# IMPLEMENTING INFORMATION SECURITY MANAGEMENT SYSTEMS

## Table of Contents:

## 1. Introduction:

SAP.Solutions is an organization which provides solutions for data maintenance, analytics, business intelligence and technology enabling. The organization business is to provide software application for ABY financial corporation and maintain its customer data. The organization experienced many breaches which are creating trouble for the business continuity. So, the organization decided to implement Information Security Management Systems(ISMS) to address defects in its information security management.

## 2. Implementation of ISMS:

The implementation of the ISMS in the organization can be done by following steps.

1. Establish the Information security in an organization:
Information security is most important for the organization. To establish the ISMS in the organization first, analyze and detail the business aspirations, important business processes and IT processes. Identify the dependency of business on IT systems and security conditions for the damages.

2. Scope for ISMS:
The process of prioritizing the safety criteria for business operations will give us the essential IT processes measure. The description of these processes will determine the organization's scope for ISMS.

3. Define Security Policy:
A security policy will give control or guidance for the organization's information security achievement as well as build trust among stakeholders.

4. Identify and Classify Assets:
The assets are grouped in to four categorized. They are data assets, operating system assets, substantial assets and services. Organization prioritize and take security measures to protect these assets.

5. Risk Assessment:
In risk assessment, organization performs a threat analysis and vulnerability analysis which give the over all vulnerability rate and asset risk evaluation.

6. Risk Management:
The identification, evaluation and prioritization of risks in the organization.

7. Risk Mitigation Strategy:
Transforming all risk management plans in to actions which are ready to implement are security policies, procedures and guidelines. Enhancement of current devices.

8. Implementing Controls:
The security controls that address each risks are implemented to mitigate them.

9. Monitor and Review the ISMS performance:
After implementing the ISMS performance is frequently monitored and reviewed for continual improvement.

## 3.Scope of ISMS:

The scope of ISMS for the organization is the enhancement, activity and administration of the Software as a service platform provided by SAP.Solutions with an intention of obtaining ISO 27001 certification in long term. As the organization doing its business with financial company, So the scope included information involved with customer data, process, systems, hardware, software and people of the entire organization.

The boundaries of the ISMS in terms of the organizational characteristics such as asserts, location, business functions and technology are.

Asserts:
The important and the only assert within scope of ISMS is hardware.

| Type | Category | Assert | Owner | Location |
|---|---|---|---|---|
| Hardware | Servers | Web servers/ Database servers/ Backup servers/ Production, Testing, Development servers | Manager | Pune, India |
| | Desktops/<br>Laptops | 72 Desktops/ Laptops Each | Employees | |
| | Printers | Office Printers | Manager | |

The desk tops are installed with windows 10 operating system. The ABY financial company access the SAP.Solution application through remote access. The application is developed, tested and maintained by the SAP.Solution which is used by the ABY financial corporation for its business.

Location:
The organization is located in Pune, India. It does not have any other branches. The ABY financial company which is the client for the organization is also located in Pune, India.

Business functions:
The business functions are categorized in to two types.
Critical business functions:

- Software Application Development and Maintenance.
- Data Security and Maintenance.
- Analytics.

Additional business functions:

- Business Intelligence.
- System Integration.
- Customer Relationship Management.

Technology:
Big Data is the technology utilizing by the organization. As, Big Data is the “fintech” technology utilizing by the most of the organizations that handling data of the financial companies. Big Data can be used to predict customer financing, market changes and create advanced approaches.

The tasks align with the priorities of the company in defining the strategy that would ensure better performance of the application and maintenance of the customer data without losing the reliability of the services.

## 4.Information Security Policy Statement:

This chronicle detail the measures to be taken by the organization and its employees to assure the safety of the organization’s information asserts, systems, infrastructure and environment from threats and damage whether external, internal, accidental or deliberate.
The administrators have the responsibility for auditing and controlling the policy and procedures and associate systems and for providing advice and guidance on their implementation.
The implementation of the information security policy, procedures and systems within the responsibility of the administrators is to observe the key principles of ISMS laid out in the organization’s ISMS procedures.

The objective of the organization is to:

- Reduce the possibility of an event occurring which might effect the security of the information held by the organization.
- The assurance of business continuity maintained and impact minimized when the event of incident happened.

This object will be met by:

- Establishing, implementing, controlling and maintaining an information management framework that meets the requirements of ISO 27001/2013, the 1998 Data Protection Act, the General Data Protection Regulation and any other relevant legislation that may be in effect from time to time.

