SWISS GERMAN UNIVERSITY

MASTER OF INFORMATION TECHNOLOGY

PROCEEDING ACMIT 2014

Annual Conference on Management and Information Technology

IT for Enabling Business Growth, Improving Government Service and Sustaining Energy Conservation.

Swiss German University, BSD City Tangerang
January 11, 2014

Supported by

PT Dian Graha Elektrika

Preface

Dear ACMIT 2014 Readers,

First of all we would like to thank you for outstanding efforts in making this proceeding to share research conducted in several topics. Without those who spent time to write papers, editing papers, reviewing papers, preparing other details we would not have this proceeding for Annual Conference on Management and Information Technology 2014 organized by Master of Information Technology Department.

The proceeding is created to provide opportunities for academic communities particularly students to publish and disseminate their exemplary works. Therefore we are very grateful for all parties dedicating their time and efforts to produce this proceeding.

Finally we hope that ACMIT 2014 meets your expectation, and becoming fruitful and benefitted not only to academic communities but also governments and industries. Furthermore we wish your participations in the next year and even years to come. May God bless us all and thank you.

Sincerely yours,

ACMIT 2014

Chairman

DR. Mohammad A. Amin Soetomo

ACMIT 2014 Committee

Commissioner: Rector, Prof. Dr. phil. Martin Löffelholz

Vice Rector of Academic Affairs, Dr. rer. nat. Filiana Santoso

Vice Rector of Non Academic Affairs, Edward B.P. Manurung, M.Eng.

Dean Faculty of Engineering & IT, Dr. Ir. Gembong Baskoro, M.Sc.

Steering Committee: Prof. Dr. Ir. Marsudi W. Kisworo (Perbanas),

Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA (APTIKOM),

Dr. Teddy Mantoro, B.Sc., M.Sc. (USBI)

Ir. Arko Djajadi, M.Sc., Ph.D. (ARCS)

Dr.-Ing. Evita H. Legowo (ARCS)

Organizing Committee: Program Studi Magister Information Technology (MIT), SGU

Chairman : Dr. Ir. Mohammad A. Amin Soetomo, M.Sc.

Secretary : Charles Lim, M.Sc.

Rachmawati, S.Sos

Treasurer : Lita I Sari, S.E. (Finance)

Communication & P.R.: Director Christie Kanter, B.A. (Dir. of Comm. & PR)

Irzan Fahmi, S.Kom. (Dir. Of Comm. & PR)—Grap. Designer & Web

Program : Dr. Ir. Gembong Baskoro, M.Sc. (Dean of FEIT)

Ir. Arko Djajadi, M.Sc., Ph.D. (ARCS)

Dr. (cand) Ir. Heru Ipung, M.Eng. (ISS)

Dr. Maulahikmah Galinium, S. Kom, M.Sc. (BIT)

Dr. Tanika Sofianti, S.T., M.T. (IE Dept.)

Dr. Rusman Rusyadi, B.Sc., M.Sc. (MT Dept.)

CEO Dr. (cand) Riri Satria, MM (Value Alignment Advisory)

Dr. Ir. Mohammad A. Amin Soetomo, M.Sc.

Program Support: ASC & EXO--projector, mics, speakers

IT Infrastructure: Dr. (cand) Ir. Heru Ipung, M.Eng. (ISS)

Luky Darmawan (ISS)

Fundraiser **:** Dr. Ir. Mohammad A. Amin Soetomo, M.Sc.

Director Ir. Herry Achmadi (PT. DGE)

Acep Mardiyana, S.T., M.Kom. (PT. AIM)

Facility **:** Hendy Budi Prasetyo (FM)--room, HVAC and physical security

Ika Kurniasih--FM assistance

Paper Reviewer **:** Charles Lim, M.Sc.

Dr. Maulahikmah Galinium, S.Kom., M.Sc. (BIT)

Dr. Harya Widiputra, S. Kom., M.Kom. (Dean Perbanas)

Dr. Anto Satriyo Nugroho

Dr. (cand) Alva Erwin, S.Kom., M.Sc. (BIT)

Benfano Soewito, B.Sc., M.Sc., Ph.D. (Binus)

CEO Dr. (cand) Riri Satria, MM (Value Alignment Advisory)

Paper Administration: CEO Ir. Bobby Suryajaya (PT. BIA Energy)

Proceeding: Dr. Ir. Gembong Baskoro, M.Sc.

Dr. Ir. Mohammad A. Amin Soetomo, M.Sc.

Charles Lim, M.Sc.

Project Management: Thomas Bachri, B.Eng., M.Kom. (Permata Bank)

*Rio Parnando, S.E. *Ignassius B., S.Kom. *Mukti A. P.

*Haryo Seto S. Razad *Denny F., S.A. *Anton Purba, S.Si.

*Ali Fauzi *Mustafa

Food & Beverage: Rachmawati, S.Sos.

Program Rundown

08:00 - 08:30	Greeting and Registration
08:30	Opening Ceremony by MC
	(2") Prayers
	(3") Indonesia National Anthem (Indonesia Raya)
	(3") Report by Chairman of The Committee (Dr. Ir. Moh. A. Amin Soetomo, M.Sc.)
	(3") Welcome Address by Dean Faculty of Engineering & IT SGU (Dr. Ir. Gembong Baskoro, M.Sc.)
	(6") Opening Remarks by Rector of Swiss German University (Prof. Dr. Phil. Martin Löffelholz)
	(3") Plaque Presentation + Photo Session (Prof. Dr. Phil. Martin Löffelholz to present Plaques to Prof. Dr. Ir. Marsudi W. Kisworo and Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA)
	Rector of Swiss German University may be excused from the event.
	Keynote Speech:
09:00	(60") Keynote Speaker for Chairman of APTIKOM (Prof. Dr. Ir. R. Eko Indrajit, M.Sc., MBA)
	(15") QA Session
	(3") Certificate Presentation by ACMIT 2014 Chairman + Photo Session
10:15 – 10:45	Coffee Break
10:45	(60") Keynote Speaker for Rector of PERBANAS (Prof. Dr. Ir. Marsudi W. Kisworo)
	(10") QA Session
	(3") Certificate Presentation by ACMIT 2014 Chairman + Photo Session
	(2") Padamu Negeri (song)
12:00 – 13:00	Break, Prayers and Lunch
13:00 – End	Plenary A: Room FB 203
	Plenary B: Room FB 210
15:00 – 15:30	Coffee Break
16:00	Certificate of Participant Presentations

See you all in ACMIT 2015

Plenary Session

Plenary A: Networking, Security and Data Mining				
No.	**Time**	**Paper ID**	**Title**	**Authors**
1	**13:00 – 13:25**	**001**	**WS-Security on PRODML**	**Bobby Suryajaya**
2	**13:30 – 13:55**	**003**	**Implementation: Information Security Management System (ISMS) ISO 27001: 2005 at PERBANAS University**	**IGN Mantra**
3	**14:00 – 14:25**	**005**	**Wireless Access Point Protection from Un-Authorized User in an Office Environment**	**Ignasius Irawan Budi P.**
BREAK 10 mins				
4	**14:35 – 15:00**	**010**	**Enhancing Web Security through Infrastructure Design**	**M. Salahuddien Manggalanny**
5	**15:00 – 15:25**	**008**	**How Sweet and Ripe are the Fruits? Data Mining Techniques for Classifying and Predicting 'Quick-Wins' Direct Capital Investment in Indonesia as One Approach to Business Intelligence Orientation and Knowledge Management Scenarios of Indonesian Enterprises**	**Ali Fauzi**
6	**15:25 – 15:50**	**011**	**Development of Intelligent Filter for RSS-based Radio Tracking and Its Application**	**Legowo Budianto**

Plenary B: Management and IT Governance				
No.	**Time**	**Paper ID**	**Title**	**Authors**
1	**13:00 – 13:25**	**002**	**Risk Assessment of Core Banking System Replacement based on ISACA Framework**	**Fenty Simanjuntak, Bobby Suryajaya**
2	**13:30 – 13:55**	**004**	**XYZ Web App Information Security Management Risk Assessment**	**Meily**
3	**14:00 – 14:25**	**006**	**In Search of Code of Ethics Principles for IT Professionals in Indonesia**	**Carlia Isneniwati**
BREAK 10 mins				
4	**14:35 – 15:00**	**007**	**Improving Productivity of Radiology Department**	**Herry Ahmadi**
5	**15:00 – 15:25**	**009**	**Conceptual Risk on System Migration Framework**	**Nicsen, Moh. A. Amin Soetomo**

Table of Contents

The Annual Conference on Management and Information Technology (ACMIT) 2014

WS-Security on PRODML

Bobby Suryajaya
Master of Information Technology, Swiss German University, Jakarta, Indonesia
Bobby.Suryajaya@gmail.com

Abstract

SKK Migas plans to apply end-to-end security based on Web Services Security (WS-Security) for Sistem Operasi Terpadu (SOT). However, there are no prototype or simulation results that can support the plan that has already been communicated to many parties. This paper proposes an experiment that performs PRODML data transfer using WS-Security by altering the WSDL to include encryption and digital signature. The experiment utilizes SoapUI, and successfully loaded PRODML WSDL that had been altered with WSP-Policy based on X.509 to transfer a SOAP message.

Keywords: SKK Migas, SOT, Web Services, WS-Security, WSDL, WSP-Policy, X.509, SOAP message

1. Background

XML schemas convey the data syntax and semantics for various application domains, such as Oil and Gas production status reports. However, these schemas seldom address security issues, which can lead to a worst-case scenario of systems and protocols with no security at all [5].

SKK Migas plans to apply end-to-end security based on Web Services Security (WS-Security) for Sistem Operasi Terpadu (SOT). Figure 1 describes how WS-Security will be implemented, which employs encryption and signing based on X.509 or Username Token.

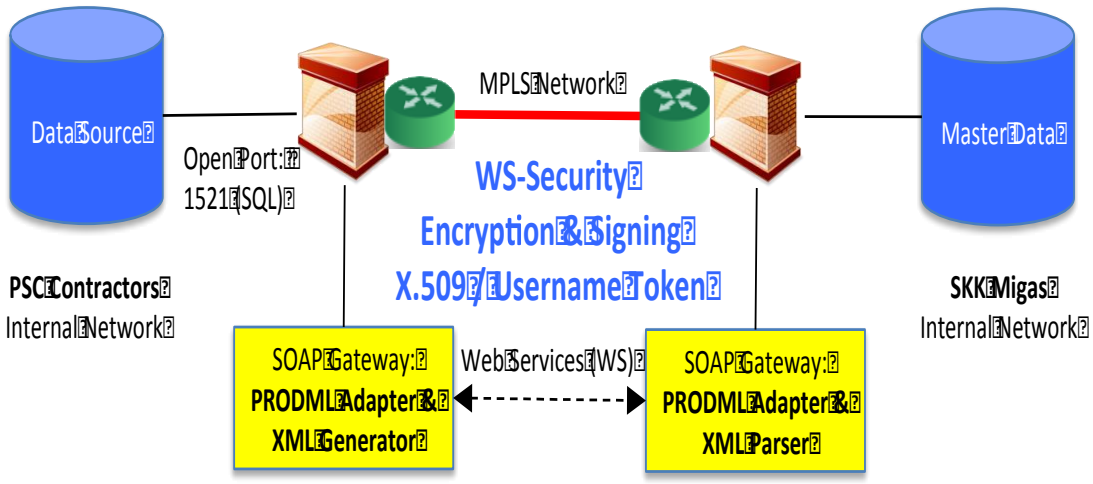


Figure 1.WS-Security Implementation Plan [8]

2. Problem Statement

SKK Migas intention's to apply end-to-end security to existing SKK Migas SOT infrastructure has been communicated to many parties, including vendors. Ideally, prior to communicating to other parties, SKK Migas should have already had a plan on how to implement the idea. Furthermore a prototype or simulation must be ready to support their intention.

The fact is SKK Migas does not have any infrastructure or environment to simulate the idea; hence, there are no prototype or simulation results that can support the plan. But there should be a way to prove whether the architecture can be implemented correctly.

This research proposes an experiment that can simulate existing SKK Migas SOT architecture to utilize WS-Security on SOT data exchange standard, PRODML. This research will perform modification to initial WSDL that was created to transfer data in PRODML format, to match WS-Security requirements, and test the modified WSDL by loading it with a web service simulation tool called SoapUI.

3. Production Markup Language (PRODML)

PRODML is an industry initiative for exchanging production-oriented data in upstream Oil & Gas, including standard data structure in XML format through web services [2].

Few major energy companies initiated PRODML in year 2005 and the initiatives were facilitated and maintained by Energistics. Development of PRODML follows successful WITSML adoption to the Oil & Gas industry as standard for drilling and completion of information architecture. International and national companies have implemented this technology to bring benefits and to add value to business process [1].

According to Weltevrede research, PRODML is a tool that enables optimization and reporting architectures and data management processes to adapt to changes in production environment faster with less effort and fewer errors, which can be used in implementing robust, trustworthy optimization and automation processes [10].

PRODML is adopted by SKK Migas as SOT first phase standard data exchange for Production and Lifting Report from the PSC Contractors as the Operator of the Upstream Oil & Gas assets.

There are four PRODML data-schema required by SKK Migas within SOT implementation for production data. They are: Product Flow Model (PFM), Product Volume Report (PV), Production Operation Report (PO), and Well Test Report (WT). Each data-schema consists of many objects and each object can be generated into a single XML file.

This research uses PRODML PFM to generate a SOAP message during the experiment.

4. WSDL and WS-Security

WSDL or Web Services Description Language is a web services interface description written in machine programmable format. WSDL defines parameters or data structures to serve the data [9].

WS-Security is a flexible and feature-rich extension to SOAP to apply security to web services. WSS specification leveraged SOAP foundation layer such as SOAP, WSDL, XML encryption, XML signature, and SSL/TLS. In this research, Encryption & Signing to PRODML WSDL using X.509 will be employed during data transfer [8].

5. X.509 Profile

X.509 is an ITU-T standard for Public Key Infrastructure (PKI). It can be used by WS-Security as a security token to ensure confidentiality and integrity of a message. X.509 specifies standard formats for public key certificates, certificate revocation list, attribute certificates, and a certification path validation algorithm [3].

Figure 2 describes the scenario on how X.509 will be implemented to provide confidentiality and integrity to data transfer through modification of PRODML WSDL. It is assumed that Certificate Authority is available to hold client and server public certificates.

6. The Testing Tool – SoapUI

The testing here means the process of executing SOAP web services that use XML language for definition of message architecture and message format, which will be in the form of WSDL. There are many tools available in the market. The core functions are the same but they are different in functionality, features, usability, and interoperability. There are several open-source testing tools available in the market, including Jmeter, Storm and SoapUI. This research will utilize, SoapUI.

SoapUI is a free and open source cross-platform Functional Testing solution. It has an easy-to-use graphical interface and enterprise-class features which allows SoapUI users to easily and rapidly create and execute automated functional, regression, compliance, and load tests. In a single test environment, SoapUI provides complete test coverage and supports all the standard protocols and technologies [7].

Beside free and cross-platform, consideration to choose SoapUI is listed as follows:

- SoapUI has complete and automated testing solution.
- SoapUI has easy-to-use graphical interface to work with SOAP-based web services.
- SoapUI has Mock-Services feature that gives unique ability to mimic Web services and create/run Functional and Load Tests against them.
- SoapUI has powerful and flexible reporting tools: Printable, Data Export, and HTML Reports.

This research utilizes SoapUI Pro Version 4.5.2 for MacOSX Version 10.8.4 with 15-days Trial License.

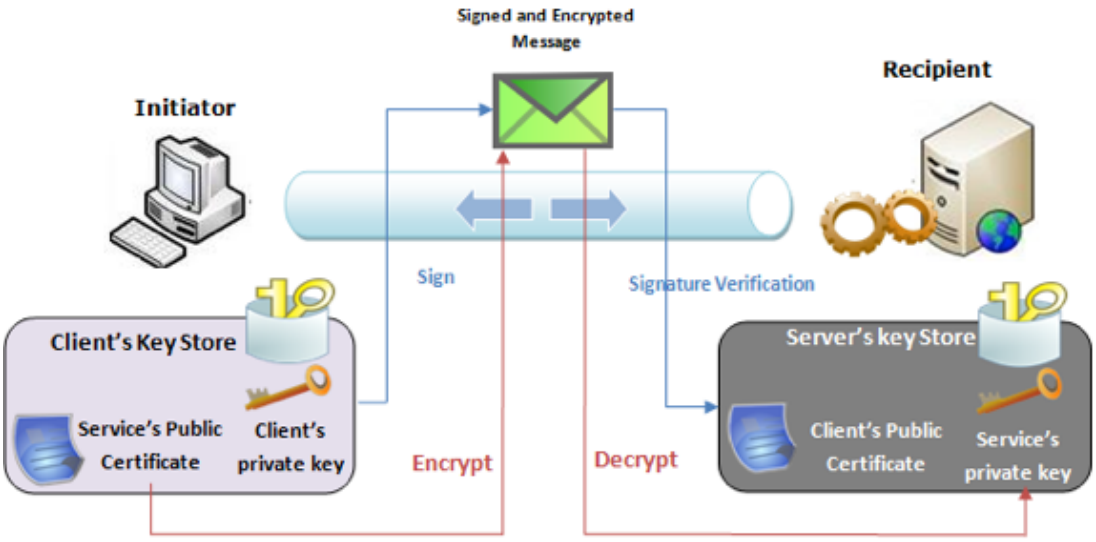


Figure 2.X.509 Implementation Scenario according to WSO2 ESB

7. Research Experiment

A. PRODML WSDL

Basically, normal PRODML WSDL (detail of PRODML WSDL can be found on Appendix) has following structure as defined by Energistics:

1. WSDL definitions
2. WSDL types (including XSD schema)
3. WSDL message
4. WSDL portType
5. WSDL binding
6. WSDL service

In normal deployment, this WSDL can be published directly to web service registry. However, related to SKK Migas SOT implementation, this WSDL must be binding with WS-Security as defined in the implementation requirement document. Therefore, it must be modified to incorporate the security mechanism.

For WS-Security to work there will be another party involved in the transaction, which are key store or certificate publisher and the key itself. The functionality of certificate publisher is to provide certificates that contain key to encrypt / decrypt soap messages, and to perform digital signing of messages and verification of its digital signature.

Implementation of WS-Security will append following structure to the original PRODML WSDL:

1. WSP Policy
2. WSP PolicyReference.

B. WSDL Load Test on SoapUI

Following is one test that was performed on PRODML WSDL with an operation called GetCapabilities.

GetCapabilities Request

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:gen="http://www.prodml.org/api/210/genericDataAccess">
   <soapenv:Header/>
   <soapenv:Body>
      <gen:GetCapabilities/>
   </soapenv:Body>
</soapenv:Envelope>
```

GetCapabilities Response

```
<soapenv:Envelope
xmlns:gen="http://www.prodml.org/api/210/genericDataAccess"
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <soapenv:Body>
      <GenericDataAccessCapabilities
xmlns:dc="http://purl.org/dc/terms/"
xmlns:gml="http://www.opengis.net/gml/3.2"
xmlns:xlink="http://www.w3.org/1999/xlink">
         <SupportedDataObjects
xmlns="http://www.prodml.org/api/210/genericDataAccess">
            <SupportedDataObject>
```

```
               <Name>productFlowModels</Name>
<SupportedOperation>PutData</SupportedOperation>
            </SupportedDataObject>
            <SupportedDataObject>
               <Name>productVolumes</Name>
<SupportedOperation>PutData</SupportedOperation>
            </SupportedDataObject>
            <SupportedDataObject>
               <Name>wellTests</Name>
<SupportedOperation>PutData</SupportedOperation>
            </SupportedDataObject>
            <SupportedDataObject>
               <Name>productionOperations</Name>
<SupportedOperation>PutData</SupportedOperation>
            </SupportedDataObject>
         </SupportedDataObjects>
         <Properties
xmlns="http://www.prodml.org/api/210/genericDataAccess">
            <NameValuePair>
               <Name>Name</Name>
               <Value>Server #1</Value>
            </NameValuePair>
            <NameValuePair>
               <Name>Version</Name>
               <Value>1.0.0.1</Value>
            </NameValuePair>
            <NameValuePair>
               <Name>Vendor</Name>
               <Value>BIA Energi</Value>
            </NameValuePair>
         </Properties>
      </GenericDataAccessCapabilities>
   </soapenv:Body>
</soapenv:Envelope>
```

C. WSP Policy

```
<wsp:Policy wsu:Id="SigEncr"
xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
>
<wsp:ExactlyOne>
<wsp:All>
<sp:AsymmetricBinding
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
>
<wsp:Policy>
<sp:InitiatorToken>
<wsp:Policy>
<sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/In
cludeToken/AlwaysToRecipient">
<wsp:Policy>
<sp:RequireThumbprintReference />
<sp:WssX509V3Token10 />
</wsp:Policy>
</sp:X509Token>
</wsp:Policy>
</sp:InitiatorToken>
<sp:RecipientToken>
```

```
<wsp:Policy>
<sp:X509Token
sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/In
cludeToken/Never">
<wsp:Policy>
<sp:RequireThumbprintReference />
<sp:WssX509V3Token10 />
</wsp:Policy>
</sp:X509Token>
</wsp:Policy>
</sp:RecipientToken>
<sp:AlgorithmSuite>
<wsp:Policy>
<sp:Basic256 />
</wsp:Policy>
</sp:AlgorithmSuite>
<sp:Layout>
<wsp:Policy>
<sp:Strict />
</wsp:Policy>
</sp:Layout>
<sp:IncludeTimestamp />
<sp:OnlySignEntireHeadersAndBody />
</wsp:Policy>
</sp:AsymmetricBinding>
<sp:Wss11
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
>
<sp:Policy>
<sp:MustSupportRefKeyIdentifier />
<sp:MustSupportRefIssuerSerial />
<sp:MustSupportRefThumbprint />
<sp:RequireSignatureConfirmation />
</sp:Policy>
</sp:Wss11>
<sp:Wss10
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
>
<sp:Policy>
<sp:MustSupportRefKeyIdentifier />
<sp:MustSupportRefIssuerSerial />
</sp:Policy>
</sp:Wss10>
<sp:SignedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
>
<sp:Body />
</sp:SignedParts>
<sp:EncryptedParts
xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
>
<sp:Body />
</sp:EncryptedParts>
</wsp:All>
</wsp:ExactlyOne>
</wsp:Policy>
```

D. WSP PolicyReference

```
<wsdl:binding name="PROD_GenericDataAccessSoap"
type="tns:PROD_GenericDataAccessSoap">
```

```
<wsp:PolicyReference URI="#SigEncr"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
/>
<soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
```

8. Result

WSP Policy and WSP PolicyReference were appended to original PRODML WSDL. The WSDL script has included X.509 token that referring to xmlsoap.org schema. The result was tested with SoapUI by loading whole XML script.

SoapUI Pro is equipped with XML-check capability, and the result come up with successful Mock Service loading and starting of modified PRODML WSDL. However, SoapUI functionality test cannot be done, since it needs more effort to create a testing script to utilize SoapUI GetCapabilities and PutData operation, and this can be considered as future work improvement to this research.

9. Conclusion

Based on the experiment results, it is concluded that:

- WS-Security as one of web services security mechanism is appropriate to secure PRODML data-exchange. Successful loading of PRODML WSDL that has been added with WSP-Policy for X.509 as well as mock-service initiation verifies the conclusion.
- By adding WS-Policy that uses X.509 Profile to PRODML WSDL, SKK Migas SOA architecture should have encryption and digital signing capability; hence; providing confidentiality, integrity, availability, authentication, and non-repudiation of the whole interoperability using PRODML.
- WS-Security works by performing encryption and digital signing to each SOAP message. This might lead to performance issues when dealing with enterprise interoperability and growth of transactions. Another mechanism called WS-Secure Conversation might be able to help answering this issue later.

10. Recommendation

There are many improvements that can be done to make this research better as listed below:

- If time permits, conduct better research preparation from all aspects that may include better data preparation (PRODML PFM, PV, PO, and WT) with more detailed documentation on the testing scenario.
- Perform manual functionality test on SoapUI, specifically when dealing with WS-Security, since automated testing is not provided, at least to the knowledge of the author. This includes test-script for GetCapabilities and PutData operation.
- Even though SoapUI Pro has mock services to simulate web services, it is better to use a real orchestration tool such as Enterprise Service Bus (ESB) since mock service has limited capability to the knowledge of the author. There are many open sources ESB where one of them that considered adequate for research is WSO2 Enterprise Service Bus. WSO2 supports security mechanism such as WS-Security.
- Expand the research with other security mechanism such as WS-Secure Conversation or other mechanism that together builds web service security management model.

References

[1] A. Beshri, D. Nixon, R. Suhaibani, N. Al-Nasser, and H. Muhawis, "Saudi Aramco Intelligent Field Data Exchange Experience Using PRODML: Case Study," *SPE Intelligent Energy International*, 2012.
[2] Energistics, n.d. PRODML Standards. [Online] Available at: http://www.energistics.org/production/prodml-standards [Accessed 30 September 2013].
[3] Myers, Michael, Rich Ankney, Ambarish Malpani, Slava Galperin, and Carlisle Adams. *X.509 Internet public key infrastructure online certificate status protocol-OCSP*. RFC 2560, 1999.
[4] Moralis, Athanasios, Vassiliki Pouli, Mary Grammatikou, Symeon Papavassiliou, and Vasilis Maglaris. "Performance comparison of Web services security: Kerberos token profile against X. 509 token profile." In *Networking and Services, 2007. ICNS. Third International Conference on*, pp. 28-28. IEEE, 2007.
[5] Naedele, Martin. "Standards for XML and Web services security." *Computer* 36, no. 4 (2003): 96-98.
[6] Lawrence, Kelvin, Chris Kaler, Anthony Nadalin, R. Monzillo, and P. Hallam-Baker. "Web services security: SOAP message security 1.1 (WS-security 2004)." *OASIS, OASIS Standard, Feb* (2006).
[7] SoapUI, n.d. SoapUI Pro. [Online] Available at: http://www.soapui.org.
[8] B. Suryajaya, C. Lim, and B. Ibrahim, "SKK Migas Sistem Operasi Terpadu-Performance Evaluation for Secure Data Exchange for Oil and Gas Contractors," *Advanced Science Letters*, vol. 20, pp. 129-133, 2014.
[9] W3C, 2007. WSDL version 2.0. W3C.
[10] Weltevrede, Ben, Alan Doniger, Laurence Ormerod, and Stanley DeVries. "The Second Stage Challenge for the PRODML Standards: Adaptive Production Optimization." In *SPE Annual Technical Conference and Exhibition*. 2007.
[11] Hussain, Shariq, Zhaoshun Wang, Ibrahima Kalil Toure, and Abdoulaye Diop. "Web Service Testing Tools: A Comparative Study." *arXiv preprint arXiv: 1306.4063* (2013).

11. Appendix – PRODML WSDL

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions
        name="GenericDataAccess"
        targetNamespace="http://www.prodml.org/api/210/genericDataAccess"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:tns="http://www.prodml.org/api/210/genericDataAccess"
        xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
        xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
        xmlns:abs="http://www.energistics.org/schemas/abstract" >
        <!--                                    -->
        <!-- Energistics License Agreement
```

```
-->
<!--                                    -->
<wsdl:types>
        <xsd:schema targetNamespace="http://www.prodml.org/api/210/genericDataAccess" elementFormDefault="qualified">
            <xsd:import namespace="http://www.energistics.org/schemas/abstract" schemaLocation="http://w3.energistics.org/schema/abstract_v1.0/xsd_schemas/sub_abstractSubstitutionGroup.xsd" />
            <xsd:complexType name="NameValuePair">
                <xsd:annotation>
                    <xsd:documentation>A generic structure for option values that are not specified in schema.</xsd:documentation>
                </xsd:annotation>
                <xsd:sequence>
                    <xsd:element name="Name" type="xsd:string" minOccurs="1" />
                    <xsd:element name="Value" type="xsd:string" minOccurs="1" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:complexType name="ArrayOfNameValuePair">
                <xsd:annotation>
                    <xsd:documentation>A collection of generic option values.</xsd:documentation>
                </xsd:annotation>
                <xsd:sequence>
                    <xsd:element name="NameValuePair" type="tns:NameValuePair" minOccurs="0" maxOccurs="unbounded" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:simpleType name="PutDataResultStatus">
                <xsd:annotation>
                    <xsd:documentation>An enumeration which specifies the status of a PutData operation with a data-object.</xsd:documentation>
                </xsd:annotation>
                <xsd:restriction base="xsd:string">
                    <xsd:enumeration value="Added" />
```

```
                    <xsd:enumeration value="Updated" />
                </xsd:restriction>
            </xsd:simpleType>
            <xsd:complexType name="ArrayOfSupportedDataObject">
                <xsd:annotation>
                    <xsd:documentation>A collection of SupportedDataObject
objects.</xsd:documentation>
                </xsd:annotation>
                <xsd:sequence>
                    <xsd:element name="SupportedDataObject"
type="tns:SupportedDataObject" minOccurs="0" maxOccurs="unbounded" />
                </xsd:sequence>
            </xsd:complexType>
            <xsd:complexType name="SupportedDataObject">
                <xsd:annotation>
                    <xsd:documentation>Describes a single element or data type
supported by a GenericDataAccess server.</xsd:documentation>
                </xsd:annotation>
                <xsd:sequence>
                    <xsd:element name="Name" type="xsd:string"
minOccurs="1">
                        <xsd:annotation>
                            <xsd:documentation>The name of the type.
This should be exactly the same as the local name (sans namespace) of the supported element or
type.</xsd:documentation>
                        </xsd:annotation>
                    </xsd:element>
                    <xsd:element name="SupportedOperation"
type="tns:SupportedOperation" minOccurs="0" maxOccurs="2" />
                </xsd:sequence>
                <xsd:attribute name="version" type="xsd:string" use="optional">
                    <xsd:annotation>
                        <xsd:documentation>A string describing the version
of the type. In the case of prodml/witsml objects, this much exactly match the version attribute found in
the top-level plural object.</xsd:documentation>
                    </xsd:annotation>
                </xsd:attribute>
                <xsd:attribute name="namespace" type="xsd:string" use="optional" />
            </xsd:complexType>
            <xsd:simpleType name="SupportedOperation">
                <xsd:annotation>
                    <xsd:documentation>Enumeration which indicates the
operations supported on a given data type for a GDA server. A server can support PutData, GetData, or
both.</xsd:documentation>
```

```
                    </xsd:annotation>
                    <xsd:restriction base="xsd:string">
                        <xsd:enumeration value="GetData" />
                        <xsd:enumeration value="PutData" />
                    </xsd:restriction>
                </xsd:simpleType>
                <xsd:complexType name="GenericDataAccessCapabilities">
                    <xsd:annotation>
                        <xsd:documentation>Describes the capabilities of this
server.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="SupportedDataObjects"
type="tns:ArrayOfSupportedDataObject" />
                        <xsd:element name="Properties"
type="tns:ArrayOfNameValuePair" />
                    </xsd:sequence>
                </xsd:complexType>
                <!-- GetCapabilities -->
                <xsd:element name="GetCapabilities">
                    <xsd:annotation>
                        <xsd:documentation>SOAP Message for
GetCapabilities</xsd:documentation>
                    </xsd:annotation>
                    <xsd:complexType>
                        <xsd:sequence />
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="GetCapabilitiesResponse">
                    <xsd:annotation>
                        <xsd:documentation>SOAP Message for response from
GetCapabilities</xsd:documentation>
                    </xsd:annotation>
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="getCapabilitiesResult"
type="tns:GenericDataAccessCapabilities" minOccurs="0" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <!-- PutData -->
```

```
<xsd:complexType name="PutDataResult">
    <xsd:annotation>
        <xsd:documentation>Contains information regarding the response to a DataOperation outside of the returned data itself.</xsd:documentation>
    </xsd:annotation>
    <xsd:sequence>
        <xsd:element name="Status" type="tns:PutDataResultStatus" minOccurs="1" />
        <xsd:element name="Id" type="xsd:string" minOccurs="1" />
        <xsd:element name="SuppMsg" type="xsd:string" minOccurs="0" />
    </xsd:sequence>
</xsd:complexType>
<xsd:element name="PutData">
    <xsd:annotation>
        <xsd:documentation>SOAP Message for PutData</xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="abs:abstractDataObject" />
            <xsd:element name="options" type="tns:NameValuePair" minOccurs="0" maxOccurs="unbounded" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="PutDataResponse">
    <xsd:annotation>
        <xsd:documentation>SOAP Message for response from PutData</xsd:documentation>
    </xsd:annotation>
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="putDataResult" type="tns:PutDataResult" minOccurs="0" maxOccurs="unbounded" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<!-- Faults -->
<xsd:element name="UnsupportedOptionFault">
    <xsd:complexType>
        <xsd:sequence>
```

```
                                        <xsd:element name="OptionName"
type="xsd:string" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                            <xsd:element name="UnsupportedDataObjectFault">
                                <xsd:complexType>
                                    <xsd:sequence>
                                        <xsd:element name="DataObjectName"
type="xsd:string" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                            <xsd:element name="InvalidXPathFault">
                                <xsd:complexType>
                                    <xsd:sequence>
                                        <xsd:element name="XPath" type="xsd:string" />
                                        <xsd:element name="XPathProcessorError"
type="xsd:string" />
                                        <xsd:element name="Position" type="xsd:integer"
minOccurs="0" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                            <xsd:element name="UnknownUidFault">
                                <xsd:complexType>
                                    <xsd:sequence>
                                        <xsd:element name="Uid" type="xsd:string" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                            <xsd:element name="UnsupportedCriterionFault">
                                <xsd:complexType>
                                    <xsd:sequence>
                                        <xsd:element name="CriterionName"
type="xsd:string" />
                                    </xsd:sequence>
                                </xsd:complexType>
                            </xsd:element>
                            <xsd:element name="MissingParameterFault">
                                <xsd:complexType>
```

```
                                        <xsd:sequence>
                                                <xsd:element name="Parameter" type="xsd:string"
minOccurs="1" maxOccurs="1" />
                                        </xsd:sequence>
                                </xsd:complexType>
                        </xsd:element>
                </xsd:schema>
        </wsdl:types>
        <!-- GetCapabilities -->
        <wsdl:message name="GetCapabilitiesSoapIn">
                <wsdl:part name="parameters" element="tns:GetCapabilities" />
        </wsdl:message>
        <wsdl:message name="GetCapabilitiesSoapOut">
                <wsdl:part name="parameters" element="tns:GetCapabilitiesResponse" />
        </wsdl:message>
        <!-- PutData -->
        <wsdl:message name="PutDataSoapIn">
                <wsdl:part name="parameters" element="tns:PutData" />
        </wsdl:message>
        <wsdl:message name="PutDataSoapOut">
                <wsdl:part name="parameters" element="tns:PutDataResponse" />
        </wsdl:message>
        <!-- Faults -->
        <wsdl:message name="MissingParameterFaultMessage">
                <wsdl:part name="fault" element="tns:MissingParameterFault" />
        </wsdl:message>
        <wsdl:message name="UnsupportedOptionFaultMessage">
                <wsdl:part name="fault" element="tns:UnsupportedOptionFault" />
        </wsdl:message>
        <wsdl:message name="UnsupportedDataObjectFaultMessage">
                <wsdl:part name="fault" element="tns:UnsupportedDataObjectFault" />
        </wsdl:message>
        <wsdl:message name="InvalidXPathFaultMessage">
                <wsdl:part name="fault" element="tns:InvalidXPathFault" />
        </wsdl:message>
        <wsdl:message name="UnknownUidFaultMessage">
                <wsdl:part name="fault" element="tns:UnknownUidFault" />
        </wsdl:message>
        <wsdl:message name="UnsupportedCriterionFaultMessage">
```

```
            <wsdl:part name="fault" element="tns:UnsupportedCriterionFault" />
        </wsdl:message>
        <wsdl:portType name="PROD_GenericDataAccessSoap">
            <wsdl:operation name="GetCapabilities">
                <wsdl:input message="tns:GetCapabilitiesSoapIn"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/GetCapabilities" />
                <wsdl:output message="tns:GetCapabilitiesSoapOut"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/GetCapabilitiesResponse" />
            </wsdl:operation>
            <wsdl:operation name="PutData">
                <wsdl:input message="tns:PutDataSoapIn"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/PutData" />
                <wsdl:output message="tns:PutDataSoapOut"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/PutDataResponse" />
                <wsdl:fault name="UnsupportedOptionFault"
message="tns:UnsupportedOptionFaultMessage" />
                <wsdl:fault name="UnsupportedDataObjectFault"
message="tns:UnsupportedDataObjectFaultMessage" />
                <wsdl:fault name="UnknownUidFault"
message="tns:UnknownUidFaultMessage" />
                <wsdl:fault name="MissingParameterFault"
message="tns:MissingParameterFaultMessage" />
            </wsdl:operation>
        </wsdl:portType>
        <wsdl:binding name="PROD_GenericDataAccessSoap"
type="tns:PROD_GenericDataAccessSoap">
            <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
            <!-- GetCapabilities Operation -->
            <wsdl:operation name="GetCapabilities">
                <soap:operation
soapAction="http://www.prodml.org/api/210/genericDataAccess/GetCapabilities" style="document" />
                <wsdl:input>
                    <soap:body use="literal" />
                </wsdl:input>
                <wsdl:output>
                    <soap:body use="literal" />
                </wsdl:output>
            </wsdl:operation>
            <!-- PutData Operation -->
            <wsdl:operation name="PutData">
                <soap:operation
soapAction="http://www.prodml.org/api/210/genericDataAccess/PutData" style="document" />
                <wsdl:input>
                    <soap:body use="literal" />
```

```
                    </wsdl:input>
                    <wsdl:output>
                        <soap:body use="literal" />
                    </wsdl:output>
                    <wsdl:fault name="UnsupportedOptionFault">
                        <soap:fault use="literal" name="UnsupportedOptionFault" />
                    </wsdl:fault>
                    <wsdl:fault name="UnsupportedDataObjectFault">
                        <soap:fault use="literal" name="UnsupportedDataObjectFault" />
                    </wsdl:fault>
                    <wsdl:fault name="UnknownUidFault">
                        <soap:fault use="literal" name="UnknownUidFault" />
                    </wsdl:fault>
                    <wsdl:fault name="MissingParameterFault">
                        <soap:fault use="literal" name="MissingParameterFault" />
                    </wsdl:fault>
                </wsdl:operation>
        </wsdl:binding>
        <wsdl:service name="PROD_GenericDataAccess">
                <wsdl:port name="PROD_GenericDataAccessSoap"
binding="tns:PROD_GenericDataAccessSoap">
                    <soap:address location="http://127.0.0.1:7521/" />
                </wsdl:port>
        </wsdl:service>
</wsdl:definitions>
```

