International Research Journal of Advanced Engineering and Science
ISSN (Online): 2455-9024

Analysis of Implementation of Information Security Based on ISO / IEC 27001:2013 (Case study at the Indonesian Insurance Company)

Bramastyo[1], Anggraeni Ridwan[2]
[1, 2]Business Information System, Gunadarma University, Depok, West Java, Indonesia-16424
Email Address: [1]bram.asik @ gmail.com, [2]neni_rid @ staff.gunadarma.ac.id

Abstract— *Analysis of implementation Information Security Based on ISO / IEC 27001:2013 case study at the Indonesian Insurance company.*

The Indonesian Insurance Company serves millions of workers with heterogeneous backgrounds, manages a broad service network in Indonesia and manages large funds, so it is demanded to be able to provide optimal and excellent services that meet the requirements for each participant. Information Technology has long been applied to provide optimal value for the company, in line with the business strategy, by develope various application systems to support the company's activities, both internal applications and those related to outside companies. Good information security management must be carried out for business continuity to balance the risks and benefits of information technology itself. One of the IT governance frameworks adopted by the Indonesian Insurance Company is Cobit 4.0 and SNI ISO / IEC 27001: 2009 for information security management.

This research was conducted to measure the extent of security of information security governance in the application system used by the Indonesian Insurance Company and provide recommendations for improvement that refer to the standards required by ISO / IEC 27001: 2013 in the Access Control, Cryptography, Operation Security, System Clauses Acquisition, Development and Maintenance. the results of the research concluded that there was one clause that was still incomplete and five controls that were not conform and had to be corrected immediately.

Keywords— *ISMS, Information Security, ISO27001:2013.*

I. Introduction

As one of the state companies Indonesian Insurance Company serves tens of millions of workers with heterogeneous backgrounds, a wide service network in Indonesia and large fund management, so it is demanded to be able to always provide optimal and excellent service that satisfies all participants, Indonesian Insurance Company has long applied information system technology that can provide optimal value for companies, in line with business strategy (strategic alignment) including developing various other application systems.

Implementation of information technology systems certainly requires control in order to ensure that the system designed and used has been effective, this is a challenge for the information technology team to be able to assist management in ensuring the reliability of information systems.

One of the efforts made by the Indonesian Insurance Company to guarantee information security is to implement the ISO / IEC 27001: 2009 Information Security Management System (ISMS) of the Indonesian National Standardization Agency (BSN) which is the Indonesian version of ISO / IEC 27001: 2005. However, since the implementation of the ISMS in June 2012, the ISMS has not been systematically evaluated or measured using standardized standards in accordance with the currently applicable ISO 27001 requirements.

Based on these conditions the researcher will conduct an analysis of the security of the Information System Security in one of the Indonesian Insurance Company Applications, namely the Participant Reporting Information System (SIPP) using ISO / IEC 27001: 2013 Standard [1].

SIPP is one application that deals with external companies, developed by the Indonesian Insurance Company in facilitating services for participants, especially companies in terms of reporting the mutation of wage and labor data

II. Literature Review

A. *Information Security*

The International Organization for Standardization (ISO) defines information security as preservation of the confidentiality, integrity and availability of information. Whereas according to ISACA information security is ensuring that only authorized users (confidentiality) have access to information (integrity) that is accurate and complete when needed (availability).

INTEGRITY
AVAILABILTY
CONFIDENTIALITY

Figure 2.1. Information Security pillar [2]

In both definitions of ISO and ISACA information security focuses on the concepts of Confidentiality, Integrity, and Availability. There are 4 scopes of information security, namely organization, people, process and technology. Each scope interacts dynamically in the form of culture, governing, architecture, emergence, enabling and support and human factors. (ISACA, 2010) illustrates the business model of information security as shown in Figure 2.1

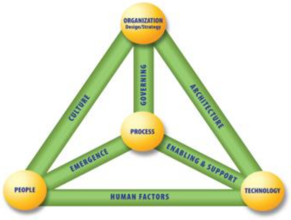


Figure 2.2. Scope of Information Security [3]

B. *ISO/IEC 27001:2013*

ISO 27001 is a management system standard that explains how organizations should manage information security. by using a risk-based approach that has been widely applied to companies that assume that information is the most important asset that must be protected.

ISO / IEC 27001: 2013 is a revision of the previous standard ISO / IEC 27001: 2005, although there is a revision of the 2005 version that adopts the PDCA (Plan-Do-Check-Action) model, the 2013 version does not expressly state the use of certain management models, however the PDCA model is still visible in the whole process in ISMS in the ISO / IEC 27001: 2013 version [4] [5].

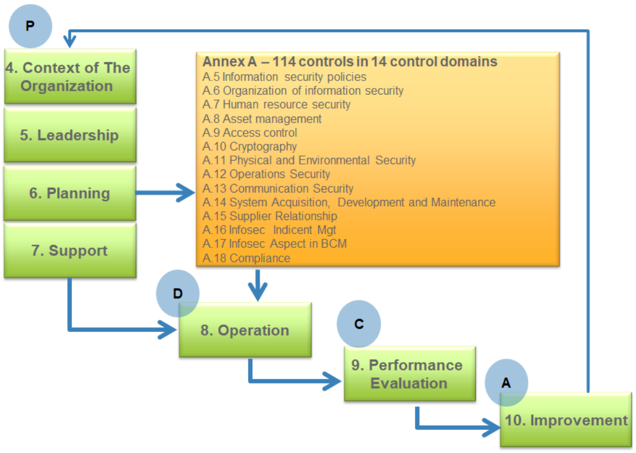

P
4. Context of The Organization
5. Leadership
6. Planning
7. Support
Annex A – 114 controls in 14 control domains
A.5 Information security policies
A.6 Organization of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and Environmental Security
A.12 Operations Security
A.13 Communication Security
A.14 System Acquisition, Development and Maintenance
A.15 Supplier Relationship
A.16 Infosec Indicent Mgt
A.17 Infosec Aspect in BCM
A.18 Compliance
D
8. Operation
C
9. Performance Evaluation
A
10. Improvement

Figure 2.3. Model P-D-C-A ISMS ISO/IEC 27001:2013

The following is a description of the PDCA ISMS ISO / IEC 27001: 2013 model.

