Journal of Physics: Conference Series **1367** (2019) 012004 doi:10.1088/1742-6596/1367/1/012004

Implementation of security system on humanitarian organization: case study of dompet dhuafa foundation

Emil R. Kaburuan[1], **ASL Lindawati**[2]

[1]Information Systems Management Department, BINUS Graduate Program – Master of Information Systems Management, Bina Nusantara University, Jakarta, Indonesia

[2]Accounting Department, Faculty of Economics & Communication, Bina Nusantara University, Jakarta, Indonesia

E-mail: [1]emil.kaburuan@binus.edu, [2]lindawati@binus.edu

Abstract. System security management can increase public confidence in the information produced and processed by a company and increase the quality assurance of information. To reduce the threat to the company's business process information system, there must be an assessment of information system security management needed to support the company's business processes, especially in the humanitarian foundation, in this case, is "Dompet Dhuafa Foundation." In the use of information systems, security risks will arise, which will hurt the institution. In order to reduce the negative impact, it is necessary to handle the security risks of the system. ISO / IEC 27001 offers a set of specifications, a code of ethics, and best practice guidelines to ensure the management of IT (Information Technology) services. ISO 27001 is a standard that is often used to determine the need to implement information system security. With the application of ISO / IEC 27001, It can protect aspects of information security, namely confidentiality, integrity, and availability.

1. Introduction

At present, the information system has a tremendous impact on human life. It is essential to use it in terms of accelerating work, and also play a role in solving problems. The development of this system is increasingly fast, but whether peoples are ready in following the development of these technologies. With this situation, the development of information systems, especially security, has received serious attention.

Dompet Dhuafa Foundation is a non-profit organization owned by the Indonesian people to help donors channel the assets that their own to people who needed. The use of the information system by "Dompet Dhuafa" in 2017 was named DESI "Dompet Dhuafa Information System." The system is web-based application programs to facilitate its services to donors, facilitate the processing of data and information in management, as a medium to market its services, and giving a sense of trust to donors of the Dompet Duafa Foundation that the funds or part of the assets they provided were distributed to those in need. However, security from DESI is critical because they being the central system for all operation. As one of the fulfillment of the responsibility of "Dompet Dhuafa" in providing superior services.

In order to keep the information contained in the application system, it is necessary to apply the security management system. This study uses ISO 27001 as an information security standard issued

by the International Organization for Standardization and the International Electrotechnical Commission [1]. This standard has the main criteria and requirements that must exist in building information system security management [2] [3]. It is made to ensure a protect the company's assets from various risks and threats that exist. Thus, the study determined "DESI Security System Implementation" Dompet Dhuafa Information System "using the ISO 27001 method" as a theme and at the same time became the title in the preparation of this paper.

In the future, The DESI will provide a competitive advantage for Dompet Dhuafa foundation with the security factor must be the most important to pay attention. This security factor can be one of the excellent features that can be highlighted by the foundation. The paper seeks to identify various problems and alternative solutions that must be done.

In this case, the foundation with DESI as the current system; has the following problems: Security threats or any risks related to transaction activities and data processing and information of donors and how the DESI security system "Dompet Dhuafa Information System "? as well as the handling of what must be done to reduce the risk of the application of DESI.

2. Literature Review

The security of information systems is how we can prevent cheating or, at the very least, detect fraud in an information-based system [4]. The threat of security is an action or event that can harm the company [5]. Losses can be in the form of money, energy, the reputation of the organization may even cause bankruptcy [5]. Security aspect, such as the system device is damaged or becomes unavailable, accessing information by unauthorized parties, parties who do not have authority not only access information but also make changes to the information, and insertion of fake objects into the system by unauthorized parties [6].

Proper management of information system security is needed to anticipate possible threats. In this case (ISO) is a private international organization engaged in the determination of standardization. It is used to support innovation in the community and provide solutions to challenges faced by business people [7]. ISO 27001 is an update of ISO 17799. ISO 27001 has been adopted by the National Standardization Body (BSN) as the Indonesian National Standard (SNI) for ISMS [8].

- ISO 27003:2010 - ISMS Implementation Guidance
- ISO 27004:2009 - ISMS Measurements
- ISO 27001:2009 - ISMS Overview and Vocabulary
- ISO 27005:2008 - Information Security Risk Management
- ISO 27007 - Guidelines for ISMS Auditing
- ISO 27006:2007 - ISMS Certification Body Requirements
- ISO 27001:2005 - ISMS Requirements
- ISO 27002:2005 - Code of Practice for ISMS

ISO 27001 contains the basic principles of ISMS, definitions of many essential terms, and inter-standard relationships within the ISMS family [8]. This standard can be used for all types of organizations, both governmental, commercial, and non-commercial organizations. The application of ISO 27001 is tailored to the goals, objectives, and needs of the organization. This process approach emphasizes the following points [7]:

1. The process of planting knowledge of organizational information security and the need for information security policies and objectives,
2. Ratification and application of control of information technology governance in shaping overall business risk mapping
3. Monitoring and rechecking the development of performance and always monitoring the development and effectiveness of the application of information system management, and
4. Measure improvement continuously so that the desired achievement can be fulfilled following the desired expectations.

