International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

Assessing Information Security Governance in Public Sector Banks of India

Koli J. Mohan[1], Saini A. K.[2]
[1]*USMS, Guru Gobind Singh Indraprastha University, Govt. of Delhi, India*
[2]*USMS, Guru Gobind Singh Indraprastha University, Govt. of Delhi, India*
Corresponding Author Orcid ID : 0009-0004-0696-3673

ABSTRACT
Purpose of the study: This study aims to investigate and analyze the Information Security governance practices within banks.
Design/methodology/approach: This is a Survey-based study. Employees of State Bank of India in Delhi region were the participants of the study.
Findings: The findings of the study will contribute to the existing body of knowledge on information security governance in the banking sector.
Research limitations: Small sample size and lack of funds for performing comprehensive quantitative study are the limitations of the study.
Practical implications: Regulatory compliance, incident response, and data recovery are all a part of this process, as well as risk assessment and management, policy and procedure creation, security awareness and training, security controls and technology, and more. Public sector organizations may improve their security posture and better secure their information assets by adopting a systematic approach to information security governance.
Social implications: Data protection, service protection, privacy, fighting cybercrime, public trust, and economic impact are only few of the societal effects of researching information security governance in public sector organizations. Organizations in the public sector can reduce the risk of financial and reputational damage as well as secure sensitive information by employing best practices in information security.
Originality/value: The research outcomes will help identify areas of improvement, highlight effective practices, and provide recommendations for enhancing information security governance within banks. Ultimately, this study contributes to the development of robust Information Security governance frameworks that can protect sensitive data, mitigate risks, ensure regulatory compliance, and maintain the trust and confidence of customers and stakeholders in the banking industry.
Keywords- Information Security Governance; IT Regulations; Public Sector Enterprises; Public Sector Banks; Government standards

1. Introduction

Information security governance refers to the framework, processes, and structures that organizations establish to ensure effective management and protection of their information assets. It involves the strategic alignment of security objectives with business goals, the establishment of policies and procedures, and the allocation of responsibilities to manage information security risks.Implementing effective information security governance helps organizations protect their sensitive data, maintain trust with stakeholders, and ensure business resilience in the face of cybersecurity threats (Flores et al., 2014). It is a holistic approach that integrates security into the organization's overall governance framework. Information Security Governance in public sector enterprises is essential for ensuring the protection of sensitive information, maintaining public trust, and meeting legal and regulatory requirements (Bauer & Bernroider, 2017). Here are some key considerations specific to information security governance in the public sector (Chang et al., 2006):

DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

- Legal and Regulatory Compliance: Public sector enterprises must comply with various laws, regulations, and government policies related to information security. These may include data protection laws, privacy regulations, sector-specific requirements, and government guidelines. Information security governance ensures that the organization understands and adheres to these obligations.
- Government Standards and Frameworks: Public sector enterprises often follow government-defined standards and frameworks for information security governance. For example, in some countries, government agencies provide specific guidelines or frameworks tailored to the public sector. Compliance with these standards helps ensure a consistent and unified approach to information security across public entities.
- Stakeholder Engagement: Public sector enterprises have a diverse range of stakeholders, including government entities, citizens, and businesses. Information security governance should involve engaging with these stakeholders to understand their security requirements, address concerns, and build trust. This may involve consultation, collaboration, and regular communication to ensure that security measures meet stakeholder expectations.
- Risk Management: Public sector enterprises face unique risks due to the sensitive nature of the information they handle, including citizen data and government secrets. Effective information security governance includes robust risk management processes. Risk assessments, threat modeling, and vulnerability assessments help identify and prioritize risks, enabling the implementation of appropriate controls and risk mitigation strategies.
- Interagency Collaboration: In the public sector, collaboration among different government agencies and entities is often necessary for effective information security governance. Sharing best practices, threat intelligence, and security incident response capabilities can enhance the overall security posture. Establishing cross-agency partnerships and information sharing mechanisms strengthens the collective defense against cybersecurity threats.
- Security in Public Service Delivery: Public sector enterprises often provide critical services to citizens, such as healthcare, social welfare, and transportation. Information security governance should ensure that these services are delivered securely, protecting sensitive data and maintaining service availability. This may involve implementing security controls in service delivery systems, securing public-facing websites, and protecting citizen data.
- Governance and Oversight: As with any organization, governance and oversight are crucial in public sector enterprises. Clear roles and responsibilities, accountability mechanisms, and governance structures ensure that information security is prioritized and monitored. This includes establishing governance committees, appointing information security officers, and conducting regular audits and assessments.
- Training and Awareness: Public sector employees need to be trained and made aware of their roles and responsibilities in information security. Training programs and awareness campaigns help ensure that employees understand security policies, procedures, and best practices. This reduces the risk of human error and improves the overall security culture within the organization.

By implementing robust information security governance practices, public sector enterprises can effectively protect sensitive information, prevent security incidents, and uphold the trust placed in them by citizens and stakeholders.

