International Journal of Early Childhood Special Education (INT-JECSE)
DOI:10.9756/INTJECSE/V14I5.206 ISSN: 1308-5581 Vol 14, Issue 05 2022

SIGNIFICANCE OF IMPLEMENTATION OF IS POLICY AND INTERNAL MONITORING MECHANISM, IN ACCOMPLISHING COMPLIANCE WITH INFORMATION SECURITY REGULATIONS, FRAMEWORKS AND STANDARDS (RFS), FOR BANKING SECTOR

[1]Ashish Ukidve, [2]Dr. S SMantha and [3]Dr. D N Reddy

[1]Principal,Vidyalankar Polytechnic, Mumbai

[2]Foermer Chairman, AICTE, Chancellor-KL University

[3]Professor, Osmania University, Former VC, JNTUH

[1]ashish.ukidve@vpt.edu.in, [2]ssmantha33@gmail.com and [3]reddydn@gmail.com

ABSTRACT

Manyorganisationsprovide IT Enabled servicesto their external as well as internal customers. These services are provided to customers irrespective of the size of business mix of the organisation or availability of appropriately skilled human and technology resources. This leads to challenges in accomplishing the compliance with the applicable Information Security Regulations, Frameworks and Standards (RFS). This paper explores the effect of comprehensive IS policies, their effective implementation and implementation monitoring audit mechanisms, in accomplishing the compliance with the applicable information security Regulations Framework and standards.

1. INTRODUCTION

Information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements. Organisational IT and Information Security (IS) practices and processes are driven and governed by these set of rules. IT and IS policies are prepared and implemented by organisations. However, For compliance with Regulations, Frameworks and Standards (RFS), for the organisations providing IT and ITES; various factors that need to be incorporated in IS policies, their implementation and monitoring mechanisms remain a domain which needs to be explored further.

This research paper, investigates various factors that need to be taken into consideration while preparing IS policies, its implementation and monitoring mechanisms for accomplishing compliance with Regulations, Frameworks and Standards, as applicable to organisations.

2. LITERATURE REVIEW

The Information Security Management discipline has evolved, as discussed by von Solms[1], in four phases. In initial technical phase, ISM was considered as primarily responsibility of IT in the organization. However as the information security challenges grew with time, ISM was techno-management responsibility. In this phase, organizations started focusing on various aspects of information security, including policy [2][3], training & awareness programmes [4][5], strategic management support and involvement [6]. The third phase, the institutional phase emerged once management phase started becoming the standard practice across organizations. In this phase attention was to build an information security culture within the organizations [5][7]. International standards and certifications (e.g.BS 7799 and ISO/IEC 17799) also evolved during this phase.

With further maturity in the ISM discipline governance phase evolved wherein, many frameworks for organizational ISM have been developed [8][9]. Singh, Gupta and Ojha [10]have summarized some of these frameworks along with their identified key external and internal factors.

Various GRC frameworks that are prevalent globally can be classified into the Generic frameworks, applicable to all type of industries and the Specific frameworks, which are applicable to a particular type of industry. Generic frameworks provide guidelines regarding information security and compliance that can be applicable to any type of business. Control Objectives for Information and related Technology (COBIT) framework, which is specialized in information security and governance, has been proposed by IT Governance Institute (ITGI) and Information Systems

Audit and Control Association (ISACA). This a frame- work provides set of best practices to maximize the benefits of IT utilization. COBIT also covers cyber security risk that can occur with the usage of IT. National Institute of Standards and Technology – NIST has proposed a customizable guide to manage cybersecurity related risk by combination of existing standards and best practices. ISO 27000:2018 (International Organization for Information Security Management) guidelines are inclusive and applicable to extensive range of businesses. Organisations can use this set of guidelines for preparing comprehensive IS policies. By implementing these comprehensive IS policies and their regular monitoring will lead to compliance with Regulations, Frameworks and Standards, for the organisations providing IT and ITES