12. Appendix – PRODML WSDL with X.509 Token Profile

```
<?xml version="1.0" encoding="utf-8"?>
<wsdl:definitions
        name="GenericDataAccess"
        targetNamespace="http://www.prodml.org/api/210/genericDataAccess"
        xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
        xmlns:tns="http://www.prodml.org/api/210/genericDataAccess"
        xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl"
        xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
        xmlns:abs="http://www.energistics.org/schemas/abstract" >
        <!--                                    -->
```

```
<wsp:Policy wsu:Id="SigEncr"
        xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"
        xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
>
        <wsp:ExactlyOne>
                <wsp:All>
                        <sp:AsymmetricBinding
                        xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
                        >
                                <wsp:Policy>
                                        <sp:InitiatorToken>
                                                <wsp:Policy>
                                                        <sp:X509Token sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/AlwaysToRecipient">
                                                                <wsp:Policy>
        <sp:RequireThumbprintReference />
                                                                <sp:WssX509V3Token10 />
                                                                </wsp:Policy>
                                                        </sp:X509Token>
                                                </wsp:Policy>
                                        </sp:InitiatorToken>
                                        <sp:RecipientToken>
                                                <wsp:Policy>
                                                        <sp:X509Token sp:IncludeToken="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy/IncludeToken/Never">
                                                                <wsp:Policy>
        <sp:RequireThumbprintReference />
                                                                <sp:WssX509V3Token10 />
                                                                </wsp:Policy>
                                                        </sp:X509Token>
                                                </wsp:Policy>
                                        </sp:RecipientToken>
                                        <sp:AlgorithmSuite>
                                                <wsp:Policy>
                                                <sp:Basic256 />
                                                </wsp:Policy>
```

```
                    </sp:AlgorithmSuite>
                    <sp:Layout>
                        <wsp:Policy>
                        <sp:Strict />
                        </wsp:Policy>
                    </sp:Layout>
                <sp:IncludeTimestamp />
                <sp:OnlySignEntireHeadersAndBody />
                </wsp:Policy>
            </sp:AsymmetricBinding>
            <sp:Wss11
            xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
            >
                <sp:Policy>
                <sp:MustSupportRefKeyIdentifier />
                <sp:MustSupportRefIssuerSerial />
                <sp:MustSupportRefThumbprint />
                <sp:RequireSignatureConfirmation />
                </sp:Policy>
            </sp:Wss11>
            <sp:Wss10
            xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
            >
                <sp:Policy>
                <sp:MustSupportRefKeyIdentifier />
                <sp:MustSupportRefIssuerSerial />
                </sp:Policy>
            </sp:Wss10>
            <sp:SignedParts
            xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
            >
            <sp:Body />
            </sp:SignedParts>
            <sp:EncryptedParts
            xmlns:sp="http://schemas.xmlsoap.org/ws/2005/07/securitypolicy"
            >
            <sp:Body />
            </sp:EncryptedParts>
        </wsp:All>
```

```
            </wsp:ExactlyOne>
        </wsp:Policy>
        <!-- Energistics License Agreement
        This file is distributed under the Energistics License Agreement at
        http://www.energistics.org
        Use of this file constitutes agreement with the Energistics License Agreement.
        Copyright (c) 2008-2011 Energistics. All rights reserved.
        Energistics, WITSML, PRODML and RESQML are trademarks or registered trademarks of
Energistics.
        -->
        <!--                                    -->
        <wsdl:types>
            <xsd:schema targetNamespace="http://www.prodml.org/api/210/genericDataAccess"
elementFormDefault="qualified">
                <xsd:import namespace="http://www.energistics.org/schemas/abstract"
schemaLocation="http://w3.energistics.org/schema/abstract_v1.0/xsd_schemas/sub_abstractSubstitutio
nGroup.xsd" />
                <xsd:complexType name="NameValuePair">
                    <xsd:annotation>
                        <xsd:documentation>A generic structure for option values
that are not specified in schema.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="Name" type="xsd:string" minOccurs="1"
/>
                        <xsd:element name="Value" type="xsd:string" minOccurs="1"
/>
                    </xsd:sequence>
                </xsd:complexType>
                <xsd:complexType name="ArrayOfNameValuePair">
                    <xsd:annotation>
                        <xsd:documentation>A collection of generic option
values.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="NameValuePair"
type="tns:NameValuePair" minOccurs="0" maxOccurs="unbounded" />
                    </xsd:sequence>
                </xsd:complexType>
                <xsd:simpleType name="PutDataResultStatus">
                    <xsd:annotation>
                        <xsd:documentation>An enumeration which specifies the
status of a PutData operation with a data-object.</xsd:documentation>
```

```
                    </xsd:annotation>
                    <xsd:restriction base="xsd:string">
                        <xsd:enumeration value="Added" />
                        <xsd:enumeration value="Updated" />
                    </xsd:restriction>
                </xsd:simpleType>
                <xsd:complexType name="ArrayOfSupportedDataObject">
                    <xsd:annotation>
                        <xsd:documentation>A collection of SupportedDataObject
objects.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="SupportedDataObject"
type="tns:SupportedDataObject" minOccurs="0" maxOccurs="unbounded" />
                    </xsd:sequence>
                </xsd:complexType>
                <xsd:complexType name="SupportedDataObject">
                    <xsd:annotation>
                        <xsd:documentation>Describes a single element or data type
supported by a GenericDataAccess server.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="Name" type="xsd:string"
minOccurs="1">
                            <xsd:annotation>
                                <xsd:documentation>The name of the type.
This should be exactly the same as the local name (sans namespace) of the supported element or
type.</xsd:documentation>
                            </xsd:annotation>
                        </xsd:element>
                        <xsd:element name="SupportedOperation"
type="tns:SupportedOperation" minOccurs="0" maxOccurs="2" />
                    </xsd:sequence>
                    <xsd:attribute name="version" type="xsd:string" use="optional">
                        <xsd:annotation>
                            <xsd:documentation>A string describing the version
of the type. In the case of prodml/witsml objects, this much exactly match the version attribute found in
the top-level plural object.</xsd:documentation>
                        </xsd:annotation>
                    </xsd:attribute>
                    <xsd:attribute name="namespace" type="xsd:string" use="optional" />
                </xsd:complexType>
                <xsd:simpleType name="SupportedOperation">
```

```
<xsd:annotation>
<xsd:documentation>Enumeration which indicates the operations supported on a given data type for a GDA server. A server can support PutData, GetData, or both.</xsd:documentation>
</xsd:annotation>
<xsd:restriction base="xsd:string">
<xsd:enumeration value="GetData" />
<xsd:enumeration value="PutData" />
</xsd:restriction>
</xsd:simpleType>
<xsd:complexType name="GenericDataAccessCapabilities">
<xsd:annotation>
<xsd:documentation>Describes the capabilities of this server.</xsd:documentation>
</xsd:annotation>
<xsd:sequence>
<xsd:element name="SupportedDataObjects" type="tns:ArrayOfSupportedDataObject" />
<xsd:element name="Properties" type="tns:ArrayOfNameValuePair" />
</xsd:sequence>
</xsd:complexType>
<!-- GetCapabilities -->
<xsd:element name="GetCapabilities">
<xsd:annotation>
<xsd:documentation>SOAP Message for GetCapabilities</xsd:documentation>
</xsd:annotation>
<xsd:complexType>
<xsd:sequence />
</xsd:complexType>
</xsd:element>
<xsd:element name="GetCapabilitiesResponse">
<xsd:annotation>
<xsd:documentation>SOAP Message for response from GetCapabilities</xsd:documentation>
</xsd:annotation>
<xsd:complexType>
<xsd:sequence>
<xsd:element name="getCapabilitiesResult" type="tns:GenericDataAccessCapabilities" minOccurs="0" />
</xsd:sequence>
```

```
                    </xsd:complexType>
                </xsd:element>
                <!-- PutData -->
                <xsd:complexType name="PutDataResult">
                    <xsd:annotation>
                        <xsd:documentation>Contains information regarding the
response to a DataOperation outside of the returned data itself.</xsd:documentation>
                    </xsd:annotation>
                    <xsd:sequence>
                        <xsd:element name="Status" type="tns:PutDataResultStatus"
minOccurs="1" />
                        <xsd:element name="Id" type="xsd:string" minOccurs="1" />
                        <xsd:element name="SuppMsg" type="xsd:string"
minOccurs="0" />
                    </xsd:sequence>
                </xsd:complexType>
                <xsd:element name="PutData">
                    <xsd:annotation>
                        <xsd:documentation>SOAP Message for
PutData</xsd:documentation>
                    </xsd:annotation>
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element ref="abs:abstractDataObject" />
                            <xsd:element name="options"
type="tns:NameValuePair" minOccurs="0" maxOccurs="unbounded" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <xsd:element name="PutDataResponse">
                    <xsd:annotation>
                        <xsd:documentation>SOAP Message for response from
PutData</xsd:documentation>
                    </xsd:annotation>
                    <xsd:complexType>
                        <xsd:sequence>
                            <xsd:element name="putDataResult"
type="tns:PutDataResult" minOccurs="0" maxOccurs="unbounded" />
                        </xsd:sequence>
                    </xsd:complexType>
                </xsd:element>
                <!-- Faults -->
```

```
<xsd:element name="UnsupportedOptionFault">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="OptionName"
type="xsd:string" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="UnsupportedDataObjectFault">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="DataObjectName"
type="xsd:string" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="InvalidXPathFault">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="XPath" type="xsd:string" />
            <xsd:element name="XPathProcessorError"
type="xsd:string" />
            <xsd:element name="Position" type="xsd:integer"
minOccurs="0" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="UnknownUidFault">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="Uid" type="xsd:string" />
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="UnsupportedCriterionFault">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="CriterionName"
type="xsd:string" />
        </xsd:sequence>
    </xsd:complexType>
```

```
                    </xsd:element>
                    <xsd:element name="MissingParameterFault">
                        <xsd:complexType>
                            <xsd:sequence>
                                <xsd:element name="Parameter" type="xsd:string"
minOccurs="1" maxOccurs="1" />
                            </xsd:sequence>
                        </xsd:complexType>
                    </xsd:element>
                </xsd:schema>
            </wsdl:types>
            <!-- GetCapabilities -->
            <wsdl:message name="GetCapabilitiesSoapIn">
                <wsdl:part name="parameters" element="tns:GetCapabilities" />
            </wsdl:message>
            <wsdl:message name="GetCapabilitiesSoapOut">
                <wsdl:part name="parameters" element="tns:GetCapabilitiesResponse" />
            </wsdl:message>
            <!-- PutData -->
            <wsdl:message name="PutDataSoapIn">
                <wsdl:part name="parameters" element="tns:PutData" />
            </wsdl:message>
            <wsdl:message name="PutDataSoapOut">
                <wsdl:part name="parameters" element="tns:PutDataResponse" />
            </wsdl:message>
            <!-- Faults -->
            <wsdl:message name="MissingParameterFaultMessage">
                <wsdl:part name="fault" element="tns:MissingParameterFault" />
            </wsdl:message>
            <wsdl:message name="UnsupportedOptionFaultMessage">
                <wsdl:part name="fault" element="tns:UnsupportedOptionFault" />
            </wsdl:message>
            <wsdl:message name="UnsupportedDataObjectFaultMessage">
                <wsdl:part name="fault" element="tns:UnsupportedDataObjectFault" />
            </wsdl:message>
            <wsdl:message name="InvalidXPathFaultMessage">
                <wsdl:part name="fault" element="tns:InvalidXPathFault" />
            </wsdl:message>
            <wsdl:message name="UnknownUidFaultMessage">
```

```
            <wsdl:part name="fault" element="tns:UnknownUidFault" />
        </wsdl:message>
        <wsdl:message name="UnsupportedCriterionFaultMessage">
            <wsdl:part name="fault" element="tns:UnsupportedCriterionFault" />
        </wsdl:message>
        <wsdl:portType name="PROD_GenericDataAccessSoap">
            <wsdl:operation name="GetCapabilities">
                <wsdl:input message="tns:GetCapabilitiesSoapIn"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/GetCapabilities" />
                <wsdl:output message="tns:GetCapabilitiesSoapOut"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/GetCapabilitiesResponse" />
            </wsdl:operation>
            <wsdl:operation name="PutData">
                <wsdl:input message="tns:PutDataSoapIn"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/PutData" />
                <wsdl:output message="tns:PutDataSoapOut"
wsaw:Action="http://www.prodml.org/api/210/genericDataAccess/PutDataResponse" />
                <wsdl:fault name="UnsupportedOptionFault"
message="tns:UnsupportedOptionFaultMessage" />
                <wsdl:fault name="UnsupportedDataObjectFault"
message="tns:UnsupportedDataObjectFaultMessage" />
                <wsdl:fault name="UnknownUidFault"
message="tns:UnknownUidFaultMessage" />
                <wsdl:fault name="MissingParameterFault"
message="tns:MissingParameterFaultMessage" />
            </wsdl:operation>
        </wsdl:portType>
        <wsdl:binding name="PROD_GenericDataAccessSoap"
type="tns:PROD_GenericDataAccessSoap">
            <wsp:PolicyReference URI="#SigEncr"
            xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy"
            />
            <soap:binding transport="http://schemas.xmlsoap.org/soap/http" />
            <!-- GetCapabilities Operation -->
            <wsdl:operation name="GetCapabilities">
                <soap:operation
soapAction="http://www.prodml.org/api/210/genericDataAccess/GetCapabilities" style="document" />
                <wsdl:input>
                    <soap:body use="literal" />
                </wsdl:input>
                <wsdl:output>
                    <soap:body use="literal" />
                </wsdl:output>
```

```
            </wsdl:operation>
            <!-- PutData Operation -->
            <wsdl:operation name="PutData">
                  <soap:operation
soapAction="http://www.prodml.org/api/210/genericDataAccess/PutData" style="document" />
                  <wsdl:input>
                        <soap:body use="literal" />
                  </wsdl:input>
                  <wsdl:output>
                        <soap:body use="literal" />
                  </wsdl:output>
                  <wsdl:fault name="UnsupportedOptionFault">
                        <soap:fault use="literal" name="UnsupportedOptionFault" />
                  </wsdl:fault>
                  <wsdl:fault name="UnsupportedDataObjectFault">
                        <soap:fault use="literal" name="UnsupportedDataObjectFault" />
                  </wsdl:fault>
                  <wsdl:fault name="UnknownUidFault">
                        <soap:fault use="literal" name="UnknownUidFault" />
                  </wsdl:fault>
                  <wsdl:fault name="MissingParameterFault">
                        <soap:fault use="literal" name="MissingParameterFault" />
                  </wsdl:fault>
            </wsdl:operation>
      </wsdl:binding>
      <wsdl:service name="PROD_GenericDataAccess">
            <wsdl:port name="PROD_GenericDataAccessSoap"
binding="tns:PROD_GenericDataAccessSoap">
                  <soap:address location="http://127.0.0.1:7521/" />
            </wsdl:port>
      </wsdl:service>
</wsdl:definitions>
```

The Annual Conference on Management and Information Technology (ACMIT) 2014

Risk Assessment of Core Banking System Replacement based on ISACA Framework

Fenty Simanjuntak

Master of Information Technology, Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia

Email: Fenty_sim@yahoo.com

Bobby Suryajaya

Master of Information Technology, Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia

Email: bobby.suryajaya@gmail.com

Abstract

Many banks are looking for a better core banking system to support their business growth with a more efficient and flexible core banking system to improve their sales and services in the competitive market and to fulfill regulatory requirements. The decision of replacing the legacy core banking system is difficult due to the high IT investment cost required for banks because they are also trying to cut costs. But maintaining the legacy system is costly in terms of upgrade. Changing the core banking system is also a difficult process and increases risks. To have a successful Core Banking System implementation, risk assessment is required to be performed prior to starting any activities. The assessment can help project teams to identify the risks and then to mitigate the risks as part of the plan. In this research the Core Banking System replacement risks were assessed based on ISACA Framework for IT Risk. Fourteen risk scenarios related to Core Banking System Replacement were identified. The high and medium rated inherent risks can become medium and low residual risk after assessment by putting the relevant control in place. The result proves that by adding mitigation plan it will help to mitigate the Residual Risk to become low risk. There are still three residual risk which categorized as medium risk and should be further mitigated they are Software Implementation, Project Delivery and Selection/Performance of Third Party Suppliers. It is also found that COBIT 5 has considered some specific process capabilities that can be used to improve the processes to mitigate the medium risks.

Keywords: IT Risk; ISACA; COBIT; Residual Risk; Inherent Risk; Core Banking System

Introduction

A core banking system is the back-end data processing application for processing all transactions that have occurred during the day and posting updated data on account balances to the mainframe. Core systems typically include deposit account and CD account processing, loan and credit processing, interfaces to the general ledger and reporting tools [1].

Changing the core banking system is a difficult process and increases risk. To have a successful implementation, risk assessment is required to be conducted before selecting and implementing the new core banking system.

The Banking Systems Market Survey results for 2012/13 indicated the following IT trends in the banking industry [2]:

- Of the respondents, 34% intend to replace their platforms; of these, 74% intend to move to packages.
- The pressure on bank IT budgets over the past five and two years is notable.
- There is considerable activity within "satellite" systems, such as payments and channels.
- Banks are placing high importance on data warehousing and business intelligence technology.
- Social media is not making a great impact on most banks as yet (other than in Southeast Asia).

Risk management can have a positive impact on selecting projects, determining the scope of project, and developing realistic schedules and cost estimates [3].

The benefit of Core Banking System replacement will help the bank achieve its business growth plan and contribute to superior sales and services to customers [4]. They are:

1. Resolving the current system constraints such as:
    - Operational instability that impacts not just branches and customers, but also the growing importance of electronic channels in Internet and mobile banking.
    - Inability to support business growth: number of customers/CIFs, number of products per customer, and transaction volumes.

- . Inability to support evolving products and services required for business growth.

2. Resolving regulatory pain points related to manual processes and lack of automated controls that lead to high operational risk, reconcilement issues with the enterprise GL, and regulatory reporting process.
3. Increasing the level of customer service by providing a sales and service platform that will enable bank's customer-facing staff to improve customer experience and increased ability to develop Cross Products.
4. Improving electronic channel capability to meet the needs of the targeted customer segment.
5. Changing the business processes to be more productive and effective by automating manual processes and controls, improving the operational risk, providing opportunities for staff to perform more value -added activities and improving customer service.

Research Framework

In this paper, ISACA framework is used to do the risk assessment and COBIT5 is used to improve the process capability. ISACA framework is used because it provides an end-to-end, comprehensive view of all risks related to the use of IT and a similarly thorough treatment of risk management, from the tone and culture at the top, to operational issues. The framework can be used to understand and manage all significant IT risk types, building upon the existing risk related components within the other ISACA frameworks, i.e., COBIT and Val IT [5].

COBIT 5 provides the next generation of ISACA's guidance on the enterprise governance and management of IT. It builds on more than 15 years of practical usage and application of COBIT by many enterprises and users from business, IT, risk, security, and assurance community.

Other frameworks that were also considered to be used in this paper beside ISACA-COBIT were ITIL, COSO, ISO 31000:2009, ISO 27005:2008, etc. However, those frameworks may not be able to provide an end-to-end, comprehensive view of all risks related to Core Banking System replacement.

Research Methodology

This research consists of several stages, beginning with defining the research questions, and whether the risk assessment based on ISACA Framework can be used to identify risks and identify controls to reduce the risks.

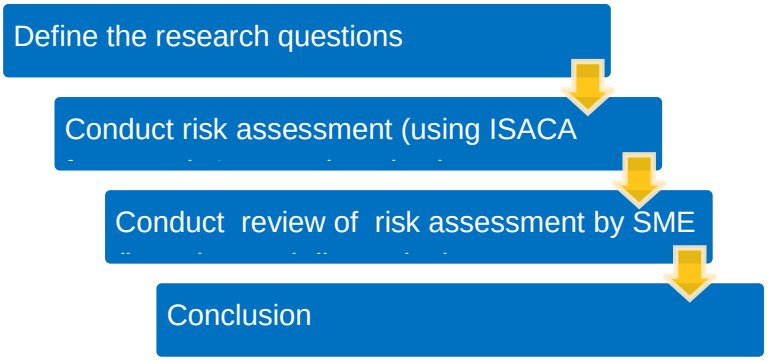


Fig1. Research Stages

Next, risk assessment was conducted based on The Risk IT Practitioner Guide [4] as shown in figure 2 and secondary data (project documentation) from Bank X.

Using ISACA Framework for IT Risk, the processes to identify risk are as follows:

- IT Risk Scenarios development
- Estimate Frequency and Impact
- Risk Response
- Risk Action Plan

ISACA in the IT Risk IT Practitioner Guide [5] provided the 36 (thirty six) IT Risk Scenarios (page 59). The risk scenarios relevant to the Core Banking System Replacement project were identified. Then the frequency and impact of each risk were calculated

Frequency or Likelihood is number of times in a given period usually in a year that an event is likely to occur. Impact is the business consequence of the scenario. The frequency and impact and risk rating will be assessed using established operational risk guidelines of the bank.

For example, for the Major impact and Possible likelihood, the risk rating is High. Before putting control in place, the inherent risk was determined. After putting the control in place for the current situation, the residual risk became known.

For the residual risk that was identified, the risk response needed to be defined. Risk response will be in line with the risk appetite and tolerance of the bank. There are four types of risk response:

- Risk acceptance
- Risk sharing/transfer
- Risk mitigation
- Risk avoidance

Risk acceptance means the risk is recognized and loss is accepted but no action will be taken. Usually the risk is low with insignificant impact.

Risk sharing/transfer is reducing risk by transferring the risk to another party, such as insurance or outsourcing.

Risk mitigation is mitigation action needed to reduce the risk. Usually an action plan is needed for mitigating risk such as putting other control processes to reduce either the frequency of events and/or the business impact as defined by ISACA framework or strengthening the process capability as considered by COBIT5 [6].

Risk avoidance is to avoid risk by applying other activities or conditions when no other response is adequate.

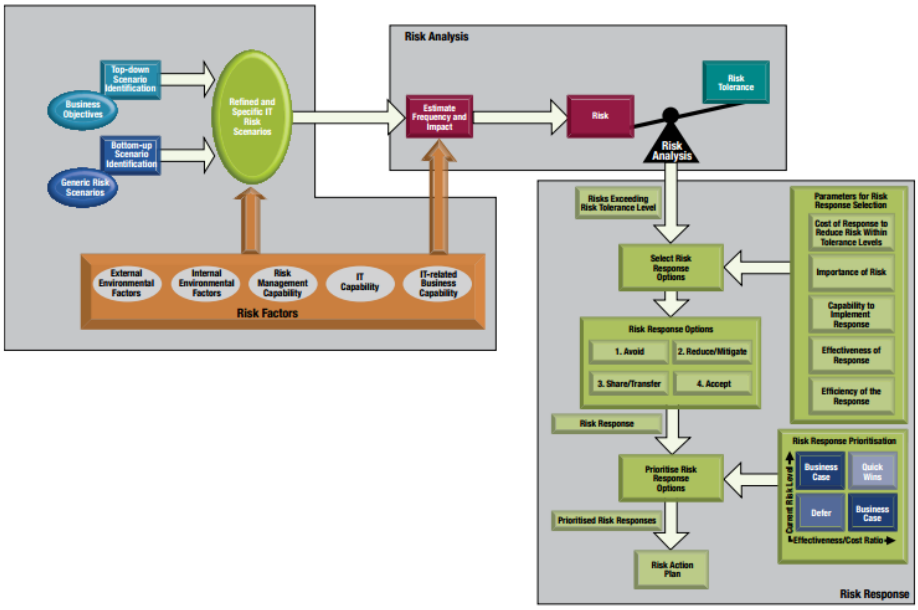


Fig 2.Risk Analysis & Risk Response Overview [5]

Next, Subject Matter Expert of Bank X reviewed the risk assessment through interview and discussion. The results are summarized in the conclusion.

Results & Analysis

The first step was to identify the risk scenarios related to Core Banking System (CBS) replacement out of fourteen scenarios. From the fourteen scenarios, the likelihood and impact were determined. For example, High Level Risk Scenario is IT project economics risk. The negative example scenarios given are:

- Isolated project budget overrun
- Inconsistent and important IT projects budget overruns
- Absence of view on portfolio and project economics.

In terms of CBS replacement, this scenario is relevant. By choosing the CBS replacement as one of the IT programme, there may be risk assosiated with it. The impact

will be major, because it will impact Financial Loss and the inherent risk is High, using Bank X Operational Risk 5 by 5 Matrix [7].

Controls currently in place at the bank were identified, which reduced the likelihood and impact. It was found that there some essential controls are in place according to Bank X Operational Risk Report [8], such as:

- The bank has implemented a cost management process comparing actual costs to budgets. Costs are monitored and reported to the Steering Committee, which is composed of the President Director and member of the Board of Directors.
- The Steering Committee monitors and controls project execution, including project budget usage
    - There are also two working groups under the Steering Committee, which are the Executive Working Committee and the Executive Project Delivery Committee
    - Both committees will control project execution from an implementation and business requirement fulfillment perspective.
- Core Banking Software (CBS) project is one of the agenda for Board of Commissioner meeting to seek guidance from the commissioner member.
- There is a dedicated Financial Controller who strictly monitors the project budget and expenses. The Project Manager periodically reviews the project budget and expenses to avoid any unnecessary expenses.
- Minimum customization approach for CBS is to avoid additional implementation cost and reduce project delivery risk. Every customization needs to be approved by the Steering Committee.
- An external party as QA does a periodic review of internal project processes, including project expenses.
- Every unexpected expense that uses a contingency budget has to go through the approval process from the Steering Committee and other project governance bodies.
- Bank X periodically reviews of contingency budget to release part of contingency budget along with project execution where more detail information is gathered for more detailed project planning. Periodic review is held at the end of each phase.

Due to the high impact controls in place, the risk becomes minor therefore it is unlikely to happen. Therefore, the residual risk becomes low.

After assessing all the risks of Core Banking System replacement, the result is described in the Risk Heat Map figure below:

- 11-risks are inherently rated as High Risk
- 3-risks are inherently rated as Medium Risk

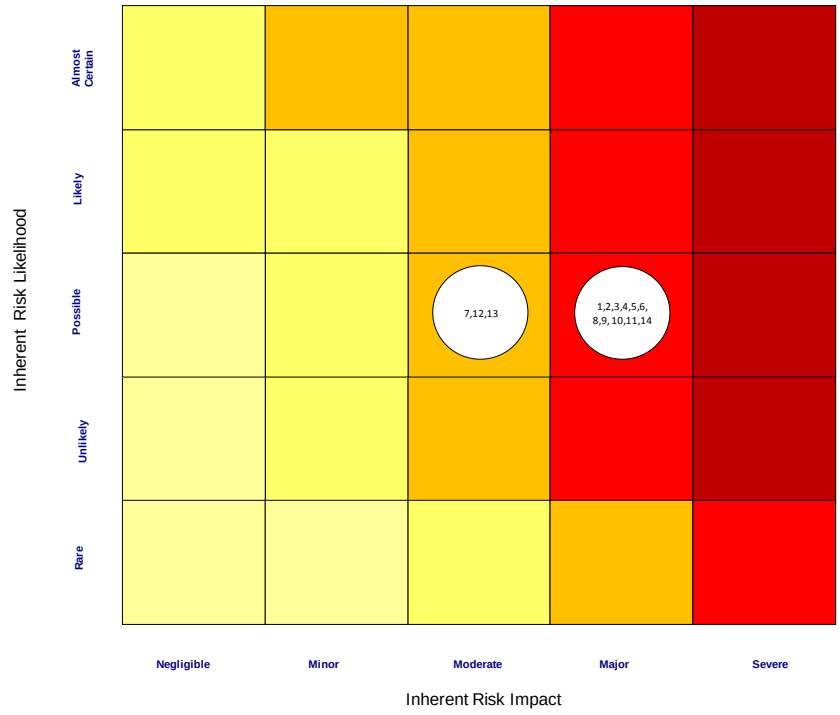


Fig 3. Inherent Risk of Core Banking System Replacement Heat Map

Risk is rated based on color from light to dark as Insignificant, Low, Medium, High, and Very High.

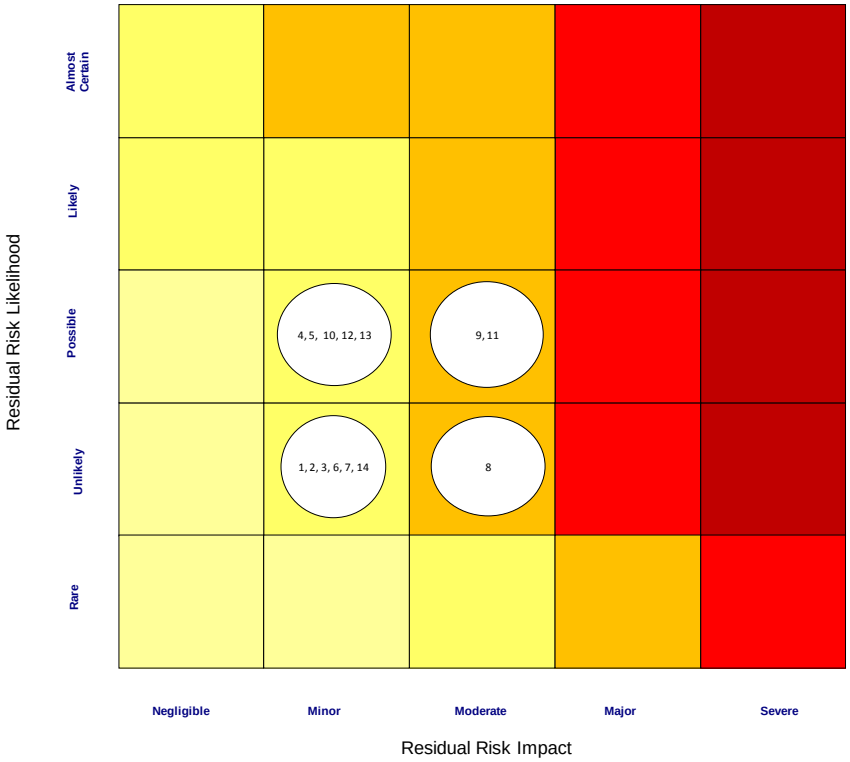


Fig 4. Residual Risk of Core Banking System Replacement Heat Map

After assessing the Control in Place for the High & Medium Risks, the Residual Risk becomes Medium & Low.

- 11-risks are rated as Low Risk
- 3-risks are rated as Medium Risk

Using COBIT 5, the Medium Residual Risk will be mitigated by adding some action plans. For example,,to reduce the project delivery risk, the project team plans to monitor the performance of the overall project including the contributions of the business and IT functions of the project and report to the project steering committee in a timely, complete and accurate manner. Escalation to management team is needed for any deviation of the plan. This action is essential control and has High effect on Impact. The risk becomes low due to reduced impact to minor eventhough the likelihood is still possible.

The table below summarizes all the risks identified, the impact, the likelihood and the Residual Risk after analysis.

Table 1. Summary Residual Risk of Core Banking System Replacement

No	Risks	Impact	Likelihood	Residual Risk
1	IT Programme selection	Minor	Unlikely	Low
2	New Technologies	Minor	Unlikely	Low
3	Technology Selection	Minor	Unlikely	Low
4	IT Investment decision making	Minor	Possible	Low
5	IT project termination	Minor	Possible	Low
6	IT project economics	Minor	Unlikely	Low
7	Architecture agility and flexibility	Minor	Unlikely	Low
8	Software implementation	Moderate	Unlikely	Medium
9	Project delivery	Moderate	Possible	Medium
10	Project quality	Minor	Possible	Low
11	Selection/performance of third party suppliers	Moderate	Possible	Medium
12	IT Staff	Minor	Possible	Low
13	IT expertise and skills	Minor	Possible	Low
14	Software performance	Minor	Unlikely	Low

Some risks are low due to the bank already having some controls in place, such as:

1. CBS Replacement is aligned with enterprise strategy and priorities.
2. Design Review Board provides architecture guidelines and advice on the software application and to verify compliance.
3. The Steering Committee monitors the key project performance such as scope, schedule, quality, cost and risk.
4. A cost management process has been established to compare actual cost to budget. There is a dedicated financial controller to monitor the project cost.

5. Quality management plan is established thatshows the project quality system and reviewed and agreed by all parties. The usage of Requirement Traceability Matrix is to ensure the solution are met with initial requirements.
6. A change management plan is established in line with organizational change management. Training and transfer knowledge is delivered to the users and IT team.
7. Suppliers were selected according to procurement policy and procedure. The performance is monitored to ensure the suppliers are meeting the business requirements.
8. IT personnel recruitment processes are in line with HR policies and procedures. The needs of external/vendor is to supplement the lack of IT related skills within IT due to new technologies.
9. Monitoring tools will be implemented to monitor the performance and capacity of IT resources. Perform the non-functional test, regression test, and production simulation and rehearsal test to ensure the software performance.

There are 3 (three) residual risks that still need to be mitigated, which are:

1. Software implementation risk
2. Project delivery risk
3. Selection/performance of third party suppliers risk

To mitigate the above risks, COBIT 5 as described in Appendix C. Mapping Examples Risk Scenarios to COBIT 5 Processes, page 67-70 [6] has considered some improvement in the relevant processes for each risk. For Software implementation risk, there are 8 (eight) COBIT5 process capabilities that can be improved.