NCIIPC has broadly identified the following as ‘Critical Sectors’:-

- Power & Energy
- Banking, Financial Services & Insurance
- Telecom
- Transport
- Government
- Strategic & Public Enterprises

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

The aim of this research was to study the information security governance in public sector enterprises. The objectives of the study are as follows:
The objectives of studying information security governance in banks are as follows:

- To provide a comprehensive understanding of the current state of information security governance practices in banks.
- To identify the key challenges and obstacles faced by banks in effectively implementing information security governance.
- To evaluate the extent to which banks comply with relevant regulatory requirements and industry standards pertaining to information security governance.
- To assess the effectiveness of risk management practices within the Information Security governance framework of banks.
- To evaluate the incident response capabilities of banks in handling Information Security incidents.
- To assess the level of employee awareness and training programs related to information security governance in banks.
- To explore the governance structure of information security within banks, including roles, responsibilities, and reporting lines.
- To identify best practices in information security governance within the banking industry

2. Research methodology

This was a survey-based study. The participants were employees of differentbranch of State Bank of India in Delhi. This a quantitative study, the Primary data was obtained through a survey designed to understand the information security governance of State Bank of India.Sampling technique adopted for the study will be Non-Probability Purposive and Conveniences sampling. Spreadsheet software was used to examine the data that was collected.

3. Results and interpretation

100 participants of Mean ± SD of age 33.41±6.17 years were included in the study. Out of the 100 participants 61 were males and 39 were females. The following are the interpretation of the questionnaires filled by the participants of the study.

Policies and Procedures:

a. Does your bank have a documented information security policy?
Yes
No

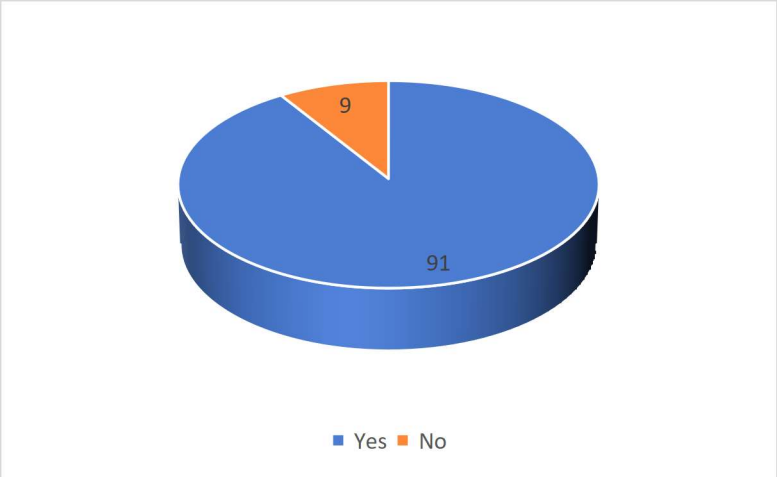

Figure 1

Interpretation: When asked whether their bank had a documented information securitypolicy, 91 participants responded Yes and 9 responded No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

b. How often is the information security policy reviewed and updated?
6 months once
Yearly once
3 years once

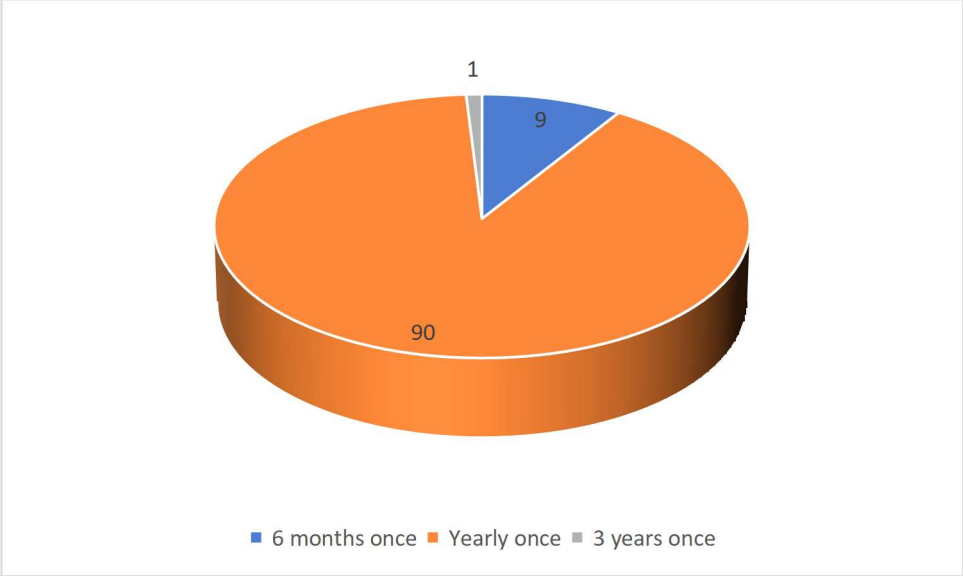

Figure 2

Interpretation: When asked how often is the information security policy reviewed and updated, 90 participants said yearly once, 9 participants told 6 months once and 1 told three years once

c. Are there documented procedures for managing information security incidents?
Yes
No

Figure 3

Interpretation:When asked if there are documented procedures for managing information security incidents 99 participants told Yes and 1 told NOo

d. Are employees required to sign an agreement indicating their understanding and compliance with information security policies?