1) Plan (Establish ISMS)

Establish ISMS policies, targets, processes and procedures that are appropriate for risk management and information security improvement to produce results in accordance with overall organizational policies and goals.

2) Do Maintain and Improve The ISMS)

Implement and operate the ISMS policy, controls, processes and procedures.

3) Check (Monitor and review the ISMS)

Assess and if applicable measure process performance against policies, SMKI objectives and practical experience and report the results to management for assessment.

4) Action (Implementation and Operations of ISMS)

Take corrective and preventive actions based on the results of the internal audit of the ISMS and management review or other relevant information, to achieve continuous improvement in the ISMS.

ISO / IEC 27001: 2013 standard consists of 10 clauses, 14 area / domain controls, 35 objective controls and 114 security controls based on attachment A (Annex A) starting from Annex 5 to Annex 18, the 14 controls are as shown in table 1 dan table 2 [6].

Annex (A) consists of controls related to organizational structure (physical and logical), human resources, information technology, and supplier management and others

Control in this case can be in the form of processes, procedures, policies and tools that are used as a means of preventing the occurrence of something undesirable.

TABLE 1. ISO/IEC 27001:2013 Clauses

1	Scope
2	Normative references
3	Terms and definitions
4	Context of the organization
	4.1Understanding the organization and its context
	4.2Understanding the needs and expectations of interested parties
	a) interested parties that are relevant to the information security management system; and
	b) the requirements of these interested parties relevant to information security.
	4.3Determining the scope of the information security management system
	a) the external and internal issues referred to in 4.1;
	b) the requirements referred to in 4.2; and
	c) interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.
5	Leadership
	5.1Leadership and commitment
	5.2Policy
	5.3Organizational roles, responsibilities and authorities
6	Planning
	6.1Actions to address risks and opportunities
	6.1.1 General
	6.1.2 Information security risk assessment
	6.1.3 Information security risk treatment
	6.2Information security objectives and planning to achieve them
7	Support
	7.1Resources
	7.2Competence
	7.3Competence
	7.4Communication
	7.5Documented information
	7.5.1 General
	7.5.2 Creating and updating
	7.5.3 Control of documented information
8	Operation
	8.1Operational planning and control
	8.2Information security risk assessment
	8.3Information security risk treatment
9	Performance evaluation
	9.1Monitoring, measurement, analysis and evaluation
	9.2Internal audit
	9.3Management review
10	Improvement
	10.1 Nonconformity and corrective action
	10.2 Continual improvement

TABLE 2. Control Objective ISO 27001:2013 (Annex 5 to Annex 18)

A.5 Information security policies	
	A.5.1 Management direction for information security **Objective**: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
	A.5.1.1 Policies for information security
	A.5.1.2 Review of the policies for information security

A.6	**Organization of information security**
A.6.1	**Internal organization**
	Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.
A.6.1.1	Information security roles and responsibilities
A.6.1.2	Segregation of duties
A.6.1.3	Contact with authorities
A.6.1.4	Contact with special interest groups
A.6.1.5	Information security in project management
A.6.2	**Mobile devices and teleworking**
	Objective: To ensure the security of teleworking and use of mobile devices.
A.6.2.1	Mobile device policy
A.6.2.2	Teleworking
A.7	**Human resource security**
A.7.1	**Prior to employment**
	Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. **Objective**: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.
A.7.1.1	Screening
A.7.1.2	Terms and conditions of employment
A.7.2	**During employment**
	Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
A.7.2.1	Management responsibilities
A.7.2.2	Information security awareness, education and training
A.7.2.3	Disciplinary process
A.7.3	**Termination and change of employment**
	Objective: To protect the organization's interests as part of the process of changing or terminating employment.
A.7.3.1	Termination or change of employment responsibilities
A.8	**Asset management**
A.8.1	**Responsibility for assets**
	Objective: To identify organizational assets and define appropriate protection responsibilities.
A.8.1.1	Inventory of assets
A.8.1.2	Ownership of assets
A.8.1.3	Acceptable use of assets
A.8.1.4	Return of assets
A.8.2	**Information classification**
	Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
A.8.2.1	Classification of information
A.8.2.2	Labelling of information
A.8.2.3	Handling of assets
A.8.3	**Media handling**
	Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.
A.8.3.1	Management of removable media
A.8.3.2	Disposal of media
A.8.3.3	Physical media transfer
A.9	**Access control**
A.9.1	**Business requirements of access control**
	Objective: To limit access to information and information processing facilities.
A.9.1.1	Access control policy
A.9.1.2	Access to networks and network services
A.9.2	**User access management**
	Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.
A.9.2.1	User registration and deregistration
A.9.2.2	User access provisioning
A.9.2.3	Management of privileged access rights
A.9.2.4	Management of secret authentication information of users
A.9.2.5	Review of user access rights
A.9.2.6	Removal or adjustment of access rights
A.9.3	**User responsibilities**
	Objective: To make users accountable for safeguarding their authentication information.
A.9.3.1	Use of secret authentication information
A.9.4	**System and application access control**
	Objective: To prevent unauthorized access to system and applications.
A.9.4.1	Information access restriction
A.9.4.2	Secure log-on procedures
A.9.4.3	Password management system
A.9.4.4	Use of privileged utility programs
A.9.4.5	Access control to program source code
A.10	**Cryptography**
A.10.1	**Cryptographic controls**
	Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
A.10.1.1	Policy on the use of cryptographic controls
A.10.1.2	Key management
A.11	**Physical and environmental security**
A.11.1	**Secure areas**
	Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.
A.11.1.1	Physical security perimeter
A.11.1.2	Physical entry controls
A.11.1.3	Securing offices, rooms and facilities
A.11.1.4	Protecting against external and environ- mental threats
A.11.1.5	Working in secure areas
A.11.1.6	Delivery and loading areas
A.11.2	**Equipment**
	Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
A.11.2.1	Equipment siting and protection
A.11.2.2	Supporting utilities
A.11.2.3	Cabling security
A.11.2.4	Equipment maintenance
A.11.2.5	Removal of assets
A.11.2.6	Security of equipment and assets off-premises
A.11.2.7	Secure disposal or reuse of equipment
A.11.2.8	Unattended user equipment
A.11.2.9	Clear desk and clear screen policy
A.12	**Operations security**
A.12.1	**Operational procedures and responsibilities**
	Objective: To ensure correct and secure operations of information processing facilities.
A.12.1.1	Documented operating procedures
A.12.1.2	Change management
A.12.1.3	Capacity management
A.12.1.4	Separation of development, testing and operational environments
A.12.2	**Protection from malware**
	Objective: To ensure that information and information processing facilities are protected against malware.
A.12.2.1	Controls against malware
A.12.3	**Backup**
	Objective: To protect against loss of data.
A.12.3.1	Information backup
A.12.4	**Logging and monitoring**
	Objective: To record events and generate evidence.
A.12.4.1	Event logging
A.12.4.2	Protection of log information
A.12.4.3	Administrator and operator logs
A.12.4.4	Clock synchronisation
A.12.5	**Control of operational software**
	Objective: To ensure the integrity of operational systems.
A.12.5.1	Installation of soft- ware on operational systems
A.12.6	**Technical vulnerability management**
	Objective: To prevent exploitation of technical vulnerabilities.
A.12.6.1	Management of technical vulnerabilities
A.12.6.2	Restrictions on software installation
A.12.7	**Information systems audit considerations**

