# Awareness and Compliance of Information Security Policy in Organizations: Case from Libya

Salima Benqdara
University of Benghazi
Benghazi, Libya

## ABSTRACT
According to a review of the literature, Many employees are unaware of information security policies or choose to disregard them, which can lead to non-compliance. Lack of compliance with the intended policy results from a failure to understand the complicated relationships in the design and implementation of information security rules. This paper assesses the gaps in information security policy compliance. The paper aims to assess the existence of any gaps in the compliance and awareness of employees in the company. In this study, A questionnaire method was utilized to provide an understanding of the compliance within the organization. The questions were carefully selected to cover several factors of the subject areas. The outcome of the questionnaire is important to assess any hypothetical noncompliance among employees, and to specify who is more responsible, the management or the employee. The result finds that many employees are unaware of disregarding information security policies, which can lead to security breaches. The results show that employees are often unaware of information security policies and that they may not understand the importance of compliance. The paper concludes with recommendations for improving employee awareness and compliance with information security policies.

## General Terms
Information security policy Awareness and Compliance.

## Keywords
Information security, Information security policy assessment, Awareness, and Compliance.

## 1. INTRODUCTION
Contemporary companies rely largely on technology to protect their information, which is extremely vulnerable to attack from both the inside and the outside. As a result, protecting information and protecting information assets has grown to be a top issue for companies and their clients. [1]Information security policy provides the necessary platform and environment of regulations in an organization to control users' security-related behavior [2]. Policies direct how issues should be addressed and technologies should be used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. It must be clear that Policy should never contradict the law because this can create significant liability for the organization. Security policies are the least expensive control to execute, but the most difficult to implement properly [3].

Contemporary companies rely largely on technology to protect their information, which is extremely vulnerable to attack from both the inside and the outside. As a result, protecting information and protecting information assets has grown to be a top issue for companies and their clients[1]. Information security policy provides the necessary platform and environment of regulations in an organization to control users' security-related behavior [2]. Policies direct how issues should be addressed and technologies should be used. Policies do not specify the proper operation of equipment or software—this information should be placed in the standards, procedures, and practices of users' manuals and systems documentation. It must be clear that Policy should never contradict the law because this can create significant liability for the organization. Security policies are the least expensive control to execute, but the most difficult to implement properly [3].

Information security policy compliance is one of the key concerns that face organizations today. Employees' compliance with Information Security Policies (ISPs) is critical to the success of an information security program[7,8].compliance with organizational rules, guidelines and requirements as stated in their ISP is a useful mechanism for influencing employee behavior toward how information resources are used [9]. Information security policy violations can be very serious for an organization, as the consequence of one non-compliant action can compromise an organization's entire information security system. The information security of an organization is dependent on employees' compliance with the organization's information security policies[10[.Even when users have received good information security training, some factors can promote non-compliance behavior. These considerations include environmental, social, and organizational issues. If their work is stressful, this could impair their focus and lead to mistakes. They may comply and act appropriately concerning information security under the influence of social and organizational factors. If the manager did not bother or care about following the security policy and procedures, then they will as well. To promote information security compliance behavior and reduce security incidents, organizational managers must create a good security environment at their workplace [11].

In Libya, human error is one of the major internal threats to implementation [12,13]. Human error caused information security incidents because employees in the organization lack recognition of potential threat vulnerabilities, undeveloped understanding of information security, and lack knowledge about information security [13]. Thus, the leader plays an important role to encourage, monitor employees in the organization aware of the organization's information security policies (ISPs), and comply with them properly.

This study focuses on employees' information security policy compliance behavior in Libyan Organizations. The objective of this paper is to assess the existence of any gaps in the compliance and awareness of employees in the company. The rest of the paper is organized as follows: Section 2 discusses the related works. Section 3 presents the proposed approach. The experimental setup is presented in Section 4. The results

and discussion of findings are presented in Section 5. Section 6 concludes the paper.

## 2. RELATED WORK

Al-Izki and. Weir (2016) Presented a study to measure management attitudes toward Information Security in Oman. The study considers how such attitudes influence Information Security governance. In addressing these issues, review current compliance with Information Security procedures in Omani public sector organizations; review management attitudes toward Information Security governance practices; and explore how management attitudes toward Information Security affect these aspects. The results showed a considerable lack of management interest in Information Security in Omani public sector organizations. In addition, results revealed a strong relationship between management attitude toward Information Security and aspects indicating the management governance activities. The study concluded that there is a strong relationship between management attitude toward Information Security and compliance with Information Security policies.

Carvalho et al. (2018) proposed a study to identify the most important and the least relevant elements in the structure of a security policy. It presents a synthesis of the literature on information security policies content and it characterizes 15 Small and Medium Sized Enterprises (SMEs). The content analysis (CA) research technique was applied to characterize the information security policies. The study shows that the relative importance of these elements is slightly changed according to the sectors of activity. SMEs need to be aware of these elements to design their security policies in a precise, concise, and unambiguous way.

Alkhurayyif et al. (2017) present study investigates the effectiveness of applying readability metrics as an indicator of policy comprehensibility. The paper focused on assessing the readability factor in affecting the success or effective operation of ISPs.Results from a preliminary study reveal variations in the comprehension test results attributable to the difficulty of the examined policies. The result shows some correlation between the software readability and human comprehension test results and supports our view that readability has an impact on understanding ISPs. These findings have important implications for users' compliance with information security policies and suggest that the application of suitably selected readability metrics may allow policy designers to evaluate their draft policies for ease of comprehension before policy release. Indeed, there may be grounds for a readability compliance test that future ISPs must satisfy.