This standard applies the "Plan-Do-Check-Art" method to form the entire security management process. This standard provides the right steps to make and implement steps in implementing and regulating risk assessments [7].

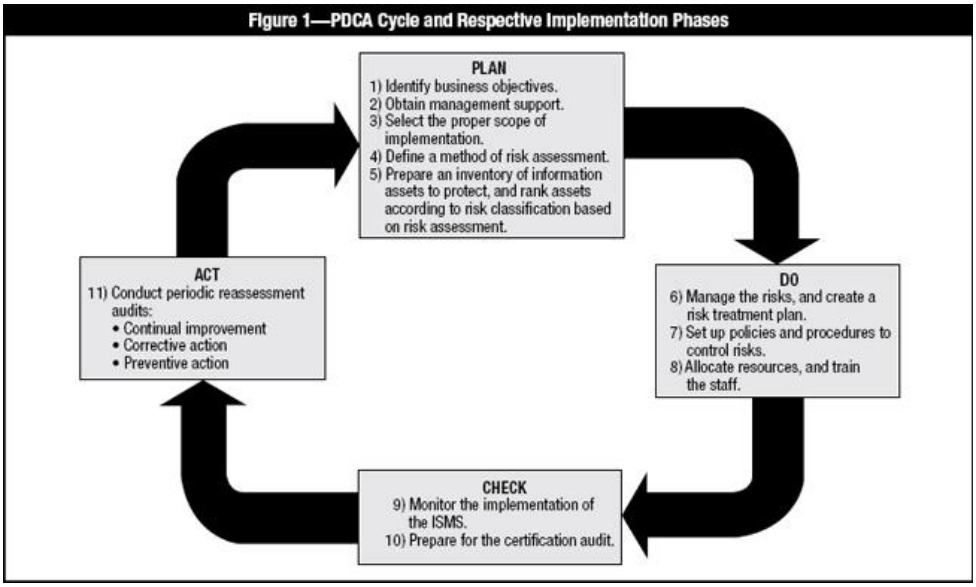

Figure 1. PDCA Model ISO 27001 [8]

The following is an explanation of the PDCA model:

1. Plan
   The process of planting knowledge of organizational information security and the need for information security policies and objectives.
2. Do
   This stage is carried out by determining the way the ISMS policy operates, controls, processes, and procedures.
3. Check
   This stage is carried out by reviewing and measuring the process performance against policies, objectives, practices in running ISMS and reporting the results for the assessment of their effectiveness.
4. Act
   This stage is carried out by taking corrective and preventive actions based on the results of evaluations, internal audits, and management review about management security or other monitoring activities to achieve continuous improvement. This standard also explains some of the main requirements that must be met, including:
   - Information security management
   - Management burden
   - Internal audit security management
   - Review of security management
   - Continuous improvement

   In addition to the above conditions, this standard also provides requirements for setting information control controls and security controls, covering 11 security areas, namely [6]:
   - Information security policy
   - Information security organization
   - Asset management
   - Human resources regarding information security

- Physical and environmental security
- Communication and operations management
- Access control
- Procurement/acquisition, development, and maintenance of information systems
- Management of information security incidents
- Business continuity management.

2.1. Security in the Design Phase

Design is a representation of decision making to meet software design requirements. In the software design phase that needs to be considered are:

1. Identifying and Evaluating Threats Using a modeling thread to systematically identify far better threats. Modeling is usually done by ranking threats that might occur based on the risk of attack. Frequency of events, which are associated with potential losses or damage that can occur. This can reduce us in dealing with threats in the right order.
2. Making a safe design We recommend that you use tried and tested design principles and focus on critical areas where the right approach and frequent errors that occur include: input validation, authentication, authorization, configuration management, sensitive data protection, cryptography, parameter manipulation, and logging. There should also be serious attention to deployment issues, including topology: network infrastructure, security policies, and procedures.
3. Checking Architecture and Design Application design must be examined with the deployment environment and related security policies. Need to make limits that are determined based on security in the infrastructure layer, including networks, firewalls, remote application servers, and analyze approaches taken in each area.

Security in the Implementation Phase makes sure the design is translated into code during execution. The following are activities that need to be carried out during implementation to achieve the code [9]. High-level programming languages provide a safe level that is close to perfection.