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

Yes
No

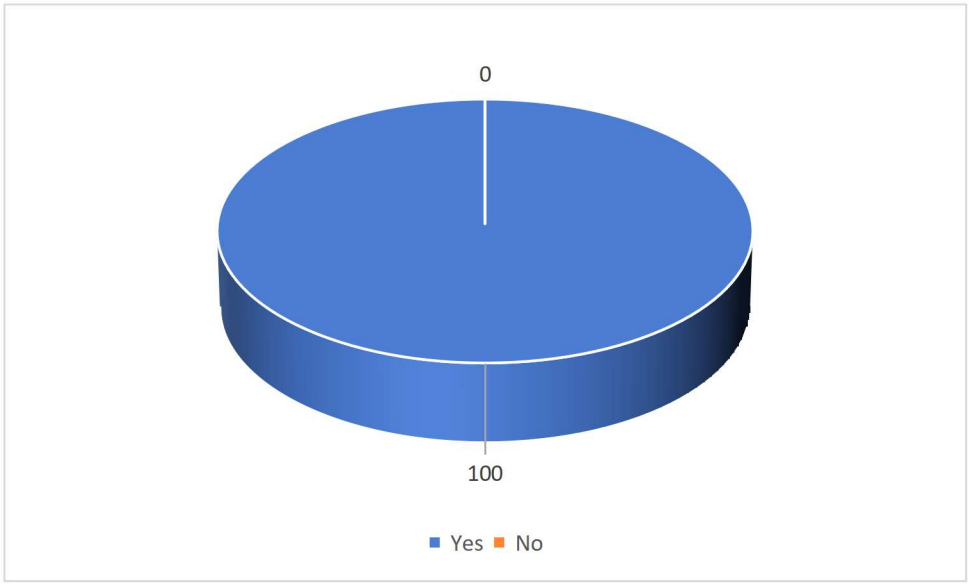

Figure 4

Interpretation:When asked are employees required to sign an agreement indicating their understanding and compliance with information security policies, 100 participants told Yes

Risk Management:

a. Does your bank have a formal risk management framework for information security?
Yes
No

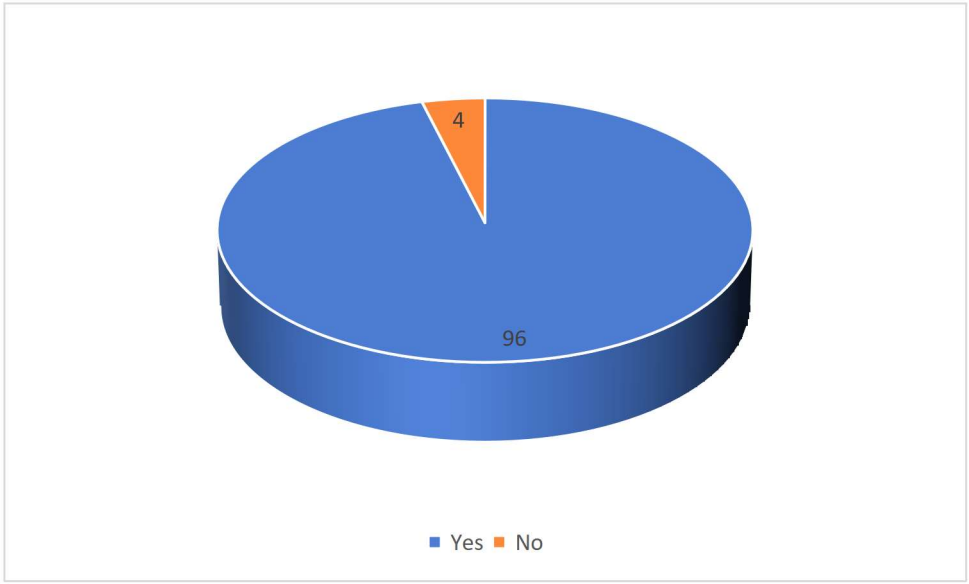

Figure 5

Interpretation:When asked did their bank have a formal risk management framework for information security 96 participants told Yes and 4 told No

b. How often are information security risks assessed?
Once a year
Once in two years
Once in three years

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

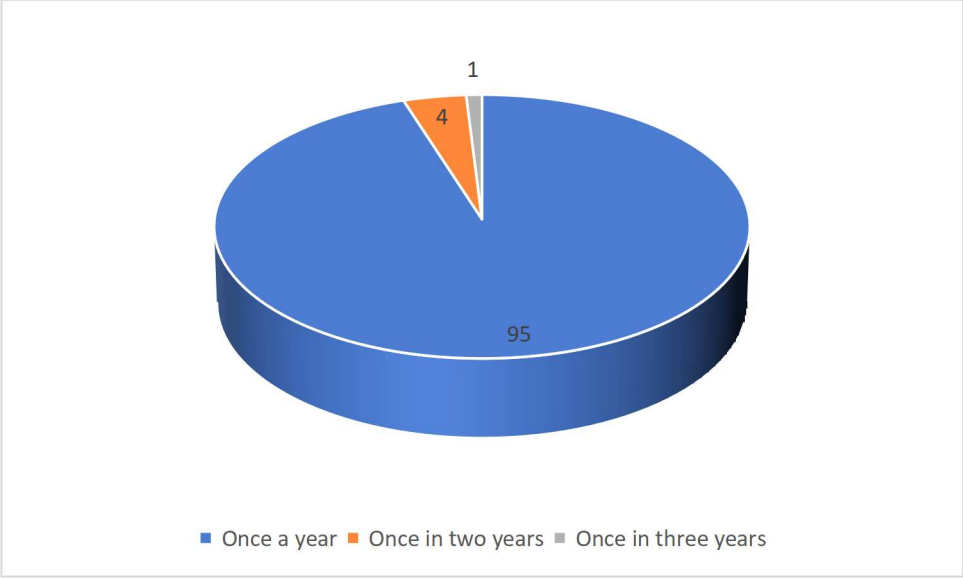

Figure 6

Interpretation: When asked often are information security risks assessed, 95 participants told once a year, 4 participants told once in two years and 1 participant once in three years

c. Does the bank have a process for identifying, assessing, and mitigating information security risks?
Yes
No

