Information System Security of Indonesia Terrestrial Border Control

Fransiskus M. H. Tjiptabudi[1] and Raul Bernardino[2]
[1−2]Information System Department, STIKOM Uyelindo
Kupang 85111, Indonesia
Email: [1]tjiptabudifrans@gmail.com, [2]bernardino_raul@yahoo.com

***Abstract*—Today, Information Technology (IT) becomes an integral part of human life. IT boosts every sector, such as infrastructure, economics, agriculture, social, organization, and politics. The institutional systems are developed according to the specific business requirements, processes, flows, and security. Pos Lintas Batas Negara 'integrated cross-border post' (PLBN) is a designated authority consisting of the Custom, Immigration, and Quarantine (CIQ). Each section has a different Standard Operation Procedure (SOP). This research aims to develop a secure information system based on Confidentiality, Integrity, and Availability (CIA) concepts. The CIA is embedded in the ISO 27001 and McCumber Cube approach. The research focuses on the Secure Immigration Information System (SIIS). This research is conducted in the Wini immigration office. The researchers observe the immigration activities on the location, interview the immigration officers, and collect information. The researchers produce an effective, efficient, and security application prototype system.**

***Index Terms*—Secure Information System, Custom, Immigration, and Quarantine (CIQ), Confidentiality, Integrity, and Availability (CIA), Integrated Cross-Border Post**

I. Introduction

TODAY all daily activities from private to the public sector or from home to work, to access a private and public education, a market, organic food from the farmers, the healthcare facilities, a public and private transportation, the banks, institutional information, and to the industrials are affected by Information Technology (IT). IT helps human to overcome issues more accurate, effective, efficient, and secure. The IT professionals are ethically responsible for information system security concepts, designs, and implementations in the society. They may have direct or indirect involvements. The society and technology interaction creates interconnecting modalities of the law, the architecture, the market, and the social norms. In the real world, the law is a state or nation expression of power and enforcement. The architecture is a geographic location in the physical layout and computer coding in the virtual environment. The market is an economic influence which has most affects in human behavior (ethical or unethical). The social norms are the values that existed in society. These four modalities are governing all aspects of society [1].

Received: Mar. 08, 2019; received in revised form: Aug. 25, 2019; accepted: Aug. 29, 2019; available online: Sept. 20, 2019.

The application and architectures of information system security are created and envisioned to meet local and global demands. The application developer and system engineers are selecting and developing the specification designs and the platforms based on business requirements, processes, flows, security, and the trends of the current technology development [2]. These are keys for architecting the Information System Security (ISS). According to Ref. [3], the most important of the operation management is transforming inputs into the expected outputs within sets of the activities to create new values in the form of goods and services.

The sustainability of the secure application, ISS, and infrastructure are depending on the institutional direction which governs by its vision, mission, goal, and strategy. The stakeholder commitment for supporting and financing the ISS projects is an ultimate remedy. The Confidentiality, Integrity, and Availability (CIA) concept have three dimensions namely desired goals of the CIA, information states (storage, processing, and transmission), and measurement (policy, education, and technology). These concepts are very important and as tools for the system developers and engineers to be based on, and for assessing and securing the application, the information system, the platform, and the infrastructure. On the other hand, the IT revolution often changes the market direction. It may not be fully reflected in the current market requirement [4]. The institutions may not afford the newly available technology and will depend on outdated or even unlicensed technologies and or systems. The researchers can study the concepts and implementation framework

details within system integration and meet customer requirement [5, 6].

Moreover, architecting ISS to meet all requirements and satisfy the needs of users, and stakeholder can be called a qualified system. The security is defined as a quality, the state of being secure, and free from the danger. Security often achieved several strategies undertaken simultaneously. Security specification areas are physical access, operation, communication, and network. Meanwhile, information security is defined as an information asset protection. Its elements are confidentiality, integrity, and availability. It includes systems and hardware to store and transmit the information. The information security will be achieved through the application of the policy, technology, and training and awareness programs [7–9]. Meanwhile, the system users awareness will form an ethical of technological users. It is because information security is no longer the sole responsibility, but it is system users and the managers [10, 11].

The act no. 43, 2008 is regarding country borders. The country border is a line between two neighbors' sovereignties. The law is based on international laws [12]. Furthermore, the border is explained as a region on the side of the Indonesia territory. The Indonesia cross border areas have few development districts. The inhabitants are unevenly spread alongside the border. The human capacity is relatively low. The border information system, education facilities, health facilities, and infrastructure get little support from the central government. The home industries are depending on the rough materials. For example, the community is living in traditional farming. Moreover, no fence is built alongside the terrestrial border. In general, it is the overview of the security and its perspective. It shows that the terrestrial borders are in the distressing situation. There are several unsolved border issues. Those are Ambalat Block, Bidadari island, and illegal border passers [13]. The central government and the province are less focus on territorial policies and strategy development [14]. Since December 8^{th}, 2014, the central government has issued national strategies and policies. The terrestrial border control becomes a primary focus. The presidential regulation number 179, in the same year, 2014 is a specific regulation for the East Nusa Tenggara province. Followed by Minister of Justice and Human Rights publication on the State Gazette number 382 on December 10^{th}, 2014, stated the implementation of terrestrial border management and security controls needed to be integrated infrastructures and supports. This is later called Pos Lintas Batas Negara 'integrated cross-border post' (PLBN).

The immigration authorities duties include controlling the communities living alongside the terrestrial border and administering all movement of the passers arrival into the country or departure from the country. The current administration processes are defined as a semi-manual system. They lack workforce to capture all necessary information. They are also inefficient due to consuming more time in services and deliveries. Data collection are unsecured for the archiving system. The access level is highly vulnerable (no confidentiality). Data structure are not trackable, or the historical data become a problem, and no verification exists (no integrity). The immigration reports are challenging to produce, which means the data are not consistent and proper available (no availability).

Moreover, the information system security policy does not exist, and this contributes to the unsecured information system too. The immigration authorities collect Pas Lintas Batas 'cross-border pass' (PLB) and use it as a base for allowing or refusing passers to enter or depart from the country [15]. The slowness and integrity of workforce service delivery contribute to the high level of the data breach and border violations for both countries. Therefore, it is important to design and implement a Secure Immigration Information System (SIIS) within the CIA concepts.

