Risk Analysis of Dutch Healthcare Company Information System

R F Septian and G C Pamuji
Master of Information System, Faculty of Postgraduate, Universitas Komputer Indonesia, Indonesia

ridwanbejo@gmail.com

Abstract. The purpose of this research is to assure the performance and quality of healthcare information system security from the Dutch Company, which is located in Rotterdam, Netherland. The research applies COBIT 5 to audit the existing information security management system (ISMS) based on ISO 27001 and NEN 7510-2 2017 toolkit to audit the information system security for healthcare-specific issue. The audit is applied in order to identify any risk that might come during the ISMS implementation. On the other hand the result will be used as an improvement for the successor version of ISMS which compatible with the ISO 27001 and NEN 7510-2. The research was composed by applying qualitative method that consists of observation of the activity of the company and reviews the existing ISMS-related documents. As a result of this audit, the company ISMS has an achievement from NEN 7510-2:2017 audit result that has a score for 92.86 % on security management section. For the COBIT 5 result, the audit yield a result that consist of two “Established Process” level on APO13 and MEA02 and “Predictable Process” level on DSS 05. The result indicates a good result and encourages the company to improve their ISMS for next period.

1. Introduction
In the Netherlands, the company should have a certificate from the NEN (Nederlands Normalisatie-Instituut / Netherlands Standards Institute) also for their credibility before their customers and partners [1-5]. The NEN itself has so many types, which could be taken by the company. This kind of certificate is eligible for a company who run their business over the healthcare market and have an IT-driven business [6-10]. On the other hand, the company has applied the ISO 27001 certificate for a twice consecutive year. The company needs the analysis process to see the compliance of their IT infrastructure and service with NEN 7510-2 2017 and ISO 27001 for the IT security aspects.

The company where the research has been taken is focusing their market on mental healthcare. The main stakeholder within the company include the therapists, patients, and the company itself as the provider. Located in Rotterdam, the company focusing their service to provide the psychologist perform therapy for a patient who has a mental health issue. Since this healthcare company is operational at the Netherlands market, the NEN 7510-2 should be considered as another standard which should be followed by the company [6-10]. The NEN 7510-2 has a toolkit for evaluating the IT infrastructure and operation for a company who try to achieve the NEN 7510-2 [2]. The toolkit is described in Appendix C within the standard.

But it needs to be translated to the English since its being written with the Dutch Language. The toolkit works for IT security measurement for a healthcare company. There is an ISO specific for a healthcare information system, but the NEN 7510-2 itself is satisfying the company vision and mission.
Moreover, the company should comply with the Netherlands standard body. Based on the proposed research, the internal audit will be conducted to evaluate the ISMS and some security activity by using the COBIT 5 and NEN 7510-2:2017 toolkit. The COBIT 5 will be applied to evaluate the security management for this company in general aspect that related to ISO 27001:2013 control [3-5]. The COBIT 5 could be applied to assess the information technology which should be aligned with the vision and mission of the enterprise and ISO 27001:2013 also [11-17]. For the healthcare-specific security issue, this research will use the NEN 7510-2-2017 toolkit to evaluate the security management of the company.

The objective of this research has to gain a result of COBIT 5 and the NEN 7510-2:2017 auditing. This result should be delivered to the management and security forum to gain awareness of the audit result and take a further step to refine or redefine the ISMS within the company due to the standard. On the other hand, the results could support the next research that works on security audit at any Dutch Company.

2. Methods
The qualitative methodology of this research was taken by these following phases which are applied during the research; 1) Research Planning, 2) Scoping the research, 3) Data Acquisition, 4) Auditing using NEN 7510-2 and COBIT 5, 5) Audit Result Reporting, 6) Conclusions and Recommendations. This research is involving 3 persons that consist of the CTO, Security Team, Infrastructure Team, and Office Manager.

To obtain the data for the research, analysis, and observation has been performed to gain input for the result by using the selected toolkit. For the secondary data, the research was initiated by a study review about auditing on the ISMS using COBIT 5 and NEN 7510-2:2017 through papers, journals, thesis, and articles. Then the references become a foundation of this research to conduct with the company for performing an auditing mechanism of the existing ISMS.

The chosen COBIT 5 processes are APO 013, DSS 005 and MEA 002 [3]. The processes are chosen due to the scope of this research about auditing the existing ISMS and its compliance. Each of the toolkits has its way to judge any control measure. The COBIT 5 PAM has an indicator to be judged to see how the level of capability is achieved by each process that consists of 5 capability levels. Each level on COBIT 5 PAM will be judged by this rating scale which is reproduced from ISO/IEC 15504-2:2003. The scale consist of Not Achieved (N), Partially Achieved (P), Largely Achieved (L) and Fully Achieved (F) [5].