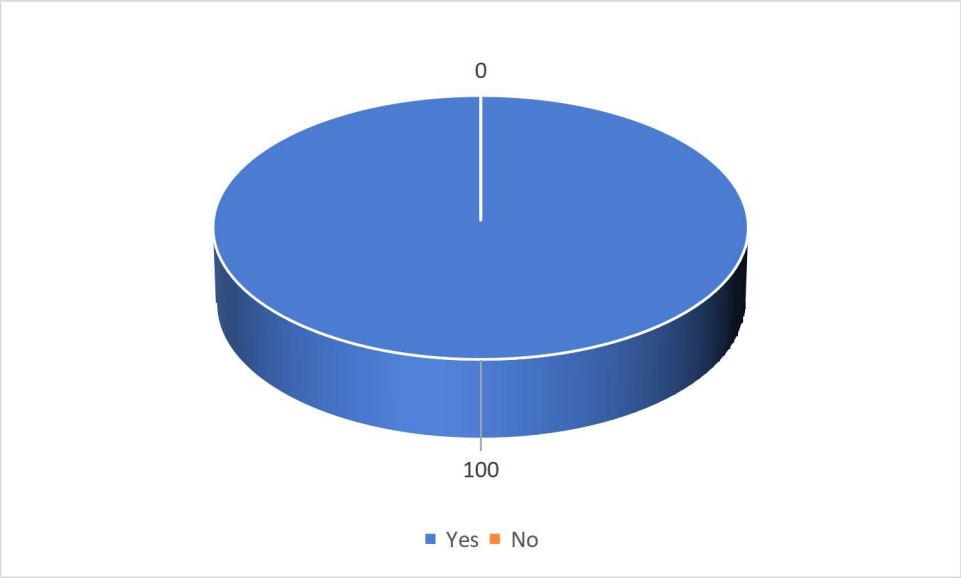

Figure 7

Interpretation: When asked whether the bank have a process for identifying, assessing, and mitigating information security risks, 100 participants told yes

Compliance:

a. Is your bank subject to any specific regulations or standards related to information security (e.g., GDPR, PCI DSS)?
Yes
No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

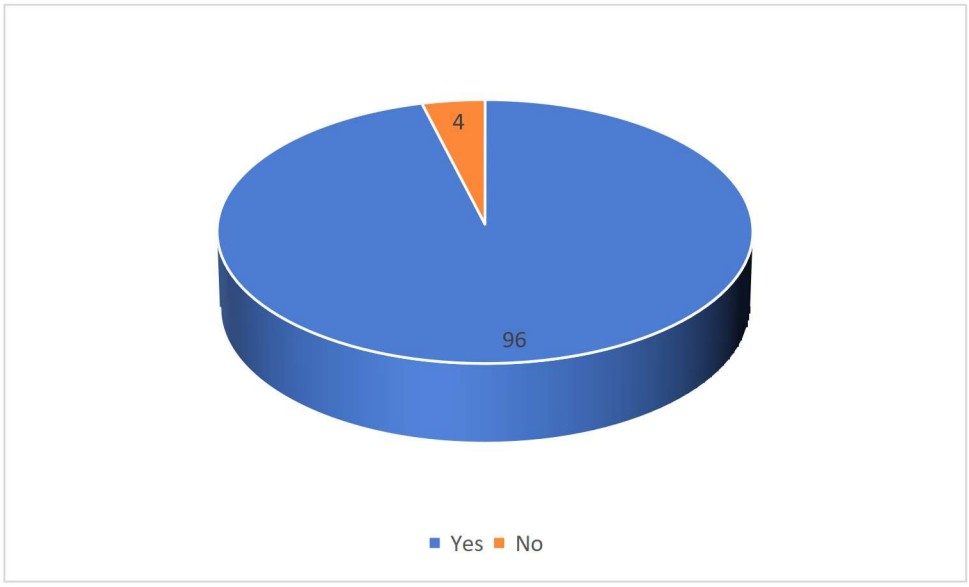

Figure 8

Interpretation: When asked does their bank subject to any specific regulations or standards related to information security (e.g., GDPR, PCI DSS), 96 participants told Yes and 4 participants told No

b. Are regular internal audits conducted to assess compliance with information security requirements?
Yes
No