	Objective: To minimize the impact of audit activities on operational systems.
A.12.7.1	Information systems audit controls
A.13	**Communications security**
A.13.1	**Network security management** Objective: To ensure the protection of information in networks and its supporting information processing facilities.
A.13.1.1	Network controls
A.13.1.2	Security of network services
A.13.1.3	Segregation in networks
A.13.2	**Information transfer** Objective: To maintain the security of information transferred within an organization and with any external entity.
A.13.2.1	Information transfer policies and procedures
A.13.2.2	Agreements on information transfer
A.13.2.3	Electronic messaging
A.13.2.4	Confidentiality or non- disclosure agreements
A.14	**System acquisition, development and maintenance**
A.14.1	**Security requirements of information systems** Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public networks.
A.14.1.1	Information security requirements analysis and specification
A.14.1.2	Securing application services on public networks
A.14.1.3	Protecting application services transactions
A.14.2	**Security in development and support processes** Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems
A.14.2.1	Secure development policy
A.14.2.2	System change control procedures
A.14.2.3	Technical review of applications after operating platform changes
A.14.2.4	Restrictions on changes to software packages
A.14.2.5	Secure system engineering principles
A.14.2.6	Secure development environment
A.14.2.7	Outsourced development
A.14.2.8	System security testing
A.14.2.9	System acceptance testing
A.14.3	**Test data** Objective: To ensure the protection of data used for testing.
A.14.3.1	Protection of test data
A.15	**Supplier relationships**
A.15.1	**Information security in supplier relationships** Objective: To ensure protection of the organization's assets that is accessible by suppliers.
A.15.1.1	Information security policy for supplier relationships
A.15.1.2	Addressing security within supplier agreements
A.15.1.3	Information and communication technology supply chain
A.15.2	**Supplier service delivery management** Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.
A.15.2.1	Monitoring and review of supplier services
A.15.2.2	Managing changes to supplier services
A.16	**Information security incident management**
A.16.1	**Management of information security incidents and improvements** Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
A.16.1.1	Responsibilities and procedures
A.16.1.2	Reporting information security events
A.16.1.3	Reporting information security weaknesses
A.16.1.4	Assessment of and decision on information security events
A.16.1.5	Response to information security incidents
A.16.1.6	Learning from information security incidents
A.16.1.7	Collection of evidence
A.17	**Information security aspects of business continuity management**
A.17.1	**Information security continuity** Objective: Information security continuity shall be embedded in the organization's business continuity management systems.
A.17.1.1	Planning information security continuity
A.17.1.2	Implementing information security continuity
A.17.1.3	Verify, review and evaluate information security continuity
A.17.2	**Redundancies** Objective: To ensure availability of information processing facilities.
A.17.2.1	Availability of information processing facilities
A.18	**Compliance**
A.18.1	**Compliance with legal and contractual requirements** Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.
A.18.1.1	Identification of applicable legislation and contractual requirements
A.18.1.2	Intellectual property rights
A.18.1.3	Protection of records
A.18.1.4	Privacy and protection of personally identifiable information
A.18.1.5	Regulation of cryptographic controls
A.18.2	**Information security reviews** Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
A.18.2.1	Independent review of information security
A.18.2.2	Compliance with security policies and standards
A.18.2.3	Technical compliance review

III. RESEARCH METHOD

Research methodology is systematic steps taken as a stage of research to achieve research objectives, from several types of research methodologies, the author uses descriptive and qualitative methods with the steps as in Figure 3.1.

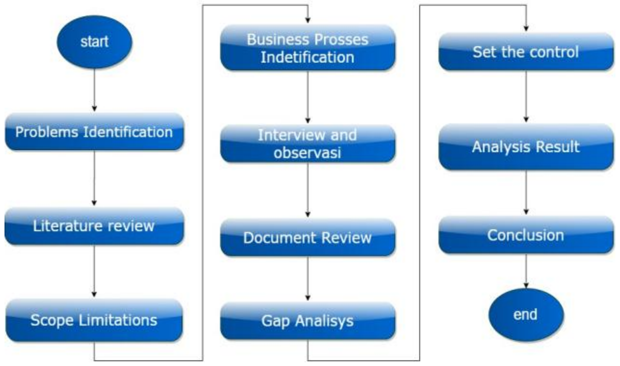


Figure 3.1. Research Method

The first stage of this research is to identify how the information security management of the Indonesian Insurance Company, which since the implementation of security standards by adopting SNI ISO / IEC 27001: 2009 in June 2012, has never been checked conformity with information security standards, as well as recommendations from the government regarding implementation obligations Ministry of Communication and Informatics No. 4 of 2016 concerning the Information Security Management System in regulations concerning the obligation to implement ISO 27001 for State-Owned Enterprises [7].