3. RESEARCH METHODOLOGY

For the analysis following methodology has been adopted–

1. Descriptive statistical analysis involving structural equation-based modelling and factor analysis have been used for testing the hypothesis, because they can assess the multiple interrelated relationships between measured independent variables, with the "constructs" and also analyse the level of relationships between these constructs.
2. Analysis of data collected from survey conducted across different organisations based on the size of organisation

3.1 Descriptive Statistical Analysis of Parameters - Comprehensive isPolicy, Its Effective Implementation and Internal Mechanism

For this investigation "Deep dive analysis of the industry vertical – banking and insurance sector" has been conducted. It included review of IS policies, their implementation and internal monitoring mechanisms for compliance of applicable information security, pertaining to the Information Technology enabled banking and insurance services, offered in India. The domains

covered in this analysis included Adoption of Comprehensive Information Security Policy, Effective implementation of adopted IS policy, Standard Operating Procedures (SOPs) regarding routine operations considering compliance, internal information Security assessment and audit framework and third party IS assessments and audits for verification of compliance of information security regulations.

It was noted that many earlier surveys had meagre response (Kotulic and Clark, 2004) because many times the information asked during the surveys was critical or non-disclosable. Keeping this in focus, inputs were taken from certified, practicing information systems assessors and auditor in the field of information security. For this analysis, evaluation of compliance was done with IS audit teams, as per guidelines provided by regulations and frameworks such as ISACA's Standards and Guidelines, RBI Regulatory Guidelines, RBI Cyber Security framework (CSF), NPCI norms & guidelines, PCIDSS standard, ISO27001:2018, ISO27002, Bank's IS Policies, Industry Best Practices.

For this analysis structural equation model has been used with the identified constructs and their independent factor parameters. The relationship between IS policies, procedures and internal monitoring , assessment and audit mechanisms with organisation's IS compliance has been analysed. For this analysis, details of the independent factor parameters and the corresponding dependent constructs are given in Table 1 –

Table 1

Dependent construct	Factor Id	Independentfactor parameter
IS Policies and Procedures	IPP1	Preparing IS policy for the organisation has been outsourced to external consultants
IS Policies and Procedures	IPP2	Adoption of Comprehensive Information Security Policy
IS Policies and Procedures	IPP3	Effective implementation of adopted IS policy
IS Policies and Procedures	IPP4	Availability of documented Standard Operating Procedures (SOPs)
Internal monitoring	IM1	Adherence of SOPs regarding routine operations considering compliance

Internal monitoring	IM2	Internal audit framework and process for information security assessment based on compliance requirements of applicable frameworks
Internal monitoring	IM3	Self-initiated third party IS assessments and audits for verification of compliance
Internal monitoring	IM4	Review of IS policies and procedures

For this investigation, sample banks were identified based on their total business mix ranging from Small size bank (Less than 1000 Cr), Medium size bank (from 1000 Cr to Less than 10000 Cr) Large size bank (from 10000 Cr to 1 lac Cr) and Very Large size bank (beyond 1 lac Cr). In order to understand the viewpoints of different hierarchical levels in the organisations respondents were selected using purposive sampling technique. The respondents were from different types of banks, having different sizes of bank's business mix, with variety of job roles/profiles within the banks including IT professionals, information security practitioners. Respondents also included members of external IS auditors, framework assessors and statutory auditors of the banks. Discussions with certified internal IS auditors, framework assessors, third party IS compliance auditors of the organisations were also conducted. Table 2 below provide findings of this survey:

Table 2: [Survey findings - impact of IS Policies and Internal monitoring in accomplishing IS compliance]