The CIA triangle concept will play a crucial role in this research. Researchers will use this concept for investigating the current state of SIIS and prototyping an ISS for the application, the networks, the operation, and the communication. The research outcomes are secure application prototype and system support. Within a time compressing demands, the secure application and support systems should ensure the secure business operation requirements such as accurate information and has data integrity (traceable data or information and history of data changes), high availability of data and information, guaranteed confidential data, the settled data protection, and accessibilities, effective, efficient, and secure communication and collaboration [16].

II. Research Method

A. Research Location

The research project is carried out in the PLBN entry port areas. The traveler arrives in the designated PLBN ports for processing the arrival and departure information. The designated PLBN ports of the country are in Wini, MotaAin, and MotaMasin PLBN.

This research focuses on Wini in the North Insana sub-district, North Central Timor, East Nusa Tenggara province. Wini has a direct border with the Timor-Leste enclave. Since 2015, the enclave (Oecusse district) becomes a special economic zone. Wini is one of Indonesia portal for the Timor-Leste's enclave (Oecusse).

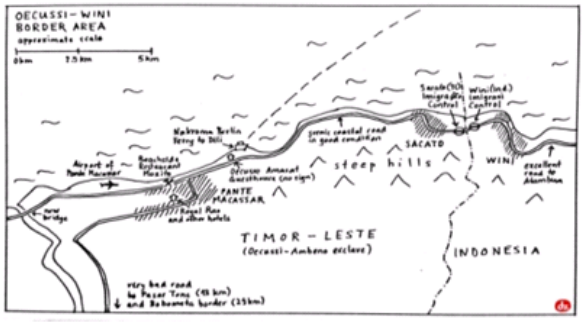

Fig. 1. Wini border as the focus area.

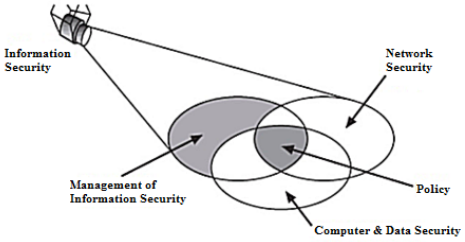

Fig. 2. Information security components.

Wini is located at 90° 10′ 51.6″ of south latitude and 124° 29′ 27.6″ of east longitude. The Wini and Oecusse region can be found on the following map in Fig. 1.

B. Information Security Architecture (ISA)

The Information Security Architecture (ISA) is based on the Committee on National Security Systems (CNSS) framework. It has five inter-dependencies of information system management. They are the information security as a core topic, the management of the information security, network security, the computer and data security, and the policy. The CNSS is United States inter-governmental organization sets policies for information security. The policy is the nucleus or the heart of every segment in the Information Security Management System (ISMS). The policy is a guide for information security planning, organizing, leading or implementation, and control or maintenance. These are called as the characteristic of the management. The CNSS information security diagram can be seen in Fig. 2.

Additionally, according to the ISO 27001:2013, the ISMS is a standard for developing the information security for any organization such as commercial enterprise, government institution, and non-profit organization. It covers all size of the businesses such as micro to multinationals and all industries (retail, banking, government, education, health, immigration, and others) [17].

Fig. 3. Confidentiality, Integrity, and Availability (CIA) triangle [18].

C. Confidentiality, Integrity, and Availability (CIA) Triangle Concepts

CIA is a concept for securing the information assets. These three elements have the same values or measurement, whether the information is classified as confidential or not. However, the information has no integrity, which means it is not classified information. If the information has integrity, the authorized person can access it every time and everywhere. However, if the information is not available in real-time, it means the information has no integrity. Therefore, they should be in balance. If it is classified, the authorized person should access the information as it is needed. These three key characteristics of the information assets should be protected in information security. First, confidential means only the authorized person can view the information. This is classified information. Second, integrity means information is correct and not altered over its lifecycle. It is not corrupted data and information. It has logs (version and all changes or histories are well recorded). Third, availability means data or information are accessible to the authorized person whenever it is needed. The CIA triangle can be seen in Fig. 3.

The CIA triangle can be emphasized by contesting several key questions. However, the way to ensure data confidentiality will not be simple. It needs a deep understating on how the data are processed, recorded, and transmitted over multiplatform infrastructures and systems. It operates by multi-access profiles of the users. For instance, data use cryptography to encrypt the data for stored or transmission. Then, the authorized person has to decrypt within strong authentication, or data have restricted access. The only authorized person has access, and data are stored and viewed in the limit numbers of places. The cryptography method can be seen in Fig. 4.

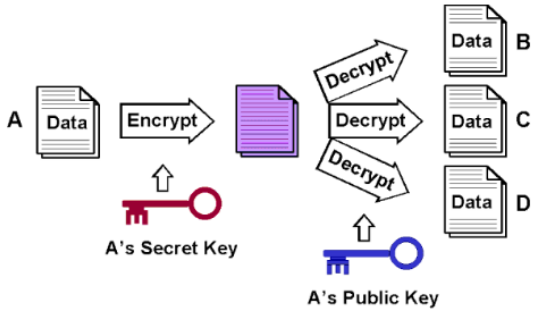

Fig. 4. Data encryption process [18].

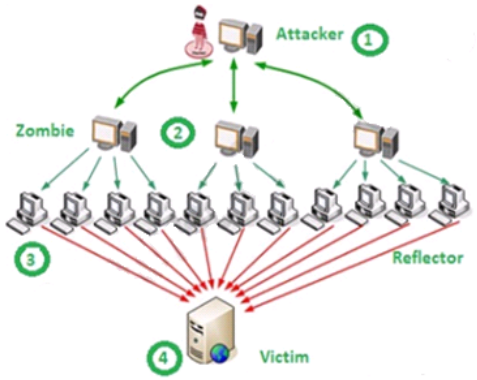

Fig. 5. Distributed Denial of Service (DDoS) attack [18].