Theory review to look for references relating to information security governance, and also to consult with practitioners of ISO 27001, The research chooses one of the application systems in the company, SIPP as the object of research, then studies the business processes at the relevant IT directorate and conducts interviews with the responsible operational units of the ISMS operational, observation, and document review until finally finding a gap between ideal conditions and controls should be based on ISO 27001: 2013, the next step is to select an objective control ISO 27001: 2013 based on the research limitations, namely in Annex A9 Access control, A.10 Cryptography, A.12 Operations security, A.14 System acquisition, development and maintenance.

To get to the conclusion the author checks the profile, policy, standards, and observes the standard operating procedure and conducts a confirmation interview related to the condition of the results of observations and documentary evidence with the Information Technology Management unit, from these results produce evidence related to the system. Existing, besides that it also mentions a cause and effect analysis that occurs, as well as recommendations that must be carried out by the organization so that it can better improve security controls according to ISO 27001: 2013 standards, especially within the scope of the SIPP Application.

IV. Discussion

1. *Compliance Results in Clause 7.5.2*

Clause 7.5.2 states that each organization in making and updating documented information must ensure the adequacy of the following:

a. Identification and description (title, date, researcher and reference number)

b. Format (language, software version, graphics) and media (paper, electronics)

c. Review and approval for adequacy.

The results of the study of researchers found that Indonesian Insurance Company already has documents related to the ISMS in the form of Policy and Standards for Management of Information Technology Services (001 / PDM / DOTI / 06/2019), but the document is still in the process of validating approval from management, please note that the document is renewal or adjustment documents from the previous documents enclosed in Directors' Regulation No.92 / 092015 concerning IT Governance Guidelines and Indonesian Insurance Company Communications, so that even though Indonesian Insurance Company have implemented SOPs or policies in accordance with those required in ISO / IEC control 27001: 2013 at documents that have not yet been signed are not in accordance with Clause 7.5.2 regarding creating and updating Document Information.

2. *Compliance Results in Area Control: A.9 Access Control*

a. *Control Objective A.9.1 Business Requirements of access control.*

The goal of this control is to limit user access to information and access to information processing facilities. In this Domain there are two security controls namely Access Control Policy (A.9.1.1) and Access to networks and network services (A.9.2.1)

This control requires that the organization must have set an Access Control policy, documented and reviewed based on business requirements and information security, access control can be physical or logical. Likewise access to the network and network services must have clear provisions on which networks can be accessed by users, including the terms of user authentication.

In general this control has been implemented by the Indonesian Insurance Company documented in the SOP of Access Management Procedure 018 / SOP / DOTI / 04/2019 which clearly provides guidance on steps in terms of access management including requests, changes, deletions and reviews of access, evidence ; This access control has been implemented is a memo of requests from other business units about changing the role of the application or adding a role to access the core application system menu. Thus the Indonesian Insurance Company has fulfilled controls in this area A.9.

b. *Control Objective A.9.2 User Access Management.*

This objective control is to ensure access of authorized users and to prevent access by unauthorized parties into the service system, this control consists of 6 security controls namely:

A.9.2.1 *User registration and deregistration*
A.9.2.2 *User access provisioning*
A.9.2.3 *Management of privileged access rights*
A.9.2.4 *Management of secret authentication information of users*
A.9.2.5 *Review of user access rights*
A.9.2.6 *Removal or adjustment of access rights*

In Security controls A.9.2.1, A.9.2.2, A.9.2.4 describe how control in management from the start of the user is registered or registered, using a unique user id, as well as granting service access rights to user IDs ensures access rights are not activated before the authority procedure is completed or to transfer access rights immediately when a user mutation occurs to another work unit, in this control the user is also asked to sign a confidentiality agreement for personal or group information.

Whereas the security controls A.9.2.3, A.9.2.5, and A.9.2.6 state that the use of special access rights must be strictly restricted and controlled which includes the validity period and also periodic reviews of user competencies, adjustments or abolition of rights access. Special access rights must be given to user IDs that are different from those used for regular business activities and regular business activities may not be carried out from special IDs

The Policy and Standards for Management of Information Technology Services (001 / PDM / DOTI / 06/2019) have regulated the control of access rights as required in the control above, this has also been proven in the document that has been received in the form of a memo related to requesting / revoking access for employees who are mutated on behalf of Miss. Putri Marlinasari who are transferred to Salemba Branch and Mr.Ari Septiana who are transferred to the Sumbagut Region, MoM / BA results of access review, MoM / BA results of log review, and user access matrix. However, the researcher did not find that security controls have been carried out. Reviews of user access rights have been carried out, there is no documentary evidence or evidence that reviews of the use of access rights are conducted periodically to ensure unauthorized users have special rights. Thus, the ISMS has been fulfilled in the control area A.9.2 User access management in all security controls except A.9.2.5 Review of user access rights.

The use of administrative systems that are not appropriate on information systems can cause overlapping application systems or application controls can be a major factor of system failure

c. Control Objective A.9.3 User responsibilities

The goal of this control is for the user to be responsible for maintaining the authentication of information from other parties, by avoiding keeping authentication records unless they have a truly secure place to store them. Security controls of A.9.3 User responsibilities, namely A.9.3.1 Use of secret authentication information from researchers experience using the SIPP application, password quality has been set including a minimum length of password, a combination of uppercase and lowercase letters, coercion to change the password the first time used and changing passwords periodically every 14 days. In this control, the ISMS has also been carried out in an organized manner in accordance with Access Management Procedure 018 / SOP / DOTI / 04/2019.

d. Control Objective A.9.4 System and application access control

This objective control is to prevent unauthorized parties from accessing the system and application. This objective control consists of 5 security controls, namely:

A.9.4.1 *Information access restriction*
A.9.4.2 *Secure log-on procedures*
A.9.4.3 *Password management system*
A.9.4.4 *Use of privileged utility programs*
A.9.4.5 *Access control to program source code*

In A.9.4.1 control of access to information and applications must be limited according to the policies set (which menus and data in the application can be accessed by the user, including the right to modify the data therein)

In A.9.4.2 and A.9.4.3 to access the system and application a safe log-on procedure with strong authentication is required to log in or use alternative authentication methods such as smartcard tokens or bio metrics, including date and time information previous log-on attempts that were successful or not. This control also requires that passwords can be managed such as forcing the use of a combination of quality passwords, forcing to change passwords at the first log-on, rejecting passwords that have been used previously.

