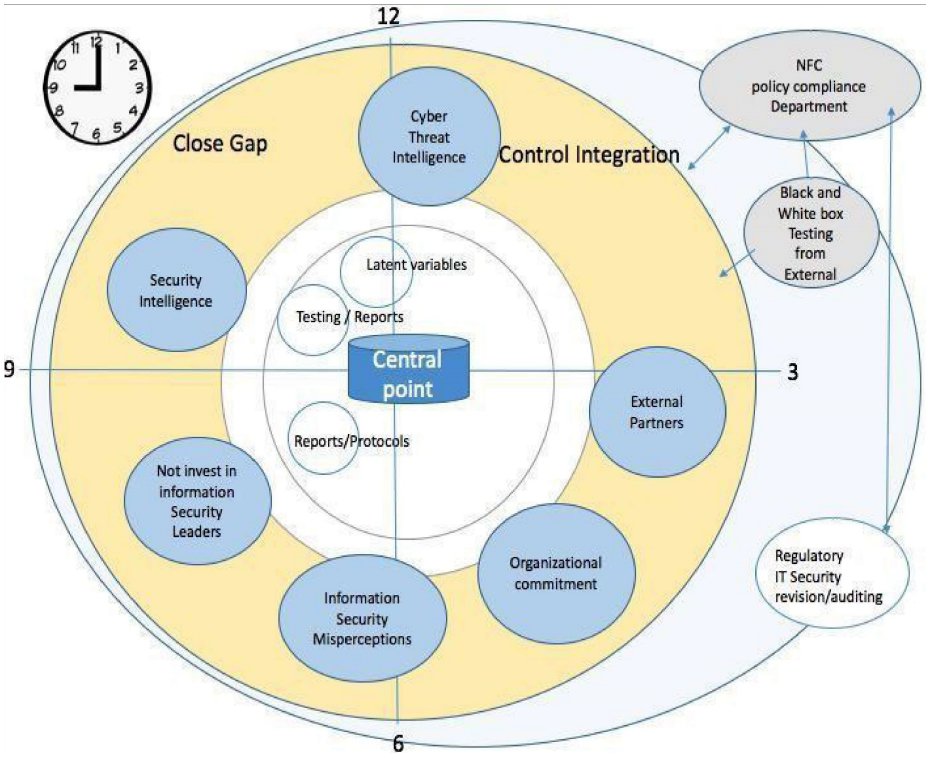
Two different measurements were performed to evaluate this effect's size and significance. We compared the differences in the number of vulnerabilities before and after the changes for both groups. Thus, if the average difference in the number of penetrations and connections per Denial of Service (DoS) attacks of Group A is significantly different from the average difference for Group B, then it is possible to conclude that the NFC affects security in comparison to the ISO27001 processes.

4.2. Discussion of NFC-ISMS

Process “The NFC steadiness is depicted using the central point, which holds all the causes and hindrances that are grouped into attributes and categorised as potential key factors. The key factors and the central point are encapsulated in the control integration and close gaps dynamic” (Stewart, 2017). This is illustrated in Figure 5.

As illustrated in Figure 5, the six key factors and the central prerequisites are enclosed in the control integration and close gaps dynamic. The rotation starts at the 9 o’clock, 12 o’clock, 3 o’clock, 5 o’clock, 6 o’clock, and 7 o’clock positions. The cycle is then repeated after the fifth round. According to Stewart (2017), the critical factor has to start at 9 o’clock, no matter how many factors are involved in a project. The minimum number of rotations is five times in each lifecycle.

Control activities and governance targets are defined and institutionalized in the integration phase. The extent to which all the critical factors and latent factors interrelate, as well as their central effects, are measured here. The NFC can represent unobserved factors or variables in these relationships and account for measurement errors. The



Source: Stewart, H. (2017). "Emerald: Information Security Management Systems".

Figure 5. The NFC Process of Information Security

procedure is controlled and measured persistently to acquire a dependable and predictable result of ISRM development and implementation in the NFC principle. To archive that, the complexities of the procedure in terms of different latent variables and interrelated variables are separated, comprehended, and re-integrated into a point of view to empower a complete understanding of the process.