By applying the NEN 7510-2:2017, the auditor should apply the checklist in the appendix C that has a purpose to enable healthcare organizations that process personal health information to meet the criteria against NEN 7510-2:2017 [2]. The checklist contains the control measures from this standard and columns as the basis of which it is possible to check whether the control measures have complied with NEN 7510-2:2017 has an explanation of each column that consists of; chapter, implemented, priority, reference, budgeted, responsible, note, follow-up. Afterward, this research is communicated to the management to find the schedule for the auditing itself, then give the result which consists of the COBIT 5 PAM result and NEN 7510-2:2017 result [2]. The management gives their review to improve the research results and improvement.

3. Result and Discussion
3.1. Audit Result using NEN 7510-2 Toolkit
Based on the NEN 7510-2 section no. 12 for Security Management, the auditor used the respective form to assess the conformity of the IT process and its compliance with the NEN 7510-2 [2]. There are 7 sections which consist of 7 categories within the form No.12 as shown in Table 1.
Table 1. Vision and Mission mapping to the Enterprise Goals.

| No | Section                                                                 | Yes | No |
|----|-------------------------------------------------------------------------|-----|----|
| 1  | Operating procedures and responsibilities (bedieningsprocedures en verantwoordelijkheden) | 6   | 0  |
| 2  | Protection against malware (bescherming tegen malware)                  | 1   | 1  |
| 3  | Back-up (back-up)                                                       | 2   | 0  |
| 4  | Reporting and monitoring (verslaglegging en monitoren)                  | 12  | 1  |
| 5  | Control of operational software (beheersing van operationele software)  | 2   | 0  |
| 6  | Management of technical vulnerabilities (beheer van technische kwetsbaarheden) | 2   | 0  |
| 7  | Considerations concerning audits of information systems (overwegingen betreffende audits van informatiesystemen) | 1   | 0  |
|    | Total of the section which meets the criteria                           | 26  | 2  |

Score for this form

\[
\text{Score} = \frac{Y}{Y + N} \\
\text{Score} = \frac{26}{26 + 2} \\
\text{Score} = 92.86
\]

That score is indicating the company security management has gone so far with the best result based on the NEN 7510-2. Many evidences have found during the internal audit which support the scoring such as: ISMS document, Employee Handbook, Multi-stage Infrastructure for Development (local, develop, staging, production environment for software development), Release guideline for each platform (portal, mobile, SDK, backend), Daily backup policy, Encryption policy, Activity log on the goalie-backend, Chat conversation logging, Personal health information logging. Every logging information contain time and network information. Periodic internal audit is performed, Backend weekly meeting, Infrastructure weekly meeting, Monthly security meeting, Log inspection for the backend and infrastructure, 2FA authentication, Secure password sharing mechanism, Backend and infrastructure monitoring and Limited access by using VPN.

On the other hand, the company has spent a quite large budget to support security management. For example, during the internal audit, there are evidences that the company subscribes to these products to support the security management and availability of the company infrastructure: Google Office Suite, Amazon Web Service Route53, Amazon Web Service IAM, Amazon Web Service S3, CloudVps OpenStack and Travis-CI.

The result does not only describe the success rate of the internal audit, but it is also left some caveat that needs to become a priority for the management:
On the paragraph 12.2.1.2 which confirming about “implementeert de organisatie passende bewustzijnstraining voor gebruikers om bescherming te bieden tegen kwaadaardige software? (does the organization implement appropriate awareness training for users to provide protection against malicious software?)”, the paragraph is marked as unmet criteria because there is no security awareness training during the year of 2018. The security awareness training is very important to emphasize stakeholder awareness about the existing ISMS and common practice of security. This will be a responsibility for the management and Security Team.

On the paragraph 12.4.2.1 which confirming about “zijn auditregistraties beveiligd en kunnen ze niet gemanipuleerd worden? (are audit records secured and can they not be manipulated?)” also did not meet the criteria. The company has some logging system and database which collect the data from all the company backend services and infrastructures. Of course the company has put some secure configuration there, but there are some caveats for that. For example, in the Elasticsearch stack which is being utilized for reporting the backend and infrastructure log data, as long someone has a VPN access could access the page and somehow modify the record. That means the company could end up with false reporting someday due to the company backend and infrastructure logging report.

