# Security Audit On Loan Debit Network Corporation System Using Cobit 5And Iso 27001: 2013

*by* Fathoni Fathoni

**Submission date:** 09-May-2023 02:21PM (UTC+0700)
**Submission ID:** 2088382543
**File name:** security_audit_loan.pdf (544.68K)
**Word count:** 287
**Character count:** 23584

Journal of Physics: Conference Series

PAPER · OPEN ACCESS

# Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013

To cite this article: Fathoni *et al* 2019 *J. Phys.: Conf. Ser.* **1196** 012033

IOP Conf. Series: Journal of Physics: Conf. Series **1196** (2019) 012033 doi:10.1088/1742-6596/1196/1/012033

# Security Audit on Loan Debit Network Corporation System Using Cobit 5 and ISO 27001: 2013

**Fathoni [1] .,Novita Simbolon [2] and Dinna Yunika Hardiyanti [3]**

[1,2,3] Information System of Universitas Sriwijaya, Indonesia
Email: fathoni@unsri.ac.id [1]., bolonnovita@gmail.com [2]., dinna.yunika@gmail.com[3]

**Abstract.** Stakeholders in a company have a right knowing about optimizing information security management. It can affect a company's performances and reputation. Information is the biggest business driver in an organization or company. This research aims to measure the capability of the company which is implemented information security governance that impacts on enterprise risk. The Loan Debit Network Corporation system is the main system that supports the company's business process for corporate lending transactions management. The capability level measurement is based on COBIT 5.0 for Information security and ISO 27001: 2013 Guidelines as a value against the Information Security Governance component rating. It starts with aligning organizational goals from COBIT 5.0 perspectives to obtain five COBIT 5.0 IT processes. The current capability is at level 2.5. Improvement recommendation from level 2.8 to level 3 refers to best practice recommended by COBIT 5.0 for Information Security.

## 1. Introduction.

Commercial banks companies in Indonesia engaged in the corporate segment that belongs to the foreign exchange bank group. The banks which always do a good internal IT Governance approach to answer the growing demands and growth of Information Technology. They has an integrated system that requires monitoring and evaluation of good governance both internally and externally. One of the systems applied in the company is System Loan Debit Network Corporation, is a system that serves to assist the process of borrowing and return transactions until the process of making the payment transaction format such as Auto Debit, RTGS, and SWIFT for corporate customers.

System Loan Debit Network Corporation extremely important role in supporting the business processes of firms, of course, is needed in Information Security Governance spanning three Information Security benefits are Confidentiality, integrity, and availability [1] [2]. In addition, Measurement Capability Governance Information Security will create an opportunity to improve the performance of a system. It aims to maintain and improve service to customers and the organization of the competition in the global economy. Measurement capability level is useful to improve stakeholder trust in system management in information security aspect [3] [4]. Measurement of the Level of Information Security Governance Capability in the Loan Debit Network Corporation system is needed to assess the level of information security accuracy since information assets are the driving force of business processes within a company to achieve business objectives [5]. In addition, these measurements are made to provide recommendations for improvements to the Information Security Governance of the system so that stakeholders can determine the business steps in improving the work function of the Loan Debit Network Corporation system [6].

In order to know the level of capability of the application of Information Security Governance, a measurement of Information Security Governance in Loan Debit Network Corporation with COBIT 5 for information security as Guideline and ISO 27001: 2013 as the standard of information security management requirement specification. The application of these two frameworks certainly provides different benefits in

accordance with the objectives of the framework. COBIT 5 for Information Security will be a guideline for the auditor to process the Information Security Capability Level measurement from the business orientation side [3]. While ISO 27001: 2013 will be an international standard to assess the system's specification to assess the performance of the system in terms of system reliability and accuracy of such systems protect the company's Information Security [7]. The merger of these two frameworks provides more detailed benefits in the measurement of Information Security Governance Capabilities.

The process of determining the Capability Level will use the PAM ( Process Capability Level ) referring to ISO / IEC 15504, so that the results will be more accurate, and represent the needs of the System Loan Debit Network Corporation and the needs of the company. The use of COBIT 5.0 for Information Security and ISO 27001: 2013 framework can provide best practice to support the achievement of company or organization's business objectives [8] [9] [10].

## 2 . System Implementation and Results

### 2.1. Mapping Goal Organization with *Enterprise Goals* COBIT 5.0 *for Information Security.*

Mapping organizational goals is the determination of the scope of information security. This mapping aims to derive and formulate organizational goals into the form of generic and related *enterprise* IT companies. This EG corresponds to that defined by the COBIT 5 *for Information Security* framework. Table 1. Shows the mapping of organizational goals. amber above will be a reference for the steps to be taken in the process of measuring the level of information security governance capability.

