Advances in Intelligent Systems Research, volume 172
Sriwijaya International Conference on Information Technology and Its Applications (SICONIAN 2019)

Information Security: Credit Service Application Analysis at Bank Indonesia

FATHONI[1], Pacu PUTRA[2], and Dinna Yunika H[3]

[1]*fathoni@unsri.ac.id, Information System, Faculty of Computer Science, Universitas Sriwijaya, Indonesia*
[2]*pacuputra@ilkom.unsri.ac.id, Information System, Faculty of Computer Science, Universitas Sriwijaya, Indonesia*
[3]*dinna.yunika@unsri.ac.id, Information System, Faculty of Computer Science, Universitas Sriwijaya, Indonesia*

ABSTRACT
This research aims to analyze the procedures and attributes of information system security from the implementation of credit service applications at Bank XYZ using a combination of COBIT Framework 5.0 and ISO 27001:13. The assessment focused on the security element of the information system consisting of its Policy & procedure, its standard Compliance, IT Security Policy & procedure, IT security Operation, and IT Project Management Office. The use of survey methods that get the domain and process used determines the security level of the information system, consisting of Ensure risk optimisation (EDM03), Manage risk (APO12), Manage security (APO13), Manage changes (BAI06), and Manage security service (DSS05). The result of data processing using the PAM method is known that the new information security process to the level of product management and information dissemination, has not reached the level of measurement and information control and there is no bank management effort To enhance the procedures and attributes of the better level of information security.
Keywords: *security, information, services, credit, bank, Indonesia*

INTRODUCTION

The quality of information Security application of low bandage Services in Indonesia is reflected in many cases of data breaches and bank customer funds. In 2011, Bareskrim Polri stated that there were at least eight major cases of bank breaches that took place and needed to be resolved. Eight cases occurred in 8 major banks in Indonesia, namely; Bank BRI, Bank BII, Bank Mandiri, Bank BNI, Bank BPR Pundi Artha Sejahtera, Bank Danamon, Bank Panin and Bank Citibank [1]. While the year 2018 there are 14 banks in Indonesia whose funds are stolen by one company with an estimated loss of 14 trillion rupiah [2].

To overcome the weaknesses of the asset securing banking information required good and true information security governance. This crucial role requires evaluation through measurement to determine the extent to which the level of the bank's capabilities has implemented information security governance [3]. Good information security governance requires a scalable, internationally compliant framework for a bank or a company. The framework will be guidelines used by researchers to measure the level of information security quality that results will be oriented towards increasing bank business operational activity through the process Evaluation, and monitoring of information security [4].

Bank XYZ Indonesia is the first commercial bank in Indonesia that is engaged in the corporate segment that belongs to the foreign exchange bank. One of the applications implemented in the operation of this bank is the Loan Debit Network Corporation system, which is a system that serves to process lending and return transactions to the process of creating transaction formats Payment such as Auto Debit, RTGS, SWIFT for corporate customers. To assess the level of security accuracy of Credit Service information It is necessary to measure the quality of information security periodically because The information asset is the business process drive of the bank to achieve Business purposes. Also, this measurement was conducted to provide improvement recommendations on the management of information security on the system so that stakeholders can determine business measures to improve work function credit Service applications.

The analysis of this quality of information security will be conducted using two international Standard framework specifications that refer to the information Security management Terms, namely; Cobit 5. 0 (Control Objective for information and Related Technology) for Information security as guidelines [5] and ISO 27001:13 [6]. The use of cobit 5.0 For information security will be guidelines for researchers to perform the process of measuring information security quality from the bank's business process point of view [7,8,9]. While the ISO 27001 framework:13 will be used to assess the specification of the system and the performance of the system in protecting the information security of the bank's application [6]. Combining the second framework can provide more detailed benefits in measuring the quality of information security governance in Indonesian banking. Use of Metode PAM (Process Assessment Model) which refers to ISO/IEC 15504-2 standard, used to ensure more objective, impartial, unbiased measurement results, Consistent, repetitive (repeatable). This Research will assessment the quality of information security to the management of bank service applications in Indonesia.

RESEARCH SCOPE

This research is conducted through a survey of the implementation of credit application services in one of the banks in Indonesia. The assessment of the security quality process of credit application information is conducted

using COBIT 5.0 for information security to measure the level of information security governance capability by international standards which will be Business activity oriented to the bank and ISO 27001:13 as specification standards for information security management requirements.

