Implementation of Information Security Management System (ISMS) Aligned with ISO 27001

Prof. Subarna Panda, Alan Alexander

1 M.Tech (CSE), Asst. Professor, Department Of MCA, School of Computer Science & IT, Jain College (Deemed To Be University)
2 Master of Computer Application (ISMS), School of Computer Science & IT Jain College (Deemed To Be University), Intern at Finnew Solutions Pvt Ltd, As Security Engineer

Abstract: Information and information systems are an important foundation for organizations. Transfer of Organizations information, data and utilization of open networks increase the risks that information and information systems are exposed to. To reduce risks and avoid damages to Organization, security measures must be taken to assure information security.

I. INTRODUCTION

Information security is very important for business not only for enterprises but also for small and medium sized financial organizations. Most of organisations adopt ISO17001 to achieve the compliance with the various regulations and corporate government rule around information key security. There is the gap between the high demands on implementation of information security standards and the actual implementation by organisation. Certification to ISO 27001 provides a host of benefits to the certified organization. It also has advantages for that organization’s customers and its other stakeholders. Whether a business complies with this standard could be a major factor when a customer is deciding if it wants to work with an organization. According to a survey conducted by IT Governance Ltd., 71 percent of industry professionals either regularly or occasionally get requests for evidence of ISO 27001 certification. With the increase in cyber-attacks and virus worldwide, it is essential for organisation to adopt innovative and rigorous procedures to protect asset of organisation. In order to protect asset from cybers-attacks, virus worldwide and information threats, the organisation should implement information security management. There are three parameters that should be considered when applying information security management in an organization:

A. Confidentiality of sensitive data by protective it from unauthorized revelation or intelligible interception
B. Integrity, by safeguarding the accuracy and completeness of knowledge,
C. Availability, by making certain that data and very important services are obtainable to authorised users once needed.

II. ISO 27001

ISO 27001 is a specification for an information security management system (ISMS). Information Security Management System is a framework of policies and procedures that includes all legal, physical and technical controls involved in an company's information risk management processes.

ISO 27001 is developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system.”

ISO 27001 uses prime down, risk-based approach and is technology-neutral. ISO 27001 defines a six-half coming up with process:

A. Outline the protection policy.
B. Outline the scope of the ISMS.
C. Conduct risk assessment.
D. Manage known risks.
E. Choose management objectives and controls to be enforced.
F. Prepare statement of relevance.
Specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The ISO 27001 customary needs cooperation from all sections of organisation. ISO 27001 standards doesn't mandate specific info security controls, however it provides a listing of controls that ought to be thought of within the related code of observe, ISO/IEC 27002:2005. This second customary describes a comprehensive set of data security management objectives and a collection of usually accepted smart observe security controls.

12 main Sections of ISO 27002:
1) Risk assessment
2) Security policy
3) Organization of information security
4) Asset management
5) Human resources security
6) Physical and environmental security
7) Communications and operations management
8) Access control
9) Information systems acquisition, development and maintenance
10) Information security incident management
11) Business continuity management
12) Compliance

III. INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS) MODEL

| PLAN   | CHECK          | DO             | ACT            |
|--------|----------------|----------------|----------------|
| Establish ISMS | Monitor and review the ISMS | Implement and Operate the ISMS | Maintain and improve the ISMS |
### IV. STATEMENT OF APPLICABILITY

| 1 Information Security Policies |
|--------------------------------|
| **1.1 Management direction for information Security** |
| 1.1.a | Policies for information security | To ensure a clear direction and visible management support for information security initiatives and to maintain the appropriate security controls in information processing systems and facilities. |
| 1.1.b | Monthly review of the policies for information security | To assess opportunities for the improvement and need for changes to the Information security management system (ISMS). |

| 2 Organization of information security |
|--------------------------------------|
| **2.1 Internal organization** |
| 2.1.a | Information security roles and responsibilities | To ensure that the security roles and responsibilities are defined and assigned at all levels ensuring that the individuals understand their security responsibilities. |
| 2.1.b | Segregation of duties | To ensure that conflicting duties and areas of responsibility are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the Company assets. |
| 2.1.c | Contact with authorities | To sustain during a crisis, company may require the cooperation of third parties. Therefore, company needs to identify such authorities beforehand and develop relationships that would ensure adequate support when needed. |
| 2.1.d | Contact with special interest group | To seek advice and evaluate whether any modifications need to be made in the existing Organization's IT and Technical infrastructure based on the advice of the Special Interest Groups. |
| 2.1.e | Information security in project management | To ensure security parameters in the project as a whole security requirements in project management needs to be defined. |