**Table 1**. Mapping of organizational goals

| ***Balance Scorecard*** | **EG** | **(Y/T)** | **Organization goals** | **Key Performance Indicators** |
|---|---|---|---|---|
| *Financial* | EG- 01 | Y | Utilize the core business and *franchise value* to achieve satisfactory performance for the stakeholders | The Policy Platform refers to the regulations of Bank Indonesia and the Financial Services Authority, and the international standards of COBIT, ITIL and ISO<br>1. Financial Statements are generally available on the official website compani<br>2. Financial reports (profit / loss) for customers who are always*real time* in the official website company.co.id |
| | EG- 02 | T | | |
| | EG- 03 | T | | |
| | EG- 04 | Y | The Policy Platform refers to the National Regulations and International Standards | |
| | EG-05 | Y | Availability of Financial information Per year or transparency of financial information in general. | |
| *Customer* | EG- 06 | Y | Focus on customers, and understand their needs, and provide integrated and value-added services | |
| | EG- 07 | T | | |
| | EG- 08 | T | | |
| | EG-09 | Y | The development of IT-based products affects several decisions in the company's strategy. | |
| *Internal Business Process* | EG -10 | T | | |
| | EG-11 | T | | |
| | EG -12 | T | | |
| | EG- 03 | T | | |
| | EG -14 | T | | |

| *Balance Scorecard* | EG | (Y/T) | Organization goals | Key Performance Indicators |
|---|---|---|---|---|
| *Learning and Growth* | EG-15 | T | HR development, towards Optimization & Employee Improvement. | Competence Development that focuses on technical operational improvement, product knowledge, *in-house* certification program training , and risk management certification, internal auditor & *dealer* |
| | EG- 16 | Y | | |
| | EG- 17 | Y | Service Innovation and Strengthening Work | Develop & distribute innovative products to support customers' business success |

### 2.2. *Mapping* IT Objectives

Mapping IT goals is a derivative of the organizational goals used to define the scope of information security that is more specific on IT. This mapping aims to derive and formulate IT goals into generic ITRG forms. Table 2. shows the organization's IT objective mapping results.

**Table 2**. The organization's IT objective mapping results

| BSC | Number | P/S | Y/T | The purpose of IT Organization | Main Work Indicator |
|---|---|---|---|---|---|
| *Financial* | ITRG-01 | P | Y | IT can help Fulfill the needs of the Company's business processes | The IT Unit refers to Bank Indonesia Regulation and the Financial Services Authority Regulation as its basic foundation, and international IT standards from COBIT, ITIL, and ISO that have been specifically adapted to the needs of the organization. |
| | | | | *Good Corporate Governance*IT fulfillment effort. | |
| | | P | Y | | |
| | ITRG - 03 | S | T | | |
| | ITRG-04 | S | T | | |
| | ITRG-05 | S | T | | |
| *Customer* | ITRG - 06 | P | Y | Access Information that can be used by customers, so that the needs of customers are met | |
| | ITRG-07 | P | Y | IT Services that facilitate the Customer in accessing Transaction information on the bank | - Use of *System Loan Debit Network Corporation*<br>-e - *banking, e-money* |
| | ITRG-08 | P | T | | |
| *Internal Business Process* | ITRG-09 | P | T | | |
| | ITRG-10 | P | Y | Information Security, infrastructure and system reliability that support business processes within each system used | |
| | ITRG-11 | S | T | | |
| | ITRG-12 | P | Y | Integration of technologies and applications into the business process | Development of *e-money* , *mobile banking* , and*System Loan Debit Network Corporation* |
| | ITRG-13 | - | T | | |
| | ITRG-14 | P | Y | The development of IT-based products affects several decisions in the company's strategy. | |
| | ITRG-15 | - | T | | |

| BSC | Number | P/S | Y/T | The purpose of IT Organization | Main Work Indicator |
|---|---|---|---|---|---|
| *Learning and Growth* | ITRG-16 | P | Y | Human resource development that focuses on internal and external training for business growth and bank operations through IT facilities | 1. *Information Security Foundation* Training *Based on* ISO 27001 and 27002<br>2. *Mastering COBIT 5 Fundamentals: A Practical Approach*<br>3. *CISSP (Certified Information System Security Professional) Exam Preparation*<br>4. *Human Resource Systems Enhancement* |
| | ITRG-17 | P | | Development of *e-money* applications | |

In Table 2, the determination of the value in the (Y / T) column is based on the relationship of generic IT and organizational objectives based on the mapping mentioned in T abel 3.1 . The mapping shown by the column (P / S) has two types of linkages: P ( *primary* ) and S ( *secondary* ). Column (Y / T) is Y value when it meets the following requirements: 1) Column (P / S) is worth P.,2). There is an organizational IT objective related to generic IT objectives.