3.2. Audit Result using COBIT 5 PAM Toolkit

3.2.1. COBIT 5 Mapping Process

First of all, the auditor cannot use all the metrics within the COBIT 5 PAM toolkit. Firstly, the auditor has to map the company vision and mission to the COBIT 5 enterprise goals as stated on the scope of the ISMS. The company has two vision and mission which are stated on verklaring toepasselijkheid and the ISMS document; 1) The company develop and provide products (apps) to support treatments in the care sector or businesses to support vitality of employees, 2) The company protect the personal data of end-users of products of the company, personal and financial details of employees of Sense Health, and confidential information of Sense Health, both physical and logical form, inside and out of the physical office space. After the mapping process from vision and mission to the enterprise goal, the mapping process shows the result that the vision and mission are not meet with the EG-8, EG-11, EG-12, EG-13, and EG-16.

Second, the auditor maps the enterprise goals to IT goals. The auditor should map the highlighted COBIT 5 enterprise goals of the company to the COBIT 5 IT goals. The auditor has to choose the primary IT goals that need to be audited. Third, the auditor map the COBIT 5 IT goals onto COBIT 5 Process. The mapping gave the result that almost all primary IT goals have its relation to enterprise goals. The auditor will use all the IT goals or just pick some of the IT goals depend on the scope. But since the auditing is only focusing this audit for ISMS at the company, the auditor should choose the IT goals that have a relation to the ISMS issue. After the mapping, 5 chosen IT-related goals have a connection to audit the existing ISMS. Next, the auditor has to map the IT-related goals to the COBIT 5 Process based on COBIT 5 guide [3-5].

3.2.2. COBIT 5 Process Selection

Based on the mapping between IT-related goals to COBIT 5 process, the result has shown that all COBIT 5 process has a relation with the selected IT-related goals. In that case, the auditor has to choose only a process that has a minimum one primary against the chosen IT-related goals. This research tries to audit the ISMS by using only three forms for this period due to the tight schedule. The auditor chooses the APO 13, DSS 05 and MEA 02 form from the COBIT 5 PAM toolkit which has a higher priority based on primary relationship.

For the next internal audit, both for internal purpose or research purpose, the next auditor could recommend using the remaining form based on the priority of their primary relationship against the chosen IT-related goals. Sorted by the greatest primary relationship to the least primary relationship, the
successor auditor could perform this audit using sorted COBIT 5 process to audit the ISMS based on their primary relationship as shown in Table 2:

| COBIT 5 Process | P | S |
|-----------------|---|---|
| EDM03           | 4 | 1 |
| APO12           | 4 | 1 |
| APO13           | 4 | 0 |
| MEA01           | 3 | 2 |
| MEA02           | 3 | 2 |
| DSS05           | 3 | 1 |
| APO01           | 2 | 2 |
| BAI06           | 2 | 1 |
| MEA03           | 2 | 2 |
| EDM02           | 1 | 0 |
| EDM05           | 1 | 2 |
| APO06           | 1 | 2 |
| APO10           | 1 | 4 |
| BAI01           | 1 | 1 |
| BAI09           | 1 | 4 |
| BAI10           | 1 | 4 |
| DSS01           | 1 | 3 |
| DSS02           | 1 | 2 |
| DSS03           | 1 | 2 |
| DSS04           | 1 | 3 |
| DSS06           | 1 | 3 |

The detailed workflow of recommended COBIT 5 process above could be accessed on COBIT 5 Guide and COBIT 5 Process Assessment Models guide.

3.2.3. **COBIT 5 Process Result**

As far as the research performed during the audit by using COBIT 5, this research got this result for the company Information Security Management System, as shown in Table 3.

Before performing the internal audit, the auditor set an audit threshold on level 3. Based on the target, APO 13 and MEA 02 reach the target. On the other hand, DSS 05 surpass the target and reach level 4. At this moment, this result could be considered that only the DSS 05, which has a higher capability than the APO 13 and MEA 02.