In A.9.4.4 and A.9.4.5 are controls that aim for companies to strictly limit the use of utility programs that can override system and application controls including restrictions on access control on program source code, the existence of program and source versioning code saved by a third party.

Policies and Standards for Management of Information Technology Services (001 / PDM / DOTI / 06/2019) that have included control of access rights to information (user registration / user de-registration), periodic review of access rights, in terms of user authentication responsibilities as well be the responsibility of the user, must follow the password management standards that have been set with a minimum length of 8 characters with a combination of uppercase and lowercase letters / numbers, while in the use of the system of utilities Indonesian Insurance Company has removed software-based utilities on personal computers as well as restrictions on access use of utility programs (trusted authorized user only). Control of access rights and password management has been the experience of researchers as one of the employees so that it becomes one of the proofs that A.9.4 controls have been carried out, but in the security control of Access control to the source code program there has not been monitoring control of the versioning source code for application changes. Thus the ISMS has been fulfilled in the area of some security controls A.9.4 System and application access control except in A.9.4.5 Access control to program source code

3. Compliance Results in the Control Area:A.10 Cryptography

a. Control Objective A.10.1 Cryptographic controls
A.10.1.1 Policy on the use of cryptographic controls
A.10.1.2 Key management

The two controls above state that policies on the use of cryptography for information protection must be developed and implemented as well as controls over the validity period throughout the entire life cycle.

From the results of observations and interviews it can be concluded that encryption must be performed for processes that involve confidential data, including application systems that process confidential information that have been carried out.

1) Key length of at least 256 bits. The algorithm used is as follows but is not limited to Advanced Encryption Standard (AES), SHA, or other algorithms that use a key length of at least 256 bits.
2) Application of HTTPS on web based application systems that are accessed from public networks.

The cryptographic provisions are regulated in the Information Technology Service Management Policy and Standards (001 / PDM / DOTI / 06/2019), thus the ISMS has been fulfilled in area A.10 Cryptography.

4. Compliance Results in Area Control A.12 Operation Security

a. Control Objective A.12.1 Operational procedures and responsibilities

This control is to ensure the operation of information processing facilities carried out correctly and safely, this control has four security controls:

A.12.1.1 *Documented operating procedures*
A.12.1.2 *Change management*
A.12.1.3 *Capacity management*
A.12.1.4 *Separation of development, testing and operational environments*

In control A.12.1.1 is a control to ensure that the Operating Standards are documented and can always be accessed for all users when needed including process facilities or communication procedures such as startup-closedown computer, backup procedures, equipment maintenance, etc. For this required control Indonesian Insurance Company is sufficient because it has all the documentation for the required operating standards.

While in control A.12.1.2 discusses the control of organizational change, business processes of information processing facilities and systems that have changed. The Indonesian Insurance Company has implemented controls in change management, for example, the process of managing configuration (recording, changing, and auditing), managing change and managing the release of information technology services, ensuring every change to the system and process of information technology services is assessed, approved, implemented and evaluated adequate, Any changes to policies, procedures, systems, information technology service infrastructure through the Change Management process by initiating Request for Change (RfC), all of that has been stated in the IT Service Policy and Management Document, thus security control A.12.1. 2 conformity requirements can be fulfilled.

In control A.12.1.3 The Indonesian Insurance Company has implemented control in capacity management in its activities and has been outlined in the SOP for Service Capacity Management Procedure number 010 / SOP / DOTI / 10/2016, it is stated that the IT Operational Unit carries out Planning, management of capacity by consider the capacity of human resources, technical (infrastructure, technology, systems), information, and financial resources in accordance with applicable standards and procedures, Thus the ISMS has been fulfilled in the control of A.12.1.3 Capacity Management.

In control A.12.1.4 there is a need for control over the separation of the development, testing and operational environments to reduce unauthorized access or changes to the operational environment. At this time the Indonesian Insurance Company has carried out environmental separation, the development server has its own machine, for testing and production machines logically separated even though the separation is still in one server machine with many processors, ISO / IEC 27001: 2013 only states that the development separation and operations must run on different systems, or computer processors in different domains or directories. Thus, the ISMS has been fulfilled in control A.12.1.4. Separation of development, testing and operational environments.

b. Control Objective A.12.2 Protection from malware

This objective control is to ensure that companies and information processing facilities are protected from malware, as the Indonesian Insurance Company has implemented security procedures against malware and has also been documented in IT Service Management Policies and Standards. So it can be ascertained that the ISMS in A.12.2.1 has been applied to the Indonesian Insurance Company.

c. Control Objective A.12.3 *Backup*

This objective control is that the company has backed up backup of information, software, and image systems and must also have been tested regularly, in this control the Indonesian Insurance Company has implemented 3 backup methods, namely:

1) Database Backup Replication
The process of replication / copying from the Production database in the data center to the standby Database at the Disaster Recovery Center (DRC)
2) Database backup file
The backup process from production to Excel database file (Hot Backup).
3) Backup Tape
The process of database backup to tape media with a certain cycle while the backup storage method there are 2 methods, namely:

a. Database backup replication method

Cycle	Backup type	information
Realtime	Transfer & Apply Archived Log to Standby DRC	Log shipping from database to operational to standby database at each log growth of 2 gb
Daily	Full/incremental Level 0	Backup of all data in the database into a backup file format that is stored internal disk database production, run every day at 17.00 WIB retention backups of 2 days

b. Database file backup Method

Cycle	Backup type	information
Daily	Cumulative Incremental level 1	Backup of all data changes since full backup (level 0) is completed, run every day at 01.00 WIB, backup retention for 2 days.
Weekly	Full/ incremental Level 0	Backup of all data is run every Friday at 17:00 WIB 2 week backup retention