Dependent construct	**Factor Id**	**Parameter**	% Respondents			
			Small size bank (Less than 1000 Cr),	**Medium size bank (from 1000 Cr to Less than 10000 Cr)**	**Large size bank (from 10000 Cr to 1 lac Cr)**	**Very Large size bank (beyond 1 lac Cr).**
IS Policies and Procedures	IPP1	Preparing IS policy for the organisation has been outsourced to external consultants	71.12	89.33	91.21	94.43
IS Policies and Procedures	IPP2	Adoption of Comprehensive Information Security Policy	42.24	57.87	76.23	92.12
IS Policies and Procedures	IPP3	Effective implementation of adopted IS policy	54.32	69.12	87.31	88.27
IS Policies and Procedures	IPP4	Availability of documented Standard Operating Procedures (SOPs)	41.23	67.43	82.12	86.13
Internal monitoring	IM1	Adherence of SOPs regarding routine operations considering compliance	39.32	65.37	76.24	87.38
Internal monitoring	IM2	Internal audit framework and process for information security assessment based on compliance requirements of applicable frameworks	42.87	57.39	79.17	89.33
Internal monitoring	IM3	Self-initiated external IS assessments and audits for verification of compliance	51.46	71.45	79.22	87.23

Internal monitoring	IM4	Review of IS policies and procedures	71.12	89.33	91.21	94.43

For further analysis, the structural equation modelling based on measurement scale and goodness-of-fit indicators (GFI), has been used [5]. The lists of independent factor parameters of the measurement scales are as per Table 3 and goodness-of-fit indicators are as per Table 4, for each construct.

Table 3 - Measurement scale – for independent factor parameters

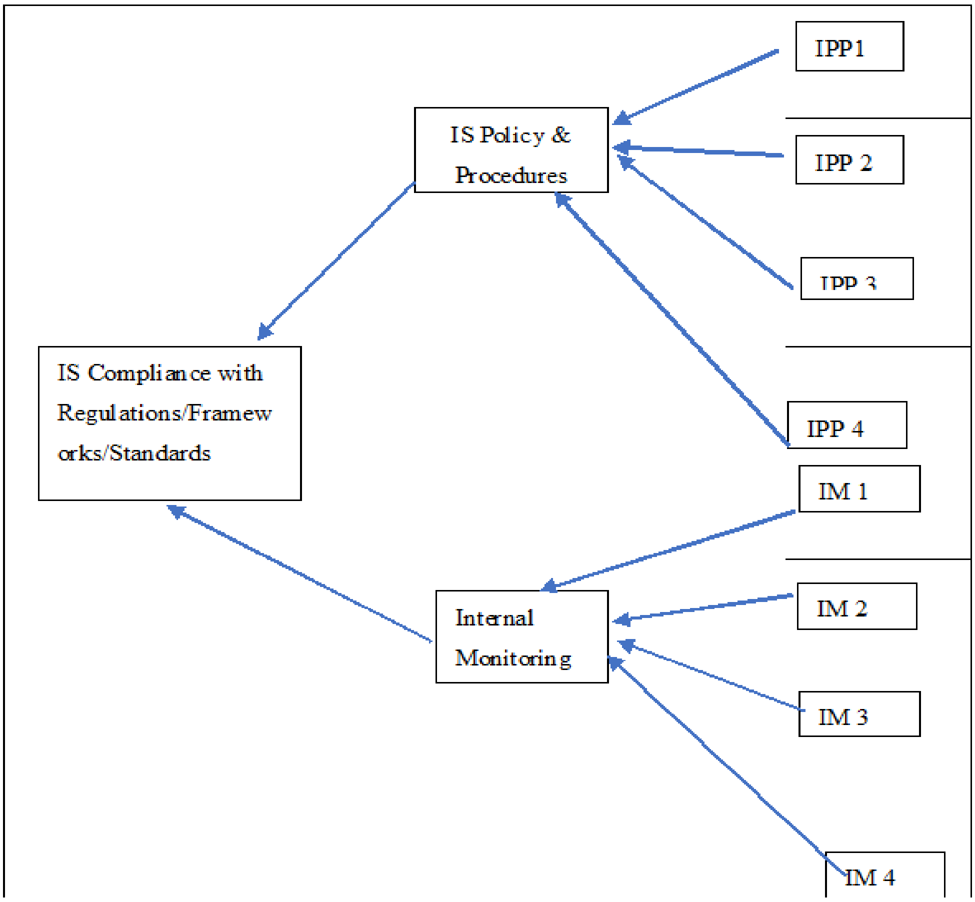
z	**Independent factor parameter**
IPP1	Preparing IS policy for the organisation has been outsourced to external consultants
IPP2	Adoption of Comprehensive Information Security Policy
IPP3	Effective implementation of adopted IS policy
IPP4	Availability of documented Standard Operating Procedures (SOPs)
IM1	Adherence of SOPs regarding routine operations considering compliance
IM2	Internal audit framework and process for information security assessment based on compliance requirements of applicable frameworks
IM3	Self-initiated external IS assessments and audits for verification of compliance
IM4	Review of IS policies and procedures