The closing gap of the NFC enhances the connections between the information points while investigating the immense amount of information that must be filtered and transformed into usable knowledge. This enhancement enabled the organizations to transform their threat intelligence information from various sources into action by connecting critical factors such as security intelligence, cyber threat intelligence, external partners, employees' commitment, IS misperception and IS investment.

5. Benchmark

As earlier determined, the ISO 27001 standard has become the industry standard framework that has been more highly rated than all the others based on the 11EC's controls. With over 19,000 international standards being used in various industries, it has effectively risen above the profiles of the other five broadly used ISMSs. Over the years, its guidelines and the scope of the issues it encompasses have developed and spread into a focus on IT governance, information security, and service management. Regardless of this, the NFC-ISMS outperformed ISO 27001 in the benchmarks that are relevant to the standards as aforementioned. Suppose we incorporate the extent of ISO27002 (control implementation), ISO27005 (risk assessment and treatment), COBIT (IT governance), BS 7799 (information security), and ITIL (service management), all of which cut across all the other standards organizations like the PCIDSS and COSO. In that case, it can be seen that the NFC-ISMS is an increasingly vigorous and encompassing standard that enhances what ISO 27001 offers. It is in this benchmarking that ISO 27001 falls behind NFC-ISMS. This is shown in Table 5.

6. Limitation

Our work looked at the efficacy of a new comprehensive to prevent cybercrimes in organizations. Although the choice of our data collection method was perfect for this work, we believe that integrating additional methods of data collection would have increased the scope and depth of our outcomes. Furthermore, because we looked only at organizations in Germany, these findings may not translate to the organizations of other countries. Also, the researchers couldn't know how faithfully different companies tried to follow the presented standards and the incentive for doing so. However, the results of our work might still be widely applicable, as they will help organizations eager to mitigate cybercrimes in all parts of the world. This is because, for instance, ISO27001 is an international ISMS standard, and we have demonstrated in this

work that organizations using these standards could still benefit from the NFC.

Furthermore, for this kind of validation approach, obtaining as much data as possible is necessary. That is why collecting the data takes a lot of time and is relatively expensive. For this specific case, six different hackers needed to analyze the 25 organizations and far more internal systems, which was a monumental task.

	ISO27001 SERIES	**NFC-ISMS**
Profile of Standards	ISMS by the International Organization for Standardization (ISO) and the International Electro-technical Commission (IEC) in the year 2005 and became the first international standard for security management that comes with certification. It is a private organization but most member institutes are part of the governmental institutes.	NFC is a portable and flexible information security framework that indicates the necessities for the implementation of operational and information security enhancements. It also puts more emphasis on the measurement and evaluation of organization information security management incidents (ISMI) performance and outsourcing as well as the enhancement of the interrelationship between technology and human factors
Launched On	1947	2017
Initiated By **Certificate Name**	25 countries Certificate Name	 None
Scope	Scope	Information security, Corporate and IT Governance
Evaluation Method	Follow certifications evaluation procedure	Nine Five Circle
Weakness	1. ISO27001 cannot be solely relied upon by customers even though it is the internationally accepted standard for the time being. 2. Cost intensive and high documented processes 3. Increases unfair competitive advantage 4. Lack of actual quality improvement since after the certification, security improvement depends on what the organization does after the certification 5. Lack of oversight and accountability since the ISO focuses on the prerequisites for certifications rather than the organizations or the certification bodies Independent since organizations have to trust in Third Party Audit Time consuming	1. NFC-ISMS solely relies upon by customers even though it is not internationally accepted standard 2. Free and less documentation processes 3. No competitive advantage or disadvantage 4. Does not lack actual quality due to its portability and flexibility 5. In-depth oversight and accountability since the NFC focuses on ISMS enhancement and not certifications 6. Dependent since organizations get their own results through their own self-assessment