Complete control of backups is documented in the Backup Management SOP, revised 01. September 2018. Thus, the ISMS has been fulfilled in control A.12.3 Backup

d. Control Objective A.12.4 Logging and monitoring

This objective control is to record events and produce evidence, there are 4 security controls that must exist in this area, namely:

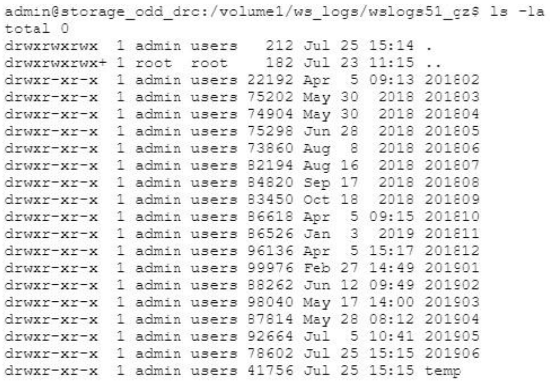
A.12.4.1 *Event logging*
A.12.4.2 *Protection of log information*
A.12.4.3 *Administrator and operator logs*
A.12.4.4 *Clock synchronization*

In the Security controls A.12.4.1, A.12.4.2, and A.12.4.3 require that the organization must record user activity, exceptions, failures or information security events that occur, to be stored and reviewed periodically, including logging the user's log or administrators who must be protected from counterfeiting or unauthorized access. In this control the Indonesian Insurance Company has controlled its logs and monitoring with the following efforts:

a. Log must be created and kept for an agreed period to assist with future investigations and monitoring access controls.
b. The logs that are activated are at least the following:
1) Access failures;
2) Log-on patterns that indicate improper use;
3) Allocation and use of special access rights (privileged access capability);
4) Other relevant security events.
c. Protect logging facilities and log information to avoid damage and access by unauthorized parties.

d. The system log must be activated, retrieved and periodically reviewed.
e. The Event Log contains a minimum of: user id; activity and time.
f. Administrators are not permitted to delete or modify logs

The following figure 4.1 are screen capture logs for user access to the SIPP application obtained while conducting research



```
admin@storage_odd_drc:/volume1/ws_logs/wslogs51_gz$ ls -la
total 0
drwxrwxrwx  1 admin users   212 Jul 25 15:14 .
drwxrwxrwx+ 1 root  root    182 Jul 23 11:15 ..
drwxr-xr-x  1 admin users 22192 Apr  5 09:13 201802
drwxr-xr-x  1 admin users 75202 May 30  2018 201803
drwxr-xr-x  1 admin users 74904 May 30  2018 201804
drwxr-xr-x  1 admin users 75298 Jun 28  2018 201805
drwxr-xr-x  1 admin users 73860 Aug  8  2018 201806
drwxr-xr-x  1 admin users 82194 Aug 16  2018 201807
drwxr-xr-x  1 admin users 84820 Sep 17  2018 201808
drwxr-xr-x  1 admin users 83450 Oct 18  2018 201809
drwxr-xr-x  1 admin users 86618 Apr  5 09:15 201810
drwxr-xr-x  1 admin users 86526 Jan  3  2019 201811
drwxr-xr-x  1 admin users 96136 Apr  5 15:17 201812
drwxr-xr-x  1 admin users 99976 Feb 27 14:49 201901
drwxr-xr-x  1 admin users 88262 Jun 12 09:49 201902
drwxr-xr-x  1 admin users 98040 May 17 14:00 201903
drwxr-xr-x  1 admin users 87814 May 28 08:12 201904
drwxr-xr-x  1 admin users 92664 Jul  5 10:41 201905
drwxr-xr-x  1 admin users 78602 Jul 25 15:15 201906
drwxr-xr-x  1 admin users 41756 Jul 25 15:15 temp
```

Figure 4.1. user access logs

With the evidence of the log and its backup the Indonesian Insurance Company has fulfilled the security of the ISMS control A.12.3 Control objective A.12.4 Logging and monitoring

While for security control A.12.4.4 Clock synchronization which aims to time the information processing system that is related in the organization or security area, must be synchronized with a single reference time source, from the results of research researchers on the application of this control there are differences in the clock in information system applications which is not synchronized with an accurate time source, the Network Time Protocol as a unitary time unit on each server has not been fully synchronized with the Indonesian Insurance Company NTP server, so that the time lag can affect the number of transactions to be backed up, other things that can occur are inaccurate audit logs that may be needed for investigations or as legal evidence or in disciplinary cases, inaccurate audit logs also make investigations difficult and undermine the credibility of the evidence.

For these conditions the Indonesian Insurance Company has not been able to prove control over security controls A.12.4.4 Clock synchronization

E. Compliance Results in Area Control A.14 System Acquisition, Development and Maintenance

a. Control Objective A.14.1 Security requirements of information systems

This control objective is to ensure that information security is an integral part of the information system in the entire lifecycle. This also includes requirements for information systems that provide services through public networks. Security controls in this area are:

14.1.1 Information security requirements analysis and specification are control requirements related to information security that must be present in developing new application systems or adding functionality to existing applications. The Indonesian Insurance Company in carrying out the development / development of the application system has fulfilled the control requirements A.14.1.1 where in every floating the application always implements a security inquiry in accordance with IEEE 830-1998 standards and is documented in the Software Requirement Specification (SRS) document.

A.14.1.2 *Securing application services on public networks* is a control that requires that information contained in application services that passes through the public network must be protected from fraudulent activities, contractual disputes and modifications or leaking by unauthorized parties. Application security services in the public network of the Indonesian Insurance Company have been implemented including the application of security features network services include:

- ✓ Information security technologies such as authentication and control of network connections.
- ✓ there is a mechanism for limiting access to network services or applications for network service users.