Da Veiga, A. (2016), Present study outlines a case study over eight years in which empirical research was conducted to examine the level of information security culture between employees who had read the information security policy and employees who had not read the policy. The result found that the overall information security culture average scores were significantly more positive for employees who read the information security policy when compared with employees who had not, illustrating the positive impact of the policy on the information security culture in the context of an Information Security Culture Assessment (ISCA). The study confirms theoretical research stating the importance of information security policies as part of an information security program and the governance of information to instill an information security-positive culture.

Carvalho et al., (2018) proposed a study to identify the most important and the least relevant elements in the structure of a security policy. It presents a synthesis of the literature on information security policies content and it characterizes 15 Small and Medium Sized Enterprises (SMEs). The content analysis (CA) research technique was applied to characterize the information security policies. The study shows that the relative importance of these elements is slightly changed according to the sectors of activity. SMEs need to be aware of these elements to design their security policies in a precise, concise, and unambiguous way.

Aisha Al-Hamar (2018) developed a comprehensive Information Security Management framework to evaluate the information security situation in Qatar. This research aimed to improve Qatari organizations' information security processes by developing a comprehensive Information Security Management framework for the implementation of the NIA policy. The main findings of this research are insufficient information security awareness in organizations in Qatar and a lack of a security culture. In addition, the current National Information Assurance (NIA) policy has many barriers that need to be addressed. The barriers include a lack of information security awareness, a lack of dedicated information security staff, and a lack of a security culture.

Gerber et al. (2016) presented a study to improve the understanding of the factors that affect employee security compliance. The objective of this study is to comply with security policies affected by attitude towards compliance. The results show that the important factor for security compliance intention is perceived top management participation in security initiatives, which in turn affects subjective norms and perceived behavioral control. Concerning actual security policy compliance, the intention to comply is only predictive value as long as no other predictors are considered. The best technology does not ensure safe operation if people do not use it as it was designed. Information security must make sense to employees, and must be easy to understand and intuitively used; otherwise, people will find shortcuts and workarounds. To receive an improvement in employee security compliance, managers need to reconsider their reward arrangements, especially if goal achievement is likely to be constrained by security policy compliance.

Downer and Bhattacharya(2022) Proposed a study to improve existing BYOD security frameworks in Australian Businesses, from the perspective of surveyed employees. This paper aims to discover how employees practice and perceive the BYOD security mechanisms deployed by Australian businesses that can help guide the development of future BYOD security frameworks. Three research questions are answered by this study: What levels of awareness do Australian businesses have for BYOD security aspects? How are employees currently responding to the security mechanisms applied by their organizations for mobile devices? What are the potential weaknesses in businesses' IT networks that have a direct effect on BYOD security? Employees particularly rely on applications for communicating with co-workers and clients, documentation, and planning schedules. Managers and information technologists are leading the trend as the most reliant on BYOD, whilst the retail and telecommunications industries have also been the most accommodating of BYOD strategies in the workplace. The assimilation rate of BYOD security mechanisms is still developing in Australian businesses, although awareness of newer BYOD security frameworks still requires growth. Employee awareness of BYOD security aspects presented positive results. Moreover, 90% of employees surveyed use at least one of their device's default security mechanisms, and a majority of employees

believed that they had adequate to good knowledge of the potential threats and risks targeting mobile devices.

# 3. PROPOSED APPROACH

A telecommunication company was chosen to be the case study of this study. The ISP of this particular company was investigated and proved optimum and updated. On the other hand, it was revealed the existence some issues in compliance with the ISP. In this study, data was collected on the current security situation for some of the telecommunication companies in Libya. A questionnaire method was utilized to provide an understanding of compliance within the organization. A questionnaire with 39 questions was designed for that purpose. The questions were carefully selected to cover several factors of the subject areas. These factors are listed in the table1 with the corresponding number of questions. For every factor of the questionnaire, answers were grouped into three categories: "Yes" answers, "Not sure" answers, and "No" answers.

**Table 1: Mapping questions to factors**

| No | factor | questions | Highlight |
|---|---|---|---|
| 1 | Security Policies | 1-3-4-8-9 | explains the security policy knowledge in the Company |
| 2 | Organizational Security | 2-6-36-37-38 | Explains the security knowledge in the Company. |
| 3 | Asset Classification and Control | 11-12 | explains the asset classification and control in the Company. |
| 4 | Personnel Security | 7-14-15-35 | explains Personnel Security in the Company. |
| 5 | Physical and Environmental Security | 16-17-19 | discusses the Physical and Environmental factors in the Company. |
| 6 | Communications and Operations Management | 20 -22-23-24 | illustrates Communications and Operations Management factors in the Company. |
| 7 | Access Control | 13-21-25-26-34-39 | explains the Access Control factors in the Company |
| 8 | Development and Maintenance | 27-28 | discusses the Development and Maintenance factors in the Company. |
| 9 | Information Security Incident Management | 29-30 | explains the Information Security Incident Management factors in the Company. |
| 10 | Business Continuity Management | 18-31-32 | illustrates the Business Continuity Management factors in the Company. |
| 11 | Compliance | 5-10-33 | explains the Compliance factors in the Company. |