INFORMATION SECURITY

Information Security is an activity to safeguard data *assets* and information against threats that may arise from unauthorized users who make modifications to Loss of information for the company [4]. Mitigation of information security risks can be done using THE COBIT framework 5.0 For information Security AND ISO 27001:13 [6.10].

A. COBIT 5.0 FOR INFORMATION

According to the research needs and area research objectives, Domain, and processes used in the capability level calculation process, COBIT 5.0 used is a *framework* that specifically addresses information security. This type of Framework is included in the COBIT 5.0 *Professional Guides*, 37 that process [11]:

1. Domain EDM (Evaluate, Direct, Monitor), Consists of 5 (five) processes, i.e.: 1. EDM01 Ensure Governance framework setting and maintenance; 2. EDM02 Ensure benefits delivery; 3. EDM03 Ensure risk optimization; 4. EDM04 Ensure resource optimization; dan 5. EDM05 Ensure Stakeholder transparency
2. Domain APO (Align, Plan, Organize), Consists of 13 (thirteen) processes, i.e.: 1. APO01 Manage the IT management framework; 2. APO02 Manage strategy; 3. APO03 Manage enterprise architecture; 4. APO04 Manage innovation; 5. APO05 Manage portfolio; 6.APO06 Manage budget and costs; 7. APO07 Manage human resources; 8. APO08 Manage relationships; 9.APO09 Manage service agreements; 10. APO10 Manage suppliers; 11. APO11 Manage quality; 12. APO12 Manage risk; 13. APO13 Manage security.
3. Domain BAI(Build, Acquire, and implement), Consists of 10 (ten) processes, i.e. : 1.BAI01 Manage programs and projects; 2. BAI02 Manage requirements definitions; 3.BAI03 Manage solutions identification and build; 4. BAI04 Manage availability and capacity; 5. BAI05 Manage organizational change enablement; 6. BAI06 Manage changes; 7. BAI07 Manage change acceptance and transitioning; 8. BAI08 Manage knowledge; 9. BAI09 Manage assets; dan 10. BAI10 Manage configuration.
4. Domain DSS(Deliver, Service, and Support). Consists of 5 (five) processes, i.e.:1. DSS02 Manage service requests and incidents; 2. DSS03 Manage problems; 3. DSS04 Manage continuity; 4. DSS05 Manage security service; 5. DSS06 Manage business process controls
5. MEA (Monitor, Evaluate, and Assess), Consists of 3 (three) processes, i.e.:1. MEA01 Monitor, evaluate and asses performance and conformance; 2. MEA02 Monitor, evaluate, and assess the system of internal control; dan 3. MEA03 Monitor, evaluate, and assess compliance with external requirements.

B. ISO 27001: 13

ISO 27001:13 is an international standard used to manage and control the security risks of information, Protect and safeguard *confidentiality*, *Integrity* and availability information [12]. Control *Annex* A is a reference document found in ISO 27001:13 that can be used to control and identify Security Risks Information in a company consisting of 14 *Control Categories (Domain/Control Area) discretionary Controls*[4,6], i.e.:

1. A.5 *Information security policies,* Consists of 1 (one) domain, i.e.: A.5.1 *Management direction for information security*
2. A.6 *Organization of information security*, Consists of 2 (two) domains, i.e.*:* A.6.1. *Internal organization*; dan *2.* A.6.2. *Mobile devices and teleworking*
3. A.7 *Human resource security*, Consists of 3 (three) domains, i.e.*:* A.7.1 *Prior to employment; 2.* A.7.2 *During employment*; dan 3. A.7.3 *Termination and change of employment*
4. A.8 *Asset management*, Consists of 3 (three) domains, i.e.*:* 1. A.8.1 *Responsibility for assets;* 2. A.8.2 *Information classification; dan 3.* A.8.3 *Media Handling.*
5. A.9 *Access control*, Consists of 4 (four) domains, i.e.*:* 1.A.9.1 *Business requirements of access control*; 2. A.9.2 *User access management*; 3. A.9.3 *User responsibilities; dan 4.* A.9.4 *System and application access control.*
6. A.10 *Cryptography,* Consists of 1 (one) domain, i.e. : A.10.1 *Cryptographic controls.*
7. A.11 *Physical and environmental security*, Consists of 2 (two) domains, i.e. : 1. A.11.1 *Secure areas*; dan 2. A.11.2 *Equipment.*
8. A.12 *Operations security*, Consists of 7 (seven) domains, i.e. : 1.A.12.1 *Operational procedures and responsibilities*; 2. A.12.2 *Protection from malware;* 3. A.12.3 *Backup;* 4. A.12.4 *Logging and monitoring*; 5. A.12.5 *Control of operational Software*; 6. A.12.6 *Technical vulnerability management*; dan 7. A.12.7 *Information systems audit considerations.*
9. A.13 *Communications security*, Consists of 2 (two) domains, i.e.*:* 1. A.13.1 *Network security management*; dan 2. A.13.2 *Information transfer*
10. A.14 *System acquisition, development and maintenance*, Consists of 3 (three) domains, i.e.*:* A.14.1 *Security requirements of information systems; 2.* A.14.2 *Security in development and support processes; dan 3.* A.14.3 *Test data*
11. A.15 *Supplier relationships*, Consists of 2 (two) domains, i.e.*:* 1. A.15.1 *Information security in supplier relationships; dan 2.* A.15.2 *Supplier service delivery management.*