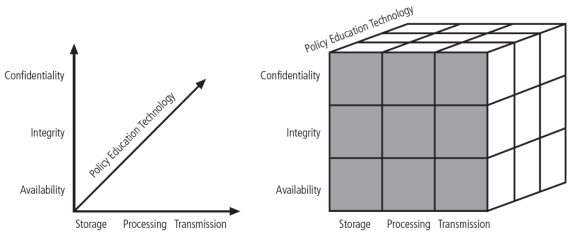

Fig. 6. McCumber cube [18].

Data encryption process has two determinant factors, namely the private/secret and public key. In the Notes and Domino environment and proprietary, private key refers to user.id and password. Meanwhile, the public key is server.id and certification.id. To link these two ids (user.id and server.id), Domino proprietary comes with the certification.id. This certification.id can certify both user and server to have the access to encrypt and decrypt data.

To ensure data integrity, it is based on strong authentication, cryptography, and document system activities (logs, records, version, and process). In this case, all historical data changes and access logs are well recorded. The purpose of this capture is aiming for future auditing.

Moreover, the data availability has to be based on proper data backup policy and procedure, the data recovery policy and procedure, and anti Distributed Denial of Service (DDoS) system. On-site and off-site data backups and recoveries should be tested periodically. Infrastructure support for business continuity plan and incident management should be appropriately designed and tested. The infrastructure should have a primary and secondary service to anticipate occurring hardware, software, and system failure. The DDoS diagram and attacks can be seen in Fig. 5.

Moreover, the CIA can emphasize several specific areas, such as privacy, identification, authentication, authorization, and accountability. Privacy means the collected information is stored and used by or for the organization. It is characterized as not freedom from the observation. In this context, data collection from cross borders or passers are protected within sets of privacy and confidentiality in the application system, and the only authorized person from the immigration office can access them. It is not for public consumption [19–21].

The identification is the characteristic to recognize the users of the system. The identification and authentication give accessing level of the users. In this case, the system is used for logging in, and the users have different credentials. The authentication occurs when it proves that users are granted for accessing the information. The authorization assures that the user has access to the information. It occurs after passing the authentication process. Accountability is when the control assures that every information has attributed to the name of the person or automatic process [22–24].

The usability of the CIA triangle over timing in the implementation of information security management has further enhancement. The CIA has three different dimensions, namely: the goal desire dimension, the information asset dimension and safeguards, and technology dimension. The goal desire consists of confidentiality, integrity, and availability. Meanwhile, information asset includes storage, processing, and transmission. Then, the safeguards are policy, education, and technology [17, 25, 26]. It can be seen in Fig. 6.

The information security threats have three major components, such as the targets, agents, and the event. The target refers to the organization assets that may potential gets attacks. The organization assets are data, information, software, hardware, system resources, network, services, and others. Therefore, the proposed system needs proper protection. Moreover, the agent is the organization or people who are from threats like employees, ex-employees, commercial rivals, terror-

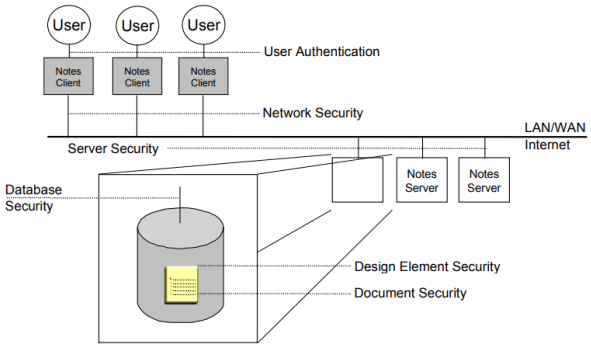

Fig. 7. Domino and Notes security architecture [33].

ists, hackers, and criminals. People are most vulnerable to information security. They need proper information security awareness class, and this has to be implemented periodically. Then, the event refers to the type of action in which it poses threats. For example, it can be the misuse of authorized information, accidental alteration of the information, and accidental destruction of the information [27, 28].

III. Results and Discussion

A. Domino Security Overview

The researchers analyze the Domino and Notes proprietary and find that they have a security layer model which complies with the CIA and ISMS standards. The security layers of the Domino and Notes are designed in the system administrators and the applications. It is done to meet institution requirement. These Domino And Notes security layers are similar to the security system at private premises (home). The guests cannot enter the house if they no access or key for the gate. In this case, to access the house, guests should pass each layer of the security such as the gate, front door, and the rooms [29].

The Domino and Notes have security features to protect the primary components such as users, network, databases, design elements, servers, and documents. Vertical security architecture is access from users to documents. The horizontal securities are all components attached to the Domino infrastructures such as users authentication, Access Control List (ACL), and document restriction [30–32]. It can be seen in Fig. 7.

Furthermore, the Domino and Notes servers and Notes Clients security environment can be investigated as follows:

1) Users security.
   The security architecture of the user’s access has a proprietary to avoid unauthorized person gaining access. Therefore, Domino and Notes provide each user with an ID file. The ID file contains the Domino certification and encryption key. The Domino certification aims to verify the user ID file on the user device. Herewith, the Domino server will indirectly verify whether the user has an ID or not. Additionally, Domino and Notes server allows the use of the encrypted password to protect the sensitivity of the user ID file. This is unlikely that the unauthorized user can obtain the user ID file and password which are encrypted. Therefore, it is imperative that users have to be educated and increase their awareness. The user should never divulge his or her user ID file and password to an unauthorized person. If it is compromised, the unauthorized person will gain access to the encrypted emails and access the server except on the Domino server. The password checking has been enabled. The two-factor authentications are applied in one single login.
2) Network security.
   The Domino and Notes servers provide some level of security, which can encrypt messages transmitted between Notes clients and servers. The Domino and Notes cannot enforce other layers of the network securities in the networks. Therefore, additional network protection has important roles such as encrypting the network traffics which will protect network packets and traffics from sniffers or spoofer using Secure Socket Layer (SSL), Secure Shell (SSH), and Transport Layer Security (TLS).
3) Server security.
   The primary role of the server security is controlling the stored information in the Domino directory. It is controlled by users, servers, a group of users, or servers that are given denied access to specific entities in the Domino environment. Every server is assigned to specific users and servers, and groups which can use ‘Passtru’ connection, create new databases, and create database replicas. On top of the Domino and Notes servers security, there are configured base on server ID and certification ID files. Similar to user security, server security has two-factor authentications. Although an unauthorized person can have the domino administrator password, the user cannot access the server unless he or she holds the server ID file. If the user wants to force and change the password, he or she should have a certification ID file. Otherwise, it cannot be changed.
4) Database security.
   Every database on the Domino servers environment has an ACL to group the users and servers

in accessing the intended databases and allowing them (users or and servers) to perform the tasks. Herewith, the initial database configurations play key roles in protecting the data.