# 4. RESULTS AND DISCUSSION

## 4.1 Factor 1 - Security Policies

Table 2 and Figure 1 demonstrate the assessment level of Asset level of security policy knowledge within the Company. The results show that 37.4%answered "NO" and 30%"Not sure", Whereas, 32.6% answered "Yes". Unfortunately, the percentage of employees not familiar with the policies in the Company is only 32.6%. On other hand, the answer with Not sure is 30%", which means an unaware employee of the policies in the Company. This is considered an issue for the Company since the employees will have no jurisdiction or guidance to follow while operating their daily tasks. The results indicate that security policy knowledge in the Company is low which itself is an alarming indication of a lack of security management in the Company. The absence of an awareness program and lack of compliance with the information security policy has contributed to the shortage of identifying information security risks and the selection of acceptable standards for the company. The result concluded that the company should implement an information security awareness and training program to improve employee awareness and compliance with the security policies. The program should include regular training sessions, easily accessible resources, and encouragement for employees to ask questions about the policies. Also, create a culture of security awareness within the company, and recognize and reward employees who comply with the policies. By following these steps, the company can help to ensure that its employees are aware of the risks they face and can take the necessary precautions to protect the company's data.

**Table 2. mapped the assessment of the Security Policies factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 0 | 3 | 27 |
| **2** | 15 | 10 | 5 |
| **3** | 1 | 18 | 11 |
| **4** | 10 | 14 | 6 |
| **5** | 30 | 0 | 0 |
| **Percentage** | ***37.4%*** | ***30%*** | ***32.6%*** |

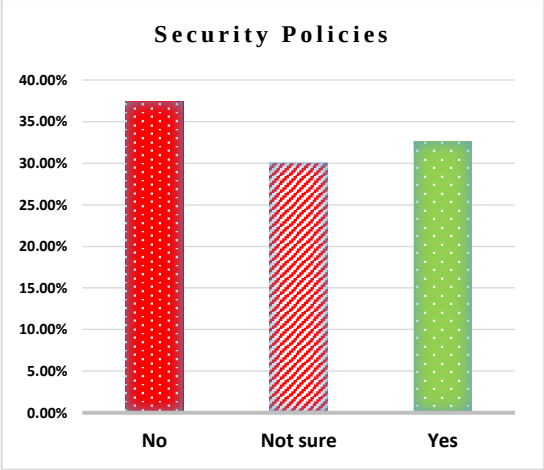


**Fig .1 Comparison assessment of Security Policies factor**

## 4.2 . Factor 2 – Organizational Security

Table 3 and Figure 2 explain the assessment level of Organizational Security within the Company. The results show that 28% answered "NO" and 39.3% "Not sure", whereas, 32.6% answered "YES". Unfortunately, the majority percentage answered "Not sure", which means an unaware employee of the security in the Company. The results also show that the company lacks clear descriptions of the tasks and responsibilities of each employee. This can lead to a lack of segregation of duties, which can increase the risk of unauthorized access to data or systems. The result finds that a Lack of description of tasks and responsibilities will enable irresponsible behavior from the organization by providing over privileges to users, which makes them a risk to the organization and a target for threat vectors. The results suggest that the company needs to improve its employee awareness and training programs. This could include regular training sessions on security policies and procedures, as well as easily accessible resources for employees to learn more about security. The organization can ensure all employees are aligned with security goals and contribute to a safer work environment through awareness and training programs to improve employee awareness and compliance levels.

**Table 3. mapped the assessment of the Organizational Security factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 24 | 6 | 0 |
| **2** | 10 | 20 | 0 |
| **3** | 2 | 11 | 17 |
| **4** | 5 | 14 | 11 |
| **5** | 1 | 8 | 21 |
| **Percentage** | ***28%*** | ***39.3%*** | ***32.6%*** |

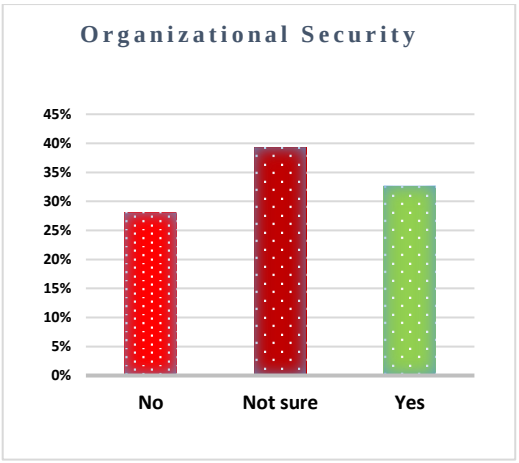


**Fig 2. Comparison assessment of Organizational Security factor**

## 4.3 Factor 3 – Asset Classification and Control

Table 4 and Figure 3 demonstrate the assessment level of Table 4 and Figure 3 demonstrate the assessment level of Asset Classification and Control in the Company. The results show that 23.3%% answered "NO" and 50% "Not sure", whereas, 26.7% answered "Yes". The result find that half of the employees answered this factor, as not sure which means that, the company's security department is not capable nor experienced to publish procedures across the organization. This leads to a lack of security management and security experience in the company. The result concluded that the company's responsibility to ensure that the defined security requirements are implemented and maintained by the data protectors. Also, identify suitable technical controls and processes to log and monitor systems for potential malicious activities. Moreover, Managers should ensure that all personnel having access to the information asset are aware of the organization's security requirements and any legal or regulatory responsibilities. The results suggest that the company needs to improve its asset classification and control procedures. This could include creating an asset inventory, classifying assets, implementing appropriate controls, and training employees on security best practices. By taking these steps, the company can help to ensure that its data and assets are properly protected.