- Ensure that any climate, engineering, risks or regulation changes are detected and the resulting steps are reviewed and enforced.
- Understanding the threats posed to the organization, its partners and customer information.
- Assessing the risks to the data stored and managed systems and ensurin g appropriate risk mitigation mechanisms are in place.
- Ensuring all employees understand and fulfill their information security obligations.
- Set ISMS annual targets as a platform to ensure that the entire system complies with the organizational standard and ensures that the system is constantly improved.

The policy will be updated annually in order to ensure conformity with the norms and the activities of the organization.

## 5.Risk Assessment:

To carry risk assessment NIST SP 800-30 model is used in the organization and risks are measured by qualitative method like very low, low, moderate, high, very high. The risk assessment that identified the information security risks to the organization, its information, systems and networks are tabled below.

### 5.1Threat Event and Sources:

| No | Threat Source | Threat Event | Relevance |
|---|---|---|---|
| R1 | Organized Cyber Criminal Group. | Whaling attack via email to acquire Credential and Identity theft from the employees. | Expected |
| R2 | Organized Cyber Criminal Group or Motivated Adversaries. | Data theft and manipulation by Social Engineering techniques. | Confirmed |
| R3 | Individual outsider. | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer transaction. | Possible |
| R4 | Adversarial-Individual Outsider. | Destructive and Disruptive Malware. | Expected |
| R5 | Motivated Adversaries. | Disinformation. | Anticipated |
| R6 | Individual Insider. | Error in code leads to software application failure. | Expected |
| R7 | Infrastructure Failure. | Server crash/ Server down/ Downtime. | Anticipated |
| R8 | Organized Cyber Criminal Group. | Dos attack (Denial of attack). | Confirmed |
| R9 | Individual outsider. | Drive-by Download, Attacker | Anticipated |

| | | | |
|---|---|---|---|
| | | introduce Trojan in to the organization’s application to crash systems. | |
| R 10 | Organized Cyber Criminal Group or Individual outsider. | Ransomware - locks the systems of entire organization. | Expected |
| R 11 | Environmental - Heavy rain with lightening. | Can cause flood or fire in the building may damage systems or servers. | Predicted |
| R 12 | Individual outsider. | Advanced Persistent threat - Intruder monitors the network activity and steal information. | Confirmed |

Appendix 1: Threat Relevance

5.2.Vulnerabilities:

| S.No | Threats Event | Vulnerability | Severity |
|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Untrained staff who does not have awareness on information security threats. | High |
| R2 | Data theft and manipulation by Social Engineering techniques. | Failure in enforcing data privacy control both inside and outside of the organization. | Very High |
| R3 | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer transaction. | Poor business and conventional security controls. | Moderate |
| R4 | Destructive and Disruptive Malware. | Poor Anti-malware programs and spam filters for emails. | High |
| R5 | Disinformation. | Expose of organization data. (Too much availability) | Low |
| R6 | Error in code leads to software application failure. | Inappropriate testing of software before deployment. | Moderate |
| R7 | Server crash/ Server down/ Downtime. | Failure in finding open ports of the server through which attacker can access the servers and crash them. Addressing system failures. | Moderate |
| R8 | Dos attack (Denial of attack). | Poor traffic monitoring, network structure and routers. | High |

| | | | |
|---|---|---|---|
| R9 | Drive-by Download, Attacker introduce Trojan in to the organization's application to crash systems who are using it. | Poor web-filtering software and some users own admin access to their systems. | Moderate |
| R10 | Ransomware - locks the systems of entire organization. | Poor smart patch management.<br>Poor spam filters for email and security to network. | Very High |
| R11 | Heavy rain can cause flood or fire by lightening in the building may damage systems or servers. | Organization located in area that prone to heavy rains with lightening. | High |
| R12 | Advanced Persistent threat - Intruder monitors the network activity and steal information. | Poor traffic monitoring, network structure and routers. | High |