Table 2. Software Implementation Risk with COBIT 5 Process Capabilities

COBIT 5 Process Capabilities	Process to be improved
APO11	Consistent and effective quality management activities
BAI01	Project management
BAI02	Requirements definitions
BAI03	Solution development
BAI05	Managing organizational changes with regards to software implementation
BAI06	Change management
BAI07	Extensive solution testing
BAI08	Knowledge support

Conclusion

Bank X has assessed the risk of Core Banking System Replacement prior to the project starting and is documented in the Business Case.

Based on discussion with Subject Matter Expert, out of fourteen risks identified using ISACA Risk Scenarios, there are still three medium residual risks should be further mitigated: Software Implementation, Project Delivery and Selection/Performance of Third Party Supplier Risk.

Risk Assessment using ISACA Framework is proven to be capable of identifying the risks for Core Banking Replacement and help the company to identify some controls to mitigate the risks. The risks scenarios will depend on the current condition of the bank.

It is also found that COBIT5 has some specific process capabilities that can be used to improve the processes to mitigate the medium risks.

Recommendations

More research is required for further analysis of the IT risks using different framework and adding more risks scenarios for a successful Core Banking System project.

Meanwhile, Surveys from other banks, which had similar experiences can help to improve the risks scenarios and risks mitigation.

Further research may also need to focus on responding to medium risks based on missing or inadequate as suggested by COBIT5 processes.

Acknowledgments

The authors wish to thank the Head of Core Banking System Transformation Program, the Head of IT Architect & Design and the Head of Operational Risk of Bank X for their full support in this research.

References

[1] Jayamaha, Ranee. "Impact of IT in the Banking Sector." *Speech by Dr Ranee Jayamaha, Deputy Governor of the Central Bank of Sri Lanka* (2008).

[2] Gartner Research. *IT Glossary - Core Banking System*. Gartner Research. 2012.

[3] IBS Intelligence. *Banking Systems Market Survey*. 2012/13.

[4] Schwalbe, Kathy. *Information Technology Project Management, Revised*. Cengage Learning, 2010.

[5] Liu, Rong, Frederick Wu, Yasodhar Patnaik, and Santhosh Kumaran. "Business Entities: An SOA Approach to progressive core banking renovation." In *Services Computing, 2009. SCC'09. IEEE International Conference on*, pp. 466-473. IEEE, 2009.

[6] Racz, Nicolas, Edgar R. Weippl, Andreas Seufert, and T. U. Wien. "Questioning the Need for Separate IT Risk Management Frameworks." In *GI Jahrestagung (2)*, pp. 245-252. 2010.

[7] Evelina, E., G. Pia, H. David, M. von Wurtemberg Liv, and ROCHA FLORES Waldo. "Process improvement framework evaluation." In *Management Science and Engineering (ICMSE), 2010 International Conference on*, pp. 319-326. IEEE, 2010.

[8] Gheorghe, Mirela. "Audit Methodology for IT Governance." *Informatica Economica* 14, no. 1 (2010).

[9] Bank X. *Business Case - Core Banking Project*. 2012.

[10] ISACA. *Risk IT Practitioner Guide*. 2009.

[11] ISACA. *COBIT® 5 Implementation*. 2012.

[12] Bank X. *Operational Risk 5 by 5 Risk Matrix*. 2011.

[13] Bank X. *Operational Risk Report - Core Banking Project*. 2012.

Glossary

Business Case is a document to describe the business background, reason and objectives for initiating a project. It is often presented in a well-structured written document about the project strategy, project scope, high-level business stakeholder requirements, benefit realization, financial summary, and project delivery approach and organization change management of a proposed project.

COBIT is a framework created by ISACA for information technology (IT) management and IT governance. It is also provided by a supporting toolset that allows managers to identify the gap between control requirements, technical issues and business risks.

Core Banking System (CBS) is the back-end system which processing banking customer transactions of banking products/services and interfaces to other systems, such as general ledger, payment, reporting tools, etc.

Heat Map is a two-dimensional representation of data in which values are represented by colors, usually using darker colors to indicate high risk and brighter colors to indicate low risk.

Inherent Risk is the risk when no controls have been put in place.

ISACA is a nonprofit, independent association that advocates for professionals involved in information security, assurance, risk management and governance.

Residual Risk is the risk remains after putting controls in place.

The Annual Conference on Management and Information Technology (ACMIT) 2014

Implementation: Information Security Management System (ISMS) ISO 27001:2005 at Perbanas University

IGN Mantra, M.Kom*

**Informatics Engineering, ABFII Perbanas Institute, Jakarta, Indonesia*

ignmantra@gmail.com, ign.mantra@perbanasinstitute.ac.id

Abstract

There is a need for an Information Security Management System Standard (ISO 27001:2005) at Perbanas University in general. Particularly ABFII Perbanas needs IT governance on Information Security. ISO 27001:2005 is an Information Security Standard that widely used as Information Security Management System (ISMS). IT Governance approach is the main interest within ISO 27001:2005 for Perbanas University.

Keywords : Information Security Management System (ISMS); ISO 27001:2005; IT Governance;

1. Introduction

Technology Advancement allows everyone to access information. Security Vulnerability is by product of networked system, therefore security approach must be developed to prevent such vulnerability.Information Systems Security is an attempt to secure information assets against threats that may arise. The importance of information security will indirectly ensure business continuity, reducing the risks that occur, and optimize the Information Security Design and Implementation. A lot of corporate information is stored, managed, and shared, therefore it is becoming greater risk for damage, loss or exposure of data to unwanted outsiders.

1.1 Background

The methods and technologies to secure the information can be done in many ways, ranging from simple to complex, and from low to high cost. Each of these methods and the associated technologies have advantages and disadvantages.

For ease in designing and implementing information security systems, the university needs guidelines. These guidelines are the minimum standard requirements that must be met in an information security system. In addition to uniformity as a standard for the university, these guidelines will facilitate the planning and technical costs.
On Perbanas Institute Vision 2019, "To be the Most Reputable Asian Banking Education Institute that aims to be Top 5 Asian Banker's Center of Excellence. By 2019 Most of our Alumni will have been Professionally Employed within 6 Months after their Graduation", and one of Perbanas mission part, "Developing Continuous Professional Education and Certification". To support those goals, the application of ISO 9001:2008 (reached 2012) and ISMS /ISO 27001:2005 (on planning), the Perbanas Institute Vision 2019 is a must that can be seen in the figure 1.0.

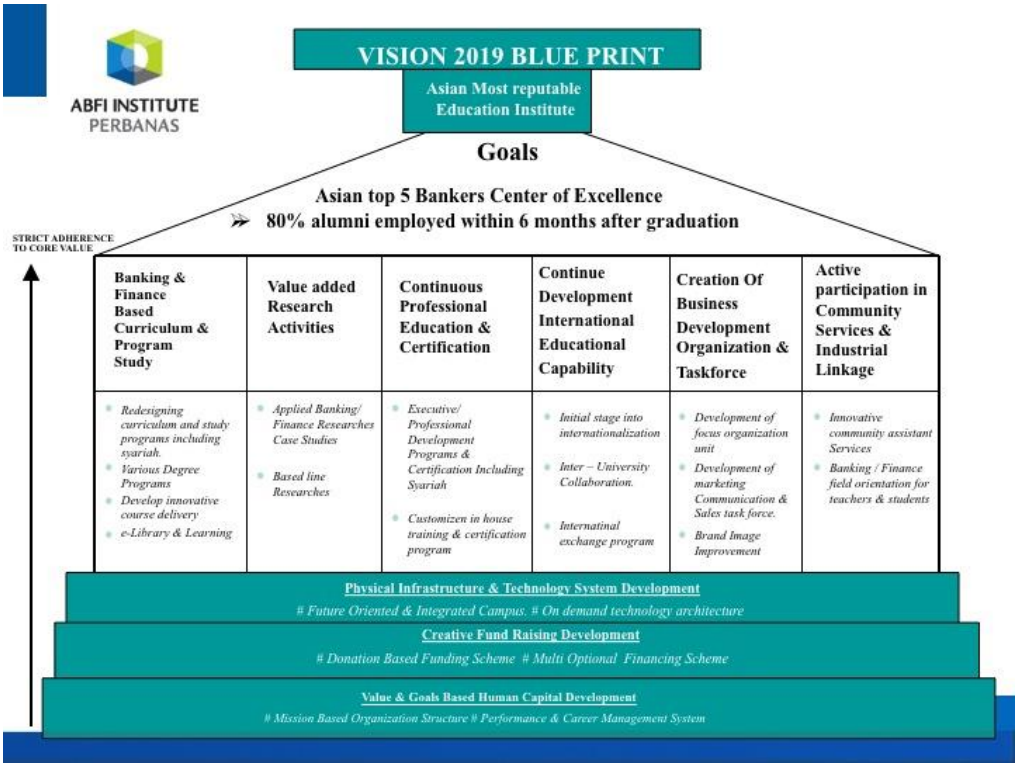


Figure 1.0. Perbanas Institute Vision 2019

2. Research Objectives

This research is to provide a reference for the integrity information security management

system. The material compiled in this research aims to:

a. Provide an overview of information security management system that prevails in the world (ISO 27001:2005)
b. Provide an overview of methods and technologies that can be used in the application of information security management system in universities.
c. Provide advice on the format and content of information security management system standard design.

3. Methodology

Two research methods were used to achieve the objectives of this study which are literature review and exploration analysis. The literature study was conducted to review secondary literature about the topics relevant to this research. This includes the general needs of education sector and its special security needs Information security management standards and best practices in establishing an information security management system; and Information security management pertaining to the Education sector. The sources used to do the literature review were selected based on availability and trustworthiness.

4. Discussion

4.1. Security Risk Management Approach

Risk is defined as the chance of something happening that may impact or result in the organization's business processes to cause the failure of an organization's business objectives. This risk is measured by the impact or influence on the likelihood of the risk posed. Risk management is a process to identify risks, analyze risks and handling to reduce the risk to their impact on business processes in an organization at a level that is acceptable or permissible. Risk management includes the following activities: identifying information, identifying threats and weaknesses, business impact analysis and risk assessment.[1]

According to ISMS, the risk is the impact on the occurrence of something that threatens the organization's Information Security. The main question of this research is on the aspects of the Information Security CIA (Confidentiality, Integrity, Availability). Risk will affect the existence of information security, the discussion in this chapter will provide an overview of the importance of risk management performed and how risks are assessed so that appropriate treatment can be done.[3]

4.2 Risk Assesment

Risk assessment is the first step or phase of the risk management process.[2] Risk assessment aims to determine the threats from the outside that could potentially interfere with the Information Security organization and potential weaknesses (vulnerabilities) that may have information on the organization. Risk assessment consists of 6 phases:

1) Information Identification.

2) Threat Identification.

3) Vulnerability Identification.

4) Determine the probability of threat.

5) Impact Analysis.

6) Determine Risk Value.

4.3. Determine Risk Value

Risk value is a picture of how large the impact to the organization received the threat that causes the failure of information security occurs. Risk value can be determined by two methods, among others[8]:

a) Qualitative Methods

Done by making estimates of costs to be incurred or issued by the organization due to the risk accepted. Risk value is usually determined by the range:

- LOW RISK
- MEDIUM RISK
- HIGH RISK

b) Quantitative Methods

Quantitative methods of risk assessment methods with a mathematical approach is used for this method; the value of the risk can be calculated using the following formula.

Calculation of the risk with a mathematical approach:

Risk value = NA x BIA x NT, where:

Asset value : NA

Business impact analysis: BIA

Threat Value: NT

4.4. Risk Value on ABFII Perbanas

This is the list of Sensitive information inside ABFII Perbanas:

1. Diploma Certificate
2. Transcript values
3. Raw/Original data on Scoring from lecturers
4. Professors Data archive
5. Operating licenses and legal papers of the university
6. Basic salaries of tenured faculty and support personnel
7. Honor credits per faculty
8. Computer Laboratory
9. Laptop or PC computer of structural employees (Director, Chairman of the department, BAAK, and Finance)
10. Computer Servers such as Web Server, Database Server, Email Server etc.
11. Academic guidelines and final project.
12. LCD Projector that able to store temporary information
13. Student data
14. Library books data
15. Subjects per semester data
16. Alumni data
17. Student financial data
18. Office inventory data
19. Extracurricular activities data of students
20. Certificates
21. Research Data
22. Certificate of accreditation

4.5. ISMS Planning

In Planning and developing the Information Security Management System (ISMS), the challenge is on the frequent use of computer networks across the public Internet

network.[9]

The fact is that the existence of interconnections between the various public and private networks is particularly related to the process of sharing some information resources to improve access and optimization. However, this benefits obtained at the same time weakens the effectiveness of centralized control, in turn it also creates a new weaknesses in the system. Furthermore, the findings shows that the majority of Information Systems are designed and built today show less information security considerations for good ISMS planning and methodological steps.[4]

The Good information security can be achieved through the implementation of a number of technical measures which is supported by various policies and procedures accordingly. The process starts from the identification number of the relevant controls to be applied within an organization, which of course must be based on an analysis of the needs of the Information Security asprk like what should be owned by the company. Once the policies, procedures, and technical guidance regarding operational controls should be established within the organization developed, the next step is the socialization of all these tools to all levels of management and employees of the organization to gain support and commitment.

Then the other interested parties outside the organization such as suppliers, customers, partners, and shareholders must also be involved in the socialization process because they are an integral part of the ISMS is built.[6] The involvement of experts and experts from outside the organization often needed to assist organizations in implementing these measures. With the knowledge they have, especially in helping organizations to identify needs and develop the necessary control, undoubtedly built ISMS can be more effective and economical.

If referring to the requirements of ISO/IEC 27001, ISMS plan is to carry out the requirements in stage 4., or the approach through the process of planning the ISMS PDCA cycle is Plan process.[5] Plan process if we look back to the Stage 3.

Formulation from step 1 through stage 5 meet the requirements based on ISO/IEC 27001, and shall do the stages in accordance with the requirements of the ISO/IEC 27001. These stages can be described as in below. There are 7 stages that must be done to plan for the ISMS are:

Stage 1: Determining the space scope of ISMS
Stage 2: Determining Policy
Stage 3: Determine how the risk assessment
Stage 4: Identification of risks

Stage 5: Analysis and evaluation of risks
Stage 6: Identify and evaluate risk management options
Stage 7: Selecting Objective Control and Controls

4.6. Selecting and Objectives Control for the Risk Management

In the earlier stages after the organization understand the risks to be acceptable and provide the safest policy organizations and determining the criteria to accept the risk, namely whether:

a). Determine the risk

b). Accept more risk with the risk management

As explained above, Sub option one risk management option is to determine what the appropriate security controls for organizations to manage risk to be accepted that the risk can be reduced to a level that is tolerated by the organization, it is termed risk mitigation. In the election of Security Control in the document ISO/IEC 27001 which is more detailed implementation guidelines are described in document ISO/IEC 27001. Security controls have a Controls and Objectives Control.

Objective Control is a statement of expected results or objectives to be achieved by implementing control procedures in the some process. Control are things that must be met for the purpose of Information Security Objectives Control.[10]

Furthermore, control is defined as actions taken by management, directors and other parties to enhance risk management and increase the likelihood of achievement of objectives as set out. Technical implementation of the organization can choose the appropriate controls and necessary in an effort to address and minimize the impact of an acceptable risk. Implementation Objectives and Controls can be a reference to the standard ISO 17799/27001:2005 which can be seen more detail in the document ISO/IEC 27001.[11]

ISO 27001 defined as 11 Clause, 39 Control Objectives and 133 controls that can be applied to build the Information Security Management System. The Clause 11's are:

1. Security Policy - Clause 5

2. Organization of information Security - Clause 6

3. Asset Management - Clause 7

4. Human Resources Security - Clause 8

5. Physical and Environmental Security - Clause 9

6. Communications and Operations Management - Clause 10

7. Access Control - Clause 11

8. Information Systems Acquisition, Development And Maintenance - Clause 12

9. Information Security Incident Management - Clause 13

10. Business Continuity Management - Clause 14

11. Compliance - Clause 15

Figure 2.0. Organization Structure of ISO/IEC 27001.

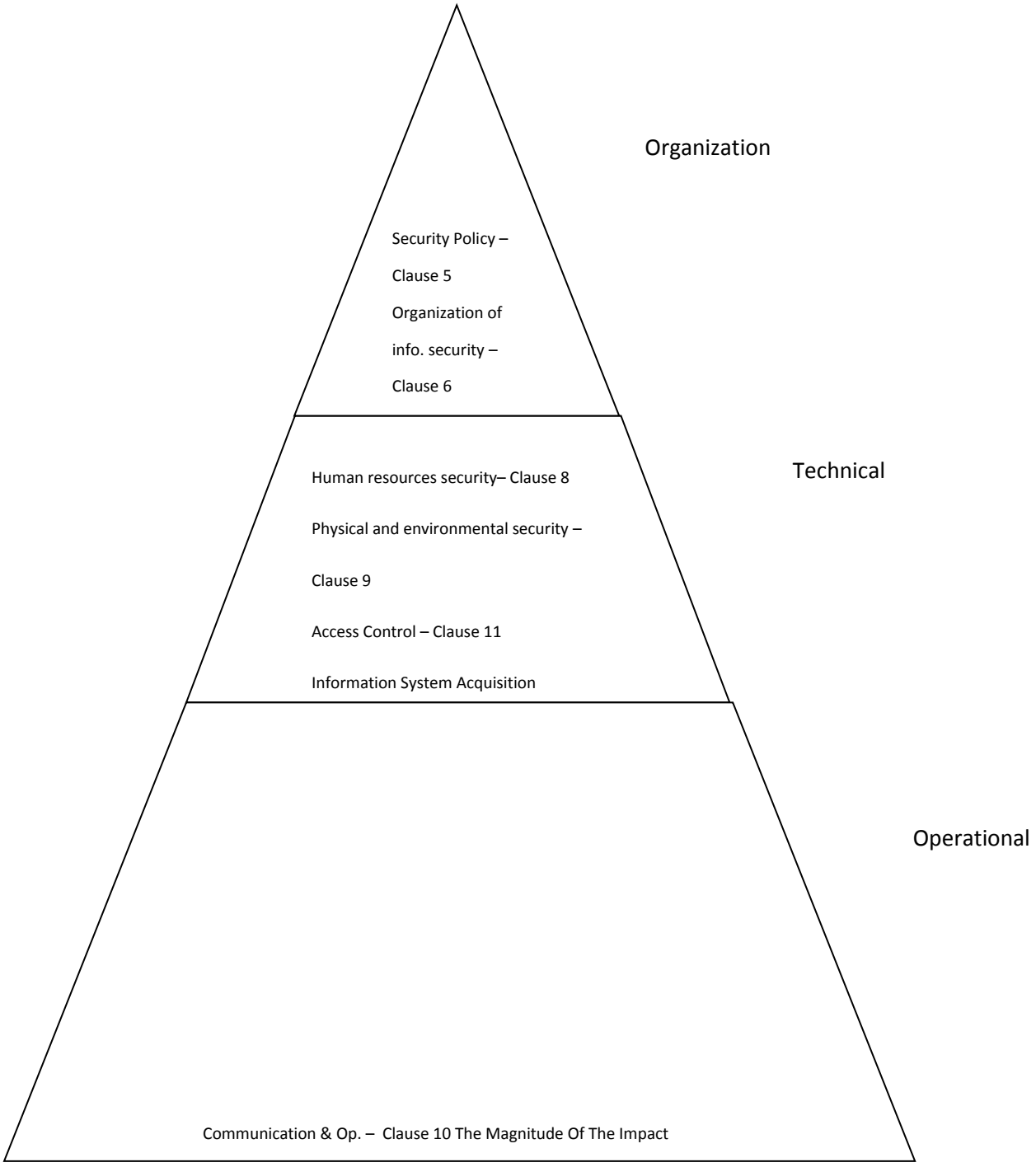


Figure. 3.0. Security Control Needs

4.7. Results and Analysis

Risk value determination on PERBANAS University (10 selected in Paper).

Risk Impact = Asset Value x Severity of Threat x Severity of Vulnerability x Probability

No	Sensitive Information System	Asset Value	Threat	Vulnera-Bility	Proba-Bility	Risk Impact Value	
						A.T.V.P	VALUE
1	Product & Services Database	7	2	2	4	7x2x2x4	**112**
2	Client & Partners Database	9	2	1	4	9x2x1x4	**72**
3	Project Database	7	2	2	4	7x2x2x4	**112**
4	Finance & Accounting Database	9	2	2	4	9x2x2x4	**144**
5	Employee Database	9	2	2	4	9x2x2x4	**144**
6	Scheduling Teaching Database	6	2	2	4	6x2x2x4	**96**
7	PERBANAS Students Database	9	3	2	5	9x3x2x5	**270**
8	PERBANAS Students Integrated Database	9	3	2	5	9x3x2x5	**270**
9	Payroll and Presence (Attendance) Database	9	2	2	4	9x2x2x4	**144**
10	E-Learning Database	5	2	1	4	5x2x1x4	**40**

The High Risk Impact in this table are *"PERBANAS Students Database" and "PERBANAS Students Integrated Database"* with the value = "270", so this is the ISO 27001:2005 Scope selected, it's better, easy and medium effort for the Perbanas management or Universities document control to do and ISO 27001:2005 certificate achievement as an education sector optimal standard.

5. Conclusions

This research has been discussed about the ISMS based on ISO 27001. ISMS becomes important when an organization has put the information as a critical infrastructure, the ISMS be a top priority to be implemented for the survival and development of the organization. Security information may indirectly ensure business continuity, reduce risk, optimize the return on investment and look for business opportunities.

The more an organization's information is stored, managed and in sharing the greater the risk of damage, loss or data was expossed to external parties that are not desirable.

It was presented at the beginning that it is important to understand the basics of information security as a cornerstone to the ISMS that begins with the understanding and the need for information Security Management, the information security standard ISO 27001 or commonly called the ISMS and the various aspects that support it.

The next analysis is on information security management system (ISMS), after it stepped in to risk management, the author have analyzed and presented.

At the end of the analysis of this study was to plan the design of an ISMS that starts with

a. Building a management commitment to the implementation of ISMS ABFII Perbanas,
b. Determine the scope of the ISMS,
c. Inventory and classify information,
d. Conduct a risk assessment to determine the value of risk information to the organization if there is a threat or disruption of information security,
e. The Last is to determine or select information security controls according to ISO 27001 standards are implemented in ABFII Perbanas based on risk assessment has been done.

So, this research results may be used by ABFII PERBANAS particular and all the universities in general in order to protect all aspects of information security held against misuse of information security threats and can be an Information Security Management Standard (ISO 27001) on All Universities.

6. Recommendations

1. The most important thing in the implementation of the Information Security Management System (ISMS) is to evaluate the implementation of the ISMS with

the monitor and review. The PDCA (plan-do-check-action) cycle, the evaluation represents the Check. Implementation of the evaluationis done internally, means carried by the organization itself as ABFII PERBANAS. The results of the evaluation material used to get a management review.

2. The main purpose of the evaluation of ISMS is to maintain that the ISMS is always appropriate to the needs of the organization and are reviewed, corrected and improved in accordance with the needs of the organization. It's a continuous process is termed in the PDCA continual improvement.

7. References

[1] Andress, Jason. The Basics of Information Security : Understanding the Fundamentals of Infosec in Theory and Practice. Syngress Pub., 2011 (208).

[2] Arnason, Sigurjon Thor & Willet, Keith D. How to Achieve 27001 Certification : An Example of Applied Compliance Management. Auerbach Pub., 2007. (352).

[3] Arkin, Stanley S. (ed.). Prevention and Prosecution of Computer and High Technology Crime. Oakland, CA: Mattew Bender, 2007. (188).

[4] Association of Insurance and Risk Managers [AIRMIC], National Forum for Risk Management in the Public Sector in the UK [ALARM], & Institute of Risk Management [IRM]. A Risk Management Standard, Retrieved March 28, 2008, from http://www.airmic.com/download.cfm/docid/285D292B-C593-4CA2-8D605B2A79D7744E

[5] Australian General Practice Network [AGPN]. Information Management Policy for the Australian General Practice Network V1.1. Retrieved October 23, 2008, from http://www.agpn.com.au/__data/assets/pdf_file/0016/1186/136800.pdf

[6] Aydin, M.N., Harmsen, F., Slooten, K., & Stegwee, R.A. An Agile Information Systems Development Method in Use. Turkish Journal of Electrical Engineering and Computer Sciences, 12(2), 127-138. Retrieved March 21, 2008, from http://journals.tubitak.gov.tr/elektrik/issues/elk-04-12-2/elk-12-2-5-0404-6.pdf

[7] Bequai, August. ISMS, Security Standards and Security Regulations. Information Security Technical Report, 11(1), 26-31, 2006. Technocrimes. Lexington, MA: D.C. Heath. Broderick, J.S. (2006). Available from ScienceDirect full-text scientific online database.

[8] Calder, Alan. IT Governance : An International Guide to Data Security and ISO 27001/27002. Kogan Page Pub., 5th edition, 2012. (380)

[9] Calder, Alan. Implementing Information Security based on ISO 27001/ISO

27002. Van Haren Pub., 2009. (84)

[10] Calder, Alan & Watkins, Steve G. Information Security Risk Management for ISO 27001/ISO 27002. IT Governance Ltd, 2010. (198).

[11] Conly, Catherine H. Organizing for Computer Crime Investigations and Prosecution. Washington, DC: U.S. Department of Justice, National Institute of Justice, 1989.

The Annual Conference on Management and Information Technology (ACMIT) 2014

XYZ Web App Information Security Management Risk Assessment

Meily[1]

[1]*Master of Information Technology Department, Faculty of Engineering and Information Technology, Swiss German University, BSD City, Tangerang 15339, Indonesia*

Abstract

Cloud computing is one of the strategic technology trends. It's pay as you go characteristic and the fact that the service is provided via a broad network, such as a web browser is what makes cloud providers incentivised by profits by providing cloud services, and cloud customers are interested in the chance of eliminating costs that come with in-house service provision. Due to its infrastructure where cloud providers maintain everything cloud customers are wary and concerned about their data and system security. Hence this paper was tries to address and answer cloud customers' concern on security by doing an overall risk analysis using ENISA framework and Commonwealth of Virginia risk assessment guide on XYZ Web App, an application provided by XYZ Company for the insurance industry that connects insurers, repairers, adjusters and other third parties for claim processing and policy creation. This paper answers all the concerns by resulting it in overall risk summaries, likelihood, impact and overall risk rating that later in used for recommendation to improve XYZ Web App security.

Keywords : Cloud Computing, Information Security Management, Risk Assessment, SaaS

1. Introduction

From the time cloud computing was introduced, it has become a technology strategy with its pay as you go characteristic and the fact that the service is provided via a broad network, such as a web browser [1]. Nowadays cloud computing is still a strategic technology trend [2]. Cloud providers are incentivised by profits that would be acquired by charging their services to their customers. Meanwhile, cloud customers benefit from this kind of business model since it means they can eliminate the costs that come with in-house service provision [3].

XYZ Web App is a product of XYZ Company, a cloud provider that provides solutions for the insurance industry using service model Software as a Service (SaaS), enabling their customers to connect their businesses anytime anywhere via Internet through a web browser. XYZ Web App connects insurers, workshops, and third party resources.

With most of the resources being maintained by cloud providers, security is the key question during almost every phase of service, i.e. presales, implementation and post go-

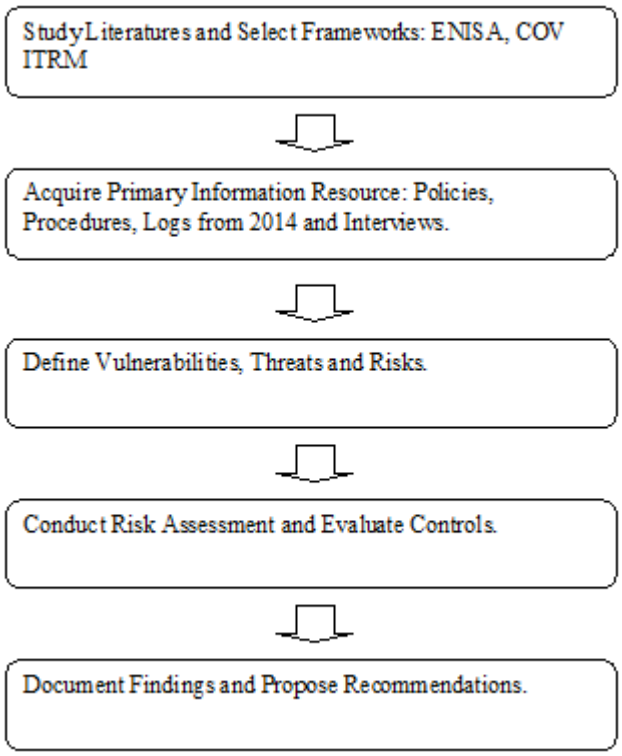
live, even after several years subscribing to the service. This is to be expected since security and privacy are the main concerns in cloud service [4].

The primary objective of the paper is aimed to address customers' concerns in regard to the risks of XYZ Web App. By doing this, the analysis on risks can help XYZ Company and its staff to understand the risks involved and thus can help to improve their information management policy concerning its service since there is no formal standard on risk assessment analysis documented. It also aims to provide an assurance and understanding to the customers that XYZ Company complies and is committed to the customers' needs and concerns in regard to the application's safety and privacy.

2. Methodology

The steps conducted in this research can be seen in figure 1, as well as the explanations below:

Figure 1. Risk Assessment Methodology



a. Acquiring XYZ Company's Information Security Management policy and other policies documents that, are related to XYZ Service i.e. Information Security Policy [5], Disaster Recovery Procedure [6], System Administration Security and Operating Procedures [7], Software Development Procedures [8], and Department Roles and Responsibilities document [9].
b. Acquiring network and or data centre related logs if available.

Data was collected manually from the start of the year 2014. Data was logged manually by XYZ Company Indonesia branch's Project Manager.

c. Acquiring application, operation and framework related data from key persons by conducting interviews via Skype and email using ENISA Information Assurance Framework [10]. Below are the key persons who were interviewed:
   1) XYZ Chief System and Security Officer
      Questions were directed in regard to the network and system security in overall and overall operations in Malaysia.
   2) XYZ Application Software Engineer
      Questions were directed in regard to the application security and related matters.
   3) XYZ Software Framework Engineer
      Questions were directed in regard to the application framework security.
   4) XYZ Indonesia Branch Operation Director
      Questions were directed in regard to SLA and overall operations in Indonesia.
   5) XYZ Singapore Business Analyst
      Questions were directed in regard to overall operations in Singapore.
d. Define vulnerabilities, threats, and risks based on the acquired data.
   Vulnerabilities, threats and risks were defined based on the data acquired, as well as using ENISA Security Risk Assessment [11] as guideline.
e. Doing a control analysis on current Information Security Management using Commonwealth of Virginia risk assessment guide [12].
f. Define the risk likelihood, risk impact and overall risk
   Risk likelihood, risk impact and overall risk were defined based on the data analysis conducted, as well as using ENISA Security Risk Assessment [11] as a factor into determining the likelihood and impact.
g. Create a recommendation based on the risks identified.
h. Document the result of risks analysis.
   Documentation of the risk analysis result was done using Commonwealth of Virginia Style [12].

3. Discussions

3.1. Vulnerabilities, Credible Threats and Risk Summaries

Vulnerabilities, credible threats and risk summaries were defined by mapping the answers of key persons, checking against current data logs and were determined by using ENISA Security Risk Assessment as guideline. Due to the service model that is provided by XYZ is of Software as a Service, out of 53 vulnerabilities defined in ENISA Security Risk Assessment Framework, only 20 are selected

based on the service model and more on XYZ's cloud providers' perspective, as determined from the questionnaire and interview via Skype and email as following:

1. Authentication, Authorisation and Accounting Vulnerabilities
2. User Provisioning
3. User De-Provisioning
4. Lack of Resource Isolation
5. Lack of Reputational Isolation
6. Lack of Impersonation Test
7. Communication Encryption
8. Lack of or weak encryption, of data in transit
9. Inability of processing data in encrypted form
10. No Source Escrow Agreement
11. Inaccurate of Resource Usage
12. Possibility of performing co-residence
13. Lack of Security Awareness
14. System OS Vulnerabilities
15. Poor Identification of Project Requirements
16. Poor Patch Management
17. Poor prediction on resource consumption
18. Data Loss liabilities
19. Lack of completeness and transparency in terms of use
20. Lack of, or a poor and untested BCP and DRP

The threats determined can be seen in table 1 below:

Table 1. Credible Threats to XYZ

Abuse and Nefarious Use	Service Hijacking	Acquisition of Cloud Provider
Malicious Insider	Traffic Hijacking	Isolation Failure
Shared Technology Vulnerabilities	Insecure Application Programming Interfaces	Resource Exhaustion
Data Loss/Leakage	Data Breaches	Economic Denial of Service
Account Hijacking	Distributed Denial of Service	Changes of Jurisdictions
Social Engineering Attacks	Natural Disasters	Insecure or Incomplete Data Deletion
Loss of Governance	Compliance Challenges	Lock In

Meanwhile, risks are identified by matching identified vulnerabilities with credible threats that might exploit them.

The pairing of vulnerabilities and credible threats along with the result of, a full risk summary can be seen in Appendix A. Meanwhile the mapping of vulnerabilities determined and selected in this paper to ENISA's Security Risk Assessment Guideline vulnerabilities can be seen in Table 2 below:

Table 2. Vulnerabilities Mapping

Vulnerabilities Determined and Scoped in this Paper	ENISA's Vulnerabilities
1	V1
2	V2
3	V3
4	V6
5	V7
6	V32
7	V8
8	V9
9	V10
10	V14
11	V15
12	V18
13	V32
14	V39
15	V45
16	V48
17	V49
18	V51
19	V31
20	V41

3.2.Control Analysis

Control analysis is done to see whether XYZ Company's control area is in place, partially in place, not in place, planned or not available at all. This control area then in correlated to the risks identified in previous steps along with other

mitigating or exacerbating factors. This is to see whether controls are in place in order to mitigate the risks identified. Full control analysis can be seen in Appendix B whilst the correlation of control area and risks can be seen in Appendix C. Meanwhile, control area and the status can be seen in table 4 below:

Table 3. Control Area Analysis [12]

Control Area	**In Place/Partially In Place/Not In Place/Planned/Not Available**
1. Risk Management	
1.1 IT Security Roles and Responsibilities	In place
1.2 Business Impact Analysis	Not Available
1.3 IT System & Data Sensitivity Classification	In place
1.4 IT System Inventory & Definition	In place
1.5 Risk Assessment	Not Available
1.6 IT Security Audits	Not Available
2. IT Contingency Plan	
2.1 Continuity of Operations Planning	Partially In place
2.2 IT Disaster Recovery Planning	In Place
2.3 IT System & Data Backup Restoration	In Place
3. IT Systems Security	
3.1 IT System Hardening	Not Available
3.2 IT Systems Interoperability Security	In Place
3.3 Malicious Code Protection	In Place
3.4 IT Systems Development Life Cycle Security	In Place
4. Logic Control Access	
4.1 Account Management	In place
4.2 Password Management	In place
4.3 Remote Access	Not Available/Planned
5 Data Protection	
5.1 Data Storage Media Protection	In place
5.2 Encryption	In place

6 Facilities Security	
6.1 Facilities Security	In place
7 Personnel Security	
7.1 Access Determination & Control	In place
7.2 IT Security Awareness & Training	In place, planned
7.3 Acceptable Use	In place
8 Threat Management	
8.1 Threat Detection	In place
8.2 Incident Handling	In place
8.3 Security Monitoring & Logging	In Place
9 IT Asset Management	
9.1 IT Asset Control	In place
9.2 Software License Agreement	In place
9.3 Configuration Management & Change Control	In place

As we can see from the table, there are 21 controls are in place, 1 control is partially in place, 2 controls are at least being planned and 5 are not available. The not available controls would have to be watched closely by XYZ Company although some controls do not necessarily have to be available, i.e. hardening procedure, since XYZ Web App does not run in a virtual environment. Some controls, even though are in place but not enforced since it would depend more on customer client company's policies instead of XYZ's policy.