| 2.2 Mobile devices and teleworking |
|-----------------------------------|
| 2.2.a | Mobile device policy | To ensure security controls are developed and implemented for users at Organization using mobile computing devices. |
| 2.2.b | Teleworking | Allows employees to work at home or local network by phone, fax etc.. |

| 3 Human resource security |
|---------------------------|
| **3.1 Prior to employment** |
| 3.1.a | Screening | To ensure that any information of the candidate obtained during the background verification process is kept confidential and the privacy of candidate’s data is maintained. |
| 3.1.b | Terms and conditions of employment | To ensure that the terms and conditions of employment reflect Organization’s information security requirements prior to employment. |

| 3.2 During the tenure of employment |
|-----------------------------------|
| 3.2.a | Management responsibilities | To ensure that the employees and external parties at Organization are properly communicated regarding their roles and responsibilities towards the information security. |
| 3.2.b | Information security awareness, education and training | To ensure that a formal Information Security Awareness Program is designed and implemented in Organization. |
| 3.2.c | Disciplinary process | To ensure that the employees and external parties in Organization are made aware of the formal disciplinary process which may be initiated against them, if they violate the Information security policy or commit/participate in any kind of security breach. |

| 3.3 Termination and change of work |
3.3.a End or change of business duties
To ensure that the termination/change of employment responsibilities of the employees and external parties at Organization are clearly defined, assigned and communicated to them.

4 Asset Management

4.1 Responsibilities for assets

4.1.a Stock of benefits
To document the assets of a Business Unit, business function/department in Organization.

4.1.b Ownership of assets
To identify asset owners for all information assets of Organization, responsible to provide protection commensurate with the asset value.

4.1.c Acceptable use of assets
To define the guidelines for the acceptable use of information and assets associated with the information processing facilities of Organization.

4.1.d Return of assets
To ensure that employees at Organization return all issued software, corporate documents, equipment, mobile computing devices, credit cards, access cards, manuals, and information stored on electronic media.

4.2 Data arrangement

4.2.a Arrangement of data
To assign an asset criticality rating to assess the relative importance of the assets for Organization and determine the level of security measures to be implemented for their protection.

4.2.b Labelling of information
To ensure proper classification level of an information asset, all assets should carry an appropriate label.

4.2.c Handling of assets
To guarantee Organization resources are taken care of appropriately as per the data arrangement conspire received by the association.

4.3 Media Management

4.3.a Removable media Management
To ensure that removable media are used with proper authorization.

4.3.b Disposal of media
To ensure that unwanted media are disposed of securely with proper authorization.

4.3.c Physical media transfer
To ensure media containing information is protected against unauthorized access, misuse or corruption during transportation.

5 Access control

5.1 Business requirements of access control

5.1.a Access control policy
To prevent unauthorized access of the Organization's information and information assets.

5.1.b Access to networks and network services
To ensure users are provided with access to the Organization's network and network services that they have been specifically authorized to use.

5.2 User access management

5.2.a User registration and deregistration
To ensure that user is registered or deregistered for granting access to the required information systems and services.

5.2.b User access provisioning
To ensure access provisioning, a process needs to be implemented to assign or revoke access rights for all user types to all Organization systems and services.

5.2.c Management of privileged access rights
To prevent unauthorized access, modification or deletion of Organization information.

5.2.d Management of secret authentication information of users
To ensure secure mechanisms is in place for allocation, storage and management of secret authentication information.