Table 4 - Goodness-of-Fit indicators

Construct	**X^2**	**Df**	**þ**	**AdjX^2**	**GFI**	**CFI**	**Cronbach "α"**
Acceptable cutoff values	NA	NA	Non-Significant þ-value	≤ 2.0	≥ 0.90	≥ 0.95	≥ 0.70
IS Policies andProcedures(4 constructs)	6.31	30	0.513	0.769	0.96	0.97	0.88
Internal monitoring (4 constructs)	4.44	30	0.442	1.360	0.98	1.0	0.77

INFERENCE

1. Good reliability and consistency of the constructs is indicated by Cronbach "α" values ≥ 0.7
2. As the three constructs have Adjusted "$X^{2"}$ values below the acceptable cutoff value "2.0", overall fit of the proposed model is indicated.
3. The observed correlations and covariances adequately fit the proposed model as indicated by the p- value [11]
4. The proposed model has overall fit of data, as indicated by values of Goodness of fit (GFI), being close to 1.0,
5. The observed comparative fit index (CFI) values are close to 1.0, which are above recommended cut-off of 0.95 for the given sample size, thereby indicating adequacy of fit [12][11]
6. As $p < 0.001$, all path relationships and factor loadings are significant, as indicated in Figure 1, which depicts the structural mode.



- **Fig 1**– The schematic structural model

Results of the above analysis indicate that IS policy, its effective implementation and internal mechanism for monitoring of IS compliance are significant factors in accomplishment of organisational IS compliance with the regulations, frameworks and standards. These findings are consistent with s relevant literature on the topic.

3.2 Analysis of parameters – comprehensive IS policy, its effective implementation and internal monitoring mechanisms, based on survey conducted across different organisations based on the size of organisation

Results of Table 1 and Fig 2 indicate that the for the same parameter there is significant variation in responses depending on the size the business mix of bank. The findings about the parameters for size of banks are as given below:

3.2.1 Respondents from 71.12% of small size banks, 89.33%, medium size, 91.21% in large size banks and 94.43% of very large size banks opined that that the task of preparing IS policy for the organisation was outsourced to external consultants.

It was noted that while preparing the policy especially in case of small andmedium size banks, there was standard template based approach, rather than consideration of inputs from banks to understand needs of the customer segment pertaining to bank, existing status of IT infrastructure, IS processes, IS culture, user and customer awareness level about IS etc. Due to this, it was observed that for many policies, the actual working in the bank deviates from the expectations of these policies leading to gaps in implementation. This would increase the risk of vulnerabilities in the systems and processes, which could be exploited by cyber threats.

3.2.2 According to 54.32%respondents from small size banks, 69.12% from medium size banks 87.31% in large size banks and 88.27% of very large size banks; the adopted IS policy has been effectively implemented in their respective organisations.

It was observed especially in case of small and medium size banks that certain deviations from policy were taken during actual banking processes and operations.