Table 3, shows the *Information Technology Process is* selected based on short-term needs each year, which is obtained through *annual report* 2016 which refers to the target in 2017. *Information Technology Process* selected as many as 37 (thirty seven processes). However, in this study there is limited scope regarding the selection of IT Process COBIT 5 *for information security*. Based on previous research conducted by Dewi & Eko, Dani (2015) to measure the level of information security governance capability based on COBIT 5 *for information security.* IT process proposed within the scope of ITRG number 10 which refers to IT objectives for information security, processing infrastructure and applications. then the selection process in accordance with the primary process of mapping *IT Related Goals* number 10 with IT Process COBIT 5 *for information security*, there are 5 main processes, namely EDM ( *Evaluate, Direct, Monitor* ) on risk optimization, APO12 ( *Align* , *Plan* , and *Organize* ) on risk management, APO13 on security management, BAI06 and DSS05 on the management of security services.

**Table 3**. *IT Process* selected

| COBIT 5.0 INFORMATION SECURITY PROCESS | | | ITRG 10- Information Security, processing infrastructure and applications |
|---|---|---|---|
| | | | *Internal Bus. Process* |
| *Evaluate, Direct, and Monitor* | EDM01 | *Ensure Governance Framework Setting and Maintenance* | S |
| | EDM02 | *Ensure Benefits Delivery* | - |
| | EDM03 | *Ensure Risk Optimization* | **P** |
| | EDM04 | *Ensure Resource Optimization* | - |
| | EDM05 | *Ensure Stakeholder Transparency* | - |
| *Align, Plan, and Organize* | APO01 | *Manage the IT Management Framework* | **S** |
| | APO02 | *Manage Strategy* | - |
| | APO03 | *Manage Enterprise Architecture* | **S** |
| | APO04 | *Manage Innovation* | - |
| | APO05 | *Manage Porfolio* | - |
| | APO06 | *Manage Budget and Costs* | - |
| | APO07 | *Manage Human Resource* | **S** |
| | APO08 | *Manage Relationships* | - |
| | APO09 | *Manage Service Agreements* | **S** |
| | APO10 | *Manage Supplies* | **S** |
| | APO11 | *Manage Quality* | - |

| COBIT 5.0 INFORMATION SECURITY PROCESS | | | ITRG 10- Information Security, processing infrastructure and applications |
|---|---|---|---|
| | | | *Internal Bus. Process* |
| *Build, Acquire, and Implement* | APO12 | *Manage Risk* | **P** |
| | APO13 | *Manage Security* | **P** |
| | BAI01 | *Manage Programmes and Projects* | **S** |
| | BAI02 | *Manage Requirements Definition* | - |
| | BAI03 | *Manage Solutions Identification and Build* | - |
| | BAI04 | *Manage Availability and Capacity* | - |
| | BAI05 | *Manage Organizational Change Enablement* | - |
| | BAI06 | *Manage Changes* | **P** |
| | BAI07 | *Manage Chages Acceptance and Transitioning* | - |
| | BAI08 | *Manage Knowledge* | **S** |
| | BAI09 | *Manage Assets* | **S** |
| | BAI10 | *Manage Configurations* | **S** |
| *Deliver, Service, and Support* | DSS01 | *Manage Operations* | **S** |
| | DSS02 | *Manage Service request and Incidents* | **S** |
| | DSS03 | *Manage Problems* | - |
| | DSS04 | *Manage Continuity* | **S** |
| | DSS05 | *Manage SecurityServ2 ces* | **P** |
| | DSS06 | *Manage Business Process Controls* | **S** |
| *Monitor, Evaluate, and Assess* | MEA01 | *Monitor, Evaluate, and Assess Performance and Conformance* | **S** |
| | MEA02 | *Monitor, Evaluate and Assess the system of Internal Control* | **S** |
| | MEA03 | *Monitor, Evaluate and Assess Compliance with External Requirements* | **S** |

### *3. Assessment* results in the Rating Level

Table 4. Shows the achievement of Information Security System Loan Debit Network Corporation governance of 2.8 means that the process has been implemented, planned, monitored, documented, and adjusted. Work Product of the process is well controlled and maintained.