5) The design element security.
   The security of the design element controls the forms of access, views, and folders. The designer should have database access before controlling the design elements. The designer can give access to specific users for accessing some document, forms, field, views, and folders in the database. The design element can also limit the access for formulas and script. For example, controlling one notes client can use the Execution Control List (ECL).
6) Document security.
   The users have to gain the document access to read or edit attributes. However, in a certain field, it can be restricted. The individual document even field in the document can be restricted. In achieving the restriction access, the document should set to Readers, Authors, and Field Signers. There are formulas, and encrypt attachments keys on the specific fields in the document. Finally, the entire document is encrypted.
7) The local database security.
   The Notes clients are connected through the network device and Domino server. Without a network connection, an authorized user cannot access the Domino server. Therefore, Notes clients or workstation users can be configured to access local replicated databases on the respect machines. The user can perform the data entries, views, emails, and other modification locally. Once the network becomes available, the Notes clients can auto replicate the Domino server.
8) The Recovery Manager (RM).
   The Notes Storage Facility (NSF) is a Domino and Notes proprietary. The Domino and Notes databases, forms, and files attributes will be ended with NSF. For example, ‘sintaswin.nsf’ refers to ‘sintaswin’ database, form, views, and file in Domino and Notes platforms. The NSF has two separate functionality databases, namely recovery logs and database itself. RM is designed to improve database integrity.
9) The logger.
   The logger is designed for the operational performance of the input and output of the database. The RM takes and manages all logger records information. It writes all transaction and undoes records to the logger, writes database and recoveries to the logger, and reconstructs the database after the server crashes.

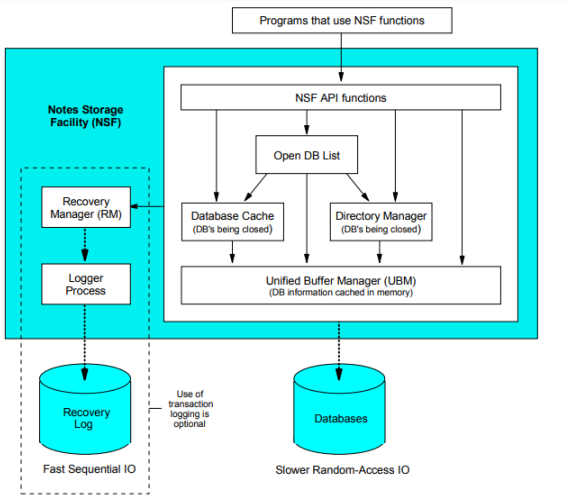

Fig. 8. Domino and Notes Recovery Manager architecture [33].

The operation of transaction logs are cache database modification in the memory and write them to the database file. Then, the logging operation is synchronous. This means all modifications are captured immediately in the log file. If the Domino server is crashed, the RM uses this log file to reconstruct database with 100% data integrity. Even, it is never recorded in the database file. The Domino proprietary elements can be seen in Fig. 8.

The Domino and Notes RM architecture aims to conduct the integrity and availability of data. Those are important elements of the desired goal dimension as it is explained previously. The processes of the logger are as follows:

1) Users interact with the database and its interfaces,
2) Domino and Notes have two different database functions. Those are RM database and database itself. All users activities are cached in memory. Then, it is recorded in the RM database. In case of system crashes, all modified (redo and undo the last activities) are recorded.
3) Once the system is active, the RM database will act first and give the option to the users to recover from the crashes.
4) If all activities are saved normally, and users close the application, when the application starts, the normal database will act first.

B. The Security Application Prototype

The application prototype for this research project uses the Domino server and database as a base platform and the Clevadesk web application database as an interface. The Clevadesk application is designed to

TABLE I
WEIGHT AND COMPLIANCE CATEGORY OF PROTOTYPE APPLICATION.

Evaluation tools	Weight
All compliance	5
Negation 1 comp.	4
Negation 2 comp.	3
Negation 3 comp.	2
Negation 4 comp.	1
Negation $>$ 4 comp.	0

optimize the Domino web application capabilities, such as security, workflow, scalability, social capability, and open standard. The Domino platform and the Clevadesk are synergic for enhancing security compliance. The security perspective for this application prototype based on the CIA and the ISO 27001:2013 on the ISMS approaches. The researchers are confident that the output of this application prototype will meet the CIA and ISO 27001:2013 compliances. Therefore, in this research project, the researchers design an application prototype which is to protect data confidentiality, integrity, and availability during a transmission, procession, and data storage by using technology, policy, and people. These are holistic information system security approach. Almost all of the requirements in the CIA and the ISO 27001:2013 standards are applied. The main reason why the researchers use ISO 27001:2013 as a reference standard are as follows:

1) Regulation of the Ministry of Communication and Information Technology number 04 of 2016 about information security management system, chapter 3, article 7, verse 1: the use of the ISO 27001 standards for information security; and chapter 3, article 7, verse 2: the use of ISO 27001 standards for implementation of the information system (electronic system),
2) Regulation of the Ministry of Communication and Information Technology number 20 of 2016 about the protection of personal data in electronic systems, chapter 1, article 2, verse 1: privacy data protection; and chapter 2, article 3, verse a-e: data gathered, processed, analyzed, stored, and transmitted has to be protected.

These arguments can be emphasized within the following evaluation tools. Table I shows an evaluation tool that the researchers set up compliance versus a weighted number to measure the implementation of the application prototype system.