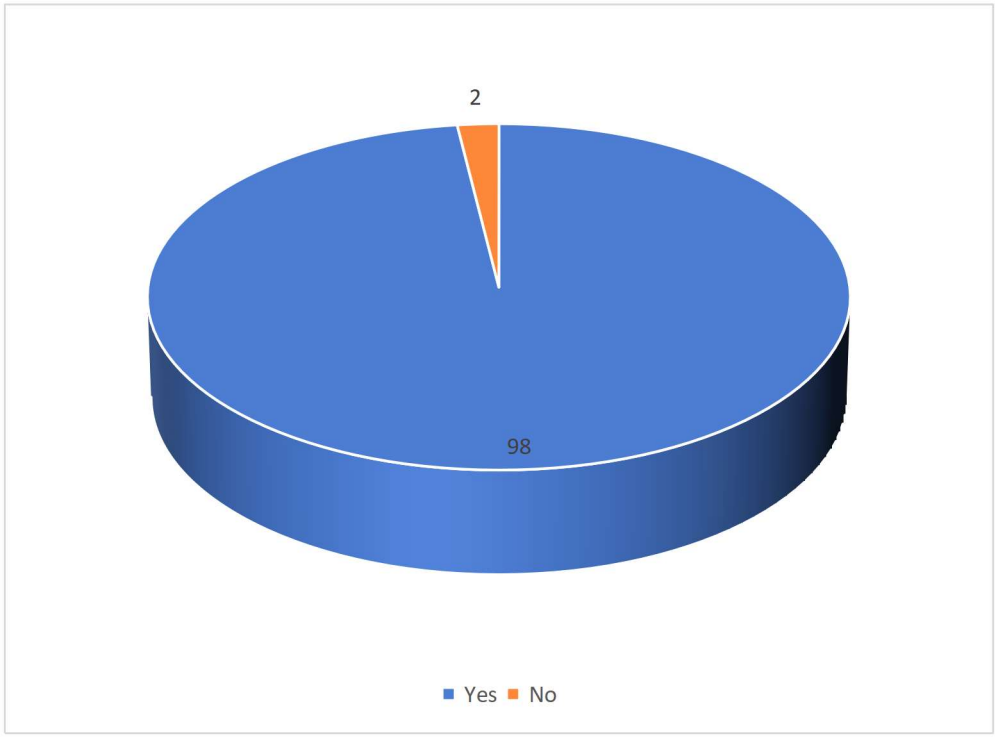

Figure 9

Interpretation:When asked is there regular internal audits conducted to assess compliance with information security requirements, 98 participants told Yes and 2 participants told No

Employee Awareness and Training:

a. Does the bank provide information security awareness training to employees?
Yes
No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

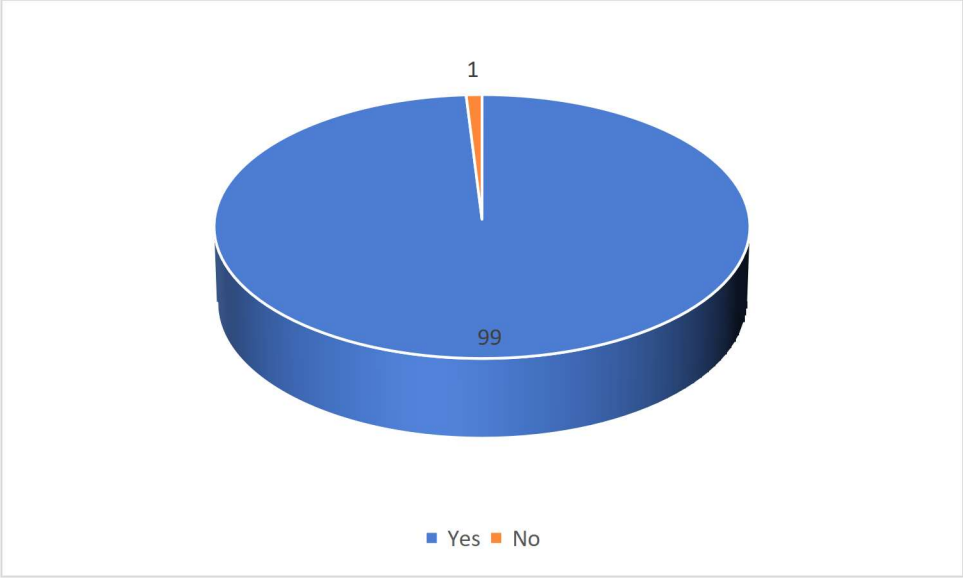

Figure 10

Interpretation: When asked does the bank provide information security awareness training to employees, 99 participants told Yes and 1 told No

b. How often is this training conducted?
6 months once
Yearly once
3 years once

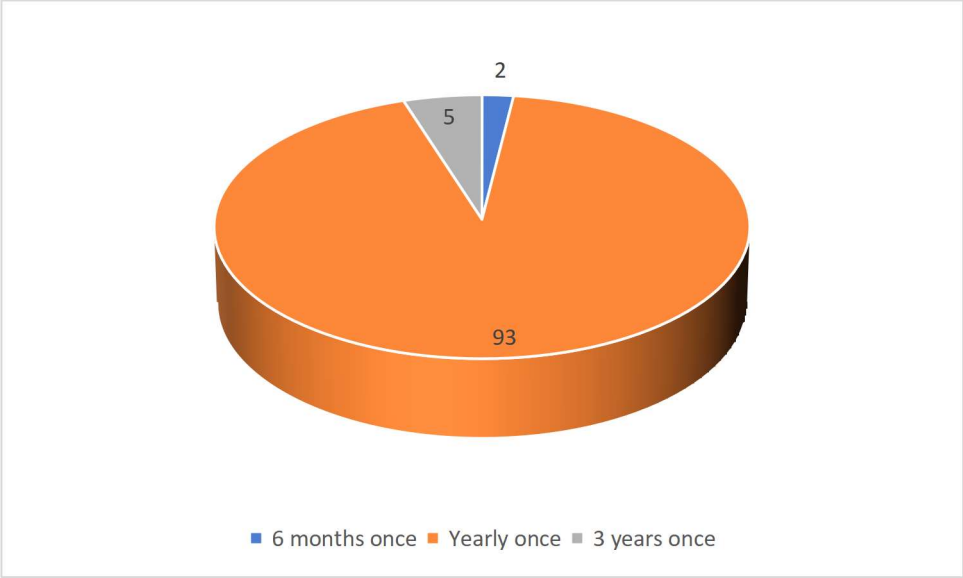

Figure 11

Interpretation:When asked how often is this training conducted, 93 participants told yearly once, 2 told 6 months once and 2 told 3 years oce

c. Are employees required to complete periodic security awareness assessments?
Yes
No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