5.2.e Review of user access rights
To ensure that users with additional rights are not overlooked.
| Section | Description                                                                 |
|---------|-----------------------------------------------------------------------------|
| 5.2.f   | Change of user responsibilities are reflected in the accesses given to the users. A periodic review of user access rights need to be conducted. |
| 5.3     | User responsibilities                                                        |
| 5.3.a   | Use of secret authentication information                                    |
| 5.3.b   | Use of secret authentication information Mechanism for secure authentication is required for very confidential work. |
| 5.4     | System and application access control                                        |
| 5.4.a   | Information access restriction To prevent unauthorized access, modification or deletion. |
| 5.4.b   | Secure log-on procedures To ensure a secure logon procedure is in place for appropriate authentication before providing access to information resources at Organization. |
| 5.4.c   | Password management To ensure Organization maintains password quality and management. |
| 5.4.d   | Utilization of advanced utility projects To guarantee the usage of utility projects that might be fit for prevailing framework and application controls are limited and firmly controlled. |
| 5.4.e   | Access control to source code To guarantee security access to program source code should be confined. |
| 5.5     | Cryptography                                                                |
| 5.5.a   | Cryptographic controls                                                       |
| 5.5.a.1 | Policy on the use of cryptographic controls To ensure encryption of data and information |
| 5.5.a.2 | Key management To ensure cryptographic keys are used.                         |
| 5.6     | Physical and environmental security                                          |
| 5.6.a   | Secure areas                                                                |
| 5.6.a.1 | Physical security perimeter To ensure that physical access restrictions are proportionate with the criticality of knowledge systems and are enforced at perimeter of all such facilities wherever information systems of Organization are hosted. |
| 5.6.a.2 | Physical entry controls To ensure that access to Organization offices, facilities and secure areas (areas hosting information systems) is controlled, recorded and monitored. |
| 5.6.a.3 | Securing offices, rooms and facilities To ensure that additional security controls are enforced to host major information processing facilities at Organization head office. |
| 5.6.a.4 | Protecting against external and environmental threats To ensure that protection against injury from natural and synthetic disaster is meant and enforced. |
| 5.6.a.5 | Working in secure areas To ensure that areas wherever essential data systems or instrumentality of Organization are set is known, and extra security controls enforced to stop intrusion and harm in these areas. |
| 5.6.a.6 | Delivery and loading areas To ensure that loading and un-loading areas are isolated from the general public access areas. |
| 5.6.b   | Equipment                                                                    |
| 5.6.b.1 | Equipment siting and protection To ensure that equipment of Organization are protected against environmental threats and unauthorized access. |
| 5.6.b.2 | Supporting utilities To ensure that all equipment of Organization are protected from power failures and other disruptions caused by failures in supporting utilities. |
| 5.6.b.3 | Cabling security To ensure that power and data cables are protected against damage. |
| 7.2.d | Equipment maintenance | A preventive maintenance exercise for all equipment of Organization must be conducted in scheduled intervals ensuring their continued availability and integrity. |
|-------|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 7.2.e | Removal of assets     | To ensure that any equipment, information system, storage device or software under the possession of or having information must not be taken outside the Organization owned or leased premises without prior authorization. |
| 7.2.f | Security of equipment and assets off-premises | To ensure that appropriate security controls are applied to all off-site equipment considering the various risks that exist outside Organization office premises. |
| 7.2.g | Secure disposal or re-use of equipment | To ensure that equipment and information systems of Organization are disposed off after an approval from authorized personnel in a secure manner. |
| 7.2.h | Unattended user equipment | To ensure that unattended equipment has appropriate protection. |
| 7.2.i | Clear desk and clear screen policy | To ensure a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities needs to be adopted. |

### 8 Operations security

#### 8.1 Operational procedures and responsibilities

| 8.1.a | Documented operating procedures | To enforce consistent security controls, Organization needs to formalize operating procedures to ensure the inclusion of appropriate security controls. |
|-------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.1.b | Change management              | To ensure operations security, Organization needs to control changes to all systems/software/applications/configurations etc. |
| 8.1.c | Capacity management            | To ensure that capacity planning process provides for a framework to monitor current performance levels and plan for future growth of information processing facilities. |
| 8.1.d | Separation of development, testing and operational environment | To ensure that security weaknesses that may be introduced in the development environment are eliminated before they are transported to the operational environment, the development and operational facilities should be adequately segregated. |

#### 8.2 Malware Protection

| 8.2.a | Security measures against malware | To ensure that malicious software cannot cause significant damage to information processing facilities and adequate steps are taken to mitigate the risk posed by them. |