Appendix 2: Severity

## 5.3.Likelihood:

| S.No | Threat Event | Likelihood of Occurrence | Likelihood of Adverse Impact | Overall Likelihood |
|---|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Moderate | High | Moderate |
| R2 | Data theft and manipulation by Social Engineering techniques. | High | Very High | Very High |
| R3 | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer transaction. | Low | Moderate | Low |
| R4 | Destructive and Disruptive Malware. | High | Very High | Very High |
| R5 | Disinformation. | Low | Moderate | Low |
| R6 | Error in code leads to software application failure. | High | High | High |

|  |  |  |  |  |
|---|---|---|---|---|
| R7 | Server crash/ Server down/ Downtime. | Moderate | High | High |
| R8 | Dos attack (Denial of attack) | High | Very High | High |
| R9 | Drive-by Download, Attacker introduce Trojan in to the organization’s application to crash systems who are using it. | Moderate | Moderate | Moderate |
| R10 | Ransomware - locks the systems of entire organization. | High | Very High | Very High |
| R11 | Heavy rain can cause flood or fire by lightening in the building may damage systems or servers. | Low | High | Moderate |
| R12 | Advanced Persistent threat - Intruder monitors the network activity and steal information. | Moderate | High | High |

Appendix 3: Overall likelihood

## 5.4.Impact:

| S.No | Threat Event | Type of Impact | Impact and Asset affected. | Level of Impact. |
|---|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Harm to Individual. | Using the credentials attacker can loin to the server and can do anything that cause damage to the organization. | High |
| R2 | Data theft and manipulation by Social Engineering techniques. | Harm to Individual and Assets. | There are many impacts like exposure of confidential data, productivity disruption and may leads to permanent business failure. | High |

|  |  |  |  |  |
|---|---|---|---|---|
|  |  |  | Which all leads to financial loss. |  |
| R3 | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer transaction. | Harm to Individual. | Loss of customer loyalty, Reputation damage of the organization. | Moderate |
| R4 | Destructive and Disruptive Malware. | Harm to Operations. | The impacts like personal information may be retrieved and spoofed, Malware can control all applications on the device can damage systems and servers. | Very High |
| R5 | Disinformation. | Harm to Individual. | Disinformation result in reputation damage to organization. Some times it may lead to the complete destruction of the organization. | Moderate |
| R6 | Error in code leads to software application failure. | Harm to Operation and Assets. | Failure of the software application deny the access and services to the customers which leads to reputation damage and loss of customer loyalty. | High |
| R7 | Server crash/ Server down/ Downtime. | Harm to Operations. | Productivity loss, Reputation damage, Impact of downtime - customers can not access the server during this time. Financial cost for restoring server. | High |
| R8 | Dos attack (Denial of attack) | Harm to Operations. | Interrupt and Disable services, Complete breakdown of the entire infrastructure of the organization. (Financial loss) | Very High |

| | | | | |
|---|---|---|---|---|
| R9 | Drive-by Download, Attacker introduce Trojan in to the organization's application to crash systems who are using it. | Harm to Operations. | Crashing the system in which the data in the system will be lost. | Moderate |
| R10 | Ransomware - locks the systems of entire organization. | Harm to Operations and Assets. | Prevents access to the data and disrupts regular business operations.<br>Financial costs to restore networks and reputation damage. | Very High |
| R11 | Heavy rain can cause flood or fire by lightening in the building may damage systems or servers. | Harm to Operations and Assets. | Destruction of the infrastructure of the organization.<br>(Financial loss) | High |
| R12 | Advanced Persistent threat - Intruder monitors the network activity and steal information. | Harm to Individual. | Interrupt and Disable services, Complete breakdown of the entire infrastructure of the organization.<br>(Financial loss) | High |

## 5.5.Risk Level:

| S.No | Threat Event | Likelihood | Level of Impact | Risk Level |
|---|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Moderate | High. | Moderate. |
| R2 | Data theft and manipulation by Social Engineering techniques. | Very High | High. | High. |
| R3 | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer | Low | Moderate. | Low. |

| | | | | |
|---|---|---|---|---|
| | transaction. | | | |
| R4 | Destructive and Disruptive Malware. | Very High | Very High. | Very High |
| R5 | Disinformation. | Low | Moderate. | Low |
| R6 | Error in code leads to software application failure. | High | High. | High |
| R7 | Server crash/ Server down/ Downtime. | High | High. | High |
| R8 | Dos attack (Denial of attack) | High | Very High. | Very High |
| R9 | Drive-by Download, Attacker introduce Trojan in to the organization's application to crash systems who are using it. | Moderate | Moderate. | Moderate |
| R10 | Ransomware - locks the systems of entire organization. | Very High | Very High. | Very High |
| R11 | Heavy rain can cause flood or fire by lightening in the building may damage systems or servers. | Moderate | High. | Moderate |
| R12 | Advanced Persistent threat - Intruder monitors the network activity and steal information. | High | High. | High |