Meanwhile, for the protection of networks from access by irresponsible parties include:

- ✓ The appointment of the person in charge of network management is separated from the management of the data center and the disaster recovery center.
- ✓ the application of special controls to protect the integrity of information that passes through public networks, among others by the use of encryption.
- ✓ documentation of the network architecture of all network hardware and software components

In the previous control regarding Cryptogaphy, it was discussed about the application of HTTPS in web-based application systems that are accessed through public networks, thus the A.14.1.2 control requirements have been fulfilled by the Indonesian Insurance Company.

b. Control Objective A.14.2 Security in development and support processes

The objective of this objective control is to ensure that information security has been designed and implemented in the information system development life cycle, there are 9 (nine) security controls that must be carried out, namely:

A.14.2.1 Secure development policy
A.14.2.2 System change control procedures
A.14.2.3 Technical review of applications after operating platform changes
A.14.2.4 Restrictions on changes to software packages
A.14.2.5 Secure system engineering principles
A.14.2.6 Secure development environment
A.14.2.7 Outsourced development
A.14.2.8 System security testing
A.14.2.9 System acceptance testing

In the Control above illustrates how control in management Information system development in the system development environment, whatever the development methodology or program language used, this control also states that every change in the system must be formally controlled, and every change made by the application must be re-reviewed and tested to ensure there are adverse impacts on operations or on the organization. Control of software that has been running must be limited / prevented from modification wherever possible, limited to changes made.

Control must also be carried out for the development of systems or applications whose development processes are outsourced to third parties which may include licensing rules, intellectual property rights, quality and accuracy of system acceptance tests and so on, at the next stage there is a test control during development / development that must be carried out namely testing the security function and the system acceptance test (user acceptance test) against the criteria must be established either for the newly created information system or upgrading from the old version

The Indonesian Insurance Company has implemented good controls in system or application development procedures so as to reduce the level of errors (errors, defects, bugs) in the application system that was built and avoid rework that must be done because of an error. In this control the Indonesian Insurance Company is very adequate because it has implemented well the stages that must be carried out in the system development cycle.

The results of the study found that the application development process is found in the Deputy Director of IT Development by implementing Good Practices related to SDLC, project management, application quality management, adequacy of application control, priority setting, testing and implementation.

Whereas the SDLC stage at the Indonesian Insurance Company includes the Planning Phase, the Business Requirements Phase, the design and development stage, the application testing phase, the implementation phase, the post implementation monitoring stage, and the evaluation phase as illustrated in Figure 4.2.

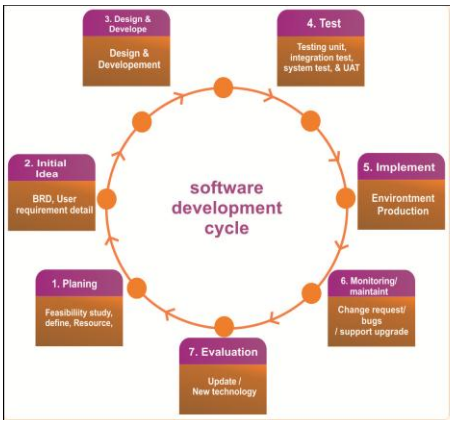

3. Design & Develope
Design & Developement
4. Test
Testing unit, integration test, system test, & UAT
2. Initial Idea
BRD, User requirement detail
software development cycle
5. Implement
Environtment Production
1. Planing
Feasibility study, define, Resource,
6. Monitoring/ maintaint
Change request/ bugs / support upgrade
7. Evaluation
Update / New technology

Figure 4.2. SDLC System Development

Information development needs requested by business units in the form of Business Requirement Development (BRD) which will be discussed with the IT development team to define problems and needs with the system translated in User Requirement Specification (URS), then the development team will pour the solutions offered and can be accommodated by the application system into the Software Requirement Specification (SRS) document. This document is also a basic two-way guarantee between the business unit and the project team for the application to be developed. The next stage determines the software, database and technology that will be used. this phase also determines the duration of time in the phases after the design, resources for the development of new systems running on time, in this phase produces a Software Design Description (SDD) is a document that describes the design of a system and the components built therein, including architecture , controls, logic, and data structures, input / output formats, face-to-face descriptions and the algorithms used. Furthermore, the development process is outlined in the Application Product Specifications (SPA) which contains information on the general description of the software that will be released and managed by the IT operational unit. The next stage to do is testing, at this stage Penetration Testing is carried out to test the weaknesses of the controls that exist in the developed application system, then proceed with User Acceptance Testing (UAT) which aims to ensure that the application system developed is in accordance with the needs user and can be used to continue the implementation process. Thus the Indonesian Insurance Company has carried out control in the control area A.14.2 Security in development and support processes.

G. *Gap Analysis*

The results of data analysis, interviews, and literature studies collected by referring to security clauses and controls in the ISO / IEC 2701: 2013 standard, obtained the results of the gap as shown in the following table:

TABLE 4.1. Analysis Result

Clause 7.5 Support		
Control Objectives	Security Control	Conformity
7.5.2 Creating dan Updating Document Information	Identification and description (e.g. title, date Author, or reference number)	Conform
	Format (e.g. language, software version, graphics) and media (e.g. paper,electronics)	Conform
	Reviews and approval for suitability and adequacy	On Progress

Control A.9 *Access Control*		
Control Objectives	Security Control	Conformity
A.9.1 Business Requirements of access control	A.9.1.1 Access Control Policy	Conform
	A.9.2.1 Access to networks and network services	Conform
A.9.2 User Access Management	A.9.2.1 User registration and deregistration	Conform
	A.9.2.2 User access provisioning	Conform
	A.9.2.3 Management of privileged access rights	Conform
	A.9.2.4 Management of secret authentication information of users	Conform
	A.9.2.5 Review of user access rights	Not Conform
	A.9.2.6 Removal or adjustment of access rights	Conform
A.9.3 User responsibilities	A.9.3.1 Use of secret authentication information	Conform
A.9.4 System and application access control	A.9.4.1 Information access restriction	Conform
	A.9.4.2 Secure log-on procedures	Conform
	A.9.4.3 Password management system	Conform
	A.9.4.4 Use of privileged utility programs	Conform
	A.9.4.5 Access control to program source code	Not Conform