12. A.16 *Information security incident management*, Consists of 1 (one) domain, i.e. : A.16.1 *Management of information security incidents and improvements*
13. A.17 *Information security aspects of business continuity management*, Consists of 2 (two) domains, i.e.*:* 1. A.17.1 *Information security continuity*; dan 2. A.17.2 *Redundancies*
14. A.18 *Compliance*, Consists of 2 (two) domains, i.e. : 1. A.18.1 *Compliance with legal and contractual requirements; dan 2.* A.18.2 *Information security reviews.*

PROCESSING RESULT

Table 1. Displays the mapping results between the information security objectives in the XYZ bank with Cobit 5.0 for security information. This mapping resulted in 5 main processes: EDM03 (*Evaluate*, *Direct*, *Monitor*) on risk optimization, APO12 (*Align*, *Plan*, and *Organise*) on risk MANAGEMENT, APO13 on security management, BAI06, and DSS05 about security services management that will determine quality Information security from the use of credit applications at XYZ bank.

Table 1. Cobit Mapping result 5.0 WITH ITRG Bank XYZ

COBIT 5.0 INFORMATION SECURITY PROCESS			**ITRG 10- Information security, processing infrastructure, and applications**
			Internal Bus. Process
Evaluate, Direct, and Monitor	ED M01	*Ensure Governance Framework Setting and Maintenance*	Secondary
	ED M02	*Ensure Benefits Delivery*	-
	ED M03	*Ensure Risk Optimisation*	**Primary**
	ED M04	*Ensure Resource Optimisation*	-
	ED M05	*Ensure Stakeholder Tranparency*	-
Align, Plan, and Organise	AP O01	*Manage the IT Management Framework*	Secondary
	AP O02	*Manage Strategy*	-
	AP O03	*Manage Enterprise Architecture*	Secondary
	AP O04	*Manage Innovation*	-
	AP O05	*Manage Portfolio*	-
	AP O06	*Manage Budget and Costs*	-
	AP O07	*Manage Human Resource*	Secondary
	AP O08	*Manage Relationships*	-
	AP O09	*Manage Service Agreements*	Secondary
	AP O10	*Manage Supplies*	Secondary
	AP O11	*Manage Quality*	-
	AP O12	*Manage Risk*	**Primary**
	AP O13	*Manage Security*	**Primary**

Build, Acquire, and Implement	BAI 01	*Manage Programmes and Projects*	Secondary
	BAI 02	*Manage Requirements Definition*	-
	BAI 03	*Manage Solutions Identification and Build*	-
	BAI 04	*Manage Availability and Capacity*	-
	BAI 05	*Manage Organisational Change Enablement*	-
	BAI 06	*Manage Changes*	**Primary**
	BAI 07	*Manage Changes Acceptance and Transitioning*	-
	BAI 08	*Manage Knowledge*	Secondary
	BAI 09	*Manage Assets*	Secondary
	BAI 10	*Manage Configurations*	Secondary
Deliver, Service, and	DSS 01	*Manage Operations*	Secondary
	DSS 02	*Manage Service request and Incidents*	Secondary
	DSS 03	*Manage Problems*	-
	DSS 04	*Manage Continuity*	Secondary
	DSS 05	*Manage Security Services*	**Primary**
	DSS 06	*Manage Business Process Controls*	Secondary
Monitor, Evaluate, and Assess	ME A01	*Monitor, Evaluate, and Assess Performance and Conformance*	Secondary
	ME A02	*Monitor, Evaluate and Assess the system of Internal Control*	Secondary
	ME A03	*Monitor, Evaluate and Assess Compliance with External Requirements*	Secondary

1. Assessment of EDM03 process capabilities (Ensure Risk Optimisation)

Table 2. Displaying capability level measurement results in the EDM03 process: *Evaluate, Direct, and Monitoring* to process risk optimization. The value of the capability level of the risk optimization process is at level 2, meaning bank XYZ has planned, monitors, documents and adjusts the risk optimization process. The *Work product* of this process is also precisely targeted, controlled and maintained. Based on the results of the assessment above, the achievement value of PA 3.2 is 56% (*Largely Achieved*), which means there is a significant achievement of the assessed process attribute. Evaluation and monitoring of risk optimization have not conducted the assessment and control process and have not done further development to further improve information security risk control in XYZ bank credit Application.