Table 4. Profile of ISO 27001 and NFC-ISMS

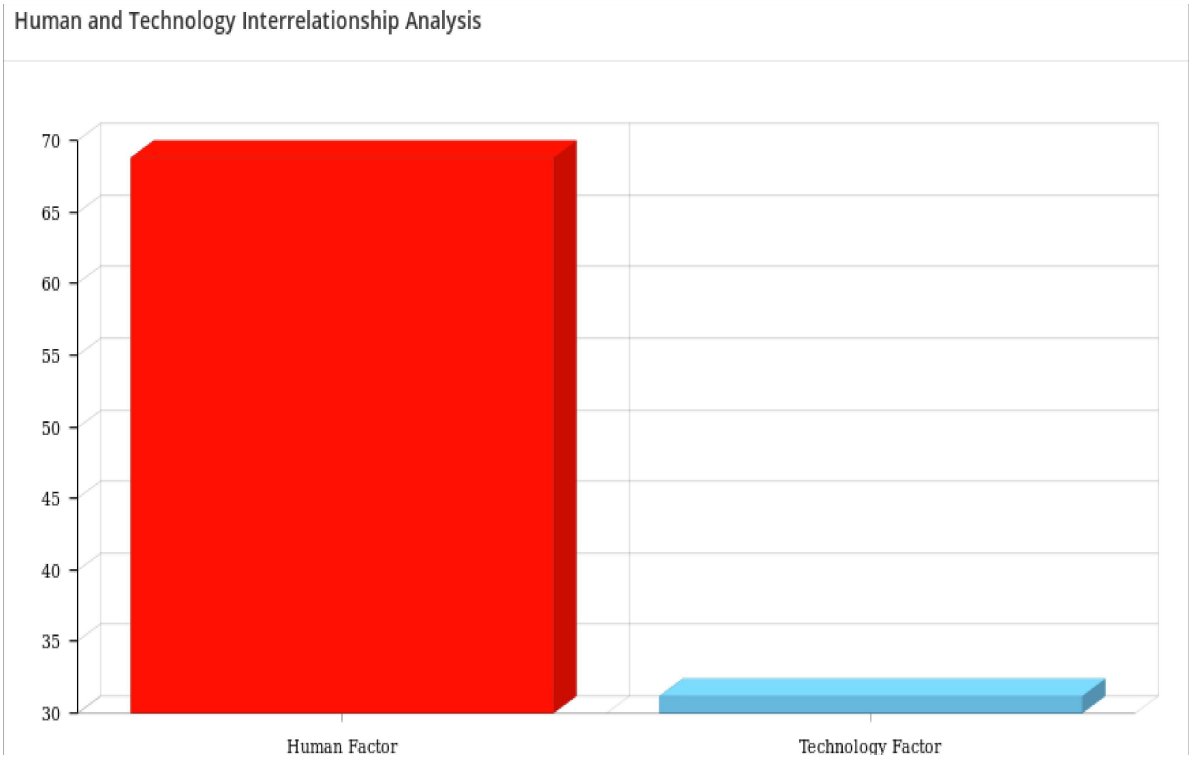


Figure 6. Human and Technology Interrelationship Analysis

Our knowledge base in this work was built on uncovering each piece of the puzzle, one at a time, and the limitations show us where further efforts need to be made.

7. Implication

The primary objectives of this paper were two-fold: to understand how organizations implement ISMS and how they make strategic decisions to derive practical implications and policy guidance for encouraging employee security awareness and acknowledgement. An underlying assumption is that the increase in data leakage in the presence of ISO certification can be mitigated by combining it with the NFC-ISMS and encouraging organizations to understand that compliance does not convey security. A practical challenge is how to promote this kind of awareness in enough instances to have a measurable beneficial effect on IS policies. The premise of our work is that by understanding the links between human, technology and individual behaviour, commitment and attitude about organization security policy, using the NFC-ISMS, ISO27001 certification can be better configured and targeted to help organizations achieve their desired outcome. Here, we cannot conclude that the human factor is the weakest link in information security but rather the technology used and how humans use these technologies, as illustrated in Figure 8 below (Stewart, 2017). From Figure 8, it is clear that the human factor has a higher risk score when compared to the technology score. However, technology scored 31%, while human error scored 69%. This indicates that there is a massive interconnection between both factors in the chain of information security.

8. Conclusion

The degree of the current ISMSs in the financial organizations surveyed was deemed insufficient. Establishing a comprehensive ISMS is essential to guarantee critical assets' confidentiality, integrity, and availability. There is a need to implement the Nine Five Circles (NFC), which fulfils international standards in the long run and closes the gaps that still exist between technology and humans. The proposed in our work demonstrates the NFC concepts, which include controls over the information technology environment, humans, culture, computer operations, access to programs and data, program development, and program changes.