**Table** 4. Achievement of Information Security Governance

| Process ID | Process Name | Level |
|---|---|---|
| **Evaluate, Direct, and Monitor** | | |
| EDM03 | Risk optimization | **3** |
| **Align, Plan and Organize** | | |
| APO12 | Managing Risk | **3** |
| APO13 | Manage Security | **3** |
| Value for APO | | **3** |
| **Build, Acquire, and Implement** | | |
| BAI06 | Manage Changes | **2** |

| Process ID | Process Name | Level |
|---|---|---|
| **Delivery, Service, and Support** | | |
| DSS05 | Managing Service Security | **3** |
| **Average Information Security Governance of the LDNC System** | | **2.8** |

**4. Recommendations for Level upgrades from 2 to Level 3**

**4.1. Recommendations for level 2 to level 3 improvement on EDM03 Process - Risk Optimization**

**1. The outcome to be achieved**

1. EDM03-01: Information Risk Management as part of overall enterprise risk management.

**2. Recommended Level 2 Capability towards Level 3 Capabilities**

1. The process of risk monitoring, risk evaluation, and risk management in the enterprise risk management integration process and information risk of the LDNC system must be run in accordance with the standards already in place.
2. The responsibility and authority of the integration process is applied and mutually sustainable between director and employee level.
3. In integrating enterprise management and risk management information must be run by competent human resources.
4. Provide, organize and maintain the resources and information that support the risk management process
5. Provide, allocate and maintain infrastructure and work environment.
6. Conduct data collection and analysis in the risk management process to determine the potential for continuous improvement of the process.

**4.2. Recommendations for level 2 improvement to level 3 on APO12 Process - Managing Risk**

**1. The outcome to be achieved**

1. APO12-01: Current Complete Risk Information Profile on technology, applications, and infrastructure in an enterprise.
2. APO12-02: Response Information security incident integrated with overall risk management process to provide capability in order to update the risk management portfolio.

**2. Recommended Level 2 Capability towards Level 3 Capabilities**

1. Establish a risk management procedure.
2. Monitoring process to determine the effectiveness of risk management.
3. Socializing risk management procedures and Provide resources and infrastructure.

**4.3. Recommendations for level 2 upgrading to level 3 on APO13 Process - Manage Security**

**1. The outcome to be achieved:**

1. APO13-01: A system that takes into account enterprise information security requirements effectively.
2. APO13-02: Security plans have been built, accepted and communicated to all parts of the enterprise.
3. APO13-03: An information security solution is implemented and operated consistently throughout the enterprise.

**2. Recommended Level 2 Capability towards Level 3 Capabilities**

1. Establish an information security procedure and authority over access to information.
2. Establish monitoring procedures to determine the effectiveness of information security management.
3. Conducting information security training on human resources.

**4.4. Recommendations for level 2 improvement to level 3 on Process BAI06- Managing Change**

**1. The outcome to be achieved**

1. BAI06-01: Information security requirements are incorporated into the appraisal and application process impact assessment
2. BAI06-2: Emergency changes are incorporated into important information security requirements.

**2. Recommended Level 2 Capability towards Level 3 Capabilities**

1. Set standards in the process of emergency change, standard sequence, details, and sub process interaction in the event of an emergency change made.
2. Apply assessment standards on infrastructure and work environment in the process of emergency change.
3. Monitoring to ensure process effectiveness.
4. Establish mutually sustainable responsibilities and responsibilities in response to an emergency change.
5. Provide, organize, and maintain resources (resources and information) in overcoming emergency and emergency maintenance.

### 4.5. Recommendations for level 2 upgrades to level 3 on Process DSS05- Managing Security Services

**1. The outcome to be achieved**

1. DSS05-01: Network and communication security suited to business needs.
2. DSS05-02: Protects information processed, stored and transmitted by endpoint devices.
3. DSS05-03: All users are uniquely identifiable and have access rights appropriate to their role in the business.
4. DSS05-04: Physical steps have been implemented to protect information from illegal access, damage and intervention while being processed, stored and transmitted.
5. DSS05-05: Electronic information is secured precisely when stored, transmitted, or destroyed.

**2. Recommended Level 2 Capability towards Level 3 Capabilities**

1. Establish standards in conducting activities in the management process.
2. Security services Apply assessment standards on infrastructure and work environment in the process of managing security services.
3. Monitoring to ensure the effectiveness of the process of the activities that have been done.
4. Assign responsibility and authority are mutually sustainable actions in response to the management of security services.
5. Provide, manage and maintain resources (resources and information) in managing the security services.
6. Provide training to improve the quality of human resources for the security services (security certification).