There is some reason why the Manage Security (APO 13) reach level 3 that indicated the process is well established in the organization. The evidences that lead the process achieved Process Definition (3.1) such as the rules within the ISMS is being applied to every sub-unit by creating the extended policy based on the ISMS, the company have security incident and infrastructure incident meeting. The evidences that lead the process achieved Process Deployment (3.2) such as; the ISMS is following the ISO 27001:2013 and try to follow NEN 7510-2 also. This process is also reached level 4 partially. This research gives us an advantage from the partial result to complete the requirements for level 4.
Table 3. Selected COBIT 5 Processes Result.

| Process ID | Process Name                                      | To be assessed | Level 0 | Level 1 | Level 2 | Level 3 | Level 4 | Level 5 |
|------------|--------------------------------------------------|----------------|---------|---------|---------|---------|---------|---------|
|            | Align, Plan and Organise                         |                |         |         |         |         |         |         |
| APO13      | Manage Security                                  | ✓              | F       | F       | F       | F       | P       | N       |
|            | Deliver, Service and Support                     |                |         |         |         |         |         |         |
| DSS05      | Manage Security Services                         | ✓              | F       | F       | F       | F       | F       | N       |
|            | Monitor, Evaluate and Assess                     |                |         |         |         |         |         |         |
| MEA02      | Monitor, Evaluate and Assess the System of Internal Control | ✓              | F       | F       | F       | F       | P       | N       |

Based on the audit result from Table 3, DSS 05 reach level 4 that indicated the process is well established in the organization and has a predictable culture which improves the process. The evidences that lead the process achieved Process Measurement (4.1) are such follow: the monitoring result of backend and infrastructure are collected due to the ISMS statement regarding the monitoring section, the physical and common security issue is also being monitored by the Office Manager and CTO, there are a measurement objectives based from the ISMS statement as Prometheus to collect the data to determine what action which need to be taken and each platform collect the data to be evaluated to handle the bug or security issue earlier. The evidences that lead the process achieved Process Control (4.2) are such follow: the analysis of bug and security related issue will be performed by quantitative and graphical analysis by support of the tools depend on the platform, the parameter that needs as objectives for analysis are defined depend on the platform as in backend and infrastructure use Prometheus and OpsGenie connected by Alert Manager.

The MEA 02 reach level 3 that indicated the process is well established in the organization. The evidences that lead the process achieved Process Definition (3.1) are such follow: scoping is taken when the internal auditor penetration testing will be performed during the planned schedule, the internal audit and penetration testing is a part of the ISMS and follow the workflow which defines by the ISMS. The company used the security assessment tools which compliance to the OWASP standard. The evidences that lead the process achieved Process Deployment (3.2) are such follow: The procedure for internal audit and related incident handling are stated in ISMS and the scope and the objectives are also defined during the specific meeting, the assignment to the internal audit and some incident handling will be performed by delegating the task to the available person and has a proper competencies to perform that task. This process is also reached level 4 partially. The company could get advantage from the partial result to complete the requirements for level 4 by define and execute the improvement objectives on ISMS. This research has conclusion of the result as depicted in Figure 1:
3.2.4. COBIT 5 Process Recommendation

Based on Figure 1, the recommendation could follow COBIT 5 Process Assessment Model guide that the APO 13 is able to be improved to level 4 by achieving the following criteria; Defined the measurement for evaluate the ISMS and RAM Tools based on the quantitative approach beside performing the internal audit and penetration testing, collect a feedback from stakeholder and quantitative data for each annexes which related to the performance of the ISMS. Based on the feedback and quantitative data, the company has to set quantitative objectives or key performance indicator that could drive the ISMS to become more agile across the organization then analyze it with the quantitative statistical method.

Similar to the previous approach, MEA 02 is also able to be improved to the level 4 by achieving following criteria; defined the measurement for evaluating the Internal Audit and Penetration Testing based on the quantitative approach, collect a feedbacks from stakeholders and quantitative data for each internal audit and penetration testing evaluation. Based on the feedback and quantitative data, the company have to set quantitative objectives or key performance indicator that could drive the internal audit, and penetration testing become more aligned with the ISMS, when the process is running with some quantitative objectives, then the company should analyze it by performing quantitative analysis.

For the DSS 05, this process is surpassing the level 3. But the company could improve the DSS 05 to reach the level 5 by achieving this criterion; each best practices should have improvement plan after certain period, and it should have an improvement action with documented result, the data for documented quantitative and qualitative analysis should be collected depend on the base practice and it could contain the failure of the best practice or its successful rate during its implementation. Finally, the company should perform quantitative and qualitative to propose improvement action with a documented result.

Those recommendations above were created based on the COBIT 5 PAM guide on Process Capability Indicator for level 4 and 5 from Appendix C. If the company want to set the plan to achieve the next level for each the results, they should reference the Process Capability Indicator and address every action point from the next level for the next achievement [4].