#### 8.3 Backup

| 8.3.a | Information backup control | To reproduce data lost in an operational environment due to a system failure or data corruption, backup of data is required. |

#### 8.4 Logging and monitoring

| 8.4.a | Event logging | To ensure monitoring, event logging is required as the event trail that is generated and is useful for fault analysis and analysing unauthorized activity on information systems. |
|-------|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8.4.b | Protection of log information | To ensure log protection, in order to help identify security events for security monitoring. |
| 8.4.c | Administrator and operator logs | To ensure logs are maintained, records of actions performed by administrators/operators need to be logged. |
| 8.4.d | Clock synchronization | To ensure and maintain parity between event logs on disparate systems. |

#### 8.5 Operational software control

| 8.5.a | Establishment of programming on operational frameworks | To ensure controls are incorporated for only authorized users to install software. |

#### 8.6 vulnerability management
### Technical vulnerability management

To reduce security risk by getting timely information about technical vulnerabilities.

### Restrictions on software installation

In order to avoid any risks of installation for any software, users need to be restricted through security parameters.

### Data frameworks review contemplations

#### Data frameworks review controls

To ensure minimal disruptions to business processes, planning of audit requirements and activities involving verification of operational systems are required.

### Management of Network Security

#### Controls for network security

To ensure protection of the systems and applications using the network, Organization realizes the need to adequately manage and control it's network.

#### Security of network services

To ensure security attributes of the network services and implement adequate security controls.

#### Segregation in network

To ensure groups of information services, users and information systems should be segregated on networks.

### Information transfer

#### Information transfer policies and procedures

To protect the exchange of information the Organization needs to implement information exchange policies and procedures.

#### Agreements on information transfer

To ensure agreements on information and software exchange between organizations are maintained.

#### Electronic messaging

Electronic messaging security parameters need to be ensured as it is used extensively at Organization and carries confidential information of the organization.

#### Confidentiality and non disclosure agreements

To ensure security important clauses must be defined in the confidentiality and non disclosure agreements in order to ensure Organization’s information protection.

### System acquisition, development and maintenance

#### Data security prerequisites examination and determination

To ensure system security, controls required in software developed in-house are specified in the requirements analysis stage.

#### Securing application services on public networks

To protect information involved in application services passing over public networks from fraudulent activity, contract dispute and unauthorized disclosure and modification.

#### Protecting application services transactions

To prevent incomplete transmission, miss-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

#### Secure development policy

To provide a control framework for secure development of software and systems.

#### System change control procedures

To ensure changes made to systems do not lead to security weaknesses.

#### Technical review of applications after operating platform changes

To ensure changes to operating systems do not lead to a decrease in the overall security level of the system.

#### Restrictions on changes to software packages

To ensure, as far as possible, vendor provided software should not be modified.

#### Secure system engineering principles

To ensure principles for engineering secure systems are required for governing information system implementation efforts.

#### Secure development environment

To ensure Secure development environment is necessary for system development and integration efforts that cover the entire system development lifecycle.
| 10.2.g | Outsourced development | To ensure organization hires a third-party provider for the development of products and services as per the need. |
| 10.2.h | System security testing | To ensure security testing is carried out during development for each functionality. |
| 10.2.i | System acceptance testing | To ensure and maintain new upgrades and versions of information systems, criteria related testing programs are conducted. |
| 10.3 | Data test |  |
| 10.3.a | Test data Protection | To ensure that the System test data is not compromised to provide misleading test results. Further, if the test data is derived from production data, it can lead to compromise of confidentiality. |

| 11 | Supplier relationships |  |
| 11.1 | Information security in supplier relationships |  |
| 11.1.a | Information security policy for supplier relationships | To ensure information security requirements are discussed and agreed with its suppliers to mitigate the risks associated. |
| 11.1.b | Addressing security within supplier agreements | To prevent unauthorized supplier access to its information systems. |
| 11.1.c | Information and communication technology supply chain | To address the data security dangers related with data and interchanges innovation administrations and item store network. |