Appendix 4: Level of Risk

## **6.Risk Response:**

| S.No | Threat Event | Risk Response | Justification for the Respond |
|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Risk Mitigation | Proper risk mitigation is done to counter the attack. Because employees credentials are most important. They give the attacker access to the systems in the organization. |
| R2 | Data theft and manipulation by Social Engineering techniques. | Risk Mitigation | Social Engineering attacks are hard to predict and can not be resisted by the organization. But by following proper risk mitigation measures they can be reduced. |
| R3 | Block-chain(technology using by the organizations for real-time multiparty transactions) recognition can reverse customer transaction. | Risk Avoidance | Block-chain is an emerging technology which is still developing and there are many risks in using it. So it is better for the organization to avoid using this technology. |
| R4 | Destructive and Disruptive Malware. | Risk Mitigation | There are different types of Malware whose impact levels are vary depend up on attack. So organization need to follow the risk mitigation to reduce their impact. |
| R5 | Disinformation. | Risk Acceptance | The adversaries use twitter bots, troll farms and fake news based on the information they obtained from the organization. One way to reduce this threat is to control the expose of organizational data or information. (control availability) |
| R6 | Error in code leads to software application failure. | Risk Acceptance | Proper testing of a software before its deployment is within the organizational risk tolerance. |

| | | | |
|---|---|---|---|
| R7 | Server crash/ Server down/ Downtime. | Risk Mitigation | Finding open ports of the server and closing them frequently and addressing system failure can be done by following the risk mitigation response. |
| R8 | Dos attack (Denial of attack). | Risk Mitigation | An unauthorized person access the organization's network and deny the service to the user. It is the failure of traffic monitoring, poor network structure and routers. A risk mitigation can enhance the technical safeguards and control measures. |
| R9 | Drive-by Download, Attacker introduce Trojan in to the organization's application to crash systems who are using it. | Risk Mitigation | The risk is not within the organizational risk tolerance. Because of poor web-filtering software and some users own admin access to their systems that have to be controlled by risk mitigation response to counter the threat. |
| R10 | Ransomware - locks the systems of entire organization. | Risk Mitigation | Every ransomware attack is new and organization does not know how it attacks. So there must be a risk mitigation response to prevent the ransomware attacking the organization. |
| R11 | Heavy rain can cause flood or fire by lightening in the building may damage systems or servers. | Risk Acceptanc e | The environmental impact is unavoidable. So the organization has to accept it. |
| R12 | Advanced Persistent threat - Intruder monitors the network activity and steal information. | Risk Mitigation | An unauthorized person access the organization's network and deny the service to the users. It is the failure of traffic monitoring, poor network structure and routers. A risk mitigation can enhance the technical safeguards and control measures. |

Appendix 5: Risk response

## 7.Security controls:

| S. No | Threats Event | Controls | Implementation | Control Reference (ISO 27002) |
|---|---|---|---|---|
| R1 | Whaling attack via email to acquire Credential and Identity theft from the employees. | Screening; | Every employee background will be checked before hiring in to organization whether he/she can fit into the role. | 7.1.1 |
| | | Management Responsibility; | Security administrators will encourage the management staff to go through information security awareness training. | 7.2.1 |
| | | Information security awareness, education and training; | Brainstorm sessions will be conducted in the organization regularly in order to educate and train the employees. | 7.2.2 |
| R2 | Data theft and manipulation by Social Engineering techniques. | Classification of Information; | Information is classified in-order to provide more protection measures to sensitive data. | 8.2.1 |
| | | Access control policy; | Access control policy will be enabled to restrict unauthorized persons to access information. | 9.1.1 |

| | | | | |
|---|---|---|---|---|
| | | Information access restriction; | In accordance to access control policy, Information access is restricted to unauthorized one's. | 9.4.1 |
| | | Information backup; | Data backup will be done on regular basis. | 12.3.1 |
| R4 | Destructive and Disruptive Malware. | Controls against Malware; | Detection, prevention and recovery controls are implemented to protect information against malware. | 12.2.1 |
| R8 | Dos attack (Denial of attack) | Access to network and network services; | Access to the network will be granted to only authorized persons and users. | 9.1.2 |
| | | Network Controls; | Networks are monitored to detect suspicious activities and prevent them for the safe transfer of information between systems and applications. | 13.1.1 |
| | | Security of network services; | All networks services are documented to identify the services which are using inside the organization and outside the organization. | 13.1.2 |
| R9 | Drive-by Download, Attacker introduce Trojan in to the | Management of privileged access rights; | User are restricted to access admin systems. | 9.2.3 |
| | | Information | Unauthorized | 9.4.1 |