Control A.10 Cryptography		
Control Objectives	Security Control	Conformity
A.10.1 Cryptographic controls	A.10.1.1 Policy on the use of cryptographic controls	Conform
	A.10.1.2 Key management	Conform

Control A.12 Operation Security		
Control Objectives	Security Control	Kesesuaian
A.12.1 Operational procedures and responsibilities	A.12.1.1 Documented operating procedures	Conform
	A.12.1.2 Change management	Conform
	A.12.1.3 Capacity management	Conform
	A.12.1.4 Separation of development, testing and operational environments	Conform
A.12.2 Protection from malware	A.12.2.1 Controls against malware	Conform
A.12.3 Backup	A.12.3.1 Information backup	Conform
A.12.4 Logging and monitoring	A.12.4.1 Event logging	Conform
	A.12.4.2 Protection of log information	Not Conform
	A.12.4.3 Administrator and operator logs	Conform
	A.12.4.4 Clock synchronization	Not Conform

Control A.14 System Acquisition, Development and Maintenance		
Control Objectives	Security Control	Conformity
A.14.1 Security requirements of information sistems	14.1.1 Information security requirements analysis and specification	Conform
	A.14.1.2 Securing application services on public networks	Conform
A.14.2 Security in development and support	A.14.2.1 Secure development policy	Conform
	A.14.2.2 System change control procedures	Conform
	A.14.2.3 Technical review of applications after operating platform changes	Not Conform
	A.14.2.4 Restrictions on changes to software packages	Conform
	A.14.2.5 Secure sistem engineering principles	Conform
	A.14.2.6 Secure development environment	Conform
	A.14.2.7 Outsourced development	Conform
	A.14.2.8 System security testing	Conform
	A.14.2.9 System acceptance testing	Conform

V. CONCLUSIONS

This study has assessed compliance with information security management at the Indonesian Insurance Company within the scope of SIPP use the framework of ISO / IEC 27001: 2013. Based on the results of the analysis and discussion it can be concluded that:

1. The Indonesian Insurance Company in general has established an Information Security Management System that is in line with ISO / IEC 27001: 2013 standards, but there is still a need for awareness of documents and procedures that are not yet operational.
2. The policies, procedures, instructions and documentation implemented in information security management in the SIPP scope still have gaps that need to be fixed, of the 37 control areas that have been tested, there are 5 controls that do not comply with the requirements of ISO / IEC 27001:2013 and one clause that is is in the progress of approval from the board of directors
3. Noted that there are 6 gaps spread on the following caluses dan security controls below:
   a. Clause 7.5.2 *Reviews and approval for suitability and adequacy*.
   b. Control A.9.2.5 *Review of user access rights*.
   c. Control A.9.4.5 *Access control to program source code*.
   d. Control A.12.4.2 *Protection of log information*.
   e. Control A.12.4.4 *Clock synchronization*.
   f. *Control A.14.2.3 Technical review of applications after operating platform changes*
4. To increase compliance with these standards, it is necessary:
   a. The Process of Ratification of Standard Policy documents and IT Service Management to be expedited immediately.
   b. Reminds the level of employee discipline back to employee tasks.

REFERENCES

[1] National Insurance Company, Participant Reporting Information System User Manual (SIPP), Jakarta: National Insurance Company, 2017.

[2] ISACA, "COBIT 5 for Information Security," Illinois, ISACA, 2012.

[3] www.isaca.org/bmis, The Business Model for Information Security, ISACA, 2010.

[4] BSN, International Organization for Standardization ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls, Jakarta: BSN, 2016.

[5] https://www.iso.org, International Organization for Standardization. ISO/IEC-27001-information-security management, ISO.org, 2019.

[6] www.iso.org, International Organization for Standardization. ISO/IEC 27002, Second edition 2013-10-01 Information technology — Security techniques — Code Of Practice For Information Security Control, Switzerland: www.iso.org, 2013.

[7] Regulation Of The Minister Of Communication And Information Republic Of Indonesia Number 4 Of 2016, "Regulation Of The Minister Of Communication And Information Republic Of Indonesia Number 4 Of 2016 About Information Security Management System".

[8] Whitman, Michael E. and Mattord, Herbert J. "Principles of Information Security (4th ed)," Boston, MA, USA Course Technologi, 2013.

[9] Sarno R and Iffano, "ISO 27001-based Information Security Management System," Surabaya, ITS Press, 2009.

[10] Leitch, Robert A. and Davis , K. Roscoe., "Information System," PT. Prenhallindo, 2001.

[11] O'Brien, James A. and George M Marakas, "Management Information System" Salemba Empat, 2014.

[12] J. F. Nash, Understanding information systems, Jakarta: Informatika, 1995.

[13] McLeod, Raymond Jr. and George P. Schell., "Management Information System," translate: Ali Akbar Yulianto., 2008.

[14] Kertahadi, "Understanding Information Systems," Yogyakarta, Information System, 2007.

[15] G.J Simons and Gene Spafford, in Practical UNIX & Internet Security, O'Reilly & Associates, Inc,2 nd edition, 1995.

[16] Rules of directors of the National Insurance Company Number: PERDIR/22/092019 , Position Name, Job Description and Position Requirements for National Insurance Company, Jakarta:The National Insurance Company, 2019.

[17] National Insurance Company, Board of Directors Decree Number .Kep/234/062012 Concerning Information Technology Policies And Standard Operating Procedures, Jakarta: National Insurance Company, 2012.

[18] BSN, International Organization for Standardization. ISO/IEC 27003, Information technology — Security techniques — Information Security Management System Implementation Guidance, Jakarta, 2016.

[19] BSN, "International Organization for Standardization ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement," BSN, 2016.