3.3.Risk Likelihood, Risk Impact and Overall Risks

Risk likelihood is determined based on answers to the interview conducted and factoring ENISA Security Risk Assessment [11] results taken as a consideration for the answer. The likelihood rating is then considered decreased or increased after checking it against data logs for certain points related to resource usage especially in the year 2014 where the number of servers down is quite high and the root of cause is not yet clear. The risk impact scale of risk calculation taken from Commonwealth of Virginia Risk Assessment Guideline [12] is defined as following:

- Low (1 to 10)
- Moderate (>10 to 50)
- High (>50 to 100)

With the formula shown in table 4 below:

Table 4. Risk Likelihood and Impact Calculation [12]

Risk Likelihood	**Risk Impact**		
	Low (10)	**Moderate (50)**	**High (100)**
High (1.0)	Low 10 x 1.0 = 10	Moderate 50 x 1.0 = 50	High 100 x 1.0 = 100
Moderate (0.5)	Low 10 x 0.5 = 5	Moderate 50 x 0.5 = 25	Moderate 100 x 0.5 = 50
Low (0.1)	Low 10 x 0.1 = 1	Low 50 x 0.1 = 5	Low 100 x 0.1 = 10

The final result of risk likelihood, risk impact and overall risks can be seen in table 3 below:

Table 3. Risk Likelihood, Risk Impact and Overall Risks [12]

Risk No.	**Risk Summary**	**Risk Likelihood Rating**	**Risk Impact Rating**	**Overall Risk Rating**
1	Poor AAA in system could facilitate unauthorised access to resources, privileges escalation, inability to track the misuse of resources, security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data	Moderate	High	Moderate
2	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Low	High	Low
3	A poor user provisioning in system could facilitate unauthorised access to resources, privileges escalation, inability of tracking the misuse of resources, security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data	Moderate	High	Moderate

4	Denial of service attack could render XYZ Web App unavailable for use	Moderate	High	Moderate
5	Isolation Failure could compromise confidentiality and integrity of XYZ Web App Data	Low	High	Low
6	Social Engineering attack due to lacking of impersonation test could compromise confidentiality and integrity of XYZ Web App Data	Moderate	Moderate	Moderate
7	Unsecured Communication Encryption could compromise confidentiality, integrity and availability of XYZ Web App Data	Low	High	Low
8	Unsecured Data in transit could compromise confidentiality and integrity of XYZ Web App Data	Low	Moderate	Low
9	Inability of processing data encryption could compromise confidentiality and integrity of XYZ Web App Data	Low	Moderate	Low
10	No source escrow agreement could compromise confidentiality, integrity and availability of XYZ Web App Data	High	Low	Low
11	Inaccurate of resource usage could compromise with confidentiality, integrity and availability of XYZ Web App Data	High	High	High
12	Loss of Governance, Change of Jurisdictions could compromise confidentiality, integrity and availability of XYZ Web App Data	Moderate	Moderate	Moderate
13	Lack of security awareness could compromise confidentiality and integrity of XYZ Web App Data	Moderate	Moderate	Moderate

14	System OS Vulnerabilities could compromise confidentiality and integrity of XYZ Web App Data	Moderate	High	Moderate
15	Poor identification of project requirements could compromise with confidentiality, integrity and availability of XYZ Web App Data	High	High	High
16	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Moderate	High	Moderate
17	Wrong prediction on resource consumption could compromise with confidentiality, integrity and availability of XYZ Web App Data	Moderate	High	Moderate
18	Liability from Data Loss could compromise with confidentiality, integrity and availability of XYZ Web App Data	Low	High	Low
19	Lack of completeness and transparency in use could compromise with confidentiality, integrity and availability of XYZ Web App Data	Moderate	Moderate	Moderate
20	Lack of Business and disaster recovery plan could compromise with confidentiality, integrity and availability of XYZ Web App Data	Moderate	High	Moderate

4. Conclusion

By conducting risk assessment, the overall risk rating of XYZ Web App and control area that correlates to it become known. Both XYZ staff and customers can then have a better understanding of the information security management of XYZ Company. Even though most controls are in place, some that are not available and are important for better security assurance improvement can be

considered to be made available. Some of the controls, in order to be optimised, XYZ would need cooperation from customers' side since customers' business processes impact heavily on how the system is ran and customised for them.

The risk assessment can be regarded as a source to improve the current policy and to contribute to the making of business continuity plan by combining it with business impact analysis.

Based on the risk finding, recommendations are then made in order to lower risk in the future for a better system security improvement regardless the risk rating. Table 4 on recommendation below is made using the formatting of Commonwealth of Virginia guide on risk assessment [12]:

Table 4. Recommendations

Risk No.	Risk Summary	Risk Rating	Recommendation
1	Poor AAA in system could facilitate unauthorized access to resources, privileges escalation, inability of tracking the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data	Moderate	XYZ Team should follow XYZ policies regarding removal of accounts, including suggesting the recommendation to the client side
2	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Low	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent not patched application security defects
3	A poor user provisioning in system could facilitate unauthorized access to resources, privileges escalation, inability of tracking the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ	Moderate	XYZ Team should follow XYZ's policies regarding removal of accounts, including suggesting the recommendation to the client side

	Web App Data		
4	Denial of service attack could render XYZ Web App unavailable for use	Moderate	XYZ Team should do a thorough vulnerability and penetration testing often to ensure there wouldn't be a port that would be suffer from DDoS, and or to close all the vulnerability ports
5	Isolation Failure compromise confidentiality and integrity of XYZ Web App Data	Low	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent not patched application security defects
6	Social Engineering attack due to lacking of impersonation test could compromise confidentiality and integrity of XYZ Web App Data	Moderate	XYZ Team should do an impersonation test before granting requestor's request to reset the password
7	Unsecured Communication Encryption could compromise confidentiality, integrity and availability of XYZ Web App Data	Low	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent unsecure communication encryption
8	Unsecured Data in transit could compromise confidentiality and integrity of XYZ Web App Data	Low	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent unsecure communication encryption
9	Inability of processing data encryption could compromise confidentiality and integrity of XYZ Web App Data	Low	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent inability of processing data encryption
10	No source escrow agreement could compromise confidentiality, integrity and availability of XYZ Web App Data	Low	None. XYZ Executive management has elected to accept this risk.

11	Inaccurate of resource usage could compromise with confidentiality, integrity and availability of XYZ Web App Data	High	XYZ Team should do a thorough stress testing to ensure that there would not be inaccurate of resource usage
12	Loss of Governance, Change of Jurisdictions could compromise confidentiality, integrity and availability of XYZ Web App Data	Moderate	XYZ Executive management should define a better policy in term of lack of completeness and transparency in use after discussing it with the inquisitor executive management
13	Lack of security awareness could compromise confidentiality and integrity of XYZ Web App Data	Moderate	XYZ should enforce the security training periodically
14	System OS Vulnerabilities could compromise confidentiality and integrity of XYZ Web App Data	Moderate	XYZ Team should update their OS regularly
15	Poor identification of project requirements could compromise with confidentiality, integrity and availability of XYZ Web App Data	High	XYZ Project Management team should confirm the correct requirements to the customers to ensure that it is already correct
16	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Moderate	XYZ Team should do a thorough testing before and after conducting the roll out to further prevent not patched application security defects
17	Wrong prediction on resource consumption could compromise with confidentiality, integrity and availability of XYZ Web App Data	High	XYZ Team should do a thorough stress testing to ensure that there would not be wrong prediction on resource consumption
18	Liability from Data Loss could compromise with confidentiality, integrity	Low	XYZ should ensure the security to the building and

	and availability of XYZ Web App Data		data backup
19	Lack of completeness and transparency in use could compromise with confidentiality, integrity and availability of XYZ Web App Data	Moderate	XYZ Executive management should define a better policy in term of lack of completeness and transparency in use after discussing it with the inquisitor executive management
20	Lack of Business and disaster recovery plan could compromise with confidentiality, integrity and availability of XYZ Web App Data	Moderate	XYZ Executive management should create business continuity plan, conduct business continuity and disaster recovery plan training periodically

Glossary

AAA : Authorisation, Authentication and Accounting

BCP : Business Continuity Plan

Changes of Jurisdictions : The jurisdictions that are different from one to another country that needsto be addressed.

DRP : Disaster Recovery Plan

In Place : The control that is available and implemented.

Isolation Failure : Failure to segregate each client's specification and access

Lock In : Customer's dependency on vendor's products or services

Partially In Place : The control that is available and only implemented partially.

Not In Place : The control that is available but not implemented.

Acknowledgement

Author would like to thank the key persons who have answered the question related to XYZ information security management so then this risk assessment could be conducted.

References

[1] Mell, Peter, and Timothy Grance. "The NIST definition of cloud computing (draft)." NIST special publication 800.145 (2011): 7.

[2] Rivera, Janessa. (2013, Oct) Gartner: The top 10 strategic technology trends for 2014. [Online]. Available: http://www.gartner.com/newsroom/id/2603623

[3] Buyya, Rajkumar, et al. "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility." Future Generation computer systems 25.6 (2009): 599-616.

[4] Leavitt, Neal. "Is cloud computing really ready for prime time." *Growth* 27.5 (2009).

[5] XYZ, XYZ Company Information Security Policy v1.0, Malaysia, 2011.

[6] XYZ, XYZ Data Centre Disaster Recovery Procedure v0.2, Malaysia.

[7] XYZ, XYZ Company System Administration Security and Operating Procedure v1.0, Malaysia

[8] XYZ, Software Development Procedures in XYZ Company v1.2, Malaysia, 2007.

[9] XYZ, Department Roles and Responsibilities v0.2, Malaysia.

[10] Catteddu, D., and G. Hogben. "Cloud computing information assurance framework." European Network and Information Security Agency (ENISA) (2009).

[11] ENISA. (2009, Feb) "Cloud computing: benefits, risks and recommendations for information security." Available: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computingrisk- assessment

[12] VITA. Information Technology Risk Management Guideline, ITRM Guideline SEC506-01, Appendix D – Risk Management Guideline Assessment Instructions, 2006 [Online].Available at: http://www.vita.virginia.gov/uploadedfiles/VITA_Main_Public/unmanaged/library/RiskManagementGuideline.pdf

Appendices

Appendix A. Identification of Risks

Risk No.	Vulnerability	Threat	Risk of Compromise Of	Risk Summary
1	Authentication, Authorisation and Accounting Vulnerabilities	Abuse and Nefarious Use, Malicious Insider, Account Hijacking, Data Loss/Leakage, Data Breaches, Insecure Application Programming Interfaces, Economic Denial of Service, Compliance Challenges	Confidentiality, Integrity and Availability of XYZ Web App data	Poor AAA in systemcould facilitate unauthorized access to resources, privileges escalation, inability to track the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data

2	User Provisioning	Abuse and Nefarious Use, Malicious Insider, Account Hijacking, Data Loss/Leakage, Data Breaches, Insecure Application Programming Interfaces, Economic Denial of Service, Compliance Challenges	Confidentiality & Integrity of XYZ Web App data	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data
3	User De-Provisioning	Abuse and Nefarious Use, Malicious Insider, Account Hijacking, Data Loss/Leakage, Data Breaches, Insecure Application Programming Interfaces, Economic Denial of Service, Compliance Challenges	Confidentiality & Integrity of XYZ Web App data	A poor system for user provisioning could facilitate unauthorized access to resources, privileges escalation, inability to track the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data
4	Lack of Resource Isolation	Service Hijacking, Traffic Hijacking, Distributed Denial of Service, Shared Technology Vulnerabilities	Availability of XYZ Web App Data	Denial of service attack could render XYZ Web App unavailable for use
5	Lack of Reputational Isolation	Loss of Governance, Lock In, Compliance Challenges, Shared Technology Vulnerabilities	Confidentiality & Integrity of XYZ Web App data	Isolation Failure could compromise confidentiality and integrity of XYZ Web App Data
6	Lacking of Impersonation Test	Social Engineering Attack, Loss of Governance, Compliance Challenges, Account Hijacking	Confidentiality & Integrity of XYZ Web App data	Social Engineering attack due to lacking of impersonation test could compromise confidentiality and integrity of XYZ Web App Data
7	Communicatio n Encryption	Traffic Hijacking, Service Hijacking, Distributed Denial of Service, Data Loss/Leakage, Data Breaches	Confidentiality, Integrity and Availability of XYZ Web App data	Unsecured Communication Encryption could compromise confidentiality, integrity and availability of XYZ Web App Data
8	Lack of or	Data Loss/Leakage,	Confidentiality, Integrity	Unsecured Data in transit

	weak encryption or archives in and data in transit	Data Breaches	and Availability of XYZ Web App data	could compromise confidentiality and integrity of XYZ Web App Data
9	Inability of processing data in encrypted form	Data Loss/Leakage, Data Breaches	Confidentiality, Integrity and Availability of XYZ Web App data	Inability of processing data encryption could compromise confidentiality and integrity of XYZ Web App Data
10	No Source Escrow Agreement	Loss of Governance, Lock In, Compliance Challenges, Change of Jurisdictions	Confidentiality, Integrity and Availability of XYZ Web App data	No source escrow agreement could compromise confidentiality, integrity and availability of XYZ Web App Data
11	Inaccurate of Resource Usage	Service Hijacking, Traffic Hijacking, Distributed Denial of Service, Shared Technology Vulnerabilities	Confidentiality, Integrity and Availability of XYZ Web App data	Inaccurate of resource usage could compromise confidentiality, integrity and availability of XYZ Web App Data
12	Possibility that co-residence checks will be performed	Loss of Governance, Lock In, Compliance Challenges, Change of Jurisdictions	Confidentiality, Integrity and Availability of XYZ Web App data	Loss of Governance, Change of Jurisdictions could compromise confidentiality, integrity and availability of XYZ Web App Data
13	Lack of Security Awareness	Loss of Governance, Compliance Challenges, Social Engineering Attacks	Confidentiality and Integrity of XYZ Web App data	Lack of security awareness could compromise confidentiality and integrity of XYZ Web App Data
14	System OS Vulnerabilities	Insecure Application Programming Interfaces, Shared Technology Vulnerabilities	Confidentiality and Integrity of XYZ Web App data	System OS Vulnerabilities could compromise confidentiality and integrity of XYZ Web App Data
15	Poor Identification of Project Requirements	Shared Technology Vulnerabilities, Insecure Application Programming Interfaces, Lock In	Confidentiality, Integrity and Availability of XYZ Web App data	Poor identification of project requirements could compromise with confidentiality, integrity and availability of XYZ Web App Data
16	Poor Patch Management	Insecure Application Programming Interfaces	Confidentiality, Integrity and Availability of XYZ Web App data	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data
17	Resource	Service Hijacking,	Confidentiality, Integrity	Wrong prediction on

	Consumption	Traffic Hijacking, Distributed Denial of Service, Shared Technology Vulnerabilities	and Availability of XYZ Web App data	resource consumption could compromise confidentiality, integrity and availability of XYZ Web App Data
18	Liability from Data Loss	Natural Disaster, Data Loss/Leakage, Data Breaches, Economic Denial of Service	Confidentiality, Integrity and Availability of XYZ Web App data	Liability from Data Loss could compromise confidentiality, integrity and availability of XYZ Web App Data
19	Lack of completeness and transparency in terms of use	Acquisition, Economic Denial of Service, Loss of Governance, Compliance Challenges	Confidentiality, Integrity and Availability of XYZ Web App data	Lack of completeness and transparency in use could compromise confidentiality, integrity and availability of XYZ Web App Data
20	Lack of, or a poor and untested, business continuity and disaster recovery plan	Natural Disaster, Acquisition, Economic Denial of Service, Loss of Governance, Compliance Challenges	Confidentiality, Integrity and Availability of XYZ Web App data	Lack of Business and disaster recovery plan could compromise confidentiality, integrity and availability of XYZ Web App Data

Appendix B. Control Analysis

Control Area	In Place/Planned	Description of Controls
1. Risk Management		
1.1 IT Security Roles and Responsibilities	In place	1. XYZ employed its System Information Security Policy with the User Management Procedure detailed in it when hiring IT administrators or other personnel with system access. The policy applied to every region uniformly.
		2. XYZ conducted brief security training for the personnel hired upon employment. There is a process of continuous evaluation that occurs annually. However security access and privilege reviews are conducted every 3 months.
1.2 Business Impact Analysis	Not Available	There is no business impact

		analysis conducted formally.
1.3 IT System & Data Sensitivity	In place	XYZ has classified its system
1.4 IT System Inventory & Definition	In place	XYZ has documented its system inventory and sensitive
1.5 Risk Assessment	Not Available	No formal risk assessment conducted before
1.6 IT Security Audits	Not Available	IT Security Audits has never
2. IT Contingency Plan		
2.1 Continuity of Operations Planning	Partially In place	XYZ maintains a documented method that details the impact of a disruption. Basically, the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are as follows: 1. For hardware equipment failure - peripherals devices: XYZ shall recover the system in 0.5 (half) working days from date of notification 2. For hardware equipment failure - servers, XYZ shall recover the system in 1 (one) working days from date of notification 3. Data Centre Internet connection failure> 1day, XYZ shall recover the system in 1 (one) working day from the date of notification 4. For Total loss of data centre: XYZ shall recover the system in 3 (three) working days from date of notification
2.2 IT Disaster Recovery Planning	In Place	A DRP Plan has been documented and approved by XYZ Management Committed. Basically, the RTO (Recovery Time Objective) and RPO (Recovery Point Objective) are as follows : 1. For hardware equipment failure - peripherals devices: XYZ shall recover the system in 0.5 (half) working days from date of notification. 2. For hardware equipment

		failure - servers, XYZ shall recover the system in 1 (one) working days from date of notification 3. Data Center Internet connection failure> 1day, XYZ shall recover the system in 1 (one) working day from the date of notification 4. For Total loss of data centre: XYZ shall recover the system in 3 (three) working days from date of notification
2.3 IT System & Data Backup Restoration	In Place	1. A Backup and Restoration plan has been documented and reviewed
3. IT Systems Security		
3.1 IT System Hardening	Not Available	1. There is no system hardening for XYZ Web App as XYZ Web App doesn't run on Virtual Environment
3.2 IT Systems Interoperability Security	In Place	1. XYZ Web App Data can be integrated with the client's back end system via the integration method upon agreement.
3.3 Malicious Code Protection	In Place	1. XYZ uses IPS (Intrusion Prevention System), Domain Security Policy, Standard Security Options, and Service Lock Down Policy to control host and network when hosting the applications and information for the end customer. 2. Virus scanners and/or detection programs in servers shall be updated on a daily basis. The anti-virus software shall remain resident throughout the computing session. 3. The complete hard drive shall be scanned on a regular basis.

3.4 IT Systems Development Life Cycle Security	In Place	1. There are no exact controls used to protect the integrity of the operating system and applications software used. All operating system and applications software used are licensed and guaranteed by the vendor. 2. XYZ Development Team validates the new releases are fit for purpose or do not have a risk by doing vulnerability scanning, penetration testing, application and OS configuration review. 3. Vulnerability scanning, penetration testing, application and OS configuration review are also done to keep the application safe. 4. If vulnerabilities are discovered, the following processes are to be done to remedying it: - Issue/Ticket raised by the bug reporter (usually Project Management Officer, Business Analyst and or Software Engineer) - Plan/Design of solution - Implementation of solution - Unit testing and box testing of solution - Apply patch to UAT sites. - Apply patch to production sites.
4. Logic Control Access		
4.1 Account Management	In place	1. There is no customer's user accounts created in Active Directory. Only XYZ's staff that needs access to the servers have accounts in AD. All customer user accounts are logically created in the

		application database. 2. Need to know is the basis for access to customer data within XYZ Web App. 3. Access rights no longer required for an individual's normal duties shall be revoked immediately. 4. User IDs that have not been accessed for 90 days shall automatically be disabled.
4.2 Password Management	In place	1. Password controls shall be implemented on all XYZ application systems. 2. Passwords created shall be composed of minimum six (6) characters in length. 3. Application systems shall be configured to check that the user has selected a quality password, based on the following: a. Passwords shall not be the same as the user ID, b. Passwords shall not be composed of repeating characters, c. Passwords shall not be common dictionary terms and, d. Passwords shall be composed of both alphabetical and numeric characters, e. Passwords shall not be displayed on the screen during input. 4. Upon ten (10) consecutive authentication failures, users shall be locked out of the application system in which they are attempting to gain access to and shall have to have their account

		manually reset. 5. Users shall be forced to change their password upon initial login after being granted access rights to any application systems. 6. Application systems shall be configured to limit the use of cyclical passwords. 7. Application systems shall use password history techniques to maintain a password history of six (6) previous passwords where it is technically feasible. 8. Users shall be forced to change passwords at least of every ninety (90) days. This shall be enforced through technical means by deploying a password aging systems. 9. Password shall have a minimum password aging of three (3) days for application systems. This shall be enforced through technical means by deploying a password aging systems. 10. Application systems shall store password files in an encrypted form separately from application systems data. 11. Passwords shall not be stored in clear text and files containing passwords shall be one-way encrypted. Auto-logon and pass-through functions which bypass user identification and authentication procedures shall be prohibited. 12. Application systems, operating systems and databases that store user account and password

		information shall be secured in the strictest manner. 13. Access to the user account database shall be restricted to only authorised personnel. This access shall be reviewed quarterly. 14. Sharing of password is strictly prohibited among the users.
4.3 Remote Access	Not Available, Planned	No remote access policy is defined. It will be defined in near time.
5 Data Protection		
5.1 Data Storage Media Protection	In place	1. If there is old media or systems to be destroyed by XYZ, there is a Data Sanitisation Procedure in which data will either be overwritten or destroyed physically.
5.2 Encryption	In place	1. Encryption in XYZ is used in data in transit, SSL if required. It is also used for selected data for data at rest, and user name and password. 2. Password and user name are encrypted properly. 3. Data is encrypted properly. 4. There is a policy that define what should be encrypted and not. The access keys are held by the Chief System Security Officer and Chief Technology Officer.
6 Facilities Security		
6.1 Facilities Security	In place	1. For XYZ office, there is no special control applied. XYZ issues proximity access card for the employees and or staffs. Upon resignation, it is handled and destroyed.

		2. As for Data Centre, in which its services are being used by XYZ, authorised visitors by XYZ Management Committee will be given biometric control in place by the Data Centre's security guard. At the data centre, only data centre's employee thumbprint can be used to open the door to escort the visitor in.
7 Personnel Security		
7.1 Access Determination & Control	In place	1. XYZ use Role Based access control. Principle of least privilege also follows the Role Based Access Control. 2. XYZ has administrator role for the customer in which customers are allowed to add new users without allowing the customer to change the underlying storage. All access controlled are strictly maintained by XYZ, and customer admin can choose the access which is made in group for their new users. 3. Access rights no longer required for an individual's normal duties shall be revoked immediately. 4. User's access rights shall be reviewed at a minimum of every six (6) months and/or after any changes to it.
7.2 IT Security Awareness & Training	In place, planned	1. XYZ conducted brief security training for the personnel hired upon employment. 2. There is a process of continuous evaluation that occurs annually. 3. Security access and privilege reviews are conducted every 3 months.

7.3 Acceptable Use	In place	1. There is no customer's user accounts created in Active Directory. 2. Only XYZ staff that need access to the servers have accounts in AD. All customer user accounts are logically created in the application database. Need to know is the basis for access to customer data within XYZ.
8 Threat Management		
8.1 Threat Detection	In place	1. XYZ uses IPS (Intrusion Prevention System), Domain Security Policy, Standard Security Options, and Service Lock Down Policy to control host and network when hosting the applications and information for the end customer. The same control is applied to protect against malicious code.
8.2 Incident Handling	In place	1. XYZ has a formal process in place for detecting, identifying, analyzing and responding to incidents and is rehearsed to properly check that incident handling processes are effective. Everyone within the XYZ's support organisation is aware of the processes and of their roles during incident handling (both during the incident and post analysis. 2. XYZ customer can report anomalies and securities events to XYZ via mail, phone and or fax. 3. However, there is no facility XYZ allowing customer selected third party RTSM services to intervene with its system as there will not be any of the services are outsourced.

8.3 Security Monitoring & Logging	In Place	1. Procedures for the logging and monitoring of information processing facilities shall be documented. The results of the monitoring activities shall be reviewed regularly. The logging facility shall be protected against tampering and unauthorised access. 2. All security relevant events shall be logged for any system handling critical information. This includes, but is not limited to: a) Login failures; b) Data modifications; c) Use of privileged accounts; d) Changes to access models or file permissions; e) Modification to installed software or the operating system; f) Changes to user permissions or privileges; and g) Use of any privileged system function. 3. All security logs shall be reviewed based on the risk factors associated with the information processing facilities. The risk factors shall include but is not limited to the following: a) The criticality of the application processes; b) The sensitivity and criticality of the information involved; c) The past experience of system infiltration and misuse; and d) The extent of system interconnection (particularly

		public networks). 4. Security logs shall be retained for a minimum of three (3) months and access to security logs during this time shall be allowed for only authorised persons. 5. Logs shall be retained on read-only media if possible. 6. System clocks shall be synchronised to an authoritative source to ensure the accuracy of audit logs. A procedure shall be implemented to ensure that any 'drift' shall be corrected. 7. All clocks shall be synchronised regularly to correct any variations over time.
9 IT Asset Management		
9.1 IT Asset Control	In place	1. XYZ maintains an automated means to inventory all assets which facilities its appropriate management. 2. There is no any specified list of assets customer has used since customer cannot choose what to use. Customers are purely using XYZ application.
9.2 Software License Agreement	In place	All XYZ Software is appropriately licensed.
9.3 Configuration Management & Change Control	In place	XYZ has documented configuration and change control

Appendix C. Control Analysis and Risk Correlation

Risk No	**Risk Summary**	**Correlation of Relevant Controls & Other Factors**

1	Poor AAA in systemcould facilitate unauthorized access to resources, privileges escalation, inability of tracking the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data	Control 4.1.3, 4.1.4 and 7.1.3 are in place for closing unneeded and unused user accounts, but are not enforced. A mitigating factor is that the risk depends on a gaining access to the client application. Physical access to the building, workstation areas, & network are adequately protected in 6.1.1.
2	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects however the lack of testing could cause the overlooked defects in system
3	A poor system for user provisioning could facilitate unauthorized access to resources, privileges escalation, inability of tracking the misuse of resources and security incidents in general, etc could compromise confidentiality, integrity and availability of XYZ Web App Data	Control 4.1.3, 4.1.4, and 4.1.8 require regular password changes, but are not enforced for XZY Web App users and or depends on client's requets. Support for required password changes is built into the software but have not been enabled.
4	Denial of service attack could render XYZ Web App unavailable for use	Control 8.1.1 and 8.2.2 is in place and provides detection for such attack. Intrusion Prevention Service is in place to monitor the attack
5	Isolation Failure compromise confidentiality and integrity of XYZ Web App Data	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects. However the lack of testing could cause the overlooked defects in system
6	Social Engineering attack due to lacking of impersonation test could compromise confidentiality and integrity of XYZ Web App Data	Control 1.1.1, 1.1.2, and 7.2.1 are in place, however there is no strict procedure on impersonation test to avoid these matters
7	Unsecured Communication Encryption could compromise confidentiality, integrity and availability of XYZ Web App Data	Control 5.1.2, 5.1.3 and 5.1.4 are in place to control the unsecured communication encryption. However there is still a need to watch over it.
8	Unsecured Data in transit could compromise	Control 5.1.1, 5.1.2, 5.1.3 and 5.1.4 are in place to control the encryption in data in transit however there is still a need to

	confidentiality and integrity of XYZ Web App Data	watch over it.
9	Inability of processing data encryption could compromise confidentiality and integrity of XYZ Web App Data	Control 5.1.1, 5.1.2, 5.1.3 and 5.1.4 are in place to control the inability of processing data encryption. However there is still a need to watch over it.
10	No source escrow agreement could compromise confidentiality, integrity and availability of XYZ Web App Data	Control 1.2.1 are in place and Control 1.2.1, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.1 are in place and could ensure the continuity of service.
11	Inaccurate of resource usage could compromise with confidentiality, integrity and availability of XYZ Web App Data	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects. However the lack of testing could cause the overlooked defects in system
12	Loss of Governance, Change of Jurisdictions could compromise confidentiality, integrity and availability of XYZ Web App Data	Control 1.2.1, 1.3.1, 1.4.1, 1.5.1, 1.6.1, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.1 are in place.
13	Lack of security awareness could compromise confidentiality and integrity of XYZ Web App Data	Control 1.1.1, 1.1.2, 1.2.1, 1.3.1, 1.4.1, 1.5.1, 1.6.1, 7.2.1 are in place.
14	System OS Vulnerabilities could compromise confidentiality and integrity of XYZ Web App Data	Control 3.4.1, 9.2.1 are in place.
15	Poor identification of project requirements could compromise with confidentiality, integrity and availability of XYZ Web App Data	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects. However the lack of testing could cause the undetected defects in system
16	Exploitation of not patched application security defects could compromise confidentiality and integrity of XYZ Web App Data	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects. However the lack of testing could cause the undetected defects in system.
17	Wrong prediction on resource consumption could compromise with confidentiality, integrity and availability of XYZ Web App	Control 3.4.1, 3.4.2, 3.4.3, and 3.4.4 are in place to control the application security defects. However the lack of testing could cause the undetected defects in system.

	Data	
18	Liability from Data Loss could compromise with confidentiality, integrity and availability of XYZ Web App Data	Control 2.3.1 is in place to ensure backup of data loss or stolen is there.
19	Lack of completeness and transparency in use could compromise with confidentiality, integrity and availability of XYZ Web App Data	Control 1.2.1 is in place. However there is no further recollection of how an acquisition will impact on this.
20	Lack of Business and disaster recovery plan could compromise with confidentiality, integrity and availability of XYZ Web App Data	Control 1.2.1, 2.1.1, 2.1.2, 2.1.3, 2.1.4, 2.2.1, 2.2.2, 2.2.3, 2.2.4, 2.3.1 are in place and tested periodically.

The Annual Conference on Management and Information Technology (ACMIT) 2014

Wireless access point protection from un-authorized user in an office environment

Ignasius Irawan Budi P

Master of Information Technology Department of Faculty of Engineering and Information Technology
Swiss German University - EduTown BSDCity, Tangerang 15339

Abstract

Extensible Authentication Protocol (EAP) is authentication method to protect wireless local area network from un-authorized user which there was interaction between radius servers, access point and client device. When EAP was used as authentication method, the authentication can be strengthened by using TLS (Transport Layer Security) certificate where client device and server will use certificate to verify the identity of each other. The certificate must meet requirement on the server and client for the successful authentication. For this time, the authentication method provides highest level for security in wireless local area network because this method can protect man-in-middle vulnerability.

The proposed framework is evaluated by using scenario in testing and live environment to ensure that the authentication has been securely for mutual device authentication.

Keywords: Wireless, Authentication, Radius, Network, Protocol, Authorized

1. Introduction

1.1 Background

Wireless local area network is usually called WLAN which using high frequency radio waves as data transmission rather than wires to communicate between network. Needs of wireless devices become the main thing in activities at the office to support business performance, it was captured from Gartner report on October 2013 about increasing of PC, Mobile computing and smartphone which equipped by wireless device that there was 4.5 % percent increase from 2012 [1].

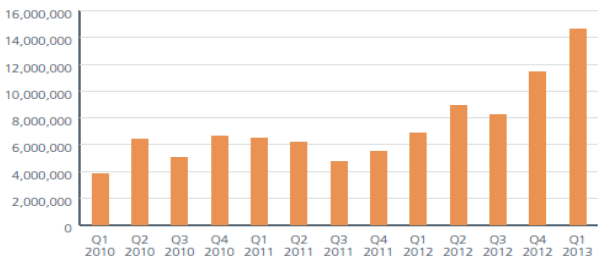


Fig. 1. Malware statistic

Based on the fact of laptops and smartphones growth during 2012 to 2013 resulted in some impact on the network security such as:

- Increasing of malware growth that passes through a wireless network, it was capture from McAfee report Q1 2013 on figure 1 that there was growth of malware from 2010 to Q1 2013 in 241% [2].
- Increasing of virus attack through wireless in matter of decades, it was captured from Trustwave report 2010 [3] on Figure 2

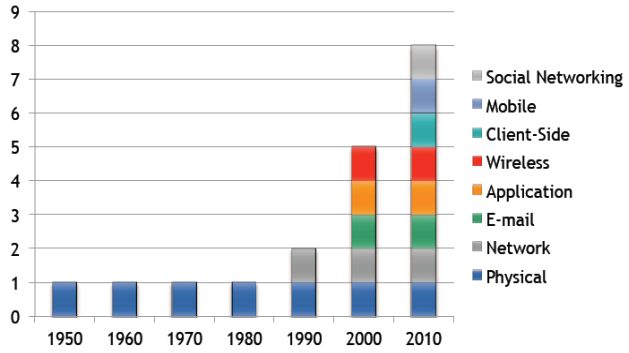


Fig.2 Virus Attack through Wireless

1.2 Problem Definition

When establishing a wireless local area network, so the organization must concern in the wireless security because anyone within range of the wireless can intercept the packet, therefore some problem was arising such as:

- All wireless packets are available to anyone who listens, so that needs security to prevent eavesdropping. Example static Shared Key
- Authentication, many user can access into the same access point and too difficult to map who did what.

1.3 Objectives

According to impact and problem that defined in this paper, an objectives has been defined to monitor and measure this research, it was Maintaining Network Security from the Un-authorized user was accessing through by Wireless Device.

Related Work

In this section we present the research direction in wireless local area network and authentication. One of EAP authentication protocol for WLAN topic from Cisco [4], in which they addressed the direction of the three party models, the authentication is based on a three-party

- The supplicant, which requires access
- The authenticator which grant access
- The authentication server which give permission

According to the development of the current authentication method, there are number of EAP authentication method which each of the method was having advantage and disadvantage. Anjani K.Rai proposed [5] EAP-TLS authentication as the one of strongest method in the authentication which the method provides mutual authentication, so that encryption can be established between supplicant (requires access) and authenticator to make secure communication. This method can protect man-in-the-middle attack, having strong credential security, need certificate for mutual authentication (supplicant and server) and fast reconnect.

Therefore, Khidir M.Ali [6] suggested for organization to select EAP authentication method for WLAN because different authentication method has different security capabilities which the EAP-authentication has to provide mutual authentication, the

selection of EAP authentication method is becoming important. There are several ways to select the algorithm as follow:

- Based on security level
- Based on possible attack
- Based on existing network infrastructure
- Based on upgrade strategy

Something to keep in mind about principle of 80/20 rule that "80% of your success comes from 20% of your effort", it means that 80% of exploit risks can be effectively reduced using 20% of the recommended security procedures and steps, therefore there are best practice to implement the EAP-authentication method such as education & training, product selection and site survey.

Research Methodology

To accomplish the objectives of the research, the following methodology will be followed:

1. *Collecting Information*: This phase is collecting information from the existing systems either in information data, network infrastructure and wireless security. To get information, a maturity assessment has to be conducted for information data, Network infrastructure and wireless security
2. *Analysis Data* : conducting study and investigate from result of maturity assessment, so that some risk can be defined during the analysis.
3. *Design* : Develop the propose network such as Specify the requirement and frame architecture , Determine the framework components
4. *Testing Design* : implement the prototype design into testing environment and live environment.