The evaluation tool represents the categories of compliance in the prototype system implementation and weighted. If all the compliances in the CIA are fulfilled in the prototype system, the weighted value is the maximum five. If one of compliance in the CIA is missed (negation 1 comp. in Table I) in the prototype, the value is four. If two of compliances are missed (negation 2 comp., in Table I) in the prototype, the value is three. Similar reading is applied to the rest of Table I. If it is more than four negations of the compliances in the prototype system, it is zero value. The researchers develop other tables to facilitate the measurement of compliances versus risk and impact. It can be seen in Table II.

TABLE II
SECURITY RISK AND IMPACT CATEGORY OF THE PROTOTYPE APPLICATION.

Risk (R)	Legend	Impact (I)
1	Low	1
2	Low Mod.	2
3	Moderate	3
4	High Mod.	4
5	High	5

TABLE III
THE CORRELATION BETWEEN SECURITY RISK AND IMPACT OF THE PROTOTYPE APPLICATION.

R 5	5	10	15	20	25
I 4	4	8	12	16	20
S 3	3	6	9	12	15
K 2	2	4	6	8	10
S 1	1	2	3	4	5
Impact	1	2	3	4	5

The risk and impact tools are designed for enabling the researchers to measure the compliance, security risks, and impacts on the application prototype system. The lower value of the risk and impact in Table II is one. It means it is almost free of risk and has no impact on the prototype system application. However, in the information system, there are always risk and weakness. For example, the system is not updated in the coming months, technology is obsoleted, backups are not proper, and others. The moderate value of the risk and impact in Table II is three. It means the implementation of the application prototype system is in the risk and has an impact on the application. However, if this application prototype has a proper treatment from the experts, it will downgrade to the low moderate and has low risk and impact. Otherwise, it should upgrade to the next level of the risk and impact (high moderate/high). The highest value of the risk and impact is five. It means that the hazard application prototype system is high, or the application prototype system is vulnerable. In the several cases, especially in information and technology sector, it may not have immediate impacts or attacks from the hackers or viruses, and losing data because of system defects, it is in an isolated place. Therefore the CIA is not affected. The correlation between risk and impact can

TABLE IV
COMPLIANCE AND SECURITY RISK.

CIA Dimension		Domino & Notes Security	CIA Dimension vs. Domino Security	Compliance (A)	Security Risk (B)	Security Impact (C)	(B) × (C)
Desired Goal	Confidential	User (1)	Confidential (No 1, 2, 3, ⋯, & 9)	5	1	3	3
	Integrity	Network (2)	Integrity (No 1, 2, 3, ⋯, & 9)	5	1	3	3
	Availability	Server (3)	Availability (No 1, 2, 3, ⋯, & 9)	5	1	2	2
Information Assets	Storage	Database (4)	Storage (No 1, 2, 3, ⋯, & 9)	5	1	2	2
	Processing	Design (5)	Processing (No 1, 2, 3, ⋯, & 9)	5	1	2	2
	Transmission	Document (6)	Transmission (No 1, 2, 3, ⋯, & 9)	5	1	2	2
Safeguard	Policy	Local Database (7)	Policy (No 1, 2, 3, ⋯, & 9)	5	1	2	2
	Education	Recovery Manager (8)	Education (No 1)	4	2	2	4
	Technology	Logger (9)	Technology (No 1, 2, 3, ⋯, & 9)	5	2	2	4

be seen in Table III.

The security risk and impact exposure in Table III will facilitate the assessment of the implementation of the application prototype system. The green area values are 1*1, 1*2, 2*1, 2*2, 1*3, and 3*1. The green areas are secure and favorable for the implementers. It means the application prototype system is secure and safe to implement and use. It is protected from unauthorized people and has the integrity and high availability according to the CIA and ISO 27001:2013 standards. The yellow area values are 1*4, 1*5, 4*1, 5*1, 2*3, 3*2, 2*4, 4*2, and 3*3. It indicates the warning or alert for the implementer and stakeholder that the implementation of the application prototype needs to be improved. Meanwhile, the red area values are 2*5, 5*2, 3*4, 4*3, 3*5, 5*3, 4*4, 4*5, 5*4, and 5*5. It shows that the application prototype is at high risk or vulnerable.

Based on these Tables I–III, the researchers can assess and evaluate the application prototype system. First of all, the researchers transpose McCumber cube into Table IV as follows:

1) The CIA dimension is in column 1 and 2. It consists of [Desire Goal{Confidential, integrity, and Availability}, Information Assets{Storage, Processing, and Transmission}, and Safeguard {Policy, Education, Technology}],
2) The Domino & Notes Security elements in column 3 are transposed from the result and discussion of (a) the Domino Security Overview. The Domino and Notes important elements are {1. User, 2. Network, 3. Server, 4. Database, 5. Design, 6. The document, 7. Local Database, 8. Recovery Manager, and 9. Logger},
3) The CIA dimension versus Domino and Notes Security is a combination of each CIA dimension elements. It can be applied or found in the Domino and Notes security elements. It consists of [Confidential{1. User, 2. Network, ⋯, and 9. Logger}, Integrity{1. User, 2. Network, ⋯, and 9. Logger}, Availability{1. User, 2. Network, ⋯, and 9. Logger}, Storage{1. User, 2. Network, ⋯, and 9. Logger}, Processing{1. User, 2. Network, ⋯, and 9. Logger}, Transmission{1. User, 2. Network, ⋯,and 9. Logger}, Policy{1. User, 2. Network, ⋯, and 9. Logger}, Education{1. User}, Techology{1. User, 2. Network, ⋯, and 9. Logger}],
4) The Compliance (a) in column 5 are assessed and valued base on the evaluation tools,Table I,
5) The Security Risk (b) in column 6 and Security Impact (c) in column 7 are assessed and valued base on the risk evaluation tools in Table II,
6) The Security Risk*Impact (d) in column 8 are assessed and valued base on the security risk and impact exposure in Table III.

The overall processes of assessing the prototype application system can be seen in Table IV.

The researchers find interesting results in Table III. First, in the compliance, the score values are mostly five except the education dimension. It means all compliance parameters are met. However, the education and awareness program for the user should be performed periodically. The prototype application system is acceptable in term of the CIA.