| 11.2 | Delivery management |  |
| 11.2.a | Review of supplier services and monitoring | To ensure and maintain supplier service delivery regularly monitor and review. |
| 11.2.b | Managing changes to supplier services | To ensure and manage the changes effectively, maintain proper review of supplier's services. |

| 12 | Information security incident management |  |
| 12.1 | Management of information security incidents and improvements |  |
| 12.1.a | Responsibilities and procedures | To ensure a quick, effective, and orderly response to information security incidents. |
| 12.1.b | Reporting information security events | To enable the remedial actions for security incidents. |
| 12.1.c | Reporting information security weaknesses | To encourage the users to proactively report the observed or suspected security weaknesses in a system. |
| 12.1.d | Assessment of and decision on information security events | To ensure the events encountered are assessed to be classified as information security event. |
| 12.1.e | Response to information security incidents | To ensure documented procedures are present so that, incidents are responded in accordance. |
| 12.1.f | Learning from information security incidents | To avoid the repetition and minimize the occurrence of information security incidents. |
| 12.1.g | Collection of evidence | To carry out the root cause analysis of security incidents. |

| 13 | Information security aspects of business continuity management |  |
| 13.1 | Information security continuity |  |
| 13.1.a | Planning information security continuity | To ensure a business continuity management process with information security is formalized in order to provide a structured and coordinated approach to the continuity strategy. |
| 13.1.b | Implementing information security continuity | To enforce a risk assessment methodology, which is required to identify critical business processes to be supported by the business continuity management process. Documented continuity plans with information security are essential to formalize and educate users of the plan on the requirements and responsibilities for continuity management. |
| 13.1.c | Verify, review and evaluate information security continuity | To ensure effectiveness of the business continuity, plans can be judged only by performing tests. Further, changes in the infrastructure, business processes and threat perceptions need |
ISO 27001 gives the Organization a best practice the executives structure for actualizing and looking after security. It additionally gives you a benchmark against which to work and either to indicate consistence or for outer confirmation against the standard. In any case, consistence or outside affirmation to ISO 27001 does not mean you are secure - it implies that you are overseeing security in accordance with the standard, and to the dimension you believe is suitable to the association. On the off chance that the Organizations hazard appraisal is defective, you don't have enough security and hazard evaluation skill and the association does not have the administration and authoritative responsibility to execute security then it is flawlessly conceivable to be completely consistent with the standard yet be unreliable. Actualizing ISO 27001 is the correct path forward to guarantee the security of the Organization. Be that as it may, to be secure, it is important to build up a culture of esteeming data and ensuring it, through:

A. A solid administration responsibility to data security.
B. Individual proprietorship and obligation regarding data security.
C. Effective data security instruction and mindfulness.
D. 

VI. ACKNOWLEDGMENT

This Research Is Partly Supported By Department Of Computer Science & Information Security Of Jain University Jayanagar, 9th Block, Bengaluru, Karnataka, India

REFERENCES

[1] https://www.bcs.org/content/ConWebDoc/26594
[2] https://encyclopedia.jrank.org/articles/pages/6625/Information-Security-Management.html
[3] https://www.iso.org/isoiec-27001-information-security.html
[4] https://www.irqs.co.in/it-standards/information-security-management-system/
[5] https://www.sync-resource.com/blog/iso-27001-implementation-step-by-step-guide/
[6] https://www.isaca.org/Journal/archives/2011/Volume-4/Pages/Planning-for-and-Implementing-ISO27001.aspx
[7] https://www.itgovernance.eu/blog/en/9-steps-to-implementing-iso-27001
[8] https://www.isms.online/iso-27001/4-key-benefits-of-iso-27001-implementation/
[9] https://www.researchgate.net/publication/268462706_Analysis_of_ISO27001_Implementation_for_Enterprises_and_SMEs_in_Indonesia
BIOGRAPHY

Subarna Panda
M.Tech (CSE)
Asst. Professor
Dept. Of MCA
School of Computer Science & IT
Jain College (Deemed To Be University)
Email: Subbarna.panda@gmail.com

Alan Alexander
Master Computer Application (Information Security and Management System)
School of Computer Science & IT
Jain College (Deemed To Be University)
Intern at Finnew Solutions Pvt Ltd as Security Engineer
Email: alanalex64@gmail.com