3.1 Resources, Methods and Tools

The following resources and methods will be required in this research:

- The required operating system to support this research such as Windows XP for Radius server and Windows 7 for client device
- A radius server is needed to keep user and password for authentication, Clearbox radius server trial was decided for radius server.
- Access point device that supported to EAP-TLS authentication, TP-Link WA601G was decided as access point device.
- The required software for monitoring testing implementation such as wirekeysview software to capture key of access point, wireshark to capture traffic and key of access point
- Working network platform in testing environment and live environment (sampling office)

3.2 Collecting Information

In this phase to collect information from existing system, then some assessment has been conducted to verify maturity of the system, therefore the maturity assessment was conducted in information data, network infrastructure and wireless security. The result of assessment was being captured as follow

Business Information data

- All client data was kept in softcopy
- The information data has kept in relevant department folder
- Active Directory has been installed for authentication into the folder

Network Infrastructure

- All wire and access point were connected to core of switch hub in locked Server room
- Mobile computing can access wire or wireless with WEP shared key
- All Communication room was properly kept and operated in server room

Existing Wireless Security

- WEP shared key was being used for Authentication mechanism
- The Access point not supported for Extensible Authentication Protocol
- The shared key will kept in the mobile computing after authentication successfully

3.3 Data Analysis

According to maturity assessment result, there was a main security risk. The risk was using of WEP shared key, some article and paper has declared that some vulnerability for using WEP shared key [7]

- In 2005, Federal Bureau investigation gave a demonstration to crack WEP protected network in 3 minutes
- In 2001, Scott Fluhrer, Itsik Mantin, and Adi Shamir was a cryptanalysis of WEP that exploits the way the RC4 ciphers and IV are used in WEP
- Possible attack from personal computer by freely available software such as aircrack-ng in minutes
- WEP relies on a single key that is used together by many users, so that be difficult to control the users.

From the analysis data, we can imagine if the attacker know the wireless/access point key where all information company was kept in the server (softcopy).

3.4 Design

When we are talking about WLAN security, the design has to think about the impact with another network when designing WLAN. Therefore, the designer has decided to provide WPA2-enterprise with EAP-TLS as authentication method for design WLAN solution to protect wireless access point.
Some reason why using WPA2-AES enterprise with EAP-TLS authentication method

- WPA2-AES enterprise was created to fix known security issue in WPA
- The key are provided by wireless client through Radius and EAP (Extensible Authentication Protocol)
- EAP-TLS authentication method can protect man-in-the-middle attack
- EAP-TLS authentication is having certificate as mutual authentication for client device and authentication server

The design of WLAN security is captured on figure 3.

EAP-TLS authentication stage

Client device / Supplicant is initializing to connect into access point. After successfully connection, blocking the access point the client to communicate further. WPA2-AES will authenticates the user to the server is used for authentication based on 802.1x (Clearbox RADIUS) by using the Extensible Authentication Protocol (EAP), the two parties (the client and server) will authenticate to each other through an access point. After the 1st authentication is successfully, the 2nd mutual authentication is using certificate to meet certificate in client device and radius server (published by certificate authority).
It was noted that Certificate authority server is being kept in radius server.

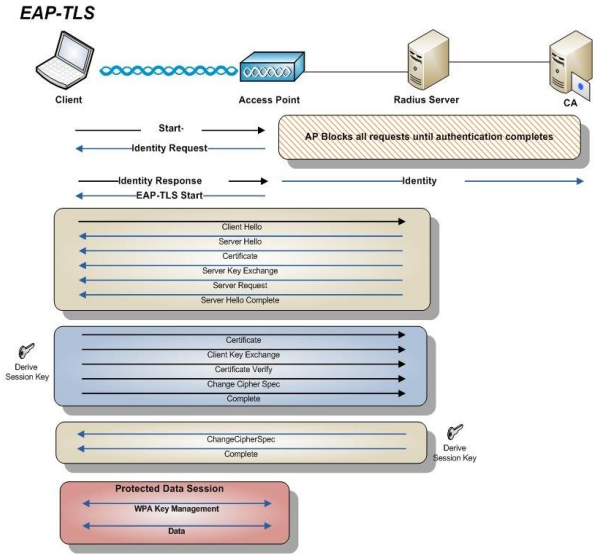


Fig. 3 WLAN authentication stage

3.5 Testing Design

To ensure that the implementation of authentication is in accordance with the required design, some scenario or methodology has to be defined:

- Capturing vulnerability of shared key authentication with WEP key in the existing wireless
- Implementation design into testing environment with 2 sample laptop
- Implementation design into live environment with 3 sample laptop
- Capturing advantage of EAP-TLS Authentication / Monitoring measurement in the existing network

3.5.1 Vulnerability of shared key authentication with WEP key

Based on some observation in laptop connecting network through by wireless / access point, the user can read WEP password through by wirelesskeyview or WZCook which the password was stored in the user laptop as figure 4.

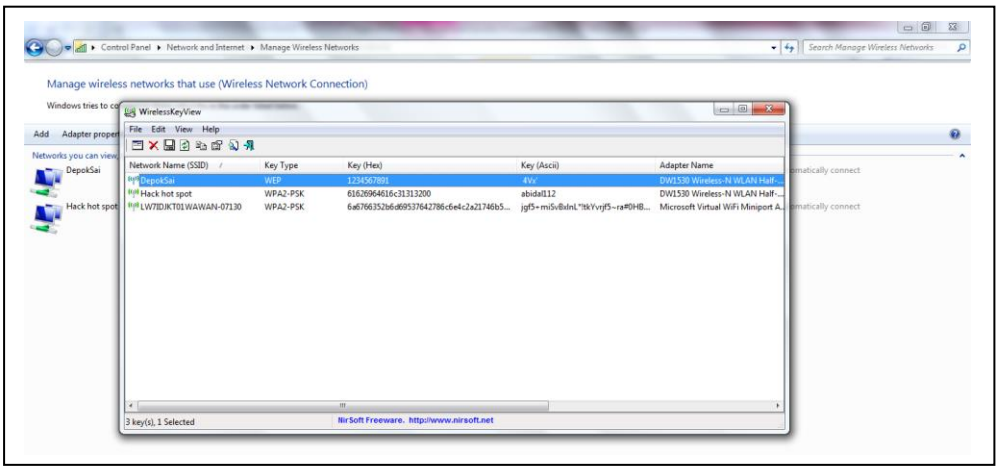


Fig.4 Snapshot of wireless key

As we know that WEP key is having vulnerability which WEP key is based RC4 algorithm. now, the algorithm is easily cracked when any process of exchanging

challenge text over the wireless link. Therefore, the key can be known by sniffing process and cracked from packet sniffer by a network software such as aircracking

3.5.2 Implementation design in testing environment with 2 sample laptop

To implement the design, then a scenario has been defined. In the scenario, the device was setting almost similar with the system existing in the corporate such as using of IP number for access point and authentication server.

2 IP has to reserve for access point and authentication server, so we are using IP address 10.xxx.xx.29 as access point and 10.xxx.xx.28 as authentication server. During the trial access was conducting from 2 clients device (dell Laptop and Gateway) as client device, so that the testing environment configuration is captured on figure 5. Result of implementation design in live environment has been successfully done in corporate local area network. To capture the implementation, then some snapshot have been captured in appendix B in this paper

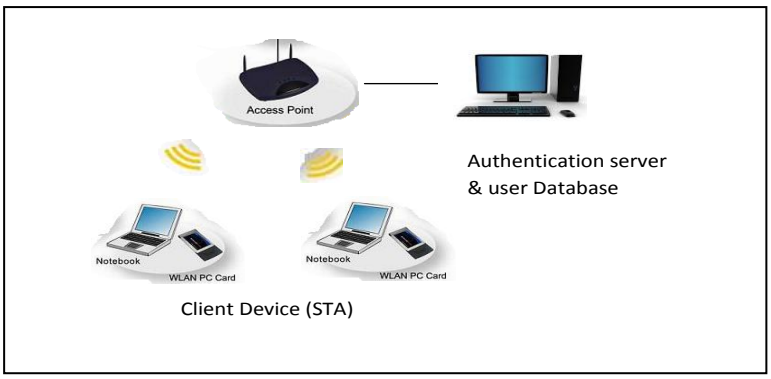


Fig.5 Testing Environment Architecture

The installation of authentication server was started which the server was installed Clearbox radius server. The server is having feature to use internal database without install SQL, LDAP or Active directory to authentic the user name and password.

To ensure that sever has fully worked as EAP-TLS authentication requirement, some log has been capture in appendix A for rejection and successfully authentication between client device and radius server.

Result from testing environment, the concept design should be used in live environment with the assumption that no changing of SSID name. Due to the purpose of this design only for testing of the EAP-TLS authentication method ability, then SSID name was not using characterize the corporate name

3.5.3 Implementation design in live environment with 3 sample laptop

After the implementation design in testing environment has been successfully, then the system carried out into live testing with a scenario that there was no changing of IP address in access point, authentication server and SSID name. Because based on some experience in testing environment while the SSID name or IP address was changed, then certificate must be re-created to meet the system requirement.

A scenario testing in live environment has been defined and the testing was conducted with 3 laptops as shown figure 6.

3.5.4. Capturing advantage of EAP Authentication/Monitoring measurement in the existing network

After all the installation was finished and trial & error for the authentication has been conducted, we are trying to monitor authentication between client device and

authentication server, the step is checking what the hex key still can be captured from client device or not.

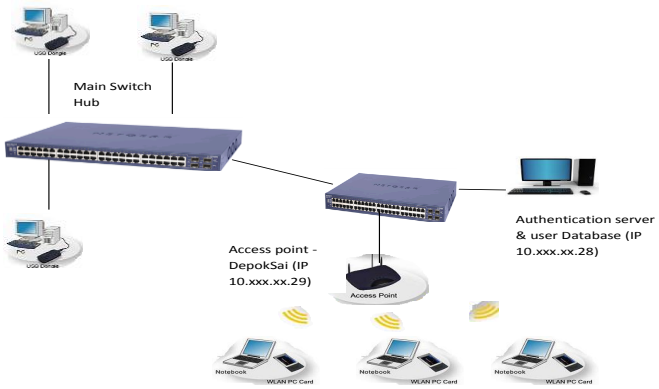


Fig. 6 Live environment Architecture

The captured result can be seen on figure 7 that the SSID name not show up in the list on wirelesskeyview software.

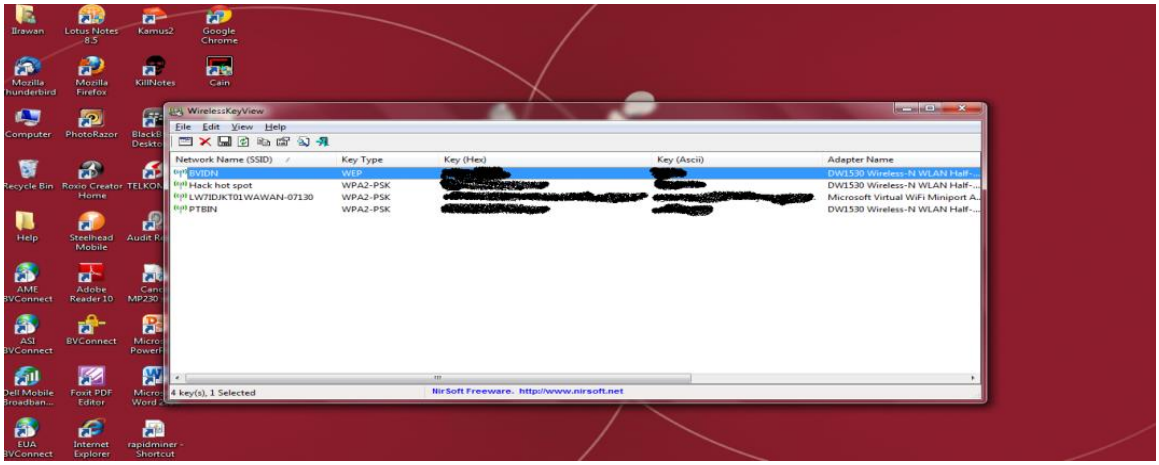


Fig. 7 Snapshot of wireless key in live environment

Conclusion

In specific can be concluded during establishing of authentication design that:

- The EAP authentication will help IT team to manage security network in office environment for Wireless Local Area Network and to ensure that only authorized people can access into WLAN
- In managing security network for WLAN, the selection of authentication method was becoming important before replacing the existing method
- According capabilities of radius server the software can joint into existing resources in the company, such as using of existing active directory.

Recommendation

According to implementation objectives that this paper is giving support to IT team to make securely of wireless connection, so that only authorized user can joint into local area network. As per the testing result in live environment that design of EAP-TLS authentication can be used in wireless on LAN of the corporate environment. Some action plan should be defined by corporate to implement this method.

- WLAN security policy should be established to keep commitment management and IT team.
- Formal process for registration and de-registration wireless user should be established to maintain wireless user.
- Review wireless user access should be regularly conducted to ensure that only personnel is having access can joint into WLAN
- To replace the existing router with router was supported for 802.1x authentication such as D-Link DWL-G730AP or TP-Link WA601G when the existing router not compatible with EAP-TLS authentication method
- To provide Authentication server (hardware and software) such Clearbox Radius or TekRadius or freeradius
- To install sniffing software to monitor the wireless connection and establish plan for network penetration test.
- Provide training for IT team to establish the authentication method and wireless monitoring

References

[1] Gartner, Inc. Press Release: Gartner Says Worldwide PC, Tablet and Mobile Phone Shipments to Grow 4.5 Percent in 2013 as Lower-Priced Devices Drive Growth. STAMFORD, Conn., October 21, 2013. Available from URL: http://www.gartner.com/newsroom/id/2610015

[2] McAfee Labs Researches, McAfee Threat report: first quarter 2013

[3] Charles Henders, Director of Application Security Services Trustwave's SpiderLabs. Global Security statistic and trend in annualy global security report ; 2011

[4] Krishna Sankar, Andrew Balinsky, Darrin Miller, Sri Sundaralingam .EAP authentication protocol for LAN. In: Sample of courtesy of Cisco press date on February 18, 2005

[5] Anjani K.Rai,Shivendu Mishra and Vimal Kumar. Strong Password Based EAP-TLS Authentication Protocol for WiMAX. In: (IJCSE) International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010, 2736-2741.

[6] Khidir M. Ali, Thomas J. Owens. Selection of an EAP authentication method for a WLAN. In: Int. J. Information and Computer Security, Vol. 1, No. 1/2, 2007

[7] Wikipedia, the free encyclopedia. Wired Equivalent Privacy. Last modified on 3 January 2014. Available from URL : http://en.wikipedia.org/wiki/wired_equivalent_privacy

The Annual Conference on Management and Information Technology (ACMIT) 2014

In Search of Code Ethics Principles for IT Professionals in Indonesia

Carlia Isneniwati
Id-SIRTII/CC, Jakarta, Indonesia
Carliacm@gmail.com

Abstract

A type of standard problem in computer ethics occurs because there is no policy about how computer technology should be used. Computers are provided to us with new capabilities and giving us a choice of use. Frequently, not only a policy that gives direction in this situation, the existence of a policy has the same function. A primary goal of the Computer Ethics is to explain what we should do in these circumstances, for example, to formulate a policy that aims to direct our activities. Of course some ethical situations are suitable for individuals and some for community. Computer ethics includes consideration of both individual and community to user ethics of computer technology. Computer ethics include (1) identification of the cause of the gap in policy; (2) clarification of the concept which is chaotic; (3) formulate policies for users of computer technology; and (4) ethics justification such as policy**.**

Keywords: Computer Ethics; IT Professionals

1. Introduction

Technology is created to help humans to cope with their physical limitation. Whether we realize it or not, act of violation starts to occur. It starts with, for instance, copying contents of a website illegally to hacking, carding and so on. Regulations to deal with violations need to be established. The regulation will be effective if the community obeys the regulation and is recognized as a type of limitation to regulate someone's behaviour. Every community has their own definition about what is right and what is wrong and every community has their own way to develop and evolve them among the members. To find out what is the right or wrong doing in a community, every individual has to have ethics to answer the question.

2. Research Problem

The author conducted interview with Mr. Teddy Sukardi and Mr. Djarot Subiantoro, both well-known IT experts in Indonesia. They were asked about IT professionals' code of ethics. Subsequently, the conclusions from mentioned critical points are:

a. There is no code of ethics for IT professionals in Indonesia.
b. Violations of IT Ethics by IT professionals have severe consequences that may impact the reputations of individuals as well as the organizations that they belong to.
c. There is an urgent need for a code of ethics for IT professionals in Indonesia.

d. It is believed that having an IT professionals' code of ethics in place would help decrease the problems of IT ethics implementation in Indonesia.

Based on the critical points above, the purpose of this study is to design a basic framework of code of ethics for IT professional in Indonesia.

3. Research Methodology

This study uses a combination of research methodologies, including qualitative and interpretative research. These methodologies are chosen because they are believed to be suitable for studies in ethics. Further explanation about both methodologies and the steps of the research process are explained below.

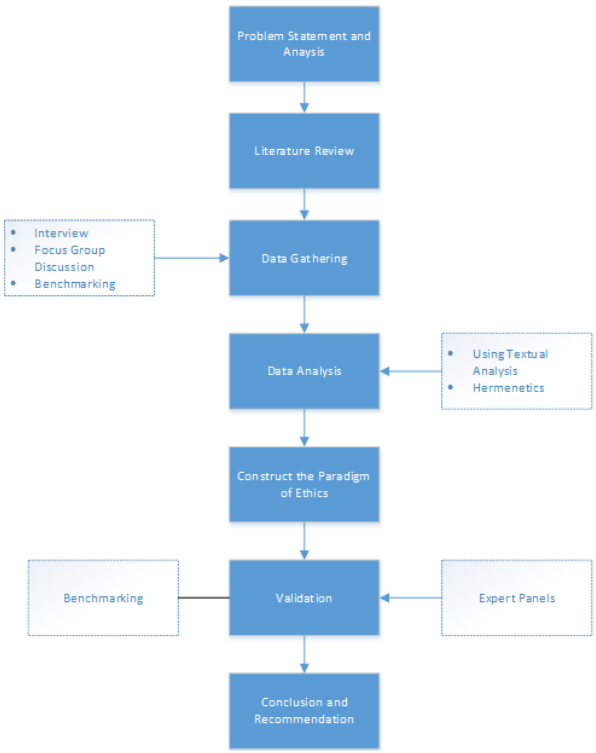


Figure 3. Research Methodology

3.1. Hermeneutics

The data obtained from the interviews of the group discussions is presented in narrative form based on the textual data. Below, pattern similarity is done to form a model.

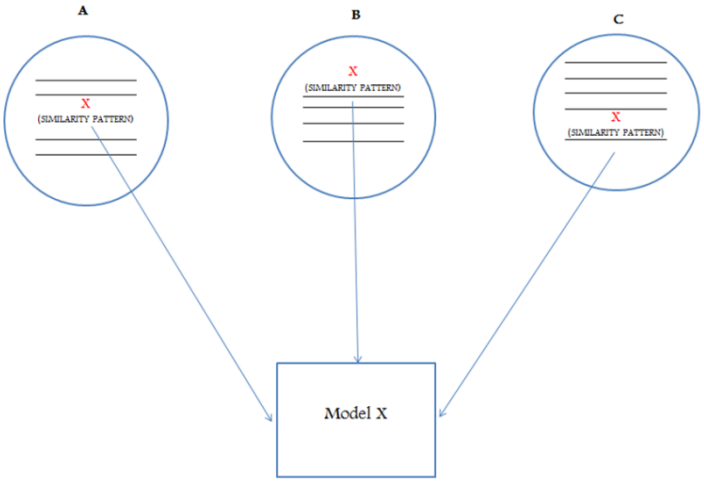


Figure 4. Hermeneutics Process

3.2. Interpretive Process

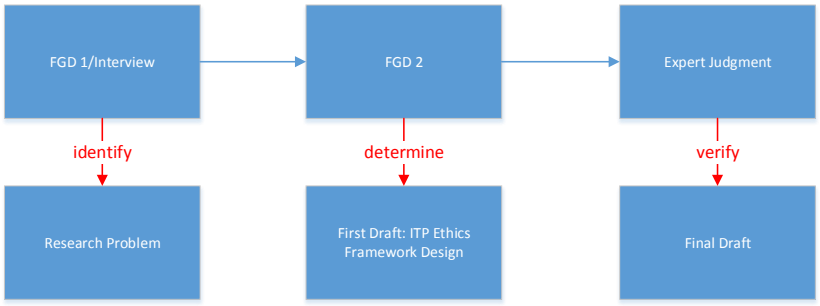


Figure 5. Interpretive Process

The Intepretative Process consists of three steps as described figure 3. The first step is the identification process through Focus Group Discussion (FGD) or Interview, and the outcome is the definition of the research problem. Second step is the process to determine the First Draft of ITP Ethics Framework Design through FGD. The final step is the verification process through Expert Judgement resulting the Final Draft of the research.

4. Research Design and Experiment

The research design and experiment conducted by the author used to formulate the framework design of IT Professional Ethics in Indonesia is based on four factors: the theory of ethics, benchmarking to best practices, macro perspectives and conditions in Indonesia. The theory of ethics may not be as dynamic as the other three factors.

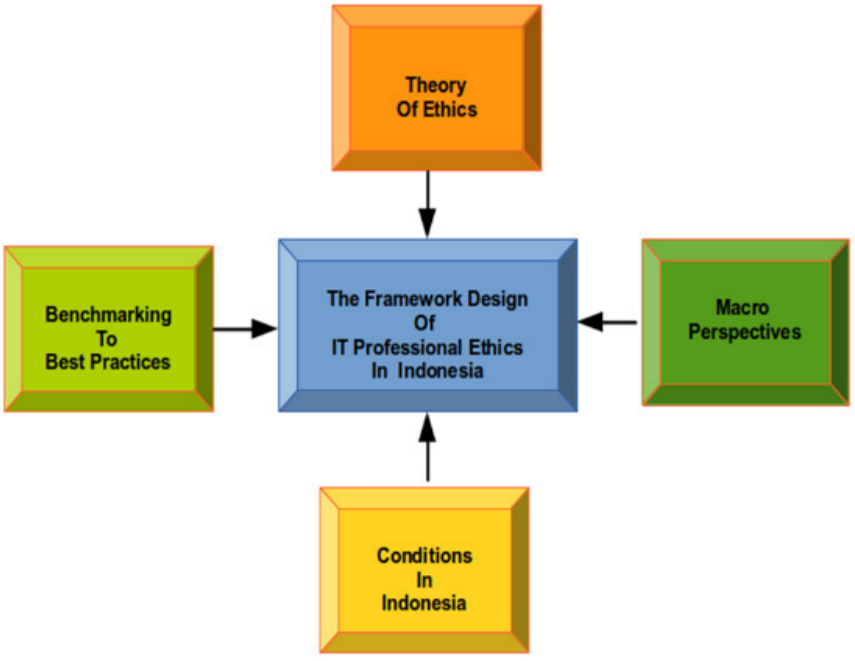


Figure 6. Research Design

4.1.Theory of Ethics

This is the summary of theory of ethics used in this research. Table 1 below shows the details.

Table 1. Summary of Theory

Author	Main issue	Field	Implication to this issue
Martin, 1993	Ethics as "the discipline which can act as the performance index or reference for our control system". Ethics will provide some sort of restriction and standard that will govern human interaction within the social group. In a sense that is specifically associated with the art of human interaction, this ethic then was prepared in the form of rules (code) systematically written deliberately by moral principles that exist. Also ethics is required to function as a tool to judge all sorts of action that deviate from the ethical code of conduct or a reflection of what is called "self-control".	Ethics definition	As the basic of theory
Wignjosoebroto, 1999	In professional environment, ethics is controlled by a built in mechanism in the form of professional code of conduct. This is assessment from the inside by colleagues	Professional ethic definition	As the basic of theory

	and fellow professionals to protect from all forms of abuse and misuse of expertise. Professionals' ethics include standard of behavior expected of professionals such as honesty, integrity, transparency, accountability, confidentiality, objectivity, respectfulness, obedience to law, and loyalty. This standard of behavior applies to the personal level as well as the organization level.		
Walter Maner, 1976	Computer ethics as a branch of ethics that studies the implementation issues of ethics "aggravation, transfer or creation of computer technology"	Computer ethic definition	As the basic of theory
Deborah Johnson, 1985	Computer ethics is a field that examine the computer, "It is a new version of standards moral issues and moral dilemmas, worsening old problems, and focuses us to apply ordinary moral norms in uncharted things". Unlike Maner, Johnson did not think that the computer created a whole new problem in ethics, but rather	Computer ethic definition	As the basic of theory

	provided a "new thinking" to issues which are well known such as ownership, power, privacy and responsibility.		
Krystyna Gorniak, 1995	Naturally the computer revolution indicates that ethics in the future will get a global character. It will be globally in a vacuum chamber, since it covers the whole world, it will also become global in the sense of all human relationships. In the future, the rules of computer ethics should be respected by the majority of mankind on this earth. In other words, computer ethics character will become universal; it will become global ethics. The computer revolution will end in a new ethical system; it will become global and naturally will cross cultural boundaries. New ethics in the information age, according to Gorniak, will replace ethical theories which are narrow in nature like Bentham and Kant - the theory is based on the relative relationship which covers cultures in	Computer ethic in the future	As the basic of theory

	Europe, Asia, Africa and other local areas around the world.		
Deborah Johnson, 1999	We will be able to say that computer ethics has become ordinary ethics and common ethics has become computer ethics. Johnson often maintains the view that computer ethics focuses on new moral issues, with the assumption that computer ethics is compared with the replacing theories such as Bentham and Kant. Current ethical theories and principles according to Johnson, will remind us to rocky foundation of ethical thought and analysis, and the computer revolution will lead to ethical revolution.	Computer ethic in the future	

4.2.Focus Group Discussion

In this study discussion were conducted in order to obtain the opinions from IT experts in Indonesia. The experts were given questions about issues related to regulations, ethics and their implementation. Subsequent to the focus group discussions, the notes were given to the experts for confirmation. The following are the results of the discussions after the confirmation and the text in bold are the keywords.

1) What is your opinion about regulations in cyberspace?	
Dr. Rudi Lumanto	**In reality regulations are always behind** the actual requirements and that is why regulations always need to be adjusted accordingly. **Code of ethics in other professions outside IT are normally created by associations and based on certain specifications related to the profession**. Some concept for the cyber space already can be found in the books “the digital age” and “the world is flat”. **We do not formulate special regulations for cyber space,**

	but eventually we will finally also come up with regulations for cyber space. One example is of Bit Coin, a digital currency, currently being used on the internet that has been a breakthrough in existing internet and financial norms.
Bisyron Wahyudi M.T.I.	It is required because **cyber space creates connections for many people**. Like in real life, civilization need rules in order for people **to respect one another and interact based on certain norms**.
Didik R Partono M.T.I.	**Cyberspace has a few unique characteristics**. One of them is the ability of people to interact with one another without actually having to meet face-to-face. In cyberspace people also build communities that represent similar communities in the non-cyber world. **These characteristics enable a lot of improvements in the quality of life. They include socializing, learning, creating, and working in teams to produce products and to conduct activities.**

2) Are rules or code necessary? Why?	
Dr. Rudi Lumanto	Naturally regulations should be there like in the day-to-day rules of traffic and transportation. Finally we end up following the regulations, even though violations will also be there. The same applies in cyber space. There will be different interests for different people. That's why perhaps **there needs to be regulations for the content of cyber space**. Most important[y other people's interests are not disturbed.
Bisyron Wahyudi M.T.I.	It is required because cyber space creates connections for many people**. Like in real life, civilization need rules in order for people to respect one another and interact based on certain norms**
Didik R Partono M.T.I.	Yes **rules and code are necessary**. Like in the real world people can be trusted but they can also misuse the trust, especially in cyberspace when we do not know the people in person nor also meet them face-to-face, the **potential for abuse and misuse exists**. In cyberspace one person activity can easily impact the lives of many people because there is no boundary of space, time, and geography. That is why **the potential negative impact of abuse can be quite high**, depending on the type of activities and the range or coverage on the particular action. The other reason why rules and code are necessary, because **law enforcement in cyberspace, even though important, has many**

	limitations; law enforcement requires evidence and in cyberspace that would be digital evidence. Obtaining and presenting digital evidence in the court of law can be complicated and very challenging. That is why the other important tools to control the citizen of cyber space beside the laws is ethic, including professionals' ethics..

3) What about the value and the sovereignty of a space/place? Is it also necessary? Why?

Dr. Rudi Lumanto	**Sovereignty is equal to identity**. In cyber space we need to firstly define sovereignty.
Bisyron Wahyudi M.T.I.	**Sovereignty is required, because it belongs to the nations**. So countries have the ability to implement regulations and sanction those who do not follow the regulations Actually the regulations can be combined and put together with the regulations of real life, meaning **there need not be separate regulations**, but because cyber space has different characteristics the way the regulations are **executed can be different.**
Didik R Partono M.T.I.	Value and sovereignty of cyberspace is also necessary because for many people cyberspace is the same as non-cyberspace if almost of your time well day to day activities is conducted in cyberspace, like what is experienced at present than cyberspace will be important and of strategic value.

4) There are some behaviour that can cause an economics aggressive disturbance. Here are the list of some of those behaviour:
   - Spamming
   - Advertising, Promotion and Demand
   - Secondary Use of Data
   - Serious Plagiarism
   - Abuse of Intellectual Property Rights (Copyright Violation)
   - Hacking
   - Viruses and Worms
   - Security Breach

Is it necessary to have IT ethic for each behaviour? Why? (Describe the reason for each behaviour)

Dr. Rudi Lumanto	Yes, indeed. In real life it is actually the same where for **criminal conduct it does not come into the dimension of ethic** because these problems already have regulations to handle it
Bisyron Wahyudi M.T.I.	Yes, **hacking initially was a positive and creative thing and not damaging**. Like hacking at first viruses was also

	not intended to damage, **but was later used by bad people**. Security breach is clearly an offense to security regulations.
Didik R Partono M.T.I.	**Spamming creates productivity issues for victims and also can be misuse to distribute malware**. **Hacking activities can also create many problems in IT infrastructure and can be used by criminals to conduct unlawful activities such as fraud, identity theft, etc**.

5) By referring to these components: honesty, integrity, transparency, accountability, confidentiality objectivity, respectfulness, obedience to law, and loyalty, what is your opinion about framework of ethics for IT professional especially in Indonesia, compared to other professional association or other country's IT professional organization that already have a professional ethics?	
Dr. Rudi Lumanto	Yes, **those are universal norms and morals that must be implemented in daily life, especially for code of IT professional ethics.**
Bisyron Wahyudi M.T.I.	**Ethics is about morals that relate to individuals. In developing countries punishment is still required**.
Didik R Partono M.T.I.	Special focus is needed to address the areas of **accountability**, **confidentiality** and **objectivity**. **Confidentially is one important area because IT professionals will have access to a lot of software, hardware proprietary of organizations/companies as well as private information that need to be protected**.

4.3.*Summary*

The focus group discussion came up with the following points

a. On Cyber Space:
   Cyber space creates connections for many people, to respect one another and interact based on certain norms, like in real life, civilization needs rules in order for people to respect one another and interact based on certain norms. There needs to be regulations for content of cyber space since regulations already exist outside cyber space
b. On Sovereignty:
   Sovereignty is equal to identity, and is required because sovereignty belongs to the nation, meaning there need not be separate regulations. But because cyber space has different characteristics, the way the regulations are executed can be different.
c. On Economic Disturbance:
d. Criminal conduct does not come under the dimension of ethics. Nevertheless criminal conduct can also be prevented by implementation of ethics by IT

professionals. Some of the behaviour that creates economic disturbance include hacking, spamming, creating and distributing of malware, and security breach.

e. On Components of IT Ethics:

The typical component of IT ethics are honesty, integrity, transparency, accountability, confidentiality objectivity, respectfulness, obedience to law, and loyalty. Those are universal norms and morals that must be implemented in daily life likewise for code of IT professional ethics. Emphasize should be given to accountability, confidentiality and objectivity, because these components are important in the field of IT professionals. The specific professional's ethics should follow the general IT professional's ethics.

f. Who should formulate the IT professional's ethics?

As we have learned from other countries, as well as in Indonesia, the ethics should be formulated by the communities of professionals, normally in the form of their respective association. This approach will also be useful for successful promotion, implementation and further development of the ethics.

5. Framework of Ethics for IT Professionals in Indonesia

IT Professional Ethics is formulated or developed from values, norms and culture existing in a community. As professional ethics has to do with a certain area or profession, IT professional ethics also need input from information technology characteristics and developments. The formulation and development is normally done by associations related to the profession. IT professional ethics will be used firstly by the professionals within the IT community itself. Secondly the stakeholders will also benefit from the IT professionals ethics implemented. The stakeholders will be the IT users, consumers, organizations that rely on IT to perform their day-to-day business including the government that provides public services. The government as a regulator will also influence and use IT professional ethics as a reference to formulate law and regulations.

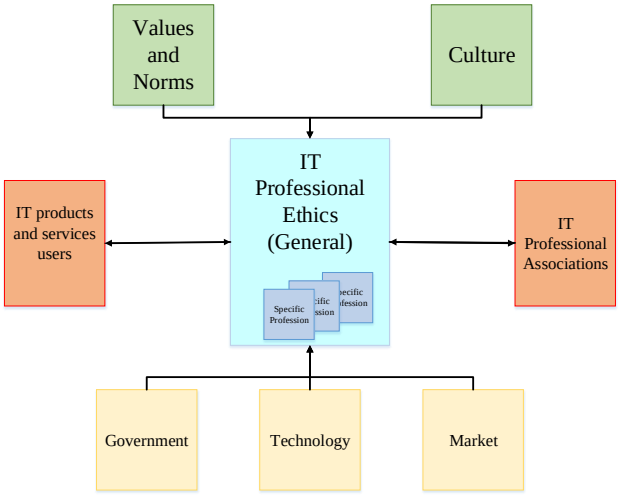


Figure 7. First Draft

6. Expert Judgement

This study uses expert judgment as a method to verify findings and make final conclusions.

This was done by forming a panel discussion of that consists of:

1. Ir. Aswin Wirjadi, Chairman of CIO Forum of the Indonesian Bank Association (Perbanas).
2. Prof. Dr. Richardus Eko Indrajit, Chairman of Indonesia IT Computer Higher Education (APTIKOM).
3. Dr. Eko Budiardjo, Chairman of Indonesian IT Professional Association (IPKIN).

The opinions, comments and suggestion from these experts are described below:

Aswin Wirjadi	IT Professional Ethics is important to have and to be used as a reference for IT professionals. He is surprised that the Indonesian IT communities do not have any professional ethics to refer to. He believes that **when norms, values and the culture is already formed to support IT Professional Ethics, then the market and IT users will immediately benefit from the IT Professional Ethics**. The influence of culture Professional ethics is not easy to define.
Eko Indrajit	IT Professional Ethics are **influenced by two major types of external factors, which are tangible and intangible external factors**. The tangible external factor includes government regulations, technology changes and the global market. The intangible external factors are value, norms and culture. This will make IT Professional Ethics be dynamic due to the many factors that influence them.
Eko Budiardjo	The feedback and claim process from IT beneficiaries/users will need to go through a body or organization and also require some formal process. The body in the professional communities, including professional associations, **may be a form of "Board of Ethics"** that monitors professional conduct, and where applicable give protection, judgment and sanctions. **The IT Beneficiaries can be represented by consumer protection organization that can address claims and feedback to the board of ethics of the respective professional community.**

6.1. Summary of Expert Judgment Panel and Suggestions.

Based on the panel conducted, it can be concluded that IT professional ethics is important. The experts' panel also provided insight suggestions on how to develop ethics, factors that influence ethics, how ethics will benefit IT professionals as well as IT users/beneficiaries. More details are described in figure 8 below.