## 5. Conclusion

This research begins by doing mapping Enterprise goal COBIT 5 and with company goals, followed by IT mapping process COBIT 5 for information security with IT Related Goals. The results of the mapping are limited by the scope of information security, processing infrastructure and applications. They cover 5 (five) IT Process COBIT 5 for information security related in IT Related Goals number 10, which is EDM03 Optimization of risk, APO12 manage risk, APO13 manage security, BAI06 managing change, and DSS05 for managing the security services. The average of the whole process has been measured. Level 2.8 capabilities are categorized into two capability in accordance with the level 0 - level 5. This condition indicates that the company has implemented processes that must be evaluated, planned, documented and adjusted, and maintain and control work product of the process. The proposed recommendations based on the Measurement Capability of Information Security Governance to reach level 3 (three) companies need to plan and implement process standards and procedures, monitoring to ensure process effectiveness, provide, manage and maintain resources (resources and Information) responsibilities and mutual responsibilities, and improving human resource competencies in every process of risk optimization, risk management, security management, change management, and management of security services.

## 6. Suggestion

Some of the things suggested by this author regarding Information Security Governance are:

1. Measurement of capability level of IT process COBIT 5 for information security using attributes that are still in character generic. For further development can be done by using more specific questions accompanied by complete support data.
2. Companies need to measure capability levels using 37 processes or the entire process provided by COBIT 5 for information security to get a more precise and objective value.
3. Companies need to realize the importance of information security investment as a necessity enterprise as a whole to maintain and enhance the company's reputation and improve stakeholder trust.

## 7. References

[1] Dhillon, G., & Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. Communications of the ACM, 43(7), 125-128.

[2] IT Governance Institute (ITGI). (2012). Board Briefing on IT Governance. http://www.isaca.org.

[3] IT Governance Institute (ITGI). (2012). COBIT 5 for Information Security. http://www.isaca.org.

[4] Weill, Peter & Ross, Jeanne W. (2004). IT Governance: How Top Performers Manage IT Decision Rights for Superior Results. Boston, MA: Harvard Business School Press.

[5] Williams, P. (2001). Information security governance. Information security technical report, 6(3), 60-70.

[6] Indrajit, R.E. (2011). Kerangka Standar Keamanan Informasi: ISO17799. Jakarta: IDSIRTII.

[7] International Standard Organization. 2013. ISO/IEC 27001 Information Technology, Security Techniques-Information Security Management System-Requirements. International Standard Organization, Switzerland

[8] Nyoman, I Sujana Saputra. (2013). Pengukuran Tingkat Kapabilitas Dan Perbaikan Tata Kelola Teknologi Informasi Berdasarkan Kerangka Kerja COBIT 5 dan ITIL V3 2011: Studi Kasus BANK ABC INDONESIA. Program Magister Teknologi Informasi Universitas Indonesia

[9] Kusumawati, Arie. (2013). Pengukuran Tingkat Kapabilitas dan Perbaikan Manajemen Layanan Tata Kelola Teknologi Informasi Berdasarkan COBIT 5 dan ITIL V3 2011: Studi Kasus PUSDATIN Kementrian Perdagangan. Program Magister Teknologi Informasi Universitas Indonesia

[10] Budi, Azis P. (2014). Pengukuran tingkat Kapabilitas Tata Kelola Teknologi Informasi Menggunakan COBIT 5: Studi Kasus PT. Lintasarta. Program Magister Teknologi Informasi Universitas Indonesia

# Security Audit On Loan Debit Network Corporation System Using Cobit 5And Iso 27001: 2013

ORIGINALITY REPORT

| 19% | 16% | 11% | 5% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | in.iphy.ac.cn<br>Internet Source | 5% |
| 2 | rizkyzaky27.wordpress.com<br>Internet Source | 5% |
| 3 | www.bbronline.com.br<br>Internet Source | 3% |
| 4 | Federico M Pont, Axel Molle, Essam R Berikaa, Sascha Bubeck, Annika Bande. "Predicting the performance of the inter-Coulombic electron capture from single-electron quantities", Journal of Physics: Condensed Matter, 2020<br>Publication | 3% |
| 5 | hal-ifp.archives-ouvertes.fr<br>Internet Source | 3% |

| | | | |
|---|---|---|---|
| Exclude quotes | On | Exclude matches | < 3% |
| Exclude bibliography | On | | |