**Table 4. Mapped the assessment of the Asset Classification and Control factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 8 | 14 | 8 |
| **2** | 6 | 16 | 8 |
| **Percentage** | ***23.3%*** | ***50%*** | ***26.7%*** |

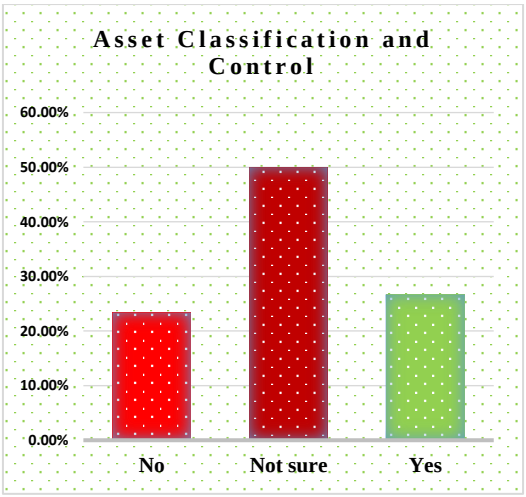


**Fig 3. Comparison assessment of Asset Classification and Control factor**

## 4.4 Factor 4 – Personnel Security

Table 5 and Figure 4 summarize the level assessment of Personnel Security in the Company. The result shows that only 37.5% were familiar with an awareness program. Whereas, the results show a low level with 30.8 % and 32.5% answering " No "and "Not sure" respectively. The results find that the organization's failure to conduct annual awareness training is a significant security risk. Employees who are not aware of the latest security threats and best practices are more likely to fall victim to phishing attacks, data breaches, and other forms of cyberattacks. The company is responsible for upholding the standards, criteria, and guidelines upon which personnel suitability determinations for risk-designated and sensitive positions are made. An awareness program is a critical aspect of any organization's security posture. The results concluded that by educating employees on the latest security threats and best practices, organizations can help to reduce the risk of cyberattacks. Annual awareness training is essential for any organization that wants to protect itself from cyberattacks. The results suggest that the company needs to keep employees up-to-date on the latest security threats, reinforcing the importance of security practices, and helping to create a culture of security within the company. also, annual awareness training is important to educate and be aware of the employees who have access to information and assets, to reduce the chance of information or assets being lost or compromised.

**Table 5. mapped the assessment of the Personnel Security factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 0 | 1 | 29 |
| **2** | 14 | 17 | 0 |
| **3** | 17 | 1 | 12 |
| **4** | 6 | 20 | 4 |
| **Percentage** | ***30.8%*** | ***32.5%*** | ***37.5%*** |

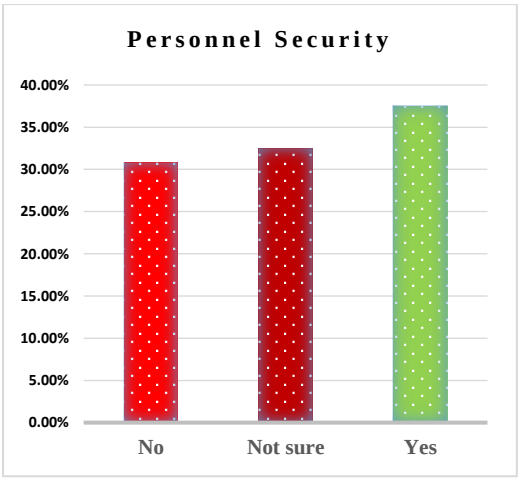


**Fig 4. Comparison assessment of Personnel Security factor**

## 4.5 Factor 5 - Physical and Environmental

Table 6 and Figure 5 summarize the level assessment of the Physical and Environmental factors in the Company. The results show that 56.7% answered "NO" and 13.3% "Not sure", however, 30%answered "yes". The result finds that the majority of answers is NO which indicates that there is a lack of interest or the board is not familiar with the risk of a rubber ducky attack on the company. The results find that. the lack of support from the company board would cause security breaches without being known they got breached. Lack of physical security in the organization increases the possibility of a physical cyber-attack using a rubber ducky tool that is capable exploit organization end-user workstations which will lead the threat vector to the organization database or financial application for example for bank SWIFT which will lead to severe loss. The results concluded that the company needs to do more to educate its employees about the risk of rubber ducky attacks. They also need to implement physical security measures to protect their systems from attack. These measures could include things like installing security cameras, using security guards and restricting access to sensitive areas. By taking these steps, the company can help to protect itself from rubber ducky attacks and other physical cyber-attacks.

**Table 6 mapped the assessment of Physical and Environmental factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 21 | 0 | 9 |
| **2** | 24 | 6 | 0 |
| **3** | 6 | 6 | 18 |
| **Percentage** | ***56.7%*** | ***13.3%*** | ***30%*** |