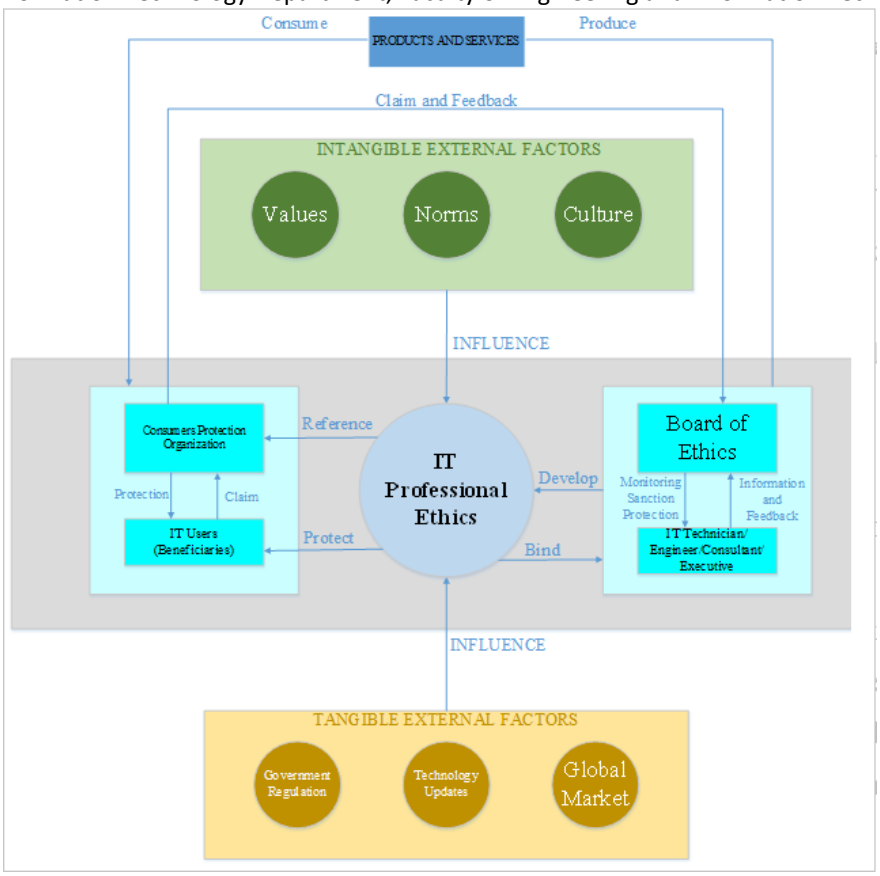


Figure 8. Final Draft

7. Conclusion

The conclusion of the study on Ethics for Information Technology Professionals: The Framework Design within Indonesian Context is as follows:

1. The Need to Have IT Professional Ethics in Indonesia
   The IT profession, as other professions, requires ethics to be used as reference for day to day practices. This is important considering how role of strategic information technology takes part in almost every aspect of our lives and the role that IT professionals play in this respective area.
2. The Existing Condition on IT Professional Ethics in Indonesia
   Implementation of IT ethics in Indonesia is not where it should be. Many challenges exist in making IT ethics part of IT practice especially by IT professionals. One particular challenge is that there are no existing documents or write up that describes IT ethics for Indonesian professionals.
3. Major Components of Ethics Framework for IT Professional in Indonesia
   The major components of ethics framework design for IT professionals in Indonesia will be:
   a. IT Professional Associations in Indonesia
      IT professional ethics is more suitable to be developed by IPKIN. Subsequently the IT professionals' ethics can be used by other specific associations, such as IKTII, as a reference for more specialized ethics.

b. Ethics Formulation and Updates
   Since IT ethics is dynamic due to the factors that influence it, respective associations need to periodically review it and make necessary updates accordingly.
c. IT Professional Ethics Implementation by IT Professionals
   The ethics will be binding to the conduct of IT Professionals and will be used as reference for ethical conduct measurement. The ethics can be further promoted and endorsed in day-to-day life by all stakeholders. IT Professional's Ethics Implementation by the IT Users/Beneficiaries.

8. Recommendation

- IT professional association defines the ethics in their respective areas and forms it in a readable document to be further used as a reference by their members.
- One association in IT, namely IKTII, already has an organization structure to handle ethical issues. This body can be activated to formulate, promote and uphold IT ethics
- Subsequently this IT ethics formulation and implementation can be used as a reference by other IT associations to implement IT ethics.
- IT ethics can also be formulated for all IT association in general format as a guideline for further detailed or specific ethics development. For this IT associations will have to sit down and work out an agreement on what should be the general IT ethics for Indonesia
- The government may facilitate this initiative and also take part in the promotion of it. It is recommended that the association consider the following components to be part of the IT ethics formulation, which are honesty, integrity, transparency, accountability, confidentiality, objectivity, respectfulness, obedience to law, and loyalty. Each component will have to be described considering specific law, regulation, values, conditions, culture, as found in the respective professional environment in Indonesia.

References

[1] Martin, Elizabeth Cooper, Morris B. Holbrook. *Ethical Consumption Expenses and Ethical Space*. 1993. UT: Association for Consumer Research.
[2] Wignjosoebroto, Sritomo. Etika Profesional: Pengalaman dan Permasalahan. 1999.
[3] Maner, Walter. Unique Ethical Problems in Information Technology. Guildford: Opragen Publications; 1996.
[4] Johnson, Deborah G. Computer Ethics. New Jersey: Prentice Hall; 1985.
[5] Gorniak, Krystyna. The Computer Revolution and the Problem of Global Ethics. Guildford: Opragen Publications; 1996.
[6] Johnson, Deborah G. Computer Ethics in the 21st Century. Rome: ETHICOMP; 1999.

The Annual Conference on Management and Information Technology (ACMIT) 2014

Improving Productivity of Radiology Department

Ahmadi, Herry

Master of Information Technology Department, Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia

Abstract

Over the years, impact of digitalization has been implemented in every aspect of human life, including the healthcare and hospital environment. Vendors and manufacturer are making the competition to implement to be the highest, the fastest, and the best solutions to the market and become the world leader that can attract the hospital and healthcare facility to use their system and their products. However all of the digital equipment are not standardize, the integration of system, data management and archive are the main problems in Radiology department eventhough using standard medical image (DICOM) protocol. We propose digital solutions in Radiology department that implemented using known as RIS or Radiology Information System and PACS or Picture Archive Communication System that using open source software and easily adaptable technology with no boundaries of applications and vendor neutral. Our paper shows that through digital solutions provided by radiology department will improve the productivity of doctor, radiographer and administration people. Digitalization products with RIS and PACS also answer the needs of speed and manageable image storage in the hospital.

Keywords: Radiology, RIS, PACS, Productivity, Image Processing

I. Introduction

Digitalization has been applied in most of the aspect of human kind recently, and it's become more of the technology driven to lead to costumer to better solution, fast and accurate. Healthcare and hospital business are also applying the digital technology, with various field of digitalization from Radiology, Laboratory, Sterilization and et cetera. Digitalization also becomes the key point to increase the productivity and the output of the healthcare and hospital. Saving time, cost reduction, reduce of waste, synergy between wards, unit and operator are the productivity that improved by using digitalization. [1]

With the incremental growth of hospital and clinics in Indonesia more than 39 % annually [2], demands of new medical equipment products are still increasing and promising. Each hospitals and clinics are in constant competition to each other's, to become better in service excellence, wide range of applications and customer satisfaction. Looking at these trends, plenty of medical equipment supplier trying to provide the best solutions and products update to fulfill the hospital needs. The current innovations that blossom are the needs of fast and accurate information about the human body. This digital innovation is known as Digital radiology. These digital solutions are spread tremendously across the hospital field, where the main objectives are to cut the cost and to improve the service to patients. More and more new equipments are coming with digital formats and the images produced by the new digital equipment are become a huge, wasting of resource and not effective in the storage and access that potentially facilitated by Radiology Information Systems.

PT. ABC also actively participates in medical and healthcare business by supplying the Radiology department. Having appointed by XYZ Healthcare a Belgian based company, to be the sole agent in Indonesia with range products of films, consumables, computer and digital products of Radiology makes PT. ABC are famous and become the 2nd biggest player in Radiology films field. XYZ Healthcare provides full range solutions for data archive known as IMPAX. And XYZ through PT. ABC are selling this products into Indonesian market with the specific target of chain hospital and teaching hospital. However over 3 years since the projects started, none of the products nor solutions sold to the hospital in Indonesia, with various reasons but the biggest are pricing issue. Learning from PT. ABC mistake, our competitor are switching the portfolio from world class principals and brand into a medium-cheap but limited application solutions from India and China. And eventually this options are become a breakthrough and remarkable.

Management of PT. ABC think that, if they don't make an alternative solutions against this facts, PT. ABC market will soon be gone and the competitive advantages are obsolete, and last PT. ABC costumer will soon move to competitor products. PT. ABC must create products that cover the state of the art of the XYZ IMPAX but can penetrate to the market like various products from India and China that already sold expansively in Indonesian market. Another perspective of facing the challenges are disruptive technology, the concept invented by Christensen in 1997 are very popular in order to find the feasible solutions and answer the challenge in digital technology war.

II. Framework

According to Saari 2006, Productivity is define as ratio of output to inputs ; basically it is like an average measure of the efficiency . And meanwhile production is define as process of combining various material inputs and immaterial inputs in order to make something for consumption or finished goods. [3]

According to the Jensen, Michael and Murphy, Kevin, performance is productions or productivity ability to generate income that creates finished goods, because the income from production is generated in the real process and has value added in the end. So the production performance can be measured as the average of the income or as an absolute income that has value added and finish products [4].

There are two main mechanisms that can affect the productivity growth, increasing competition which drives out poorly performing sales and the adoption of new technologies. Increasing competition such as increase the sales, reduce the price and create additional products that can broaden the product diversifications. Adoption of new technology is implementing ICT in the business process and reduces unnecessary non value added work [5]. According to Tracy, 2012 Radiology Information System (RIS) is defined as computerized database of information that used by radiology departments to store image, manipulate image, and distribute patient radiological data and imagery to all over the radiology network and respective user that have the access of the information. And it's also explained that the system basically consists of patient tracking of information and scheduling not only to meet the doctor's needs, but also to receive the result, the diagnosis reports and even image tracking capabilities over the network of the radiology department. RIS are implemented in many hospitals nowadays and the improvement of the workflow are tremendous not only for the time saving of the patients but also for the radiologist because it's shortened the process, deliver consistent image and clear image quality for diagnosis and expertise. [6]

According to Brya, 1999 the workflow in many radiology departments was considered as a closed system; because from the moment patient enter the radiology department, taking the x-ray, waiting for the result, and processing the image according to the subject of the body parts, delivering the image to the doctor, and giving the result back to the patient are under one system and manually repetitive. Therefore PACS benefit and advantages are undoubtable, important and cost effective. Not only saving the time of the patients, saving time for the nurse and radiologist, but alsp considered as the important aspects on improving the effectivity and efficiency of the hospital itself [7].

III. Digitalization products

Plenty of hospital implement digital products only to connect between the equipment into the DICOM printer, where the printer will print a films in the plastic materials showing the part or full part of the body that having radiation process. The image printing is the evidence and the reference for the doctor to read the diagnosis of the disease and symptoms of the illness. With the normal average of the patients per month around 3000 – 4000 patients, in 2 year we can have more than 72.000 stack of plastic films in the x-ray filing rooms.

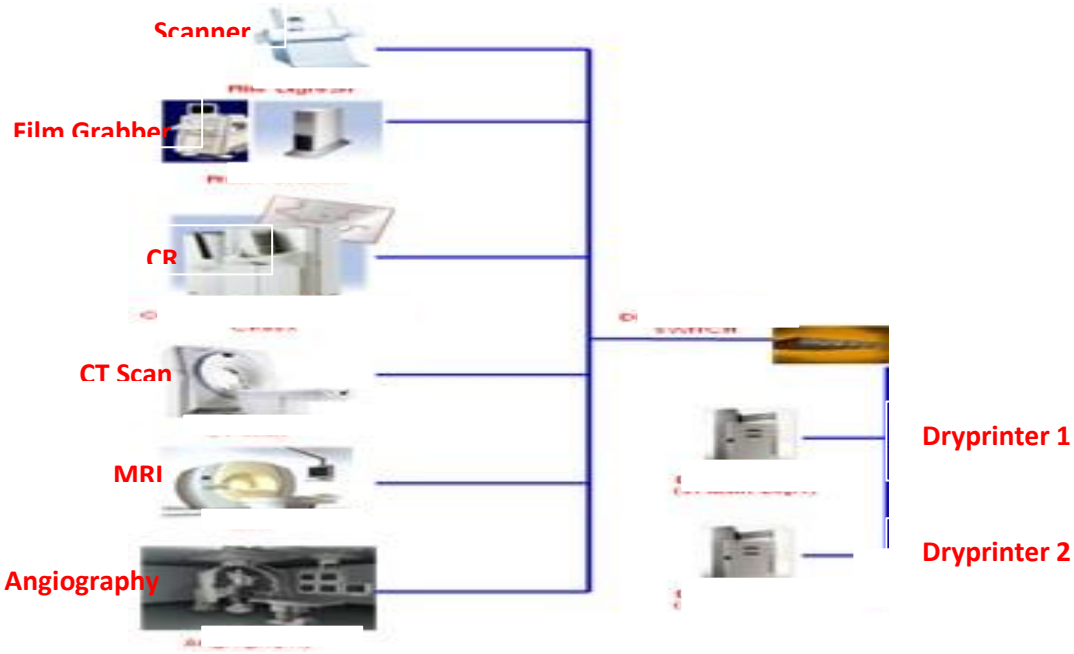


Fig 1. Architecture of the Radiology network

Picture below are showing the conditions of the x-ray filing room after 2,5 years of storage.

Fig 2. X-ray filing room

Eventhough hospitals are implementing digitalizations, but the fact is that the image data managements are still manual approach. The impact of the big filling is becoming unmanageable. Therefore implementing full digitalizations is mandatory and this will lead to cost saving process in comparasion with buying new equipment.

III.1 Picture Archive Communication System (PACS)

Digitalization in radiology department is not only connecting all medical equipment under single network and communicates to each other. But beyond this, users can have

access of patient data and image for further analysis and further discussion during the post treatment process. Users can also access the image from remote locations and diagnose the potential diseases that attack the patients. Patient also can access their image and ask for second opinion from other doctors. Image storage can be online and patients don't have to bring the films that cannot be read by them, and doesn't consume big space. PT. ABC develops opensource application called OSIRIX, which run in the apple systems. Why OSIRIX are clear since its opensource, users can also have medium to full access of all menu and applications. And PT. ABC builds the interface from the equipment and OSIRIX in order to easily integrate and image storage purposes. The interface we called PT. ABC-PACS developed using PHP and SQL. it's setup as the host of the OSIRIX, where OSIRIX will role as application of Radiology function, and PT. ABC PACS will role as data management. The interface of the patient selection as shown below:

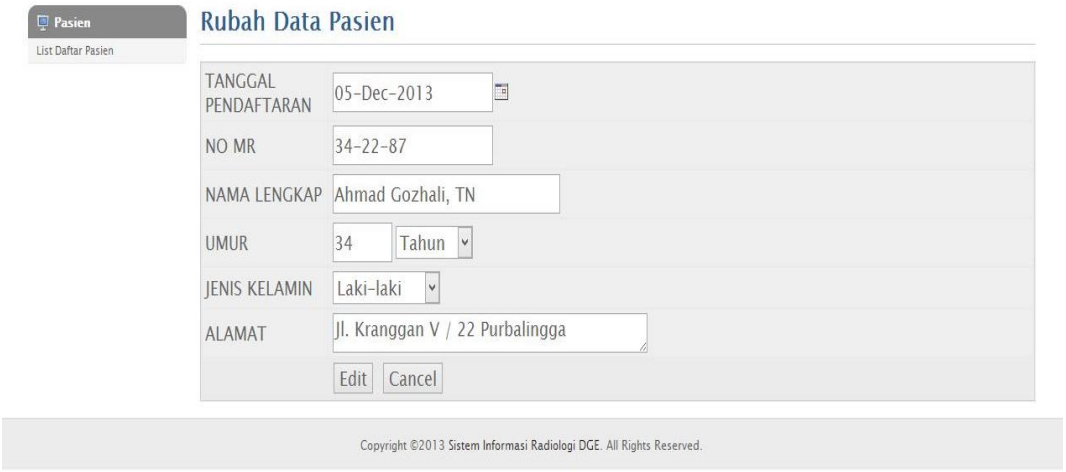


Fig 3. Select patient name and registration

Sub menu of examination in PT. ABC PACS functions. Another function that has been developed is online diagnosis using word editor.

Fig 4. Type of examination

Doctors doesn't have to write down the analysis, but they can type the analysis and diagnosis of the patient while image observations and preview are shown the right side of his/her monitor.

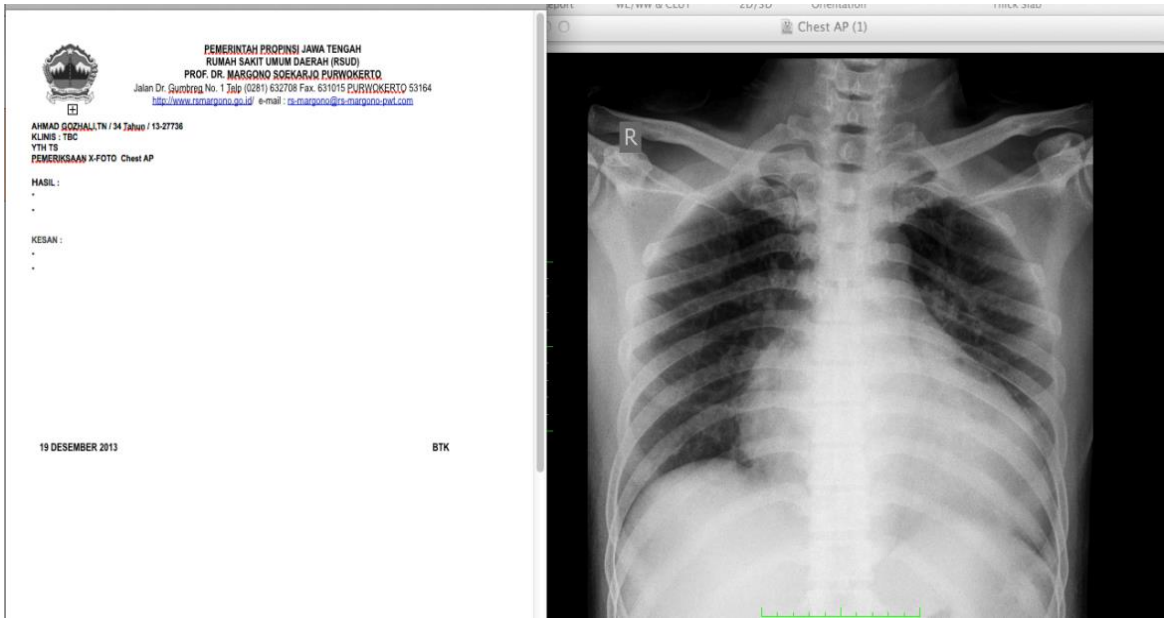


Fig 5. Image review and diagnosis

III.2 Radiology Information System (RIS)

Radiology Information System applications that develop called PT. ABC-RIS are the platform develop tailor made based on customer expectations and hospitals goals. Image below are the network

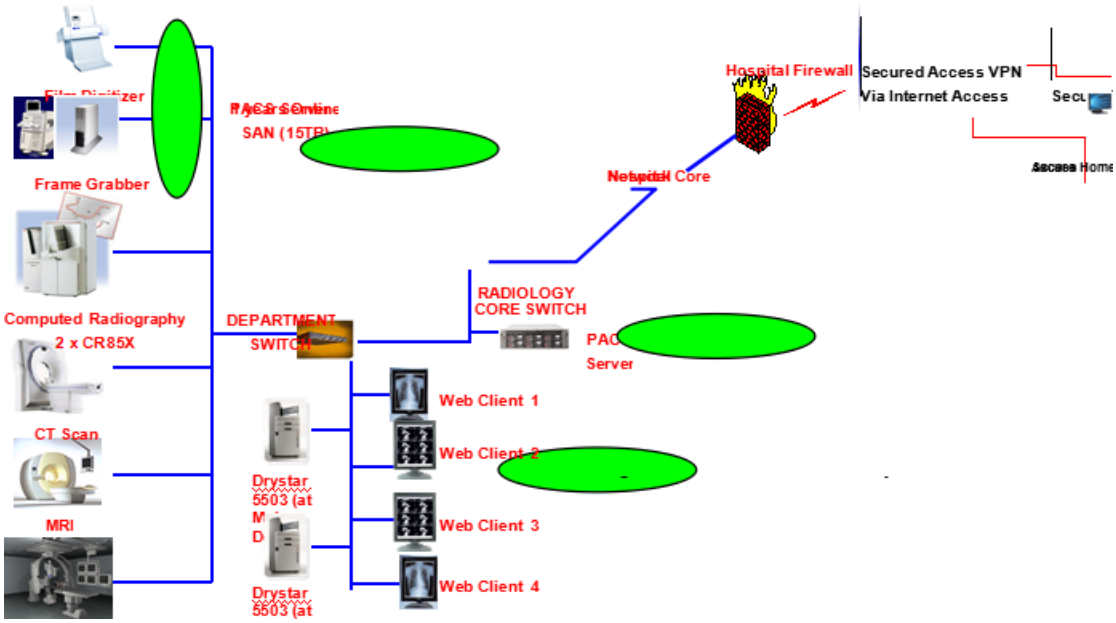
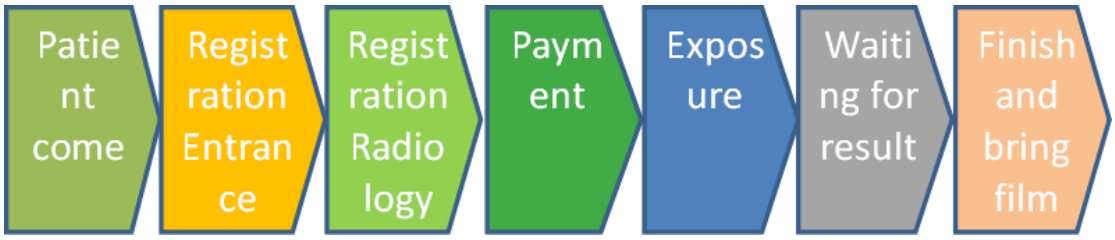


Fig 6. PT. ABC-RIS network topology

In the network topology all equipments are connected under single system, and image printer also connect not only to the equipment but also the user and web client. Users can print the image directly into the printer or store the image under image storage server. User can also make the print from remote locations and access the image via web browser and for PT. ABC-PACS menu.

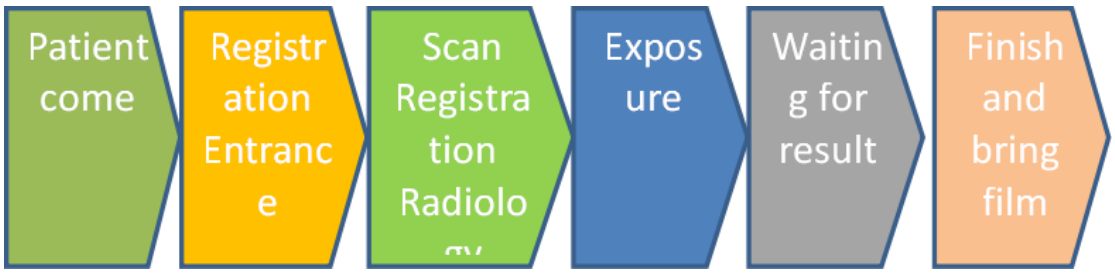
Existing workflow for patients :



Total time needed :59 minutes (average time sample during peak hour 09.00AM – 12.00PM)

Fig 7. Old patient workflow Before (PACS/RIS)

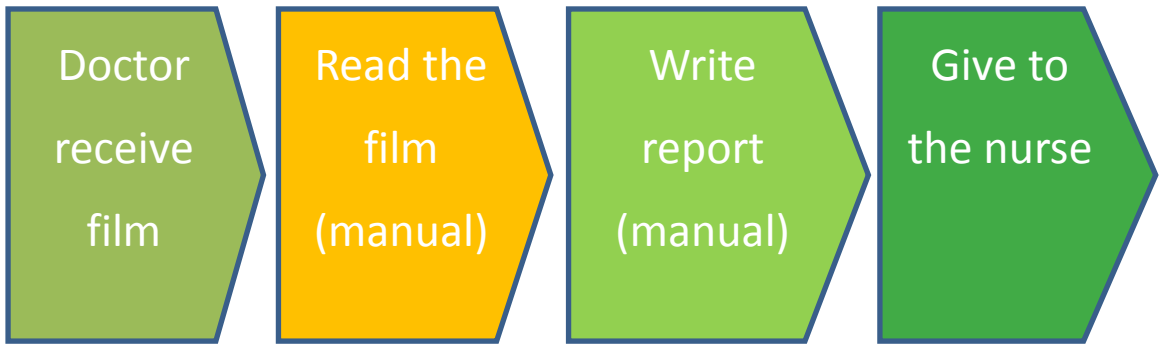
New workflow for patients :



New total time needed : 29,2 minutes (average time sample during peak hour 09.00AM – 12.00PM)

Fig 8. New patient workflow after (PACS/RIS)

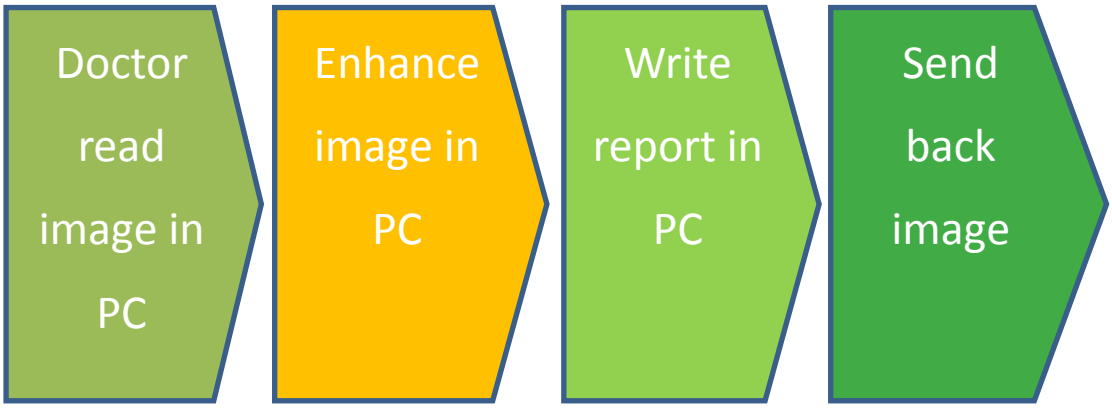
Existing workflow for doctor :



Total time needed : 12 minutes (average time sample during peak hour 09.00AM – 12.00PM)

Fig 9. New doctor workflow (after PACS/RIS)

New workflow for doctor :



Total time needed : 7 minutes (average time sample during peak hour 09.00AM – 12.00PM)

Fig 10. New doctor workflow (after PACS/RIS)

IV. Conclusion

By applying the RIS and PACS designed by PT. ABC, hospital get more productivity by accelerate the administration process, image viewing, image reporting and image transfer from one point to another. Also image storage that has been a big problem because of image size of each patient are different. By online storage image archive are easy to manage, patient no longer need to bring the piece of films, radiologist can read and review the image without any waiting and manual process anymore.

Benefit of the RIS/PACS

- Productivity of the hospital environment are increase due to time saving
- Eliminates error and misfile the films
- Eliminates fraud and mismatch of invoice since scattered payment
- Improve patient satisfaction for reduce waiting time, process and consultancy
- Doctors and nurse can give more time to the patient for better treatment and diagnosis
- Image archive and access are secure, smooth and redundant

For future research should address on security aspects for image manipulation and data storage for patient. Digital encryption and secure storage are mandatory if someone wants to have access for the image or raw data of the patients.

References

[1] Center, McKinsey, Perspective on digital business, McKinsey company, 2012

[2] Thabrany, Hasbullah, Seminar Membangun rumah sakit Indonesia yang tangguh, RSPAD Gatot Subroto, 2011

[3] Saari, Seepo, Productivity Theory and Measurement in Business, European productivity congress, 2006

[4] Jensen, Michael, Murphy Kevin, Performance pay and top management incentives, Journal of Political economy, 1990

[5] Griffith, Rachel, Harmgart, Heike, Retail productivity,The institute of fiscal studies, 2004

[6] Herrman, Tracy, Fauber Terri, Best practice in Digital radiography, American society of Radiologic Technologist, 2012

[7] Bryan S, Weatherburn G, The benefit of hospital wide PACS and RIS, The british institute of Radiology, 1999

[8] Wiley, G, UCLA's data migration : got picture, Imaging econ, 2004

[9] Ratib O, Swiernik M, McCoy JM, From PACS to integrated EMR, Computer Med Imaging, 2003

[10] Ratib O, Rosset A, Heuberger J, Opensource software and social networks : disruptive alternative for medical imaging, European Journal of Radiology, 2011Glossary

Glossary

RIS : Radiology Information System

PACS : Picture Archive Communication Systems

DICOM : Digital Imaging Communication in Medicine

EMR : Electronic Medical Record

CR : Computed Radiography

CT Scan : Computed Tomography Scanner

MRI : Magnetic Resonance Imaging

The Annual Conference on Management and Information Technology (ACMIT) 2014

How Sweet and Ripe are the Fruits? Data Mining Techniques for Classifying and Predicting 'Quick-Wins' Direct Capital Investment in Indonesia as One Approach to Business intelligence Orientation and Knowledge Management Scenarios of Indonesian Enterprises

Ali Fauzi

Master of Information Technology Department - Swiss German University, Indonesia

Abstract

The existence of big data of Indonesian FDI (foreign direct investment)/ CDI (capital direct investment) has not been exploited somehow to give further ideas and decision making basis. Example of data exploitation by data mining techniques are for clustering/labeling using K-Mean and classification/prediction using Naïve Bayesian of such DCI categories. One of DCI form is the 'Quick-Wins', a.k.a. 'Low-Hanging-Fruits' Direct Capital Investment (DCI), or named shortly as QWDI. Despite its mentioned unfavorable factors, i.e. exploitation of natural resources, low added-value creation, low skill-low wages employment, environmental impacts, etc., QWDI , to have great contribution for quick and high job creation, export market penetration and advancement of technology potential. By using some basic data mining techniques as complements to usual statistical/query analysis, or analysis by similar studies or researches, this study has been intended to enable government planners, starting-up companies or financial institutions for further CDI development. The idea of business intelligence orientation and knowledge generation scenarios is also one of precious basis. At its turn, Information and Communication Technology (ICT)'s enablement will have strategic role for Indonesian enterprises growth and as a fundamental for 'knowledge based economy' in Indonesia..

Keywords: Direct Capital Investment; Data Mining Techniques; Business Intelligence; Knowledge Management Scenarios

1. Introduction

First priority in Indonesian Investment Roadmap (Presidential Decree No. 16, 2012) is to catch 'Quick Wins' Direct Investment (QWDI), a.k.a. low hanging fruits' investment (See Figure 1). On the following/paralleling steps, Indonesia must also prioritize on: Infrastructure, foods and energy sectors, large capital/large impact investments, knowledge based economy investment. As an initiative or solution aimed to yield rapid positive results with minimal effort (Eustance, 2008), QWDI's contribution to enable ignitions for those further priority steps is still high. In this study, QWDI samples comprise almost all business sectors in all regions in Indonesia ranging from agriculture/plantation, mining, industry, trade and services. We have found quite significant differentiation in terms of Employment Creation Index (ECI-employment creation times per capita income compared to total capital investment amount) and Smart Capital Index (SCI-intangible capital amount, i.e. Intellectual Property/IP matters: training and development, software/application development, initial research projects, etc. compared to total capital investment amount) of DCI.

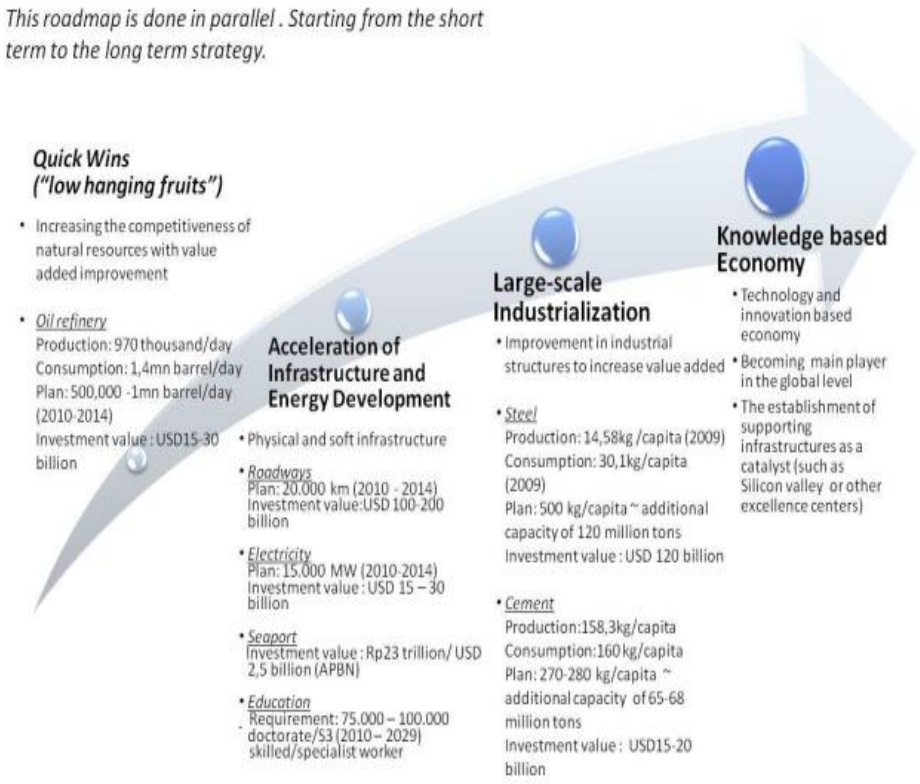


Figure 1 – Indonesia Investment (DCI) Roadmap

2. Backgrounds

Several facts regarding QWDI implantation in Indonesia as of today's issues have been defined as follow: 1.Lack of quantification/rating of these 'quick wins/low hanging fruits' investments based on some fundamental externality factors, e.g. job creation, export potential, transfer of technology, forward/backward linkage potentials, 2. Need for quick profiling/classification based on possible criteria: source of capital (by country), business

sector, startup/expanding company state, location, technology orientation, etc, 3. Big data of overall capital direct investment make such 'pattern' somehow unclear to be developed, 4.Lack of information on how business intelligence and knowledge generation scenarios have been done by Indonesian enterprises. Such pool of data as foundation for examination is available currently from the Data Center of BKPM (Investment Coordinating Board of Indonesia) as one of business support agencies in Indonesia. Indeed, the intention to see (somehow to urge) whether DCI has really initialized technology and knowledge spilloversc (Petters, 2009) and innovation, and whether it has managed to exploit the power of Information and Communication Technology (ICT) in Indonesian business fields will somehow be the central issue of our current study and hopefully for further studies.

FDI or DCI is not a panacea for economic growth and employment creation (Ernst, 2005). So far, rule-of-thumb consideration for DCI might be only based on the amount of investment. In practice, large investment used to be roughly associated to large externalities. But large capital (internality) doesn't always mean high magnitude of externalities, i.e. job creation, high export market penetration, large transfer of technology potential, etc.

3. Data Mining Techniques for QWDI Clustering and Prediction

Use of Data Mining techniques is said quite powerful to give some precious information and knowledge building based on very large data (which is sometimes unstructured, patterns-non-visible) available (Tan, 2006).