Table 2. Achievement OF EDM03 process capability Level

Rating Criteria By Respondent	ASSESSMENT OF RISK OPTIMIZATION PROCESS								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Policy & procedure		100	83	0	0	0	0	0	0	0
IT Standar Compliance		100	100	100	100	100	100	20	0	0
IT Security Policy & Procedure		100	100	100	100	80	0	0	0	0
IT Security Operation		100	66,4	0	0	0	0	0	0	0
IT Project Management Office		100	100	100	100	100	85.68	20	0	0
Average Rating		100	89.88	60	60	**56**	37.13	8	0	0
Capabilities	**FALSE**	F	F	L	L	L	P	P	N	N

2. Assessment of APO12 process capabilities (Manage Risk)

Table 3. Displaying the capability level value of the risk management process at level 3 with the achievement value of PA 4.1 of 54.27% (*Largely Achieved*), IT indicates that XYZ bank has implemented, set the process standard, Then implement and be able to achieve the *outcomes* of the risk management process. The risk management conducted on the bank's credit application services has not achieved the measurement and risk control process of any tested attributes and stages to improve risk management sustainably.

Table 3. Achievement of APO12 process capability Level

Rating Criteria By Respondent	ASSESSMENT OF RISK MANAGEMENT PROCESS								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Policy & procedure		100	100	100	100	83	0	0	0	0
IT Standar & Compliance		100	100	100	100	100	85.68	20	0	0

Responden IT Infrastructure		100	100	100	100	100	85.68	20	0	0
IT Operation		100	100	100	80	0	0	0	0	0
IT Project Management Office		100	100	100	100	100	100	20	0	0
Average Rating		100	100	100	96	76.60	**54.27**	12	0	0
Capabilities	**FALSE**	F	F	F	F	L	L	N	N	N

3. Assessment of APO13 process capabilities (Manage Security).

Table 4. Displaying the value of the capability level for the process of managing the security of information located at level 3 with the achievement value of PA 4.2 that is 31.41% (*Partially Achieved*) WHICH means that XYZ bank has implemented, set the process standard, Then implement as a well-defined process and be able to achieve the *outcomes* of the process of managing information security. Management of the bank XYZ has done the measurement of information security from the services of credit applications, but has not done the optimal process of information security control and has not performed the development and improvement activities Information Security.

Table 4. Achievement OF APO13 process capability Level

Rating Criteria By Respondent	ASSESSMENT PROCESS OF SECURITY MANAGEMENT								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Security Policy & procedure		100	100	100	100	83	0	0	0	0
IT Standar &Compliance		100	100	100	100	100	85.68	20	0	0
IT Infrastructure		100	83	0	0	0	0	0	0	0
IT Security Operation		100	100	100	80	0	0	0	0	0
IT Project Management Office		100	100	100	100	100	71.4	0	0	0
Average Rating		100	96.6	80	96	76.6	**31.41**	4	0	0
Capabilities	**FALSE**	F	F	L	F	L	**P**	N	N	N

4. Assessment of BAI06 process capabilities (Manage Changes)

Table 5. Display the capability level n Ilai result for change management process located at Level 2 with the achievement value of PA 2.2, which is 25% (*Partially Achieved*). This indicates that the XYZ bank has implemented and already planned, monitor, plan and package the standard change process in a previously unidentified incident. The results of *work product* have been managed precisely but not meet the target achievement, because the result of the process is still low. It can be some evidence of an unpredictable process attribute. This aspect means that the results of the *work product* have not been maximally managed properly.