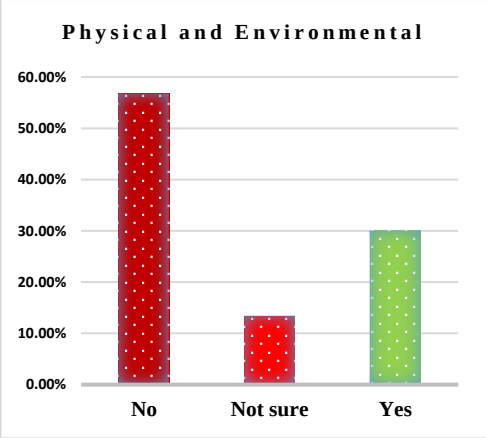


**Fig 5. Comparison assessment of Physical and Environmental factors**

## 4.6 Factor 6 – Communications and Operations Management

Table 7 and Figure 6 summarize the level assessment of the Communication and Operations Management factor in the Company. The results show that 18.3%answered "NO" and 22.5%"Not sure", On the other hand, the majority of answers "Yes" with 59.1% “Yes". The result finds that the company has put in place appropriate controls to prevent unauthorized access, misuse, or failure of information systems and equipment. However, the Company is responsible for establishing appropriate controls to prevent unauthorized access, misuse, or failure of information systems and equipment. Moreover, the company is responsible to establishes appropriate controls to prevent unauthorized access, misuse, or failure of the information systems and equipment. Moreover, the company ensures the information that is processed by or stored in the information systems/equipment protection. The results concluded that the company requires implementing safeguards, including policies, standards, and procedures that guide how systems are operated and how the institution processes information. These safeguards would help to protect the company's information assets and ensure the confidentiality, integrity, and availability of its information systems. The company should regularly review its security controls to ensure that they are still effective, train its employees on security best practices, and have a plan in place to respond to security incidents. The company can help to protect its information assets and ensure the continued operation of its information systems by following these steps.

**Table 7. Mapped the assessment of the Communications and Operations Management factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 10 | 14 | 6 |
| **2** | 2 | 1 | 27 |
| **3** | 4 | 5 | 21 |
| **4** | 10 | 7 | 13 |
| **Percentage** | ***18.3%*** | ***22.5%*** | ***59.1%*** |

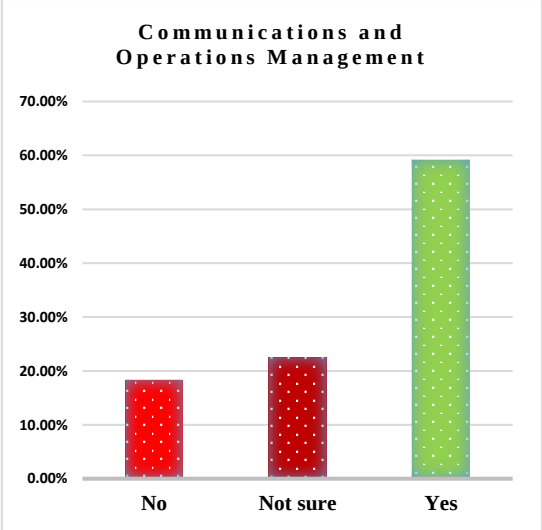


**Fig 6. Comparison assessment of Communications and Operations Management factor**

## 4.7 Factor 7 – Access Control

Table 8 and Figure 7 summarize the level assessment of Access Control in the Company. The results show that 25% of respondents answered "NO" and 29.4% answered "Not sure" to the question "Does the company have a formal access control policy in place?" On the other hand, less than half (45.6%) answered "Yes". These results indicate that the company's access control policy is not as robust as it could be. This could leave the company vulnerable to unauthorized access to physical and computer systems, as well as sensitive data. The company needs to advance infrastructure and procedures that limit access to networks, computer systems, applications, files, and sensitive data. Moreover, the company ensures that security technology and access control policies are in place to protect confidential information. The results concluded that The company can improve its access control by developing a formal policy, implementing it, training employees, using technology, and monitoring the policy. This will reduce the risk of unauthorized access and protect sensitive data.. By ensuring that employees understand the importance of access control and how to comply with the company's policy, the company can help to protect its data and systems.

**Table 8. Mapped the assessment of the Access Control factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 17 | 9 | 4 |
| **2** | 12 | 7 | 11 |
| **3** | 1 | 4 | 25 |
| **4** | 0 | 24 | 6 |
| **5** | 10 | 1 | 19 |
| **6** | 9 | 8 | 13 |
| **Percentage** | **25%** | **29.4%** | **45.6%** |

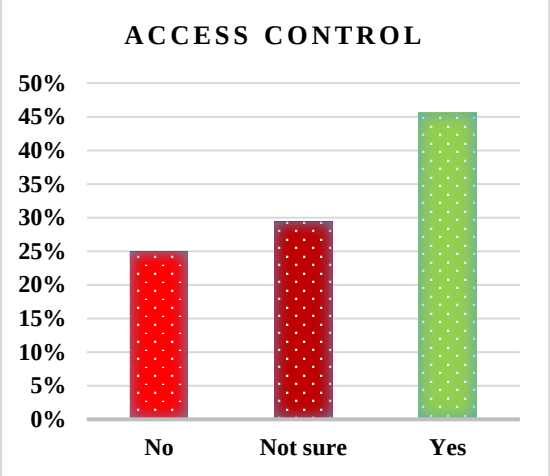


**Fig 7. Comparison assessment of the Access Control factor**

## 4.8 Factor 8– Development and Maintenance

Table 9 and Figure 8 demonstrate the assessment level of Development and Maintenance in the Company. The results show that 1.7% answered "NO" and 65% "Not sure", whereas, 33.3% answered "Yes". Unfortunately, the majority percentage answered "Not sure" which means that the security department is not capable nor experienced to publish procedures across the company. This could lead to a lack of security management and security experience in the company. The result concluded that the company's responsibility for information security is applied to software systems within the company and that security is included within the policies. This helps the company to prevent errors, loss, and misuse of a company's information. Routine maintenance can include ensuring that critical software, such as antivirus and anti-malware, is fully updated and running correctly. It can also include scheduled scans and deployment of security patches to remediate software vulnerabilities. The company can improve its security department by providing the security department with the necessary training and resources, creating a culture of security awareness, and implementing a security incident response plan. These steps will help the company to improve its security posture and protect its sensitive data.