Second, in the security risk, the researchers find that almost all CIA dimensions have one score except for education and technology. It implies that application security is in a green area with low and low moderate. The prototype application system has low risk. However, the user needs information security training (continuous education). Meanwhile, the technology needs to be updated accordingly.

Third, in the security impact, the researchers notice that almost all Domino and Notes Security elements score two except user and network. The platform has

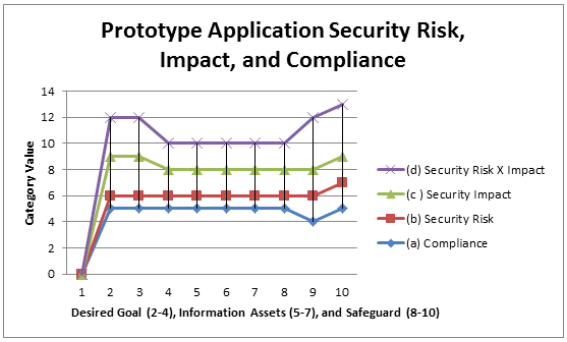

Fig. 9. Compliance and Security Representation (See Table IV).

a low moderate risk in the implementation like how security impact can arise from the user end or the network (public network/internet).

Fourth, the security risk*impact shows that all exposure scores are in the green area between score values of 2, 3, and 4. It means the prototype application system is capable of protecting privacy data (confidential), highly secure, and has data integrity and high availability.

The implementation of the prototype application system is viable and secure. It is a preferable choice for securing the immigration information system. The researchers can find that all security risk and impact exposure are in the green area. Moreover, almost all of the compliances from the CIA dimension and ISMS ISO 27001:2013 standards are met. The graphical representation of Table IV is shown in Fig. 9.

In Fig. 9, the researchers find several results. First, series (a) to (d) in point 2 to 4 represents the desired goal (CIA). On average, the distribution values are the sum of $((5+1+3+3)+(5+1+3+3)+(5+1+2+2)) = 34$. Then, 34 is divided by 12. It equals to 2.833. If the researchers refer to this distribution result to Table 3, it is in the low moderate area. Second, series (a) to (d) in point 5 to 7 shows the information assets (storage, process, and transmission). On average, the distribution values are the sum of $((5+1+2+2)+(5+1+2+2)+(5+1+2+2)) = 30$. After being divided by 12, it equals to 2.5. In Table III, this result is in the low moderate area. Third, series (a) to (d) in point 8 to 10 refers to the safeguard (policy, education, and technology). On an average, the distribution values are the sum of $((5+1+2+2)+(4+2+2+4)+(5+2+2+4)) = 35$ and divided by 12. It equals to 2.916. Referring to Table III, this result is in the low moderate area.

Overall the prototype system and platform are in the low moderate area. However, it is acceptable for implementation. Therefore, to secure the immigration information system in the Wini immigration office, the preferable options are Domino and Notes platform. Designing and prototyping the application system layout can be based on all business requirements and needs.

C. The Design Specification of Prototype

First, it is business roles. It consists of several types of users as follows:

1) The Anonymous User (First time in the system) User (ever using the system, and the user information has been recorded).
2) Immigration Officer (IO) 1 - a manager (see all documents, approve and reject the document).
3) Immigration Officer (IO) 2 a supervisor (see only approved documents, final verification, and expired document, approve or reject the document).
4) Admin - Admin (The developer who sees everything in the idea).

Second, it is the application form. There is the main page of the site which there is a button of "Fill the Form". When the anonymous user or user click, she/he can choose a preferred language. The user gets access to fill out the form (a very simple form on the smartphone and the terminal). The user only sees the form with the fields and the submit button. There is a simple validation (*). The list of fields are name, surname (as in the passport) (*for filling); gender(*for filling); nationality (*for filling); place of birth; date of birth (* for filling is not current and not future); passport number (*for filling); place of issue of passport (*for filling); date of expiry of the passport (for completion); a resident of which country (* for completion); the place of landing (where he took a plane) (*for filling); flight number or airplane number or registration number of the aircraft; final destination; occupation; purpose of the visit; place of residence at the time of visit; length of stay; address in Indonesia; for official visits - (Visa); email (this is a new feature and optional to fill up. there is a notification or a reminder to your email when it is approaching the expired date, or clicking submitted button); date of completion (when the form is completed from filling up to approve or reject); registration number (automate number for ID form; and barcode (automate system).

Third, it is view process. If the documents fall into the Agreed Visitors view, it is allowed to be edited. Once the document is agreed, the information on the border is recorded. Then, the counter is turned on how many days the user can be in the country. Moreover, if a user flies out of the country on time (30 days) or not on time (paid additional day), it does not matter. The document goes to the alert mode if that person still does not leave the country. View reports or prints are based on the date of entry to the country (daily, weekly,

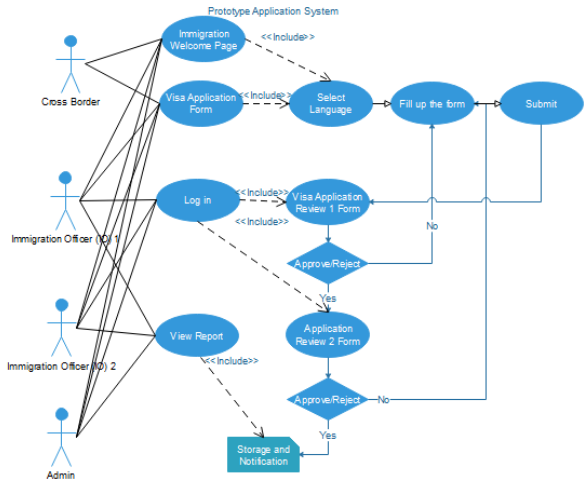

Fig. 10. Prototype of the application system.