First Technique: Clustering using K-Mean Method

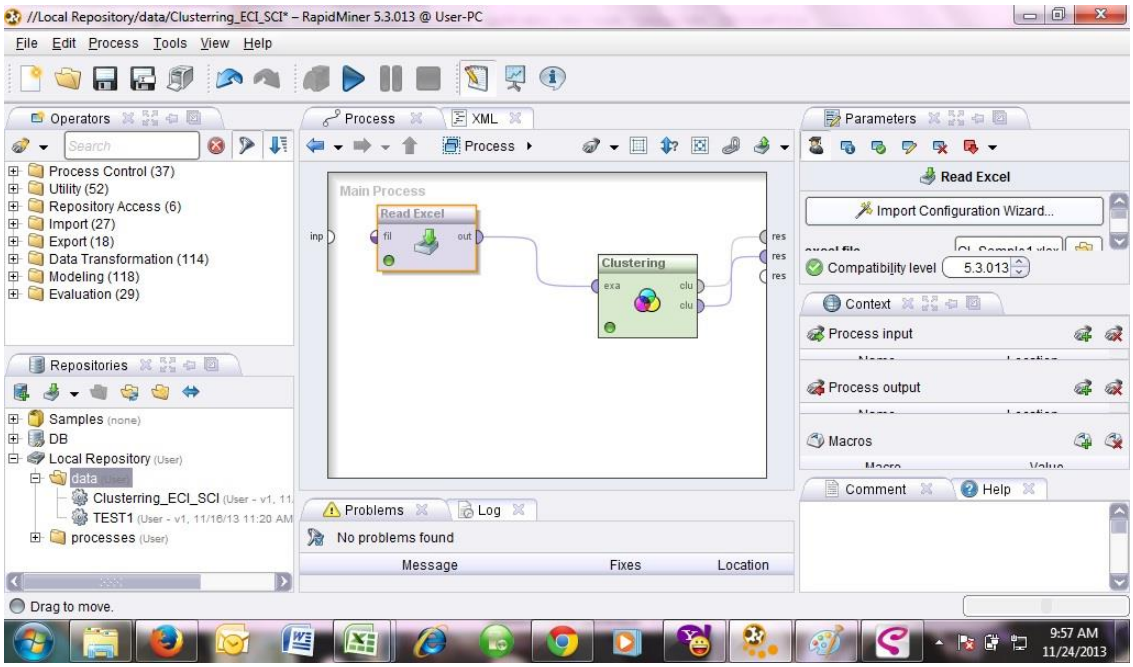


Figure 2 –QWDI Clustering process using K-Mean Method in Rapidminer

Mostly used querying tools and statistical analysis is said only can read the lines, but somehow are failed to see what actually exist between the lines. The availability of some predictive analytics tools or namely Open Source Business Intelligence, which began with the conception of On Line Analytical Processing (OLAP) System, has been very helpful to enable us to deal with such situation. In this study we have been able to use some data mining techniques using Rapidminer which was first developed in 2001 by some researcher at the Artificial Intelligence Unit of the Dortmund University of Technology. The Rapidminer 5.0 or older version is still available as open source software under certified Open Source License (OSL), while the newest version Rapidminer 6.0 (with some feature enhancement) is now released with commercial lines.

Following the need to have QWDI rating based on two externality factors: Employment Creation Index (ECI) and Smart Capital Index (SCI), firstly we use clustering technique by K-Mean Method. The data available for this process contains around 3783 rows of data, which was sorted by focusing only the 2 attributes, i.e. ECI and SCI (other attributes, i.e. country name, location and line of business are left behind for a while). We have been preprocessing this data by excluding some outliers, which was less than 0.1 % (40 rows) of existing data. The process and graphic result from Rapidminer could be seen in Figure 2.

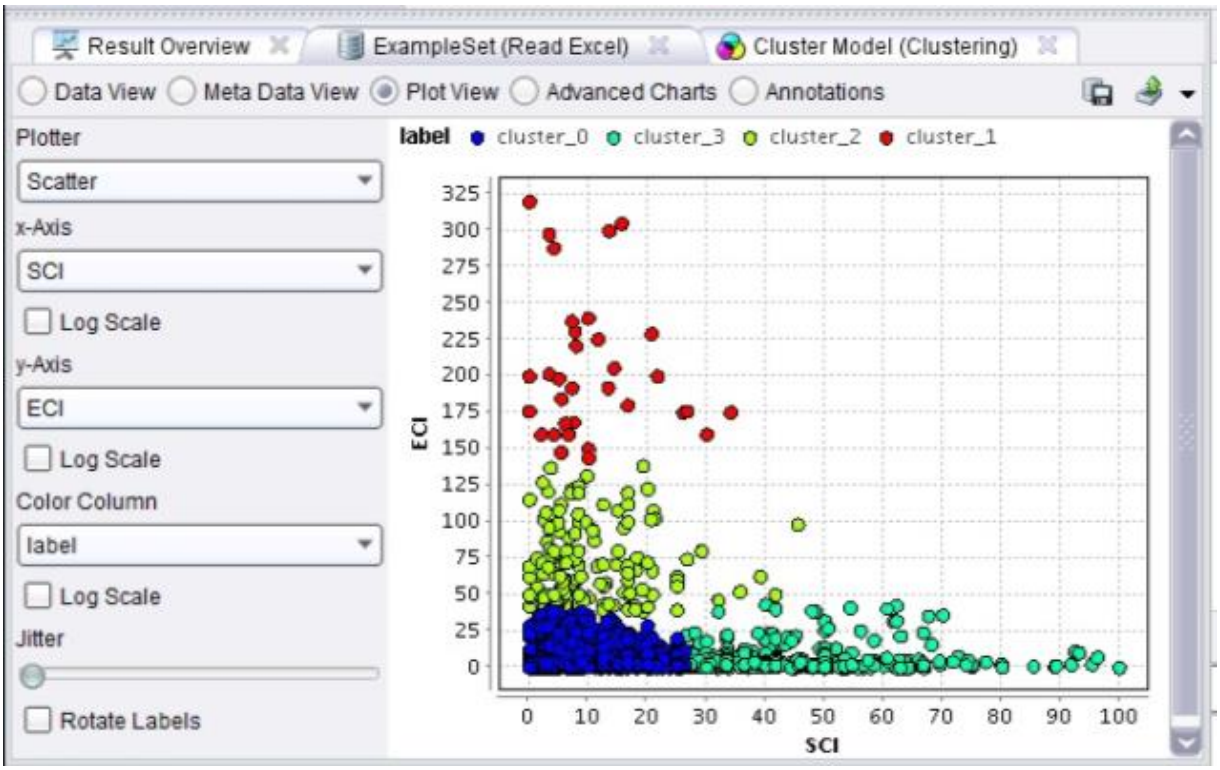


Figure 3–QWDI Clusters: Sweet, Sour, Bitter, Ripe

Second Technique: Classification and Prediction using Naïve Bayesian

From the clustering result we have been given 4 clusters that will be differing QWDI by ECI-SCI combination (Figure 3). This result indeed is actually beyond our expectation. At the beginning we have expected there will be such high ECI-high SCI cluster (supposedly will be at the right-top of the chart/Figure 3), but such cluster is in fact does not exist. Following the fact, by the given result then we have consequently given labels for each cluster formed. The 'Sweet QWDI' (high employment creation-in red color) should be most favorable than 'Sour QWDI' (middle employment creation-in light green color). Most of QWDI seems to be shown up as 'Bitter QWDI' (low employment creation-in blue color), but that was being paid somehow, in case many of them also tend to be 'Ripe QWDI' (high smart capital-in soft green color). This result from data clustering and further by giving labels to Direct Capital Investment (DCI) is indeed one of noble findings of this study. Such clustering and labeling of DCI seems has not been exercised or proposed by previous studies or researches.

After we made such clustering which means also assigning labels (Sweet, Sour, Bitter, Ripe) for every data row, we have then exploited other attributes of the data, i.e. country of origin, location and line of business of QWDI investment projects. These attributes are essential for the next task to be accomplished, which is to make classification, and furthermore for predictive forecasting. Classification was done using Naïve Bayesian method (which also widely used for text processing). First, we were sending Training Data Set (the same 3783 rows data, with more attributes involved, i.e. country of origin, location, line of business and Labor-Smart Capital State). Sample of our Training Data Set (first rows) is in Figure 4. to Naïve Bayesian Classification or processor, than we examine a given Sample Data Set to follow that classification rule. Process in Rapidminer could be seen in Figure 5.

Country Name	Line of Business	Location	Labor-Smart Capital State
Thailand	Industri kapal dan perahu	Daerah Khusus Ibukota Jakarta	Bitter
Thailand	Industri cat, perdagangan besar, kegiatan konsultas	Jawa Barat	Bitter
R.R.China	Jasa pengurusan transportasi	Daerah Khusus Ibukota Jakarta	Bitter
Gabungan Negara	Portal Web	Daerah Khusus Ibukota Jakarta	Bitter
Gabungan Negara	Perdagangan besar	Daerah Khusus Ibukota Jakarta	Bitter
Gabungan Negara	Industri semen dan industri mortar atau beton siap p	Banten	Bitter
India	Industri pakaian jadi (konveksi) dari tekstil	Jawa Barat	Bitter
R.R.China	Perdagangan besar	Daerah Khusus Ibukota Jakarta	Ripe
Singapura	Industri karet remah (crumb rubber)	Sumatera Barat	Bitter
Gabungan Negara	Industri semi konduktor dan komponen elektronik lain	Jawa Barat	Bitter
Gabungan Negara	Industri semi konduktor dan komponen elektronik lain	Banten	Bitter
Gabungan Negara	Kegiatan konsultasi manajemen bisnis	Daerah Khusus Ibukota Jakarta	Ripe
Luxembourg	Industri produk farmasi	Jawa Barat	Bitter
Luxembourg	Perdagangan besar	Daerah Khusus Ibukota Jakarta	Bitter
Korea Selatan	Penggalian krikil dan industri mortar atau beton siap p	Sumatera Utara	Bitter
Singapura	Jasa persewaan dan sewa guna usaha tanpa hak c	Daerah Khusus Ibukota Jakarta	Bitter
Singapura	Industri berbagai barang jadi dari logam bukan besi	Kepulauan Riau	Bitter
Uni Emirat Arab	Pembangkitan tenaga listrik	Aceh	Bitter
Malaysia	Pertambangan batubara	Aceh	Bitter

Figure 4 –Training Data Set Sample (Total: 3783 rows)

The classification rule will further assume what Labor-Smart Capital State (as key attribute: Sweet, Ripe, Sour or Bitter) an investment (which comes from certain country, in certain line of business, in certain region) has. This classification/prediction is indeed the core of data mining techniques in this study which will bring somehow more valuable findings.

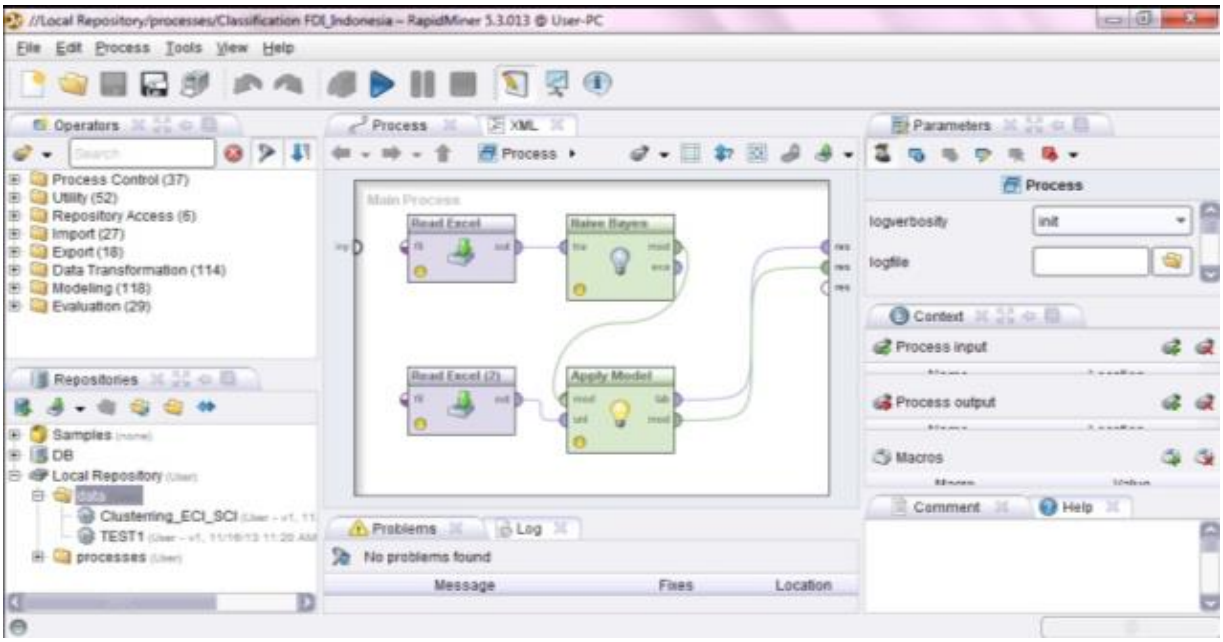


Figure 5 –QWDI Classification using Naïve Bayesian Method

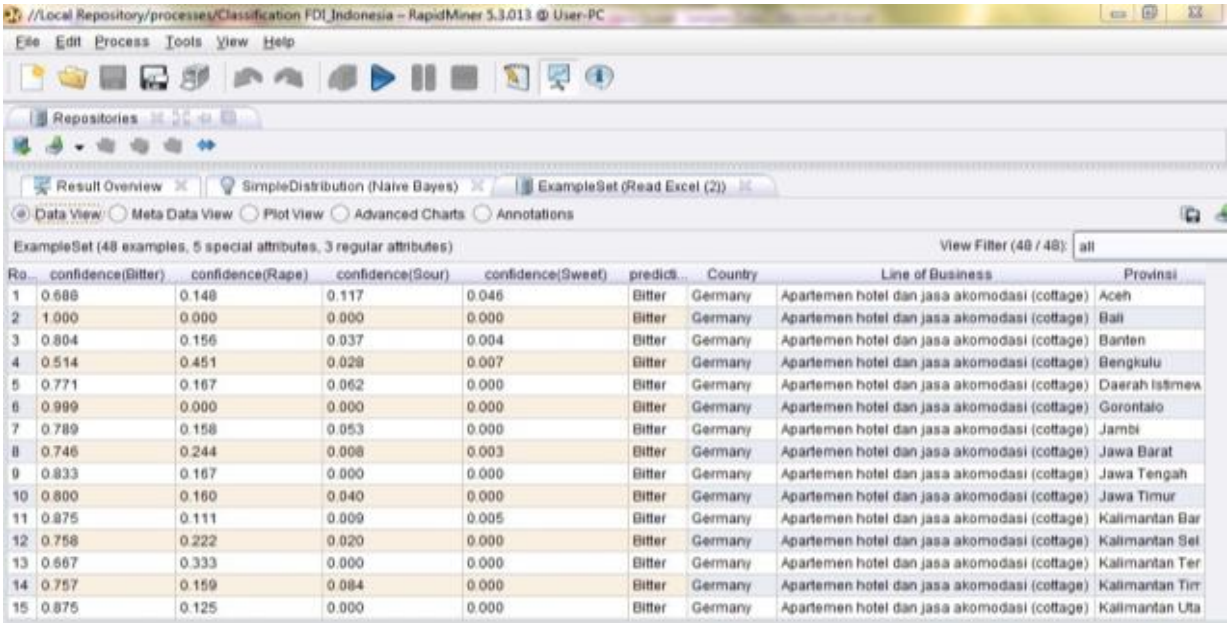
Making a prediction from classification rule is then could be done. Here, a sample data set could be given to the classifier. Our sample data set is shown in Figure 6. As an illustration we give 2 attributes (source country name and line of business) all the same for every region to be exercised. Supposedly, a German businessman aims to build a DCI project in Indonesia in hotel and cottage industry, and he wants to have an idea of job-technology mode to be applied. For this need, he simply can examine for every possible location in Indonesia. By this classifier, a set of confidence level for every label are given. One of the results as an example, that in Bengkulu, he found out that a relatively more business intelligence orientation ('Ripe' confidence level is 0.451, compared to only 0.156 in Banten) has been applied by previous investors. By decision/policy maker side, i.e. central or local government, this sector should be more preferred because confidence levels for Sweet, Sour and Ripe are relatively high (respectively 0.007, 0.028, and 0.451).

Country	Line of Business	Location
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Aceh
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Bali
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Banten
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Bengkulu
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Daerah Istimewa Yogyakarta
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Gorontalo
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jambi
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Barat
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Tengah
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Timur
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Barat
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Selatan
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Tengah
Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Timur

Figure 6 - Sample Data Set

From the illustration, the prospective hotel investor should further verify and examine the fact that sort of business intelligence

orientation would be done as prompted by quick prediction. In his intended location, it seems that some hoteliers have been investing significant amounts of their investment to sort of hotel management software, central reservation system or other enhanced business intelligence features. It could also be assumed from these facts that such business in the region has good prospective market in the future and somewhat tough competition forecast, that hoteliers did some innovations/modernizations.



Ro...	confidence(Bitter)	confidence(Rape)	confidence(Sour)	confidence(Sweet)	predicti...	Country	Line of Business	Provinsi
1	0.686	0.148	0.117	0.046	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Aceh
2	1.000	0.000	0.000	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Bali
3	0.804	0.156	0.037	0.004	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Banten
4	0.514	0.451	0.028	0.007	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Bengkulu
5	0.771	0.167	0.062	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Daerah Istimew
6	0.999	0.000	0.000	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Gorontalo
7	0.789	0.158	0.053	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jambi
8	0.746	0.244	0.008	0.003	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Barat
9	0.833	0.167	0.000	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Tengah
10	0.800	0.160	0.040	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Jawa Timur
11	0.875	0.111	0.009	0.005	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Bar
12	0.758	0.222	0.020	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Sel
13	0.667	0.333	0.000	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Ter
14	0.757	0.159	0.084	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Tim
15	0.875	0.125	0.000	0.000	Bitter	Germany	Apartemen hotel dan jasa akomodasi (cottage)	Kalimantan Uta

Figure 7 –Examination of assigned location for hotel /cottage Investment by German businessman

Further variations of prediction could be made by selecting which attributes to be set, and which attribute being exercised. We can see that from this data mining technique alone, which is to build such classifier as one of our research result, a very wide variety of findings and further sources of analytics are possible. For this sample of interest, we previously did not have any idea or assumption of what is really happen in reality. But, after doing some examinations/exercises using the tools, then the results are quite close to the reality according to what we've informed.

4. Technology vs. Employment

Correlation between technology development (innovation) and employment creation is somewhat viewed as being substitutive or being applied as synergy. At substitutive/leverage meaning, when we decide to introduce new technology, one thing that should be taken is downsizing, i.e. reducing the employment. At the meaning of synergy, the increased productivity resulting from technological enhancement may not threaten employment (Hernandez, 2001). Innovation instead could be a motor to increased competitiveness and furthermore overall economic growth. Higher income for more skillful employee and increasing consumption levels at its turn will compensate the jobs lost and would create new employment.

The synergy seems to be the favorable situation that we are expecting of. However, one thing that should be assured for such situation is that technology enhancement should be done in a high readiness environment which mainly and basically supported by one of important factors, i.e. Information and Communication Technology (ICT) as general purposes tools providing enablement for every sector of interest and the other support is human resources responsiveness for technology enhancement.

From Figure 8 (derived from our data query), we can see the profile of Indonesian QWDI enterprises. With relatively uniform spread of business categories, we only can see what business lines are altogether contributing as current Indonesian economic backbone.

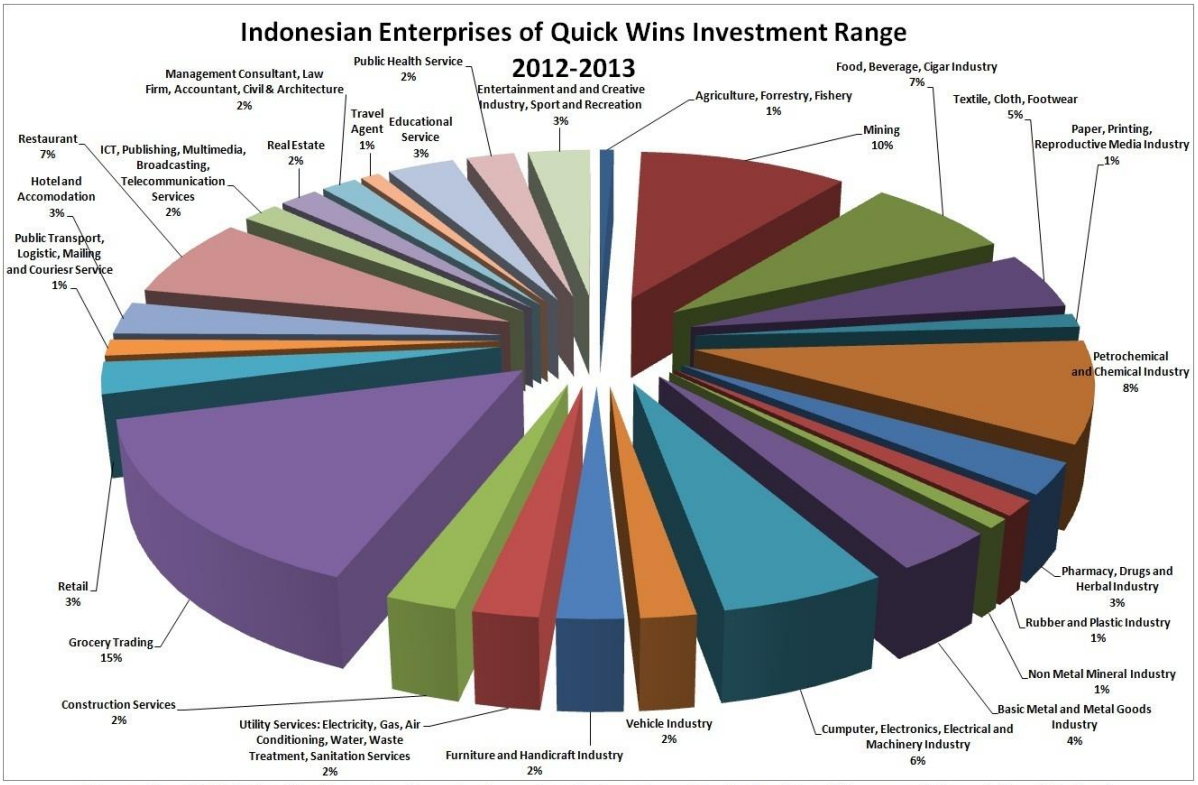


Figure 8 – QWDI Profile Samples from Indonesian Enterprises (Excl. Banking/Finance, Oil and Gas Mining)

Figure 9 is a brief resume from one of our data mining work in this study (clustering), explaining how these enterprises are classified into 4 groups based on labor-technology mode or business intelligence orientation (Sweet, Sour, Bitter and Ripe). It is notable that most of Indonesian enterprises (QWDI) have not only relatively low employment creation, but also relatively low initial orientation for business intelligence (Bitter state, 78% of the samples). Significant portion has shown a quite high initial effort for business intelligence, with employment creation is relatively low (Ripe state, 17%).

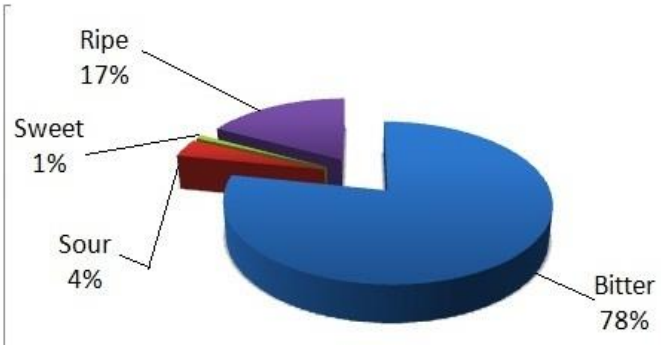


Figure 9 - Indonesian Enterprises' Labor-Technology Mode

Still from the query and statistical tools, we have examined some business fields that already have significant business intelligence orientation (See Figure 4, measured in index/ percentage), most of them are from service sector (educational services, travel agent, civil and architecture services, head office and management consultant, programming and computer consultancy, food and beverage services and civil construction). Besides the trading sector (grocery and retail), some certain mining sectors (coal mining, mining services) as well have shown significant orientation for business intelligence.

5. IT Enablement Importance

From IT Strategic Planning point of view, those above initial facts could open eyes to realize that there are still wide spaces for IT enablement (as a basic support for knowledge based economy) in Indonesia and that we can identify each sector characteristics to apply such IT enablement. But before we move further to business intelligence orientation and knowledge management scenario, it is important to say that clustering (using data mining) and further making some query, statistical analysis are somehow still very limited to tell the complete story and to cope with growing needs of further analysis.

6. Knowledge Generation Scenarios of Indonesian Enterprises

We have learnt so far, the process of mining the historical data, which are establishing such grouping (clustering) and classifying the majority of Indonesian businesses, and further generating such predictive modeling. For some categories which have been managed to be revealed (Sweet, Sour, Bitter and Ripe; as measures for business intelligence orientation), it is then interesting to see which knowledge management scenarios are recommended for each category. As we can see from Figure 11 (matrix), each knowledge-generation activities (Keri E. Pearlson, 2010), i.e. Research and Development (R&D), Adaptation, Buy or Rent, Shared Problem Solving, Communities of Practice are being rated for given categories.

As we already also managed to identify some tendencies from data query and clustering, we have been able to make such redlines. “Bitter” investments mostly comprise of basic and intermediate manufacturing industries (e.g. chemical/petrochemical, metal and basic metal, rubber and plastic, automotive, non-metal minerals); they are mostly capital intensive, use relatively low number of employment and mostly applying full adoption of overseas technologies. “Sour” investments mostly are of emerging manufacturing industries (e.g. food and beverages, textile, building materials, modern handicraft and creative arts); they could be capital intensive but also labor intensive, use relatively medium to high number of employment and applying a mix between overseas and local competence technologies. “Sweet” investments mostly come from ‘third-world’ manufacturing industries (e.g. garment, leather and footwear); they are labor intensive and applying very basic technologies. “Ripe” investments tend to be of research oriented industries and market oriented services sectors (e.g. mining, pharmacy, hotel and restaurant, travel agent, educational, construction, retail and general trading, ICT providers); they are technology intensive, use relatively low number of employment and

must maintain technology or market intelligence enhancement in order to survive and grow.

As we already established above mentioned redlines, further suggestion is all about knowledge management scenarios (knowledge generation processes). A "Bitter" company, for example must prioritize first on R&D (indicated as No. 1 in the column in Figure 11), doing (and funding) researches of many aspects within company's business process, involving some task force groups, and then secondly hiring new personals or contracting consultants (Buy or Rent). The company must also maintain adaptation along the product lifecycle (third priority), before being able to establish communities in practices platform (fourth) and furthermore sophisticated shared problem solving. This roadmap must regard also the nature of expenditure (example; 'bitter' means low labor expenses) of businesses under concern, which then suggest R&D (usually relatively high expense) as top priority.

7. Conclusion and Remarks

The use of data mining techniques is proved to be powerful in processing our large data of direct capital investment in Indonesia and more possibilities of having the correlation between more involved factors/attributes. This research has proposed idea of labeling, classification and prediction of one big portion of capital direct investment in Indonesia, which is Low Hanging Fruits/Quick Wins Direct Investment. Compared with some of similar researches (which use data mining approach) in CDI/FDI field, namely the impact of financial development on FDI (Korgaonar, 2012), and data mining in banking and its application (Pulakkazhy, 2013), this research has approached the correlation between variation of CDI/FDI (source country of capital, line of business, and location, or other variables possible) with quite new and emerging parameter, which is technology orientation. Though the findings (labeling) and classification rule have to be proven by further examination, this research could be used as a quick prediction tool for technology orientation. The importance of IT enablement along with its wide proposed subjects (e.g. Enterprise Resource Planning (ERP), Data Security, Enterprise Architecture, etc.) at its turn quite important theme for Indonesian knowledge based economy, which will be the core of our further researches.

8. References

[1] Ernst, C. (2005). Employment Strategy Paper. Retrieved 2013, from The FDI – employment link in a globalizing world: http://www.oit.org/wcmsp5/groups/public/---ed_emp/---emp_elm/documents/publication/wcms_114029.pdf

[2] Eustance, C. (2008). Quick Wins- Some Questions to Consider. Retrieved 2013, from UG-Flex Project: http://jiscdesignstudio.pbworks.com/w/file/fetch/35181477/QUICK%20WINS%20-%20SOME%20QUESTIONS%20TO%20CONSIDER.pdf

[3] Hernandez, H. (2001). Impact of Technological and Structural Change of Employment - Prospective Analysisi 2020. Seville: European Commission Joint Research Center.

[4] Keri E. Pearlson, C. S. (2010). Managing and Using Information Systems, A Strategic Approach, 4th Ed. Danvers: John Wiley & Sons.

[5] Petters, E. D. (2009, November). Don´t Expect Apples From a Pear Tree: Foreign Direct Investment and Innovation in Mexico. Retrieved 20132, from Global Development and Environment Institute (GDAE) - Tufts University: http://ase.tufts.edu/gdae/Pubs/rp/DP28DusselNov09.pdf

[6] Tan, P.-N. (2006). Introduction to Data Mining. Boston: Addison Wesley.

The Annual Conference on Management and Information Technology (ACMIT) 2014

Conceptual Risk on System Migration Framework

Nicsen

Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia

Email: divine.ogre@gmail.com

Mohammad A. Amin Soetomo, D.Sc

Swiss German University, Edu Town BSD City, Tangerang 15339, Indonesia

Email: mohammad.soetomo@lecturer.sgu.ac.id

Abstract

IT Risk is defined as potential lost on IT process. This IT Process may vary from design, development, implementation, or migration. This paper focuses on IT risk assessment in the migration plan. While planning migration, there are some potential risks to be considered. This can help the migration team to minimize risk during migration. The risk assessment was created by using a combination of several frameworks or guidelines. ISACA IT Risk Framework [1] and Commonwealth of Virginia ITRM Guideline [2] were used to construct the framework. For the discussion, AIIM migration plan [3] was given as an example. This conceptual framework covers four main phases: creating migration plan and system diagram, mapping migration plan to risk scenario, risk assessment, and risk control.

Keywords : Risk Framework; Migration Plan;

1. Introduction

Migration is a critical part of the IT process. Bloor Research states that the data migration project failure rate is 38% [4] whereas the failure rate of large projects is reported as being between 50% and 80% [5]. IT system life cycle was dilemmatic case whether to stay on legacy system or migrate to the new one. Bisbal et al [6], state that it is costly to be maintenance legacy system and the migration from the legacy system is very expensive and have risk to be failure. Risks in computer-based information systems are surprisingly under managed in both the private and public sector [7]. Risk management is a process to find a combination of optimum loss prevention and reasonable cost [8]. Measuring the risk is the key to preventing loss. While migration has many potential losses, the risk should be measured to prevent or lessen the loss. The focus of this study is to find a way to measure the risks in the migration process and then control them. ISACA Risk IT framework is used because it has risk scenario and risk control which is fit to construct our framework. To assess the risk Commonwealth of Virginia ITRM guidelines were used. For the discussion AIIM migration plan was taken as an example.

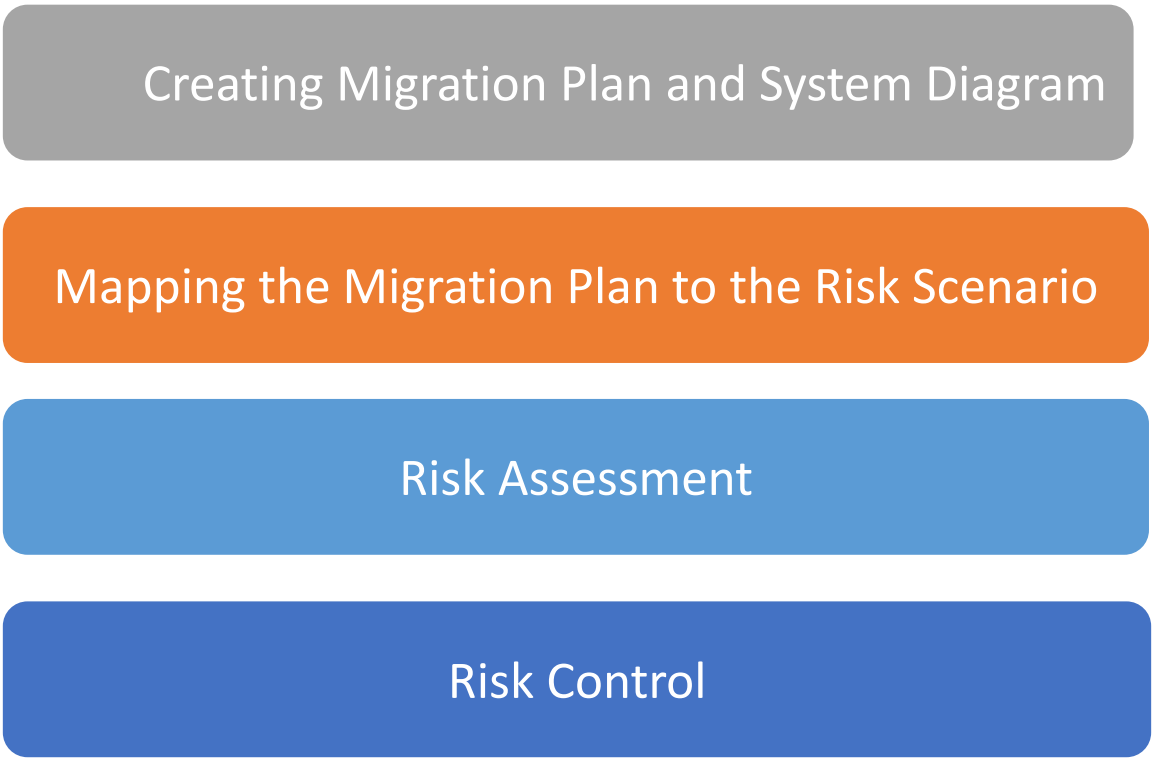


Figure 1. (a) Proposed model

2. Methodology

In the first step, we tried to find the related framework and guideline which could be used to assess the risk. From this step found several frameworks or guidelines such as ISACA Risk IT framework [1], and Commonwealth of Virginia ITRM guideline [2]. The second phase is learning how the framework or the guideline is used. By learning how they work, so later on we can adjust it to fit our needs. The last step is constructing the theoretical framework based on the finding.

3. Proposed Model

Our approach consists of four main processes, Figure 1. (a). The first step is creating migration plan and system diagram. Migration plan address issues associate with migration process from legacy system to the new one [9]. Migration plans will differ between organizations. It depends on what issues they want to address. Organization also need to understand the legacy system and specify target system development [10]. To give better understanding to the legacy and target system we can create system diagram for current system and target system development.

The second process is mapping the migration Plan to the risk scenario. One or several scenarios can be mapped to the respective risk scenario. This risk scenario will be used to assess the migration process.

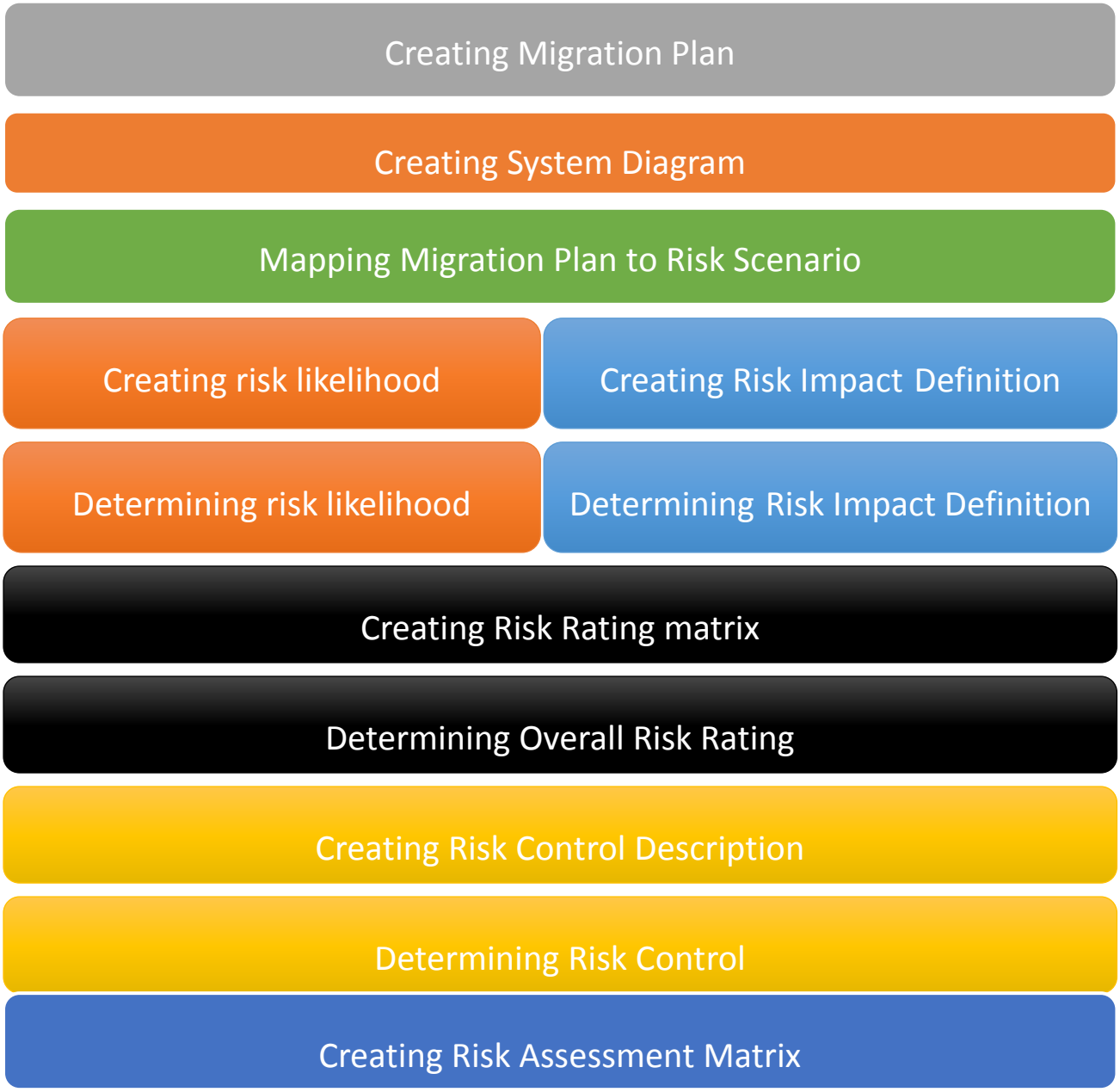


Figure 1. (b) Complete framework

The third process is conducting risk assessment. The vulnerability and the impact is measure here. There are three things we need to assess. They are risk likelihood, risk impact analysis, and overall risk determination.
The last process is risk control. This process is to specify what control should be taken after it is known what risks might occur in the migration process. Figure1. (b) shows the complete framework.