| | | | | |
|---|---|---|---|---|
| | organization’s application to crash systems who are using it. | access restriction; | persons are restricted to access application system functions. | |
| | | Secure log on procedures; | Access to the application and systems are controlled to the users. | 9.4.2 |
| | | Restriction on software installation; | Users are advised to install the software which is authorized by organization. | 12.6.2 |
| | | Securing application services on public networks; | Organization confirms with the user whether the information in the application received by the user without modification. | 14.1.2 |
| R10 | Ransomware - locks the systems of entire organization. | Information security awareness, education and training; | Organization will educate and train the employees to prevent ransomware attack. | 7.2.2 |
| | | Management of privileged access rights; | User are restricted to access admin systems. | 9.2.3 |
| | | Control against malware; | Detection, prevention and recovery controls are implemented to protect information against malware. | 12.2.1 |
| | | Technical vulnerability management; | Vulnerabilities in the organization are detected and preventive | 12.6.1 |

| | | | | |
|---|---|---|---|---|
| | | | measures will be taken. | |
| | | Planning information security continuity; | To ensure the security standards, Information security continuity plan is maintained at the times of disasters. | 17.1.1 |

## 8.Conclusion:

Finally the plan to implement the Information Security Management Systems(ISMS) in the organization includes the scope, information security policy statement, risk assessment, response to risks and implementation of security controls. The risk assessment helps to identify the asset that need to be concentrated. The mitigation strategy and the security controls helps to reduce the risks.

## 9.References:

1.Margaret Rouse.(2009).ISO 27001, [online], Available:https://whatis.techtarget.com/definition/ISO-27001 [Accessed 19 October,2019].

2.PJR(2017)Determine the scope of ISMS, [online], Available:http://www.pjr.com/downloads/webinar_slides/2.15.17_Scope%20of%20Your%20ISMS.pdf[Accessed 19 October,2019].

3.Accenture security.(2019)Future Cyber Threats, [online], Available:https://www.accenture.com/_acnmedia/pdf-100/accenture_fs_threat-report_approved.pdf [Accessed 21 October,2019].

4. INFOSEC.(2019)The Most Common Social Engineering Attacks, [online], Available:https://resources.infosecinstitute.com/common-social-engineering-attacks/#gref [Accessed 21 October,2019].

## 10.APPENDICES:

Appendix 1: Threat Relevance.

| Value | Description |
|---|---|
| Confirmed | Threat event visible to the organization. |
| Expected | Threat event seen by employees and leaders. |
| Anticipated | Threat event reported by close relations or partners. |
| Predicted | Threat event predicted by external source. |
| Possible | Threat event described by different factors. |

Appendix 2: Severity.

| Values | Description |
|---|---|
| Low | Vulnerabilities that possess minor threats and are not easily exploitable. It includes non-critical systems. |
| Moderate | Vulnerabilities that possess high impacts and result in partial loss of data but the difficult to gain access to. |
| High | Vulnerabilities that includes complete loss of confidentiality, availability and integrity if exploited. |

Appendix 3: Overall Likelihood.

| LIKELIHOOD OF OCCURRENCE | LIKELIHOOD OF ADVERSE IMPACT | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

Appendix 4: Level of Risk.

| LIKELIHOOD | LEVEL OF IMPACT | | | | |
|---|---|---|---|---|---|
| | Very Low | Low | Moderate | High | Very High |
| Very High | Very Low | Low | Moderate | High | Very High |
| High | Very Low | Low | Moderate | High | Very High |
| Moderate | Very Low | Low | Moderate | Moderate | High |
| Low | Very Low | Low | Low | Low | Moderate |
| Very Low | Very Low | Very Low | Very Low | Low | Low |

Appendix 5: Risk Response.

| Risk Response Strategy | Definition |
|---|---|
| Accept | Accepting the consequences and impacts of the risk to the organization completely where there is no possibility to eliminate the risk. |
| Avoid | Initiating specific activities to avoid the potential that are basis for the risk. |
| Mitigate | Implementing controls, security measures to reduce or eliminate the risk. |
| Transfer | Transferring the liability of the potential risk from one organization to another. |
| Share | Potential risk is shared between two organizations. |