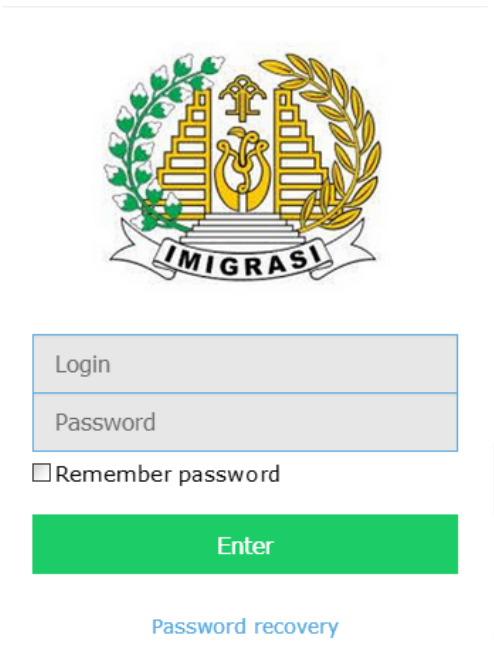

Fig. 11. Log in to the system.

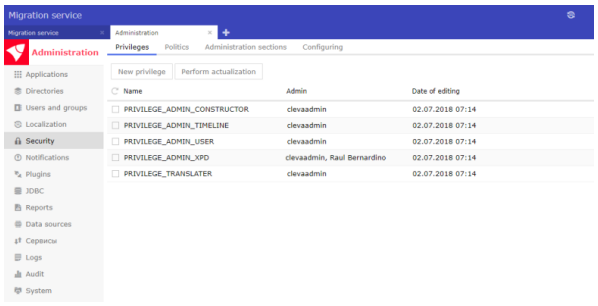

Fig. 12. Access Control List (ACL).

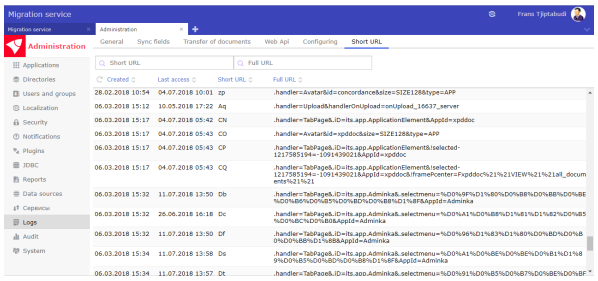

Fig. 13. Domino logs.

monthly, person, aim of the visit, and use advanced embedded search). The Use case diagram can be seen in Fig. 10.

The implementation can be found in Figs. 11–14. The prototype application is created to ensure that the application users have a proper credential to access the application resources. For example, there are data and information which may be stored, processed, or transmitted over system and networks. This starts with the user's identification process, the authentication with the right password credential, and system authorized. It is when the user ID and password are met as it is configured within the prototype application. It can be seen in Fig. 11. Moreover, the Access Control List (ACL) purpose is to give authorities to the users of the prototype application. The example can be seen in Fig. 12.

The access control list is a Domino and Notes proprietary. It performs the identification, authentication, and authorization of the prototype application users. Once users are registered in the prototype application, they have the right to access the resources base on the access levels. For example, Admin has access to design elements, database, and others. Other normal users can access the assigned database, but they will not be able to access the other databases, elements, and admin functions.

The RM takes all activities logs and registers those in the log file or a Domino Log database. In the case of power down or electrical failure, the prototype application system takes all recent events in the logs database. Once electrical power comes back, the RM will recover all events that are not saved before automatically. The logs can be found in Fig. 13.

The logs are identified linking to fields elements that have been modified, a timer to records data history, and the user to records who does what. This is to ensure the integrity and availability of the prototype application system. The prototype application system checks the tasks and displays information in real-time. The graph shows the utilization of the system, accesses, memory,

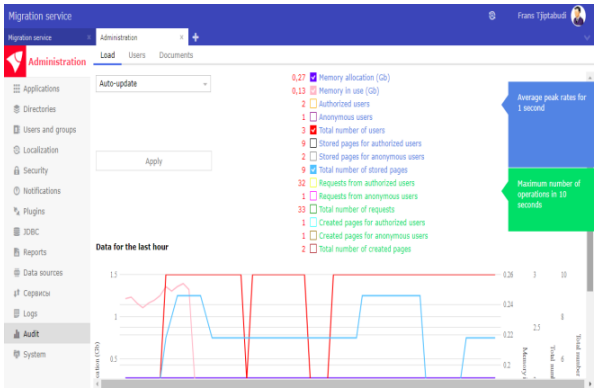

Fig. 14. System performance audit and monitoring.

and others. It is in Fig. 14.

This audit can help the system administrator to review the prototype application. The administrator can know how much memory that has been used, what activities that have been done, and who creates and requests the process forms or pages.

From the result, the researchers can summary several things. First, any chosen platform for securing the electronic information system has to be cross-platform. It means that the prototype application platform (Domino and Notes) can be integrated with the existing and future application systems. The prototype application (Domino and Notes) has a cross-platform proprietary. It can import data from other platforms and interrogate or export data to other different platforms. Second, Domino and Notes have high-security elements which can encrypt confidential data of the user.id (private key), server.id (another private key), and cert.id (public key). Third, Domino and Notes have RM proprietary. It can ensure data integrity and availability. Last, the development of the system has to comply with existing regulation like regulation of the Ministry of Communication and Information Technology number 04 of 2016 about information security management system in ISO 27001 standards and number 20 of 2016 about the protection of personal data in electronic systems.

IV. Conclusion

The Wini PLBN is a designated authority which consists of CIQ. The application prototype system is implemented and designed in the immigration office for SIIS. The information security system of this application prototype system parameters and compliances components such as CIA and ISO 27001:2013 are fulfilled. The result is a secure, effective, and efficient application prototype system. The researchers see there is a need for further research on the integration of the systems among custom, immigration, and quarantine applications.

References

[1] A. A. Adams and R. McCrindle, *Pandora's box: Social and professional issues of the information age*. John Wiley & Sons, 2008.

[2] J. L. Bower and C. M. Christensen, "Disruptive technologies: Catching the wave," *Harvard Business Review*, vol. 73, no. 1, pp. 43–53, 1995.

[3] J. Heizer and B. Render, *Operations management*. New Jersey: Pearson, 2011.