**Table 9. Mapped the assessment to the Development and Maintenance factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 0 | 20 | 10 |
| **2** | 1 | 19 | 10 |
| **Percentage** | ***1.7%*** | ***65%*** | ***33.3%*** |

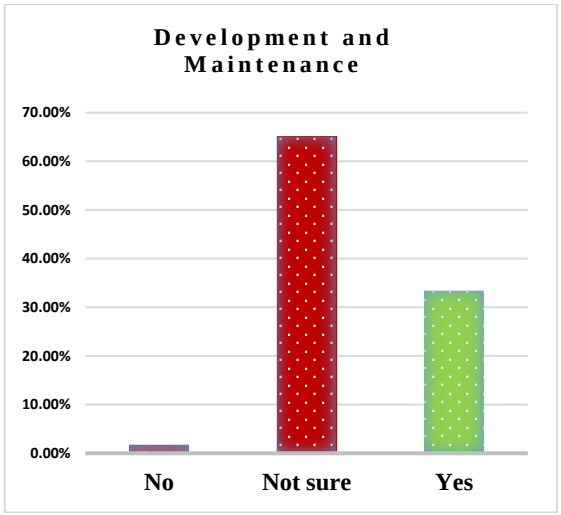


**Fig 8. Comparison assessment of Development and Maintenance factor**

## 4.9 Factor 9–Information Security Incident Management

Table 10 and Figure 9 demonstrate the assessment level of Information Security Incident Management in the Company. The results show that 6.7% answered "NO" and 41.7% "Not sure", While, 51.7%answered "Yes". On the other hand, the majority answered "Yes" with an average of 51.7%. The result finds that the company has put in place appropriate procedures, steps, and responsibilities for its incident response program. However, the company could improve its incident response program by enhancing its ability to identify, respond to, and recover from security incidents. This can be done by implementing security monitoring tools and systems to detect suspicious activity, developing and implementing a comprehensive incident response plan, and having a plan in place to restore data and systems that have been compromised. In addition, Critical documentation is required from most security compliance standards. This documentation can help the company to demonstrate its compliance with these standards. In addition, documenting procedures is helpful for employees in the organization to follow when an accident occurs. This can help to ensure that the company can respond to and recover from security incidents in a timely and effective manner. The results suggest that to improve an incident response program, it is important to make sure that all employees are aware of the plan and know what to do in the event of an incident. Regular drills and exercises should be conducted to test the plan and identify any areas that need improvement. The plan should also be kept up to date as new technologies and threats emerge. Finally, it is important to partner with a qualified security firm to help develop and implement an effective incident response program.

**Table 10. Mapped the assessment to the Information Security Incident Management factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 1 | 19 | 10 |
| **2** | 12 | 15 | 3 |
| **Percentage** | ***6.7%*** | ***41.7%*** | ***51.7%*** |

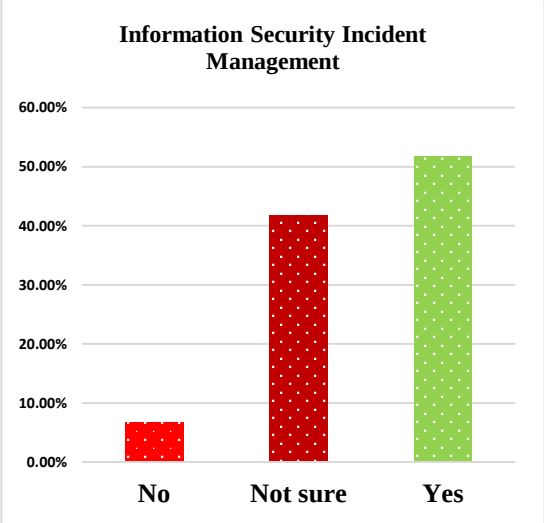


**Fig 9. Comparison assessment of Information Security Incident Management factor**

## 4.10 Factor 10– Business Continuity Management

Table 11 and Figure 10 describe the assessment level of Business Continuity Management (BCM) in the Company. The results show that 42.2% answered "NO" and 21.1%% "Not sure" whereas, 36.7% answered " Yes". Unfortunately, the majority percentage answered No. The result finds that the majority of answers is NO which indicates that the company does not have a business continuity plan in place. This could lead to a lack of the company's ability to maintain essential functions during and after a disaster has occurred. Business continuity planning is important because it helps to ensure that the company can continue to operate in the event of a disaster. This can help to protect the company's revenue, reputation, and employees. The results concluded that the company is not doing enough to educate its employees about BCM. BCM is essential for ensuring that the company can continue to operate in the event of a disaster or other disruption. Without a well-defined and communicated BCM plan, the company could be at risk of significant financial losses, damage to its reputation, and even legal liability. The company should take steps to improve its BCM program. This includes educating employees about BCM, developing a clear and concise BCM plan, and conducting regular drills to test the plan. The company should also make sure that its employees are aware of the risks that they face and the importance of following BCM procedures. By taking these steps, the company can improve its BCM program and reduce its risk of disruption. This will help the company to protect its employees, its customers, and its bottom line.