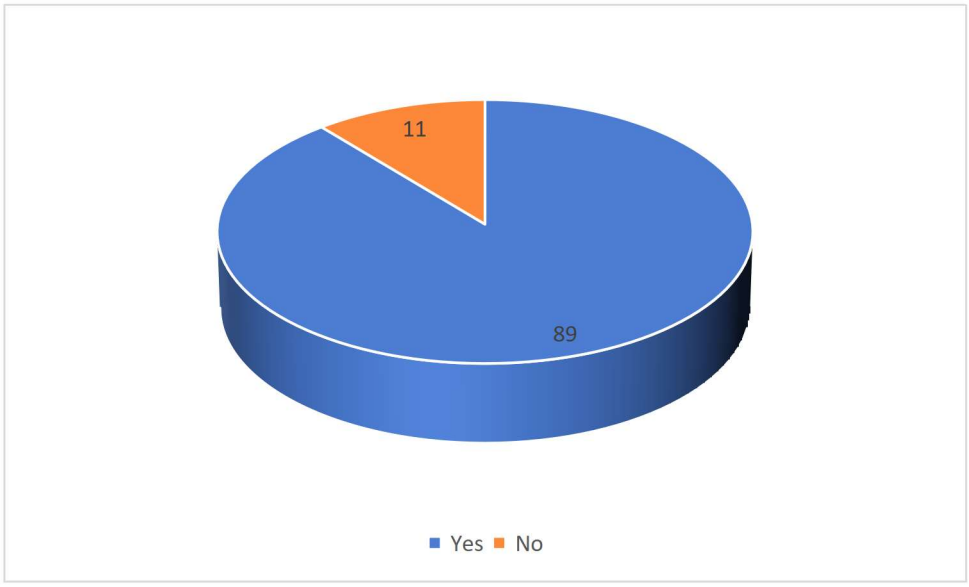

Figure 12

Interpretation: When asked are the employees required to complete periodic security awareness assessments 89 participants told Yes and 11 told No.

Security Controls:

a. Are there security controls in place to protect sensitive data (e.g., encryption, access controls)?

Yes

No

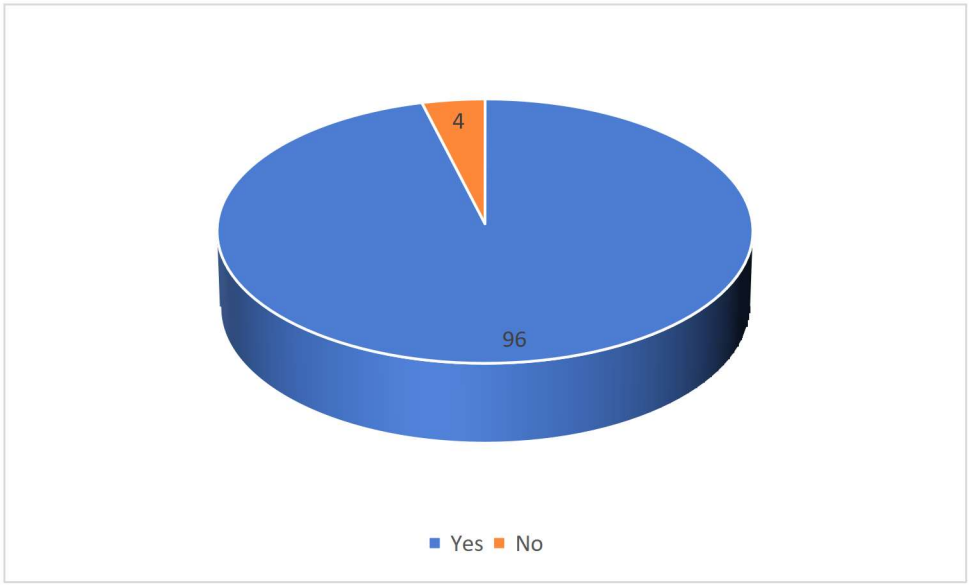

Figure 13

Interpretation: When asked are there security controls in place to protect sensitive data (e.g., encryption, access controls), 96 participants told Yes and 4 told No

b. Are regular vulnerability assessments and penetration tests conducted?

Yes

No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

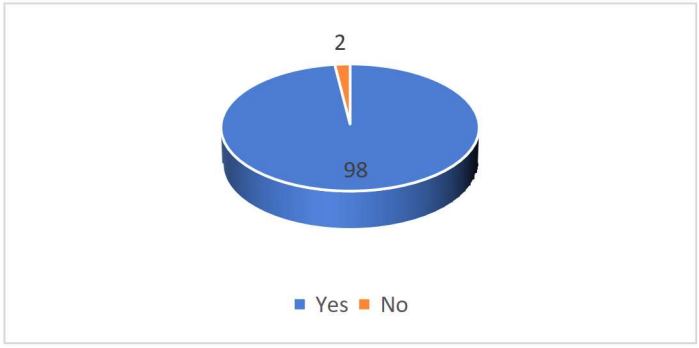

Figure 14

Interpretation: When asked are regular vulnerability assessments and penetration tests conducted, 98 participants responded Yes and 2 told No

Security Incident Reporting:

a. Are employees encouraged to report suspicious activities or security incidents?