[4] C. M. Christensen, *The innovator's dilemma: When new technologies cause great firms to fail*. Boston, MA, USA: Harvard Business School Press, 1997.

[5] Y. Park and P. Hong, "The role of it for global firms in emerging markets," *International Journal of Business Information Systems*, vol. 18, no. 4, pp. 490–505, 2015.

[6] J. E. Smith and C. Ulu, "Technology adoption with uncertain future costs and quality," *Operations Research*, vol. 60, no. 2, pp. 262–274, 2012.

[7] M. Rhodes-Ousley, *Information security: The complete reference*. McGraw Hill Education, 2013.

[8] C. Buchta, D. Meyer, A. Pfister, A. Mild, and A. Taudes, "Technological efficiency and organizational inertia: A model of the emergence of disruption," *Computational & Mathematical Organization Theory*, vol. 9, no. 2, pp. 127–146, 2003.

[9] E. Kremp and J. Mairesse, "Knowledge management, innovation, and productivity: A firm level exploration based on french manufacturing CIS3 data," National bureau of economic research, Tech. Rep., 2004.

[10] D. Lauren. (2017) Models of ethical behavior in business. [Online]. Available: https://bizfluent.com/list-6406921-models-ethical-behavior-business.html

[11] S. L. Alter, "How effective managers use information systems." *Harvard Business Review*, vol. 54, no. 6, pp. 97–104, 1976.

[12] M. Indra, "Urgensi pengelolaan wilayah perbatasan dalam kaitannya dengan kedaulatan Negara Kesatuan Republik Indonesia," *Jurnal Selat*, vol. 1, no. 1, pp. 13–18, 2013.

[13] F. Rani, "Strategi pemerintah Indonesia dalam meningkatkan keamanan wilayah perbatasan menurut perspektif sosial pembangunan," *Jurnal Transnasional*, vol. 4, no. 01, pp. 1–17, 2012.

[14] R. Mulyawan, "Implementasi kebijakan pembangunan bidang pertahanan di wilayah perbatasan antaranegara dalam konteks otonomi daerah (Studi kasus di wilayah perbatasan Indonesia dengan Timor Leste)," *Jurnal Sosial Politik*, vol. 2, no. 1, pp. 85–112, 2012.

[15] Efendi, "Studi tentang pelayanan publik Pas Lintas Batas (PLB) Krayan_Ba'Kelalan Malaysia Di Kantor Imigrasi kecamatan Krayan Kabupaten Nunukan," *EJournal Ilmu Administrasi Negara*, vol. 3, no. 2, pp. 613–627, 2014.

[16] L. M. Markus, "Toward a theory of knowledge reuse: Types of knowledge reuse situations and factors in reuse success," *Journal of Management Information Systems*, vol. 18, no. 1, pp. 57–93, 2001.

[17] International Organization for Standardization. ISO/IEC 27001:2013-Information technology Security techniques Information security management systems Requirements. [Online]. Available: https://bit.ly/1MspEIj

[18] N. Vlajic. (2013) Computer science: Assessment and forensic - Introduction to information security. [Online]. Available: https://bit.ly/2lRqecQ

[19] S. Aldossary and W. Allen, "Data security, privacy, availability and integrity in cloud computing: Issues and current solutions," *International Journal of Advanced Computer Science and Applications*, vol. 7, no. 4, pp. 485–498, 2016.

[20] A. Tchernykh, U. Schwiegelsohn, E. G. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *Journal of Computational Science*, vol. In Press, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877750316303878

[21] Y. Benslimane, Z. Yang, and B. Bahli, "Information security between standards, certifications and technologies: An empirical study," in *2016 International Conference on Information Science and Security (ICISS)*. Pattaya, Thailand: IEEE, Dec. 19–22, 2016, pp. 1–5.

[22] A. Tanović and I. S. Marjanovic, "Development of a new improved model of ISO 20000 standard based on recommendations from ISO 27001 standard," in *2019* 42^{nd} *International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. Opatija, Croatia: IEEE, May 20–24, 2019, pp. 1503–1508.

[23] C. C. Huang and K. J. Farn, "A study on e-Taiwan promotion information security governance programs with e-government implementation of information security management standardization." *IJ Network Security*, vol. 18, no. 3, pp. 565–578, 2016.

[24] I. H. Al-Mayahi and P. M. Sa'ad, "Information security policy development," *Journal of Advanced Management Science Vol*, vol. 2, no. 2, pp. 135–139, 2014.

[25] J. McCumber, "Information systems security: A comprehensive model," in *Proceedings of the* 14^{th} *National Computer Security Conference*. Washington DC: National Institute of Standards and Technology, Oct. 1–4, 1991, pp. 328–337.

[26] W. V. Maconachy, C. D. Schou, D. Ragsdale, and D. Welch, "A model for information assurance: An integrated approach," in *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, vol. 310. New York: United States Military Academy, West Point. IEEE, June 5–6 2001.

[27] R. Pressman and B. Maxim, *Software engineering: A practioner's approach*. New York: McGraw-Hill, 2014.

[28] H. Kashfi, "Software engineering challenges in cloud environment: Software development lifecycle perspective," *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, vol. 2, no. 3, pp. 251–256, 2017.

[29] P. A. V. Hall and J. C. F. Ramil, *Managing the software enterprise: Software engineering and information systems in context*. Cengage Learning EMEA, 2007.

[30] T. R. Peltier, *Information security risk analysis*. Florida: CRC Press, 2010.

[31] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *2013 International Conference on Availability, Reliability and Security*. Regensburg, Germany: IEEE, Sept. 2–6, 2013, pp. 546–555.

[32] R. Schwartz. (1997) The architecture of the domino web server, part 1. [Online]. Available: https://www.ibm.com/developerworks/lotus/library/ls-Architecture_of_the_Domino_Web_Server_Part1/index.html

[33] Lotus Development Corporation. (2000) Inside notes: The architecture of notes and the domino server. [Online]. Available: http://www-12.lotus.com/ldd/doc/uafiles.nsf/70817c90542892178525695b0051105c/2e559b131d346a028525697c00652c2b/$FILE/InsideNotes.pdf