In this manner, it demonstrates security best practices that could be utilized as a part of a comprehensive IS approach to resolve data breaches in the financial industries. This work highlights the benefits of the NFC, such as improving IS performance in terms of enhancing the security, reliability, and integrity of data, facilitating the change management process, and lowering the risk of fraud. In addition to the aforementioned outstanding features, it can be said that the NFC-ISMS can compare favourably with any of the ISO/IEC standards for information security. The outcomes could be utilized by financial technology innovators to improve their information security and to organize the efficient crosswise defence of infrastructure that might be vulnerable to technology and human assaults, which also answers our research questions one and two.

This paper targets a critical cybersecurity field and focuses on the ISMS approach, which can sometimes be complex and cumbersome for organizations to adopt and use. Any support along these lines is ideal and benefits the wider community. It is also great to see the research engagement with such a set of companies and individuals to build on their security.

References

[1] Anderson, H.L. (1986) Metropolis, *Monte Carlo and the MANIAC. Los Alamos Science*, 14, 96–108.

[2] D'Agostino, R., Pearson, E.S. (1973) Tests for departures from normality. *Empirical results for the distribution of b1 and b2. Biometrika,* 60, 613–622

[3] Enck, W., Gilbert, P., Chun, B.-G., Cox, L.P., Jung, J., McDaniel, P., Sheth, A.N. (2010) Taintdroid: An information-flow tracking system for realtime privacy monitoring on smartphones. *In*: Proceedings of the 9th USENIX Conference on Operating Systems Design and Implementation, OSDI'10. *USENIX Association*: Berkeley, CA, USA, 1–29.

[4] Ishikawa, K. (1985). What Is Total Quality Control? *The Japanese Way (trans. David)*, p. 56–61.

[5] Lu, J..NJ: Englewood Cliffs (2005). ISO/IEC. Prentice Hall, Inc. ISO/IEC: Englewood Cliffs, USA. International Organization for Standardization/International Electrotechnical Commission, p. 27002 – *Information technology – Security techniques – Information security management systems – Requirements*.

[6] ISO/IEC (2009) ISO/IEC, 27000. Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. International Organization for Standardization/International Electro technical Commission.

[7] Jouini, M., Rabai, L.B.A., Aissa, A.B. (2014) *Classification of security threats in information systems*. Procedia Computer Science, 32, 489–496.

[8] Kandias, M., Mylonas, A., Virvilis, N., Theoharidou, M., Gritzalis, D. (2010). *An insider threat prediction*. In: *The 7th International Conference on Trust, Privacy, and Security in Digital Business (TrustBuse2010)*, Vol. 6264 *of LNCS*, p. 26.e37.

[9] Loch, K.D., Carr, H.H., Warkentin, M.E. (1992) Threats to information systems: *Today's reality, yesterday's understanding. MIS Quarterly,* 16, 173–186.

[10] Luo, T., Hao, H., Du, W., Wang, Y., Yin, H. (2011). Attacks on webview in the android system, *In. Proceedings of the 27th Annual Computer Security Applications Conference, ACSAC'11. ACM*: New York, USA, p. 343–352.

[11] Neumann, P.G. (1999) *Inside risks: Risks of insiders. Communications of the ACM*, 42, 160–160.

[12] O'Mahony, M. (1986). Sensory Evaluation of Food: Statistical Methods and Procedures. CRC Press: Boca Raton, p. 487.

[13] Stewart, H., Jürjens, J. (2017) Information security management and the human aspect in organizations. Information and Computer Security, 25, 494–534.

[14] Stewart, H., Jürjens, J. (2018) Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, 26, 109–128.

[15] Von Solms, R., Van Niekerk, J. (2013) From information security to cyber security. *Computers and Security*, 38, 97–102 .

[16] Von Solms, R. (1998) Information security management (3): The Code of Practice for Information Security Management (BS 7799). I*nformation Management and Computer Security*, 6, 224–225.

[17] Vroom, C., Von Solms, R. (2004) Towards information security behavioural compliance. *Computers and Security*, 23, 191–198.

[18] Warkentin, M., Willison, R. (2009) Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, 18, 101–105.

[19] Wilson, M., Hash, J. (2003). Building Information Technology Security Awareness and Training Program [NIST special publication], Vol. 800, p. 1–39.