Yes

No

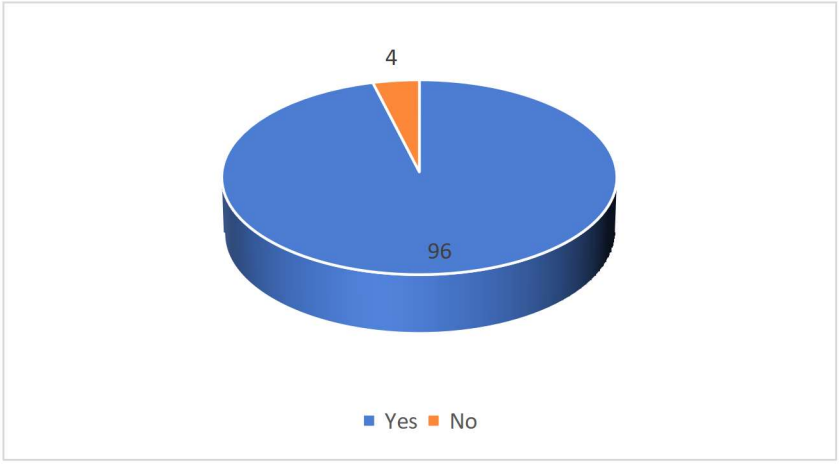

Figure 15

Interpretation: When asked are employees encouraged to report suspicious activities or security incidents, 96 participants responded Yes and 4 told No

b. Is there a formal process in place for reporting security incidents?

Yes

No

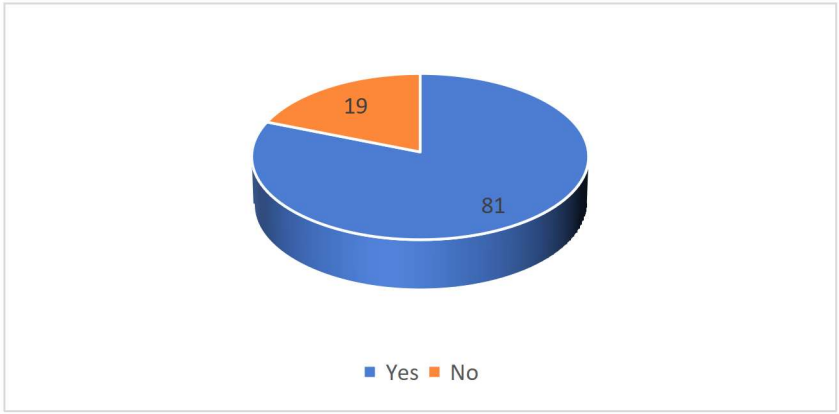

Figure 16

Interpretation: When asked is there a formal process in place for reporting security incidents, 81 participants responded Yes and 19 participants responded No

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

4. Suggestions and recommendations:

Effective information security governance is crucial for banks to protect sensitive data, mitigate risks, and comply with regulatory requirements. Based on the existing best practices and research in the field, here are some suggestions and recommendations for enhancing information security governance in banks:

1. Establish a Comprehensive Governance Framework:
   - Develop a formal information security governance framework that aligns with industry standards and regulatory requirements.
   - Clearly define roles, responsibilities, and reporting lines for information security governance stakeholders, including the board of directors, senior management, and information security teams.
2. Involve Senior Management and the Board of Directors:
   - Ensure that senior management and the board of directors actively participate in information security governance activities.
   - Promote a culture of information security awareness and accountability throughout the organization.
3. Conduct Regular Risk Assessments:
   - Implement a robust risk management process to identify, assess, and prioritize information security risks.
   - Regularly review and update risk assessments to address emerging threats and vulnerabilities.
4. Develop and Communicate Policies and Procedures:
   - Establish comprehensive information security policies and procedures that address areas such as access control, data protection, incident response, and business continuity.
   - Communicate these policies and procedures to all employees and ensure their understanding and compliance.
5. Implement Security Controls and Monitoring Mechanisms:
   - Deploy appropriate technical and organizational security controls to protect critical systems, networks, and data.
   - Implement continuous monitoring mechanisms to detect and respond to security incidents promptly.
6. Foster Employee Awareness and Training:
   - Develop an ongoing awareness program to educate employees about information security risks, policies, and best practices.
   - Provide regular training sessions and promote a culture of security awareness and responsibility among all staff members.
7. Manage Third-Party Risks:
   - Implement a robust third-party risk management program to assess the security practices of vendors, suppliers, and outsourcing partners.
   - Include information security requirements in contracts and agreements with third parties and regularly monitor their compliance.
8. Establish an Incident Response Plan:
   - Develop and regularly update an incident response plan that outlines roles, responsibilities, and procedures for addressing security incidents.
   - Conduct regular drills and simulations to test the effectiveness of the plan and improve response capabilities.
9. Regularly Review and Audit Information Security Governance:
   - Conduct periodic internal and external audits to assess the effectiveness of information security governance practices.
   - Use the findings from audits to identify areas for improvement and implement necessary changes.
10. Stay Updated with Emerging Trends and Regulations:

DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

- Continuously monitor and adapt to changes in the information security landscape, including emerging threats, technologies, and regulatory requirements.
- Stay informed about industry best practices, standards, and frameworks related to information security governance.