**Table 11. Mapped the assessment to the Business Continuity Management factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 20 | 7 | 3 |
| **2** | 7 | 5 | 18 |
| **3** | 11 | 7 | 12 |
| **Percentage** | ***42.2%*** | ***21.1%*** | ***36.7%*** |

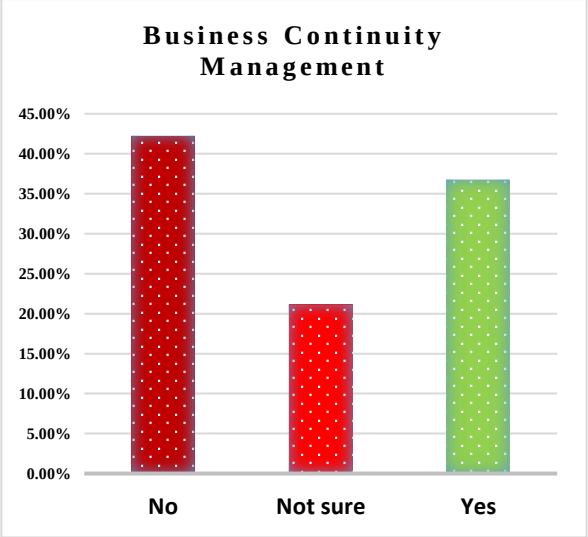


**Fig 10. Comparison assessment of Business Continuity Management factor**

## 4.11 Factor 11– Compliance

Table 12 and Figure 11 describe the assessment level of Compliance in the Company. The results show that 24.4% answered "NO" and 28.9% "Not sure". While less than half answered "yes" with an average of 46.7%, this means that employees do not have any intentions to be compliant with an ISP. They only tend to do so as an exception if there is no way else to carry out their job. This is a significant concern, as non-compliance can leave the company vulnerable to cyberattacks. There are several reasons why employees may not be compliant with the ISP. Some employees may not be aware of the ISP, while others may not understand it. Still, others may simply choose not to comply. The results concluded that it is strongly recommended that the company consider a proper implementation and compliance of its ISP to benefit properly from it. The goal of compliance in the company is to direct the company's policies toward mitigating existing cyber threats and monitoring potential threats that might crop up in the future. The company can improve employee compliance with the ISP by making it easy to understand, providing regular training, creating a culture of compliance, providing incentives for compliance, and enforcing the ISP. By taking these steps, the company can protect its information assets.

**Table 12. Mapped the assessment to the Compliance factor**

| Question | No | Not sure | Yes |
|---|---|---|---|
| **1** | 12 | 17 | 1 |
| **2** | 20 | 10 | 0 |
| **3** | 30 | 0 | 0 |
| **Percentage** | ***24.4%*** | ***28.9%*** | ***46.7%*** |

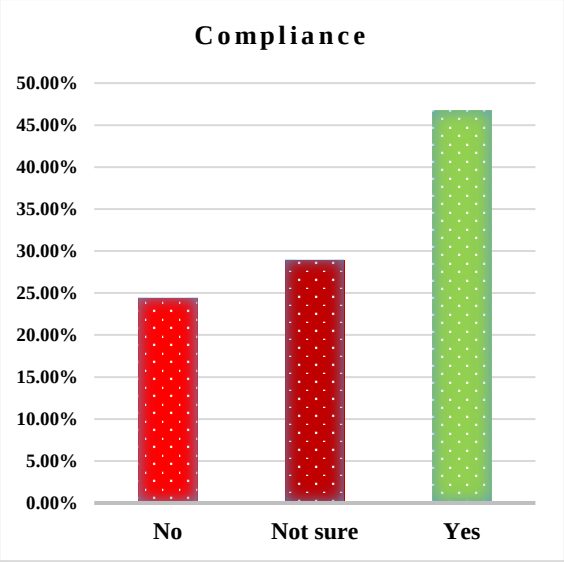


**Fig 11. Comparison assessment of Compliance factor**

## 4.12 Comparison of the Security Awareness and Compliance Assessment

Table 13 summarizes the results comparison of the Security Awareness Assessment. The table lists all factors with "Not ", "Not sure" and "YES" answers. The results show that the Physical and Environmental Security factor has scored the highest ratio of "NO" answers with an average of 56.7%. While the Development and Maintenance factor indicated the highest rate of "Not sure" answered with an average of 65%. On other hand, "YES" answers scored the highest ratio with an average of 51% for Information Security Incident Management. The high percentage of "No" answers for Physical and Environmental Security is a concern, as it indicates that employees may not be aware of the company's security policies or procedures in this area. This could leave the company vulnerable to physical security breaches, such as unauthorized access to facilities or theft of equipment. Moreover, the high percentage of "Not sure" answers for Development and Maintenance is also a concern, as it indicates that employees may not be clear about their roles and responsibilities in this area. This could lead to security vulnerabilities, as employees may not know how to properly secure their systems or applications. In addition, the high percentage of "Yes" answers for Information Security Incident Management is encouraging, as it indicates that employees are aware of the company's procedures for responding to security incidents. However, it is important to note that this is only one factor in overall security awareness. Unfortunately, the majority percentage answered "Not sure", which is an important indicator for the company. This means that an unaware employee of the security in the Company which leads to a lack of security management and security experience in the company. This leads to a lack of security management and security experience in the company. The results conclude The Company should mitigate this gap through training sessions and encouraging employees to ask questions to improve understanding and awareness of the security policy. The company can ensure all employees are aligned with security goals and contribute to a safer work environment through awareness and training programs to improve employee awareness and compliance levels. To improve security awareness, the company should provide regular security awareness training to all employees, encourage employees to ask questions about security policies and procedures, create a culture of security awareness throughout the company, and make security a top priority for all employees.