1. However, sometimes we need to use a low-level programming language to get direct access to Hardware. High-Level programming languages must be selected but must still see the requirements of software development programming.
2. Standard coding security and following instructions must be followed to avoid source code errors.
3. Unit testing (testing) must be done by thinking about security issues. A security error will be reported in the software that is used as a reference.

2.2. Assurance Phase

During the guarantee phase, the software must be checked periodically to meet the requirements. Activities carried out during this phase are as follows [9]:

1. The code must be checked (if there is an error based on a list of previously reported errors) to identify the software and security errors. Besides, static analysis tools must be used to find errors. Errors found must be resolved immediately.
2. Test cases must be developed based on functional and security needs.
3. Integration and testing need to be carried out based on testing security requirements. Penetration must be done based on known vulnerabilities and potential attacks that will be encountered by the software user. Security errors found must be removed.

3. Explanation

Desi (Dompet Dhuafa Information System) is a management system to record, manage and monitor the Dompet Dhuafa Foundation's finances which can easily track company expenses and revenues and help companies know where and when foundation funds are used.

This application is equipped with many menus needed by its employees in doing their work. Validation of all interested parties is all made so that the process of receiving zakat can be recorded correctly.

In its implementation, the Dompet Dhuafa foundation tried to start by applying authentication for all accounts connected to the DESI System, and DESI used encryption to protect existing data and information so that it could not be read and utilized by unauthorized people. Besides that, there is also an anti-virus implementation which always updated; the use of their firewall is trying to implement it all

In the management of the Dompet Dhuafa Foundation, they created a Segregation of duties which aims to restrict access to applications and the distribution of access rights is given according to the required positions and needs, they also try to implement SOPs in IT management.

Therefore, by applying the ISO 27001: 2013 standard, Dompet Dhuafa foundation can protect and maintain the confidentiality, integrity, and availability of information and to manage and control information security risks in their organizations or foundations.

Some of the benefits to be achieved from the application of ISO 27001 standards, such as:

- Providing confidence and assurance to donors or business partners, that the Dompet Dhuafa foundation company has an information security management system that is in line with international standards. Besides, ISO 27001 can also be used to market the company.
- Ensure that the Dompet Dhuafa foundation has control over information security on the environment of its business processes that may pose a risk of interference.
- ISO 27001 forces the Dompet Dhuafa Foundation to continue to improve the information security of their zakat institutions. This helps the Dompet Dhuafa Foundation to determine better the exact amount of security needed for the company. Resources will be in the right amount.

4. Conclusion

The main cause of the vulnerability is because there is a hole in the software. Software security must be systematically located in the software development life cycle (SDLC). Each phase has a security stage that must be considered when building software so that later can make a reliable and safe product. Security in software can be measured by performing calculations using the equations described earlier or by using tools to audit the sequence of codes. That way, we can build security software can help build security "built-in". Software that has "built-in" security will get more trust from users. Now it is time to build software that has security "built-in". In addition to providing high trust, the security phases of the software "built-in" will provide a minimal warranty cost (time and cost), and provide more assurance to the user compared to software that has no "built-in" security. Mitigation measures that have been determined then summarized into 12 statements in the form of questionnaires, and distributed to the parties involved in the use of information systems to obtain feedback regarding the application of such measures.

References

[1] Disterer, G. (2013). ISO/IEC 27001, 27001, and 27002 for information security management. *Journal of Information Security*, *4*(02), 92.

[2] Gillies, A. (2011). Improving the quality of information security management systems with ISO27001. *The TQM Journal*, *23*(4), 367-376.

[3] Susanto, H., Almunawar, M. N., & Tuan, Y. C. (2011). Information security management system standards: A comparative study of the big five. *International Journal of Electrical Computer Sciences IJECSIJENS*, *11*(5), 23-29.

[4] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

[5] Messerges, T. S., Dabbish, E. A., & Sloan, R. H. (2002). Examining smart-card security under the threat of power analysis attacks. *IEEE transactions on computers*, *51*(5), 541-552.
[6] Bedi, P., & Agarwal, S. K. (2011, June). Managing security in aspect oriented recommender system. In *Communication Systems and Network Technologies (CSNT), 2011 International Conference on* (pp. 709-713). IEEE
[7] BSN, (2009): Information technology - Security techniques - Information security management systems - Requirements (ISO/IEC 27001:2005, IDT). BSN. Jakarta.
[8] C. Pelnekar, "Planning for and Implementing ISO 27001," vol. 4, p. 8, 2011
[9] Khan, M. U., & Zukernine, M. (2009). Actifity and Artifact views of a secure software development proses. IEEE Computer Society , 2