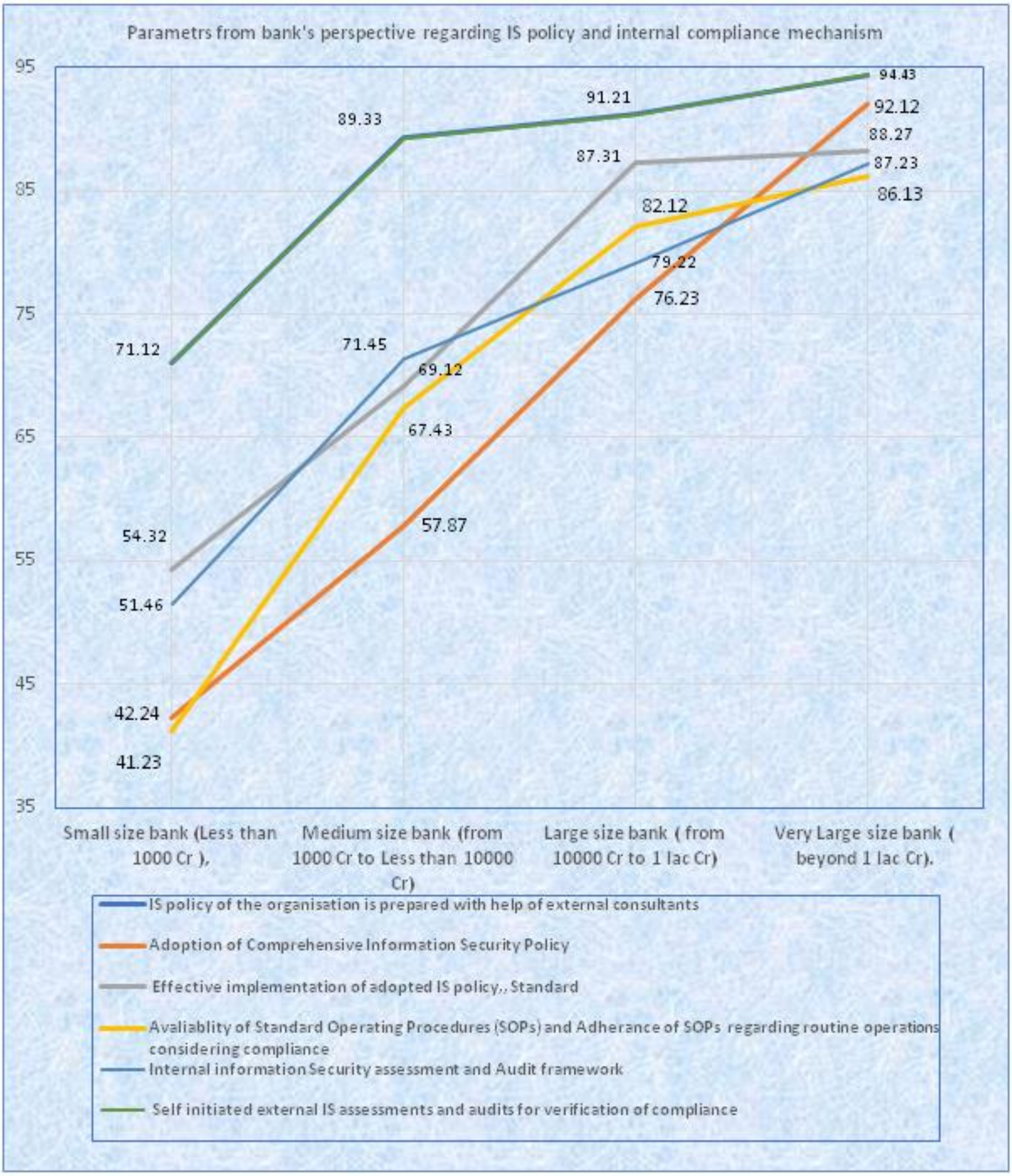


Fig 2. Analysis of parameters from banks' perspective regarding IS policy, compliance mechanisms

3.2.3 41.23% of respondents from small size banks, 67.43%, from medium size, 82.12% from large size banks and 86.13% respondents from very large size banks stated that documented Standard Operating Procedures (SOPs) were available and that adherence to SOPs in view of IS compliance was implemented in their respective organisations.