4. Conclusions

As a result of this audit, the company ISMS has an achievement which has to be compliance with the NEN 7510-2 2017 and ISO 27001:2013 based on the scope of this audit. NEN 7510-2:2017 has a score for 92.86 % on Security Management section. COBIT 5 as an ISO 27001:2013 compliance toolkit, give us a result that the internal audit using COBIT 5 has two “Established Process” level on APO13 and MEA02 and “Predictable Process” level on DSS 05 based on the scope that agreed before the auditor perform this internal audit and the auditor set target on level 3 for each selected COBIT 5 processes.
The recommendation based on the NEN 7510-2 2017 and COBIT 5 (ISO 27001:2013) could be referenced whenever the company organizes an external audit based on the NEN 7510-2 2017 or becomes an improvement plan to the existing security process. This paper might be referenced to support the next research regarding a healthcare information system auditing by using the NEN 7510-2 toolkit and COBIT 5.

Acknowledgement
We want to send our gratitude for the Dutch Company which located at Lloydstraat, Rotterdam who allowed us to conduct this research. We would like to say thank you very much for the organizer of INCITEST 2019.

References
[1] Mors, R., & Jonkers, H. (2017). Effect on concrete surface water absorption upon addition of lactate derived agent. Coatings, 7(4), 51.
[2] Van der Hoek, J. P., Struker, V. D. A., & De Danschutter, J. E. M. (2017). Amsterdam as a sustainable European metropolis: integration of water, energy and material flows. Urban Water Journal, 14(1), 61-68.
[3] Neerhof, A. R. (2017). Gebruik van normalisatie door de Europese en de Nederlandse overheid:: een rechtstastelijke en democratische blik. Jurisprudentie bestuursrecht plus, 3, 195-220.
[4] Brunesi, E., & Nascimbene, R. (2017). Experimental and numerical investigation of the seismic response of precast wall connections. Bulletin of Earthquake Engineering, 15(12), 5511-5550.
[5] Belfrage, H., Strand, S., Storey, J. E., Gibas, A. L., Kropp, P. R., & Hart, S. D. (2012). Assessment and management of risk for intimate partner violence by police officers using the Spousal Assault Risk Assessment Guide. Law and human behavior, 36(1), 60.
[6] Felix B, et al 2018 Effectiveness of a transdiagnostic individually tailored internet-based and mobile-supported intervention for the indicated prevention of depression and anxiety (ICare Prevent) in Dutch college students: study protocol for a randomised controlled trial Trials (pp. 1-13)
[7] Matthijs B, Arnold V E, Bastian R and Jack D 2016 Blended internet care for patients with severe mental illnesses: An open label prospective controlled cohort pilot study 2016 Elsevier – Internet Interventions 5 (pp. 51-55)
[8] Vincent A V G, et al 2017 Web-based consultation between general practitioners and nephrologists: a cluster randomized controlled trial Oxford Health Service Research – Family Practice 34 (4) (pp. 430-436)
[9] Fieke H, et al 2018 National quality registries: how to improve the quality of data Journal of Thoracic Disease 10 (pp. 3490-3499)
[10] Susan J, et al 2017 Development and Validation of an Interactive Internet Platform for Older People: The Healthy Ageing Through Internet Counselling in the Elderly Study Mary An Lieber. Inc – Telemedicine and e-Health 23 (2) (pp. 1-9)
[11] W Trianto 2018 Evaluation of Patient Information System in Public Health Service Using the COBIT 5 Framework IOP Conf. Ser.: Mater. Sci. Eng. 407 012166
[12] Destianti C A and Suryanto E C 2018 Evaluation of Information Technology Governance with COBIT 5 in XYZ for ISO 27001:2013 Readiness International Journal of Engineering and Techniques 4(4) (pp. 76-86)
[13] Rafael A, Renato L and Miguel M S 2018 A Model for Assessing COBIT 5 and ISO 27001 Simultaneously 20th Conference on Business Informatics on (pp. 60-69) IEEE
[14] Tim H, Steven D H, Anant J and Wim V G 2018 Answering Key Global IT Management Concerns Through IT Governance and Management Processes: A COBIT 5 View Proceedings of the 51st Hawaii International Conference on System Sciences (pp. 5335-5344)
[15] I Wayan P B, I Made S and Putu W B 2017 Internal Control Improvement for Creating Good Governance International Journal of Information Engineering and Electronic Business
(IJIEEB) 9(3) (pp. 9-17)

[16] I Nengah P, Abdul H, Sholeh H P and Herman T 2017 Adopted COBIT-5 Framework for System Design of Indonesia Navy IS/IT: An Evaluation International Journal of Applied Engineering Research 12 (17) (pp. 6420-6427)

[17] Dalibor D and Branko L Frameworks for Audit of An Information System in Practice 2016 Journal of Information Technology and Applications (JITA) (pp. 78-85)