Table 5. Achievement OF BAI06 process capability Level

Rating Criteria By Respondent	ASSESSMENT OF CHANGE MANAGEMENT PROCESS								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Infrastructure		100	83	0	0	0	0	0	0	0
IT Standar Compliance		100	66,4	0	0	0	0	0	0	0
IT Security Policy & Procedure		100	49.8	0	0	0	0	0	0	0
IT Security Operation		100	100	50	0	0	0	0	0	0
IT Project Management Office		100	100	75	0	0	0	0	0	0
Average Rating		100	79.84	**25**	0	0	0	0	0	0
Capabilities	**FALSE**	F	L	**P**	N	N	N	N	N	N

5. Assessment of DSS05 process capabilities (*Manage Security Services*)

Table 6. Showing the capability level of the results for the management process of information security services located at Level 3 which means that Bank XYZ has implemented, set and Implement The service process according to standards. The process has been defined and able to achieve *outcomes*. Based on the results of the assessment above, the achievement value of PA 4.2 by 4% (*Not Achieved*) which means that the overall process achievement has not been reached, an achievement only has Little evidence or even no evidence at all. This value indicates that the quantitative measurements used as process stabilization were not yet.

Table 6. Achievement OF DSS05 process capability Level

Rating Criteria By Respondent	ASSESSMENT PROCESS OF SECURITY SERVICES MANAGEMENT								
	Level 0	Level 1	Level 2		Level 3		Level 4		Level 5	
		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
IT Infrastructure		100	100	100	100	83	0	0	0	0
IT Operation		100	100	100	100	66.4	0	0	0	0
IT Security Policy & Procedure		100	100	100	100	100	14.28	0	0	0
IT Security Operation		100	100	100	100	100	0	20	0	0
IT Project Management Office		100	100	100	100	100	0	0	0	0
Average Rating		100	100	100	100	89.88	2.85	**4**	0	0
Capabilities	**FALSE**	F	F	F	F	F	N	**N**	N	N

SUMMARY

Based on the results of information security evaluation using credit Service application at XYZ Bank, the following conclusions are obtained:
Level 1: Performed. The process of EDM03, APO12, APO13, BAI06, and DSS05 has been well done and systematic. Assessed attributes can be significantly achieved and no weaknesses found in process attributes are evaluated.
Level 2: Managed. The process of EDM03, APO12, APO13, and DSS05 processes have been proven to be implemented comprehensively and systematically. Full achievements of the attributes of the assessed process, as well as invisible weaknesses in the process attributes. While the BAI06 process is still found the weakness of the assessed attributes, and this needs to get a splash.
Level 3: Established. The EDM03, APO12, APO13, and DSS05 processes are systematic business evidence and a significant achievement of the attributes assessed, but there are still weaknesses of the attributes evaluated for EDM03 and APO12 processes. As for the BAI06 process, there are several achievements of the process attributes assessed, but some aspects of the achievement of other attributes are still not predictable.
Level 4: Predictable. The APO13 process has been done, but has not been systematically and well so it found many disadvantages of the assessed process attribute. The EDM03, APO12, BAI06, and DSS05 processes have not been conducted at this level. This may cause insecurity against users who are not entitled to use the information.
Level 5: Optimizing. The entire process evaluated hasn't done this activity.

REFERENCES

[1] Herry Febrian, Bismar Nasution & Mahmul Siregar, Juridical Analysis On Fund Hit Of Customer Of Citibank In Perspective Of Banking Act And Act Of Eradication And Prevention Of Money Laundry., TRANSPARENCY, Jurnal Hukum Ekonomi, Volume I, Nomor 2, 2013.

[2] Devina Halim, Bareskrim: PT SNP yang Lakukan Pembobolan Bank adalah Perusahaan Resmi., Kompas Online, 2018.

[3] De Haes, Steven & van grembergen, Wim& S. Debreceny, Roger, COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities., Journal of Information Systems, 2013.

[4] Eko Indrajit, Kerangka Standar Keamanan Informasi: ISO17799., IDSIRTII, Jakarta, 2011.

[5] ISACA, *Process Assessment Model COBIT 5*., ISACA, 2012.

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

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

[8] Nyoman, I Sujana Saputra, 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, 2013.

[9] Arie Kusumawati, 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, 2013.

[10] Destianti, C.A dan Suryanto, Evaluation of Information Technology Governance with COBIT 5 in XYZ for ISO 27001:2013 Readiness., *International Journal of Engineering and Techniques - Volume 4, Issue 4, 2018.*

[11] ISACA, *COBIT ® Process Assessment Model (PAM): Using COBIT ® 5.*,ISACA, 2013.

[12] Becker, J. & Bailey, E., A Comparison of IT Governance & Control Frameworks in Cloud Computing., *Association for Information Systems Conference*, 2014, pp.1–16. 4.