11. Foster Collaboration and Information Sharing:
- Engage in industry collaborations and information-sharing initiatives to stay informed about emerging threats and effective security practices.
- Participate in forums, conferences, and industry working groups to exchange knowledge and experiences with peers.

5. Conclusion

Information Security Governance is of paramount importance in the banking industry to ensure the protection, integrity, and confidentiality of sensitive financial data. Banks are prime targets for cyberattacks due to the high-value information they possess, making it imperative to establish robust governance frameworks (Alber & Nabil, 2016).

By implementing effective Information Security Governance practices, banks can achieve several significant outcomes. Firstly, it enables the identification and assessment of potential risks and vulnerabilities, allowing proactive measures to be taken to prevent security breaches. This helps protect customer data, financial transactions, and critical systems from unauthorized access, fraud, or theft.

Secondly, Information Security Governance promotes compliance with industry regulations and standards. The banking sector is heavily regulated, with stringent requirements for data protection, privacy, and risk management. A strong governance framework ensures that banks meet these regulatory obligations, reducing legal and reputational risks and maintaining customer trust.

Furthermore, Information Security Governance enhances operational resilience within banks. By implementing robust controls and security measures, banks can safeguard against system failures, cyber threats, and operational disruptions. This ensures the availability and continuity of banking services, minimizing downtime and financial losses.

Moreover, Information Security Governance facilitates effective incident response and recovery. Banks must have well-defined incident management procedures in place to detect, respond, and recover from security incidents promptly. A governance framework helps banks establish incident response plans, coordinate actions, and minimize the impact of potential breaches or attacks.

Additionally, Information Security Governance promotes a culture of security awareness and accountability within banks. Training programs, awareness campaigns, and regular communication help educate employees about security risks and their responsibilities in safeguarding sensitive information. This helps create a security-conscious workforce that can identify and report potential threats, reducing the likelihood of security incidents.

In conclusion, Information Security Governance is critical for banks to protect customer data, comply with regulations, maintain operational resilience, and foster a culture of security awareness. By implementing robust governance practices, banks can effectively manage risks, protect their reputation, and build trust among customers and stakeholders in an increasingly digital and interconnected banking landscape.

Furthermore, Information Security Governance enhances the overall operational efficiency of public sector enterprises. By implementing effective controls and security measures, organizations can minimize the likelihood of security incidents, system disruptions, and data breaches. This leads to uninterrupted service delivery, reduced downtime, and increased productivity. In addition, Information Security Governance helps organizations in effectively responding to security incidents or breaches. It establishes incident response plans, including detection, containment, eradication, and recovery procedures, enabling timely and coordinated actions to mitigate the impact of any security event.

DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

Lastly, Information Security Governance contributes to the establishment of a culture of security awareness and accountability within public sector enterprises. It promotes education and training programs, ensuring that employees are equipped with the necessary knowledge and skills to protect information assets and adhere to security policies and procedures.In conclusion, Information Security Governance is crucial for public sector enterprises to protect sensitive information, comply with regulations, maintain operational efficiency, respond to incidents effectively, and foster a culture of security awareness. By prioritizing and implementing robust governance practices, these organizations can effectively manage risks and secure their information assets, ultimately fulfilling their responsibilities to citizens and stakeholders.

6. References

Flores, W. R., Antonsen, E., &Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & security*, *43*, 90-110.

Alber, N., & Nabil, M. (2016). The impact of information security on banks' performance in Egypt. *Available at SSRN 2752070*

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, *106*(3), 345-361.

Venkatraman, S., &Delpachitra, I. (2008). Biometrics in banking security: a case study. *Information Management & Computer Security*, *16*(4), 415-430.

Bauer, S., &Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems*, *48*(3), 44-68.

Appendix

Policies and Procedures:

a. Does your bank have a documented information security policy?
Yes
No

b. How often is the information security policy reviewed and updated?
6 months once
Yearly once
3 years once

c. Are there documented procedures for managing information security incidents?
Yes
No

d. Are employees required to sign an agreement indicating their understanding and compliance with information security policies?
Yes
No

Risk Management:

a. Does your bank have a formal risk management framework for information security?
Yes
No

b. How often are information security risks assessed?
One a year
Once in two years
Once in three years

c. Does the bank have a process for identifying, assessing, and mitigating information security risks?
Yes

International Journal of Engineering Technology and Management Sciences
Website: ijetms.in Issue: 5 Volume No.7 September - October – 2023
DOI:10.46647/ijetms.2023.v07i05.012 ISSN: 2581-4621

No

Compliance:
a. Is your bank subject to any specific regulations or standards related to information security (e.g., GDPR, PCI DSS)?
Yes
No
b. Are regular internal audits conducted to assess compliance with information security requirements?
Yes
No

Employee Awareness and Training:
a. Does the bank provide information security awareness training to employees?
Yes
No
b. How often is this training conducted?
6 months once
Yearly once
3 years once
c. Are employees required to complete periodic security awareness assessments?
Yes
No

Security Controls:
a. Are there security controls in place to protect sensitive data (e.g., encryption, access controls)?
Yes
No
b. Are regular vulnerability assessments and penetration tests conducted?
Yes
No

Security Incident Reporting:
a. Are employees encouraged to report suspicious activities or security incidents?
Yes
No
b. Is there a formal process in place for reporting security incidents?
Yes
No