# 5. CONCLUSION

Information security policy compliance is one of the key concerns that face organizations today. Employees' compliance with Information Security Policies (ISPs) is critical to the success of an information security system. This study focuses on assessing the existence of any gaps in the compliance and awareness of employees in the company. In this study, the results showed that there are security gaps in the current security system. The management of information security in the Company should improve its processes and be aware of the benefits and advantages arising from complying with information security standards. The results showed that there is no full deployment of the standard in reality. Information security management is free to choose the appropriate standards for the organization. The Company should implement a comprehensive and adequate set of information security components that aid in addressing threats on the technical, process, and people levels based on identified information security gaps. Also, The Company should compile and implement a formal well-defined ISP and its derivatives (guideline, Procedure, and Standard) that give guidance and direction to all members and stakeholders regarding the management and protection of information assets. Further, The Company should also work on assurance and recovery controls. Avoidance control is a proactive guarantee that tries to minimize or mitigate the risk of intentional intrusion

# 6. RECOMMENDATIONS

- The company should review its current security processes and identify any areas that can be improved. This may include updating policies and procedures, providing additional training to employees, or implementing new security technologies.
- The company should educate employees about the benefits of complying with information security standards. This may include reducing the risk of data breaches, improving customer trust, and protecting the company's reputation.
- The company should compile and implement a formal well-defined ISP and its derivatives. This will provide employees with clear guidance on how to protect the company's information assets.
- The company should work on assurance and recovery controls. This will help the company to identify and respond to security incidents quickly and effectively.
- The company should Make security a top priority for all employees.

# 7. REFERENCES

[1] Richardson, R..2009. 14th Annual CSI Computer Crime and Security Survey. Executive Summary. Available: http://www.personal.utulsa.edu/~jameschildress/cs5493/CSISurvey/CSISurvey2009.pdf

[2] Ibrahim, A.l. and Sa'ad, P. M. 2013. Information Security Culture Assessment: Case Study. Third International Conference on Information Science and Technology. Yangzhou, Jiangsu, China, 23-25.

[3] Klein, R. H.and Luciano, E. M. 2016. What Influences Information Security Behavior? A Study with Brazilian Users. JISTEM-Journal of Information Systems and Technology Management. vol 13(3), 479-496.

[4] Boss, S. R., Kirsch, L. J., Shingler, I. R.and Boss, R. W. 2009. If someone is watching, I'll do what I masked: mandatories, control, and information security. European Journal of Information Systems, vol. 18, 151- 164.

[5] Puhakainen, P. and Siponen, M. 2010. Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. MIS Quarterly. vol. 34, 757-778.

[6] D'Arcy, J., Hovav, A. and Galletta, D.2009. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research, vol. 20, 79-98.

[7] Kraemer, S., Carayon, P. and Clem, J.2009. Human and organizational factors in computer and information security: Pathways to vulnerabilities. Computers & Security, vol. 28, 509-520.

[8] K. Beznosov and O. Beznosova. 2007. On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security, vol. 15, 420-431.

[9] Bulgurcu, B., Cavusoglu, H. and Benbasat, I. 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Q. vol 34 (3), 523–548 .

[10] Yuanxiang John Li and Elizabeth Hoffman. Information Security Policy Compliance. Available online: https://www.researchgate.net/publication/337144310_Information_Security_Policy_Compliance

[11] T. Herath and H. R. Rao. 2009. Encouraging information security behaviors in organizations: Role of penalties, pressures, and perceived effectiveness. Decision Support Systems, vol. 47(2), 154-165.

[12] Salima. B, Almabruk, S, Awad., E. 2020. Assessment of Security Issues in Banking Sector of Libya, International Journal of Computer Applications, Vol 176 (13), 975 – 8887.

[13] Williams, P. 2008. In a trusting" environment, everyone is responsible for information security. Information Security Technical Report, vol.13(4), 207-215.

**Table 13 summarizes the results comparison of the Security Awareness Assessment**

| No. | factor | No. of Questions | Answers | | |
|---|---|---|---|---|---|
| | | | No | Not sure | Yes |
| | | | Percentage | Percentage | percentage |
| 1 | **Security Policies** | 5 | 37.4% | 30% | 32.6% |
| 2 | **Organizational Security** | 5 | 28% | 39.3% | 32.6% |
| 3 | **Asset Classification and Control Maintenance** | 2 | 23.3% | 50% | 26.7% |
| 4 | **Personnel Security** | 4 | 30.8% | 32.5% | 37.5% |
| 5 | **Physical and Environmental Security** | 3 | 56.7% | 13.3% | 30% |
| 6 | **Communications and Operations Management** | 4 | 18.3% | 22.5% | 59.1% |
| 7 | **Access Control** | 6 | 25% | 29.4% | 45.6% |
| 8 | **Development and Maintenance** | 2 | 1.7% | 65% | 33.3% |
| 9 | **Information Security Incident Management** | 2 | 6.7% | 41.7% | 51.7% |
| 10 | **Business Continuity Management** | 3 | 42.2% | 21.1% | 36.7% |
| 11 | **Compliance** | 3 | 24.4% | 28.9% | 46.7% |