It was observed especially in case of small and medium size banks that certain deviations from policy were taken during the actual banking processes and operations.

3.2.4 Internal audit framework and process, for assessment of information security based on compliance requirements of applicable frameworks, was incorporated in their respective banks; according to 51.46% of respondents from small size banks, 71.45%, from medium size banks, 79.22% from large size banks and 87.23% respondents from very large size banks

It was observed especially in case of small and medium size banks that the internal monitoring and assessments of compliance were not implemented as per the compliance requirements of regulations, frameworks and standards, applicable to the banks.

3.2.5 According to 71.12% of respondents from small size banks, 89.33% respondents from medium size banks, 91.21% from large size banks and 94.43% respondents from very large size banks; the process of self-initiated external IS assessments and audits for verification of compliance has been implemented by their organisations.

It was noted that except very large banks, other banks do not undertake due cognizance of shortfalls in compliance identified by these external IS audits because of which they remain unattended. This would increase the risk of vulnerabilities in the systems and processes, which could be exploited by cyber threats.

4. CONCLUSIONS

Considering the foregoing analysis including the results of 3.1&3.2, it can be established that –

1. The task of preparing IS policy for the organization has been outsourced to external consultants by many organisations. These consultants usually take standard template-based approach, rather than considering confluence of requirements of applicable regulatory frameworks. They should also consider inputs from banks to understand the customer segment, existing status of IT infrastructure, IS processes, IS culture, user and customer awareness about information security processes and IS compliance, while preparing IS policies.
2. It was observed that documented Standard Operating Procedures (SOPs) were available and that adherence to SOPs in view of IS compliance was implemented in their respective organisations. It was observed especially in case of small and medium size banks that certain deviations from policy were taken during the actual banking processes and operations.
3. Internal audit framework and process for information security assessment, based on compliance requirements of applicable frameworks, was incorporated. It was observed especially in case of small and medium size banks that the internal monitoring and assessments of compliance were not implemented as per the compliance requirements of regulations, frameworks and standards, applicable to the banks.
4. The process of self-initiated external IS assessments and audits for verification of compliance has been carried out by their organisations. It was noted that except very large banks, other banks do not undertake due cognizance of shortfalls in compliance identified by these external IS audits because of which they remain unattended. This would subsequently lead to non-compliance of regulatory frameworks, increase the vulnerabilities in the systems which would effectively increase the cyber risks to the organisation's information security.

5. REFERENCES

1. Solms, Basie Von. "Information security-The third wave?.", Computers & security 19.7 , pp. pp 615-615., 2000.

2. Knapp, Kenneth J., et al., " "Information security: management's effect on culture and policy."," Information Management & Computer Security, 2006.

3. Thomson, K. L., Von Solms, R., & Louw, L., " Cultivating an organizational information security culture," Computer fraud & security,, pp 7-11, 2006.

4. Wolden, Mark, Raul Valverde, and Malleswara Talla, ""The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system."," IFAC-PapersOnLine 48.3 : pp 1846-1852., 2015

5. Bulgurcu, Burcu, Hasan Cavusoglu, and Izak Benbasat., " "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness."," MIS quarterly (2010): 523-548..

6. Hong, Kwo-Shing, et al., " "An empirical study of information security policy on information security elevation in Taiwan." ," Information Management & Computer Security (2006)..

7. Furnell, Steven M., Alastair G. Warren, and Paul S. Dowland. , ""Improving security awareness through computer-based training." ," in IFIP World Conference on Information Security Education. Springer, New York, NY, 2003.

8. Kankanhalli, A., Teo, H. H., Tan, B. C., & Wei, K. K. , " An integrative study of information systems security effectiveness," International journal of information management, 23(2), 139-154, (2003).

9. Perks, Col, and Tony Beveridge, "Guide to enterprise IT architecture," . Springer Science & Business Media, 2007.

10. Singh , Gupta , Oza , "“Identifying factors of "organizational information security management",” September 2014 , Research gate , European Journal of Marketing 27(5).