4. Discussion

4.1. Creating Migration Plan

In general the migration plan is created based on organization needs. In this reseach, the migration plan from Association of Information and Image Management (AIIM) was

taken [3] as an example. Table I contains detailed information which can be added to the migration plan [3]. This information is needed to map the migration plan to risk scenario which will be discussed later on in the paper. For instance, detail information can be filled with person who becomes the stakeholder in identifying the stakeholder point in the first phase.

Table 1. Migration plan and detail information.

Migration Phase	Actions[3]	Detail Information
Strategy	Determine the purpose of the migration	
	Identify the stakeholders	
	Identify the migration team	
Planning	Determine the scope of the migration	
	Establish stakeholder expectations	
	Determine the schedule	
	Identify dependencies	
	Identify applications and/or data to be migrated.	
	Identify locations of data to be migrate	
	Identify bandwidth and network concerns	
	Identify target migration requirements	
Preparation	Identify migration tools.	
	Design the target solution.	
	Normalize data and metadata.	
	Test the migration.	
	Pilot the migration.	
	Estimate the time required for migration.	
	Create a full backup.	
Migration	Confirm readiness to begin migration.	
	Start the migration.	
	Monitor throughout the process.	
	Maintain existing records and systems until migration is verified	
	Validate success of migration.	

4.2. IT System Diagram

An IT system diagram will help the risk assessment team to provide the big picture of the whole system before and after the migration. A brief explanation can be written above the diagram to make sure there is no ambiguity in understanding the diagram.

4.2.1. Legacy System Diagram

Brief explanation: Clients via internet input purchasing order and then an order is saved to the database to feed the other system. The legacy system takes care of sales invoicing, tax invoicing, and settles the receivables. The data is also given to the accounting software by converting the data to a text file format. The data is imported to the accounting software to be processed to the income statement.

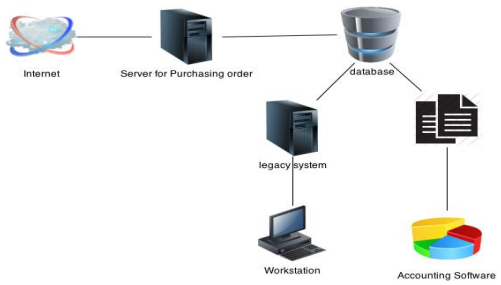


Figure 2. Brief explanation and system diagram before migration

4.2.2. Targeted System Diagram

Brief information: The new system replaces the legacy system and accounting software into one system which was previously separated. The new system gets data from the database and processes it and supplies it to the respective department in the organization.

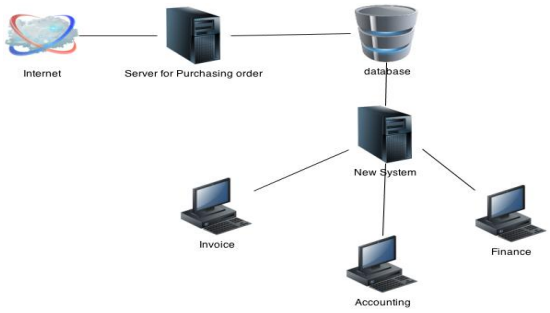


Figure 3. The expected system after the migration

4.3. Mapping Migration Plan to Risk Scenario

After the detailed migration plan has been compiled, the risk scenario can be mapped to the migration plan action. We put risk scenario from ISACA risk scenario diagram. ISACA group risk scenario divides into five categories: actor, threat type, event, asset/resources, and time. Each category has its own risk list. This will assist to easily map the migration plan action into the compatible risk scenario.

Table 2 shows the migration plan is mapped into the risk scenario. By merging several points in migration plan to the risk scenario provided by ISACA (fig 4) is mapped. For

instance, migration plan on bandwidth and network concern and physical data location can be put into one risk scenario, risk on infrastructure [asset].

Figure 4. ISACA risk scenario [1]

Table 2. Mapping Migration Plan to Risk Scenario

Phases	Actions	Risk scenarios
Strategy	• Determine the purpose of the migration • Identify the stakeholders • Identify the migration team	• Identify the risk if the system is not upgraded [asset] • Risk on stakeholder[actor] • Risk on migration team [actor]
Planning	• Determine the scope of the migration • Establish stakeholder expectations • Determine the schedule • Identify dependencies • Identify applications and/or data to be migrated. • Identify locations of data to be migrate • Identify bandwidth and network concerns • Identify target migration requirements	• Identify the risk of the time and project scope [time] • Ineffective execution of schedule [event] • Risk on system dependencies [resource] • People and organization risk [asset] • Risk on IT infrastructure[asset] • Risk on infrastructure(facilities) [asset]
Preparation	• Identify migration tools. • Design the target solution. • Normalize data and metadata. • Test the migration. • Pilot the migration. • Estimate the time required for migration.	• Accidental and failure risk [threat type] • Choose proven application [resource] • Ineffective design risk [Event] • Duration risk [time] • Reassurance of Information availability

	• Create a full backup.	[asset]
Migration	• Confirm readiness to begin migration. • Start the migration. • Monitor throughout the process. • Maintain existing records and systems until migration is verified • Validate success of migration.	• Ineffective execution risk [event] • Modification risk[event] • Interruption risk [event] • Risk on losing the data [resource]

4.4. Risk Likelihood, Risk Impact Analysis, and Overall Risk Determination

4.4.1. Risk Likelihood

Risk likelihood is something that might happen and cause risk to the system. Risk likelihood can be measured as qualitatively and quantitatively. Measuring the risk likelihood is qualitatively conducted. A detailed explanation can be written in the risk likelihood column and impact rating can be put in the rating column

Table 3. Risk likelihood definition [2]

	Probability of Threat Occurrence		
Effectiveness of Migration	Low	Moderate	High
High	Low	Moderate	Moderate
Moderate	Low	Moderate	High
Low	Moderate	High	High

Table 4. Risk likelihood rating

Risk Scenario	Risk Likelihood	Rating
Identify the risk if the system is not upgraded [asset]	The legacy system cannot afford the future complex business	High
Risk on Stakeholder [actor] Risk on Migration Team [actor]		
Identify the risk of the time and project scope [time]		
Ineffective execution of schedule [event]		

Risk on system dependencies [resource]
People and organization risk [asset]
Risk on IT infrastructure[asset]
Risk on infrastructure(facilities) [asset]
Accidental and failure risk [threat type]
Choose proven application [resource]
Ineffective design risk [event]
Duration risk [time]
Reassurance of Information availability [asset]
Ineffective execution risk [event]
Modification risk [event]
Interruption risk [event]
Risk on losing the data [resource]

4.4.2. Risk Impact Analysis

Risk impact analysis is a study to analyze how big the risk causing trouble to the system is. Determining impact rating as risk likelihood can be qualitative or quantitative. Table 5 shows impact rating definition [2]. Impact definition can be adjusted to fit the company's characterization

Table 5. Risk Impact Definition [2]

Magnitude of impact	Impact Definition
High	Occurrence of the risk: (1) may stop company operations; (2) record or sensitive data is lost or erased during backup process; (3) may harm company reputation and credibility to deliver services
Moderate	Occurrence of the risk: (1) may interfere company operations; (2) may reduce company profit during delayed on project; (3) may harm company reputation for services;

Low	Occurrence of the risk: (1) some company division may not work effectively; (2) may affect some resource and asset not work properly.

Table 6. Risk Impact Rating

Risk Scenario	Risk Impact Analysis	Rating
Identify the risk if the system is not upgraded [asset]	The company won't survive the competition	High
Risk on Stakeholder [actor]		
Risk on Migration Team [actor]		
Identify the risk of the time and project scope [time]		
Ineffective execution of schedule [event]		
Risk on system dependencies [resource]		
People and organization risk [asset]		
Risk on IT infrastructure[asset]		
Risk on infrastructure(facilities) [asset]		
Accidental and failure risk [threat type]		
Choose proven application [resource]		
Ineffective design risk [event]		
Duration risk [time]		
Reassurance of Information availability [asset]		
Ineffective execution risk [event]		
Modification risk [event]		
Interruption risk [event]		
Risk on losing the data [resource]		

4.4.3. Overall Risk Determination

Overall risk determination is used to determine the final risk since risk is defined as likelihood multiplied by impact. The qualitative attribute of risk likelihood and risk impact is transformed to quantitative measurement. Table vii shows the matrix of overall risk rating with the risk scale. The weighted score can be adjusted to fit the company characteristic. The result of the multiplication is transformed back to the qualitative measure and then the result is written into table 8.

Table 7. Overall risk rating matrix [2]

	Risk Impact		
	Low	Moderate	High
Risk Likelihood	(15)	(65)	(100)
High	Low	Moderate	High
(1.0)	15 x 1.0 = 15	65 x 1.0 = 65	100 x 1.0 = 100
Moderate	Low	Moderate	Moderate
(0.6)	15 x 0.6 = 9	65 x 0.6 = 39	100 x 0.6 = 60
Low	Low	Low	Low
(0.15)	15 x 0.15 = 2.25	65 x 0.15 = 9.75	100 x 0.15 = 15
Risk Scale: Low (1 to 15); Moderate (>15 to 65); High (>65 to 100)			

Table 8. Overall Risk Rating

Risk Scenario	Risk likelihood rating	Risk impact analysis rating	Rating
Identify the risk if the system is not upgraded [asset]	High	High	High
Risk on Stakeholder [actor]			
Risk on Migration Team [actor]			
Identify the risk of the time and project scope [time]			
Ineffective execution of schedule [event]			
Risk on system dependencies [resource]			
People and			

organization risk [asset]
Risk on IT infrastructure[asset]
Risk on infrastructure(facilities) [asset]
Accidental and failure risk [threat type]
Choose proven application [resource]
Ineffective design risk [event]
Duration risk [time]
Reassurance of Information availability [asset]
Ineffective execution risk [event]
Modification risk [event]
Interruption risk [event]
Risk on losing the data [resource]

4.5. Risk Control and Review

Based on ISACA IT risk framework, there are four risk controls which can be selected to deal with the risk. The four risk controls are avoiding the risk, reducing or mitigating the risk, sharing or transferring the risk, and accepting the risk. Detailed descriptions of the risk controls are presented in table 9 [1].

Table 9. Risk control description [1]

Risk Control	**Description**
Avoidance	Avoidance means that the risk response is adequate so it is better to exit the activities or condition which may raise risk.
Reduction / Mitigation	Risk is detected and it can be reduce to prevent bigger loss.
Sharing / Transfer	Some portion of the risk can be transferred to reduce the loss.
Retention / Acceptance	The impact is relatively low and loss which probably occurred is accepted

Table 10. Risk Control

Risk Scenario	Overall risk rating	Control	Review
Identify the risk if the system is not upgraded [asset]	High	Mitigate the risk	Upgrade the system to the new one.
Risk on Stakeholder [actor]			
Risk on Migration Team [actor]			
Identify the risk of the time and project scope [time]			
Ineffective execution of schedule [event]			
Risk on system dependencies [resource]			
People and organization risk [asset]			
Risk on IT infrastructure[asset]			
Risk on infrastructure(facilities) [asset]			
Accidental and failure risk [threat type]			
Choose proven application [resource]			
Ineffective design risk [event]			
Duration risk [time]			
Reassurance of Information availability [asset]			
Ineffective execution risk [event]			
Modification risk [event]			
Interruption risk [event]			
Risk on losing the data [resource]			

5. Conclusion and Future Work

The result is the summary of the risk assessment on migration plan. The risk assessment can become consideration on migration team to control the risk might happen and measure how big the impact on the company. This framework and discussion is a conceptual. Further validations for future works through expert judgment, focus group discussion or pilot project are needed. The result of the risk assessment can be looked up in the appendix.

References

[1] ISACA, *The Risk IT Framework*, 2009.
[2] V. I. T. Agency, "Information Technology Risk Management Guideline," ed, 2006.
[3] E. C. Wiki. (March 16, 2014). *The Migration Plan*. Available: http://www.aiim.org/community/wiki/view/The-Migration-Plan
[4] T. Boardroom. (2013, 16 March 2014). *Why do so many data migration projects end in disaster?* Available: http://www.cbronline.com/blogs/technology/why-do-so-many-data-migration-projects-end-in-disaster170113
[5] P. Dorsey, "Top 10 reasons why systems projects fail," *Retrieved February*, vol. 10, p. 2005, 2000.
[6] J. Bisbal, D. Lawless, B. Wu, and J. Grimson, "Legacy information systems: Issues and directions," *IEEE software*, vol. 16, pp. 103-111, 1999.
[7] L. Willcocks and H. Margetts, "Risk assessment and information systems," *European Journal of Information Systems*, vol. 3, pp. 127-127, 1994.
[8] R. K. Rainer Jr, C. A. Snyder, and H. H. Carr, "Risk Analysis for Information Technology," *J. of Management Information Systems*, vol. 8, pp. 129-148, 1991.
[9] J. K. Bergey, L. O'Brien, and D. B. Smith, "DoD Software Migration Planning," 2001.
[10] J. Bisbal, D. Lawless, B. Wu, J. Grimson, V. Wade, R. Richardson, *et al.*, "A survey of research into legacy system migration," *Technique report*, 1997.
[11] L. Kong, E. Stroulia, and B. Matichuk, "Legacy Interface Migration: A Task-Centered Approach," in *HCI (1)*, 1999, pp. 1167-1171.
[12] H. C. Kwon, H. H. Kim, J. T. Lee, and K. J. Yoo, "A migration strategy of mobile agent," in *Parallel and Distributed Systems, 2001. ICPADS 2001. Proceedings. Eighth International Conference on*, 2001, pp. 706-712.
[13] T. C. Powell and A. Dent-Micallef, "Information technology as competitive advantage: the role of human, business, and technology resources," *Strategic management journal*, vol. 18, pp. 375-405, 1997.
[14] G. Stoneburner, A. Goguen, and A. Feringa, "Risk management guide for information technology systems," *Nist special publication*, vol. 800, pp. 800-30, 2002.

Glossary

ISACA Risk IT framework is a framework created by ISACA (Information Systems Audit and Control Association) to understand and manage all significant IT risk type.

IT risk is potential loss related to process in the information technology.
ITRM (Information Technology Risk Management) is the application of risk management dealing with IT risk.

Migration plan is a collection of process or procedure to be followed to move data, application, or software.

Risk assessment is a way or procedure to evaluate the vulnerability and impact to determine the potential risk.

Risk scenario is a description of event may be occurred and contain risk which can impact to the business

Appendix A. Risk Assessment Matrix

Phase	Risk Scenario	Risk Likelihood Rating	Risk Impact Rating	Overall Risk Rating	Control	Review
Strategy	Identify the risk if the system is not upgraded [asset]	High	High	High	Mitigate the risk	Upgrade the system to the new one
Planning	Risk on Stakeholder [actor]					
	Risk on Migration Team [actor]					
	Identify the risk of the time and project scope [time]					
	Ineffective execution of schedule [event]					
	Risk on system dependencies [resource]					
	People and organization risk [asset]					
	Risk on IT infrastructure[asset]					
	Risk on infrastructure(facilities) [asset]					
Preparation	Accidental and failure risk [threat type]					
	Choose proven application [resource]					
	Ineffective design risk [event]					
	Duration risk [time]					
	Reassurance of Information availability [asset]					
	Ineffective execution risk [event]					
Migration	Modification risk [event]					
	Interruption risk [event]					
	Risk on losing the data [resource]					

Annual Conference on Management and Information Technology 2014

Enhancing Web Security through Infrastructure Design

Muhammad Salahuddien Manggalanny

Id-SIRTII/CC, Ravindo Tower, 17th Floor, Kebon Sirih Raya 75, Jakarta 10340, Indonesia

Abstract

Security is a dynamic situation. The web system threat will always increase in line with traffic growth. Improving system weakness, as a standard security approach will not sufficient to defend web system. It needs different security approach allowing optimization over existing deployment with minimum effort and can be effectively overcome the complexity and uncertainty challenges. This can be done through infrastructure design approach, which was proven in enhancing web security.

Keywords: web; security; infrastructure; design

1. Background

Most of methods to strengthen web security are focused on the effort to improve system weakness. For example, upgrading to the latest Operating System, applications engine i.e. PHP, ASP, Java etc. and CMS (Content Management System), database structure and/or hardening the configuration. This approach will need a lot of time and procedures to assess the system from time to time to figure out common vulnerability in each system components. Then, every security holes found need to be patched with the latest updates. [1] Sometimes new patches triggered new problems, i.e. compatibility issues and dependencies, and performance degradation. Prior test on development platform needs to be conducted first to ensure safer implementation and prevent later disruption. Then, after series of complex patching and hardening procedures it is still has another weakness, which is zero day vulnerability. [2]

This paper proposes an approach (that are rarely used) to enhance web security through architecture design improvement. It is proven in many web development project in Indonesia – including official presidential and vice president sites, others high profiles and government services – especially to avoid lack of periodic security assessment and zero day vulnerability. And it may help system administrator, which have limited resources and security knowledge (updates) to defend its services.

Advantages of this enhancement approach are: one time deployment with minimum requirement and possibility to deploy on top of existing infrastructure with selected modification and reconfiguration. It does not need heavy maintenance, long run security procedures i.e. audit and change management and minimum operational cost, including human resource (expertise).

2. Problems

Typical web system implementation in Indonesia has similar problems, especially for government agencies sites and its online public services. Sustainability and governance issues – because of budget problems and bureaucracy – are the biggest challenges. Common security approach i.e. maintenance, inspection, patches are often could not be held regularly due to resource uncertainty.

Based on latest Id-SIRTII/CC assessment and incident reports we can identify such related issues:

- ***Poor web infrastructure design (no staging/protection)***. Most of web system project are not implementing infrastructure design. Often because of its only cover web development and basic operation (co-location/hosting). Without proper infrastructure design the system are consider exposed and should dealt with the threat directly i.e. zero day attack.
- ***Inadequate application maintenance (no update/patch)***. The complexity of project policy, directly affecting to maintenance program. It is not popular in government budget compared with (goods) procurement. The administrator should prioritize which services are most critical and need to be updated immediately. Then the others should be restrained. In the other way, the attacker always uses the weakest security chain, which is unpatched host.
- ***Bad configuration (default/no fine tune/hardening)***. Many government projects are considered as "last minute" project. Proper development and fine tune and hardening need time. Impact of this problem is: bad configuration can be easily found and exploited by the attacker.
- ***Infrequent audit (penetration/performance testing)***. Government budget availability is very limited so it is not possible to do full system assessment (including pre/post-test) periodically. Penetration and post-performance test will only conducted if required by regulation. Without system audit/assessment it is difficult to find out any weakness and vulnerability.
- ***Careless management (no supervision/policy/SOP)***. Most of Web System implementation is outsourced to Third Party Company. So, it is not attached directly to the business process. Then management thinks this contract is enough, they don't have to write any policy/SOP.
- ***No sense of belonging/sense of crisis from the owner***. Because it is operate by third party. If something happened, the management simply feels that it is not their problems and somebody (third party) will or should solve it for them. But it's not. The outsourcing contract usually is for development and operation not for periodic maintenance and/or incident handling.

Complexity is the enemy of security and both are always evolving. It is not possible to handle many kind of dynamic threat while managing dependencies factors at the same time – for example patching vulnerability may cause another issues: compatibility and zero day. [1] [2] But, implementing the patch is mandatory to prevent ongoing security threat. Even there is a change management procedure: pre-test on development environment, there is no guarantee it will succeed. Even worse it will raise uncertainty. As describe previously, it is clear that complexity is the root cause of insecurity in Indonesia.

3. Infrastructure Security Design

This paper proposes Infrastructure Security Design approach as a solution. Although it is not new but already proven and helps administrator to defend web system effectively. Even if they are suffer from typical implementation problems in Indonesia – which are complexity and uncertainty. MSDN was also discussing the importance of Architecture and Design Issues for Web Applications. [3]

Infrastructure security design consists of four major sections, as follows:

- ***Virtual separation***. In order to have redundant system with fail over capability, we separate each system component into different virtual server image instead of expensive and ineffective physical server. With this approach, we can optimize resource utilization while at the same time build redundancy. For example, typical web system will have at least three components, which is web interface, application and database. With this design, we can easily replicate each component into separate virtual system image then doubled it into synchronized fail over system and spare another identical image as a master copy for backup.
- ***Service staging***. Common web system are exposed directly to the users, and in the other hand is: the attacker, it is easy to reveal web programming codes and follow the system process or application command, even looking up to the application version. Or using web exploitation tools, it's easy to figure out any vulnerability. How to prevent direct exposure are an essential security strategic need to be employed. Service staging design will separate application engine and database from the web interface and put a proxy as a front end. In this design, the system will interact with the users without exposing its processes. The users, or the attacker, will only view static HTML format that are forwarded from the web interface – instead of the original dynamic content that are usually generated from common web application system. Even web exploitation tools will gets nothing.
- ***Perimeter protection***. It is also an essential security protection but very rare to use. Having WAP (Web Application Firewall) in front of the system is always a good idea. It will automatically eliminate malicious traffic and mark suspicious activity for further inspection. This appliance has another capability: sent alert, create statistic report and helps administrator to analyze an incident. Conventional IDPS and SIEM – log correlation analyzer – are also still needed. The whole integrated combination features will effectively helps mitigation process, preserved artifact and event evidence for investigation or examination.
- ***Access control management***. Gaining an access will always be the first attempt of attack. Exposing CMS and Control Panel at the front-end interface – as default configuration – are common drawback of access control management. This weakness is too easy to be exploited successfully. The basic idea of this design is: putting access control management at the back end using separate virtual VPN server with AAA (Authentication, Authorization, Accounting) features as a baseline access security. Then the administrator can avoid unwanted or unknown direct access gathering from external network. For example brute force (dictionary) attack, fake users ID and IP spoofing.

Since VPN/AAA service are separated from the web system, only verified user with allowed IP's can access the CMS and/or Control Panel.

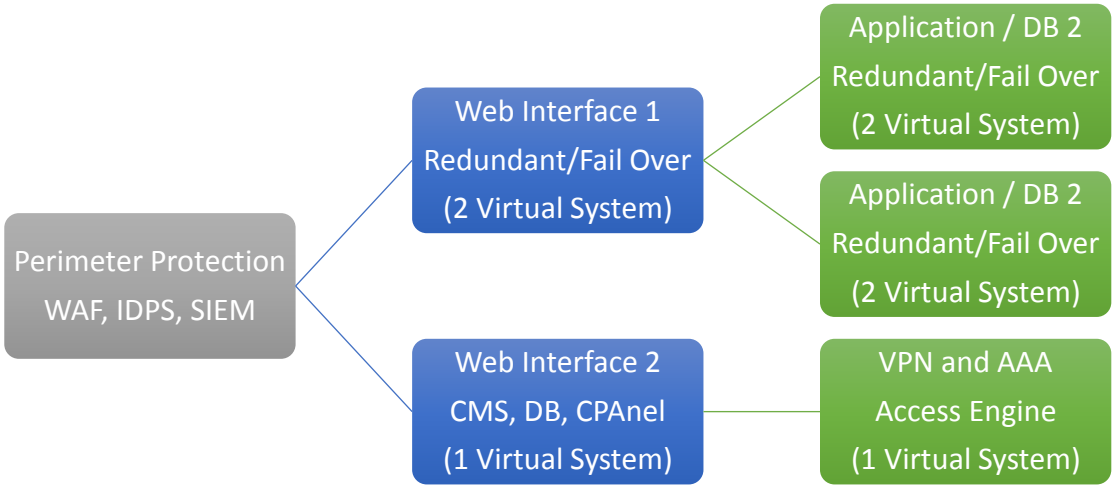


Figure 1 Secure Web Infrastructure Design

This figure explains basic implementation of each component in infrastructure security design. The first layer is Front End in which Perimeter Protection was employed. The users can only interact with Front End and the back end system also can only interact with Front End. Second layer is where the actual Web Interface – also acting as content replication engine and redundancy was built virtually. Those layers typically are connected through private IP's that are not routed anywhere. Sometimes it needs enhancement for example encryption with local SSL. Suggested content replication method is push (one way) from Web Interface to front end. The third layer is production application with VPN and AAA services. It's also virtually redundant and synchronized.

4. Perimeter Protection

Perimeter protection is a basic network based security that is essential in defending web system. In this security infrastructure design approach we must consider to employ as many as possible. There are many suitable perimeter protection solutions available as follows:

- ***Intrusion Detection and Prevention System (IDPS)***. Security threat are dynamically changes over the times, rules based protection are still relevant and effective to address some known issues. Employing any IDPS are always helpful to detect and eliminate most threat. Its more powerful than conventional firewall, despite the lack of updates and false positive misconfiguration, the event alert are always useful for better situation awareness.
- ***Web Application Firewall (WAF)***. One of the most essential web security protection is how to safeguarding the access. WAF defend web from known attacks proactively. From a famous SQL Injections, Cross Site Scripting, Cross Site Request Forgery to Local and

Remote File Inclusions. Most WAF relies on signatures to detect and block attacks. But some application i.e. NAXSI uses a simpler model: it detects unexpected characters in the HTTP requests or arguments. Each kind of unusual character will increase the score of the request. If it reaches a score considered "too high", the request will be denied or redirected to a landing page.

- ***Security Information and Event Management (SIEM)***. This capability includes monitoring real time traffic to identify threat and correlating security events. Conducting data gathering, analyzing and presenting information from operating system, database, application, network and security devices logs. Analyzing event characteristics such as the source, target, protocol or event type then storing for further mitigation including forensic and artifact examination.
- ***Network Behavioral Analysis (NBA)***. After establishing a benchmark for normal traffic, NBA program passively monitors network activity and flags unknown, network unusual patterns that might indicate the presence of a threat. The program can also monitor and record trends in bandwidth and protocol use. NBA is particularly good for spotting new malware and zero day exploits and malicious (abnormal) transaction or traffic.
- ***IP Reputation Engine (RE)***. It is a simple procedure to check the IP's or domain reputation databases to prevent fraud, scams, spam and phishing. Many host that are being connected to the web system are infected by bots and malware or connected through malicious proxies, and does not have valid domain name etc. It's better to reject this suspicious access.
- ***Anti Distributed Denial of Services (DoS)***. Subscribing to anti DoS services will reduce cost and safe in house resources. DDoS attacks are getting bigger and more complex. With limited bandwidth and sophistication, in house stand-alone DDoS appliance can no longer mitigate or prevent today's multi-vector DoS and multi-layer (including application) DDoS attacks.

5. Enhancing Performance

There is additional benefit in this design, which is enhancing performance. The same HTTP reverse proxy technology can be used to accelerate delivery of web content through integrated caching, stream splitting or aggregating through load balancer and bandwidth controls. Many additional plug in and modules are available for these purposes. Another fine tuning configuration will scale up web farms by managing off-loading user authentication and SSL tunnels. In some cases we can also employ web compression module as an in-line content optimization, if needed.

In this scenario, we configure front-end interface as load balancing host with simple round robin mechanism. Each request will be handled equally separated by different virtual server and both server will replicate and synchronize its content deliberately. Downside of this scenario is, load balancer will continue to send data to the virtual servers even if they are not responding (inactive). To prevent this flaw we should set up *maximum fails* and *fall time out* mechanism with some certain number i.e. 10 times and 15 seconds. It means, if the virtual servers not responding after 10 request and or 10 seconds, it should be considered inactive. Traffic will redirect to another servers.

Simple load balancing may not appropriate for heavy load sites with tons of request per time. Users will experience numerous error, process disruption and possible data lost in the middle of transaction. In this case, we should employ another load balancing methods, which is weighted traffic distribution and IP hash control. In this configuration each request from the same IP will handle by one specific virtual server every time they visit the site unless the VPS (Virtual Private Server) is down. Then it will be redirected to an alternate VPS – based on pre-defined weighted

allocation. VPS with larger weight number will handle more than others VPS. More likely, similar requester will be handled by the same VPS. If some VPS was down, in the middle of transaction, the users will be rolled back to its initial state and passes to the next VPS available seamlessly, without disruption.

NGINX *maximum fails* and *fall time out* with weighted value and IP hash, sample configuration:

```
upstream backend {
 ip_hash;
 Server backend1.example.com max_fails=3 fail_timeout=15s;
 server backend2.example.com weight=2;
 server backend3.example.com weight=4;
}
```

Another sophisticated option for load balancing and fail over redundancy capability are using LVS (Linux Virtual Server) and VRPP (Virtual Router Redundancy Protocol) technology. LVS is a robust virtual server cluster management system, allowing integration of different VPS into single managed cluster. And the VRPP is a very simple Layer-2-redundancy protocol, which provides virtual MAC (Media Access Control) address into each VPS. This protocol defines one VPS to act as master routers that can be taken over seamlessly by the next in line VPS as a redundant backup.

Load balancing is essential to availability and quality of service issues, and also important for security reason. For example, it could prevent TCP syn flood and surf attack to be successful in a first place, since every request will be distributed to different VPS. Content replication capability will avoid file inclusion attack, since it will refresh (rewrites) with newer content periodically.

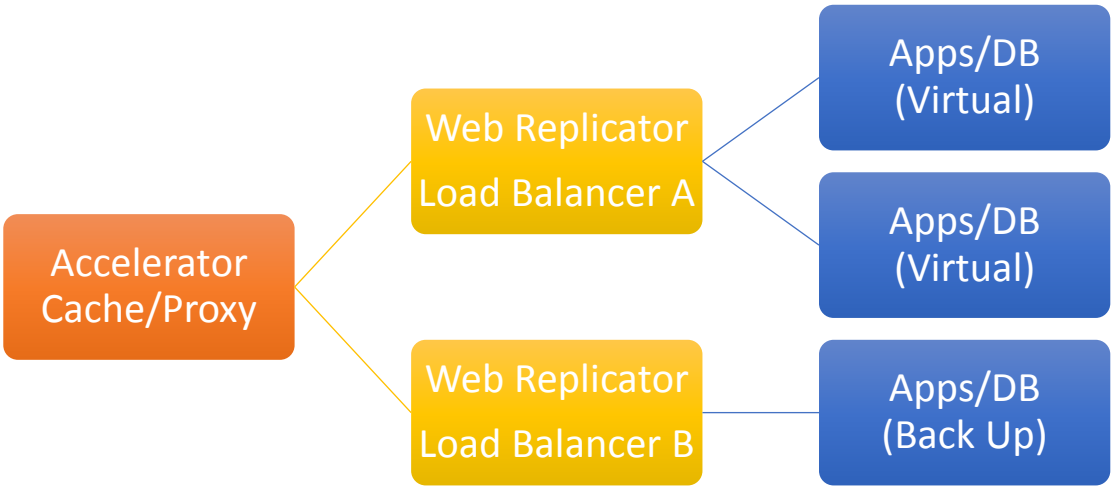


Figure 2 Web System Enhancements Design

Explained in this figure how the enhancements design works through fine-tune reconfiguration. For example we can activate NGINX cache accelerator function within Front End box.

6. Case Study

The reason of why this effective approach is not famous is because its came from the networking point of view. For example, the origin Perimeter Protection design are comes from the basic host based security theory. And the origin Service Staging designs are comes from the DMZ theory. Then, here is the problem: most of web system project owner are looking for web developer (designer, programmers, analyst, database administrator and system engineer), but unfortunately none of them will pay attention to the infrastructure design. Even if then they are hiring an expert (security consultant) to conduct audit or to review the implementation. Assessment will only seek for the flaws within programming codes, application and system vulnerability or perform penetration test – as described in any ISMS.

Most of those reported web sites were followed ISMS assessment and none of them using infrastructure security design as a methodology to protect its systems. [14] Some of web sites suffer from recurrence event, even after conducting comprehensive audit and hardening. [15] Some of web site was removed from recurrence list after succeeded implementing infrastructure security design. [16]

There are ongoing infrastructure security design projects for example Supreme Court and Internal Revenue Services that was experiencing incident. [11] [12] Those agencies hold hundreds of distributed intranet web system nationwide. [13] We found out similar situation causing vicious circle of evolving threat and vulnerability. It is clear that conventional approach

is not doing well. In this case, an expert needed to recast the topology and strongly suggesting the implementation of centralized system.

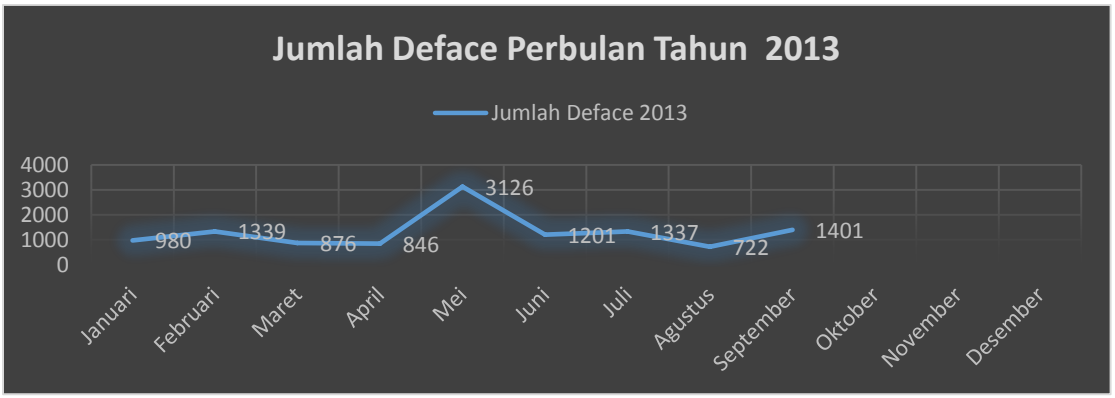


Figure 3 Web Defacement Report 2013 – Source: Id-SIRTII/CC

High profile with heavy load web system like Indonesian Presidential and Vice President web site, experiencing thousands hits every day and hundreds attack with any type of attempt. Including L/RFI, XSS, SQL injection, brute force (dictionary), surf, TCP syn flood, DDoS and regular port scanning or BOT crawling. But none of that attempt was succeeded since the establishment in 2006, even though the result of annual system audit always shown many misconfiguration, flaws and also vulnerability. [10]

We also conducting proof of concept by using major assessment tools i.e. Acunetix, Web Scarab from OWASP and light weight Wapiti, Skip fish, SC Labs Exploit-me plug-in (XSS, SQL, Access test), for the purpose of this paper. The result findings similar weakness was shown by official annual audit. And, we engage test using common exploitation tools i.e. Metasploit but none of the penetration attempt was succeed. Note: exposing further details are forbidden by the NDA.

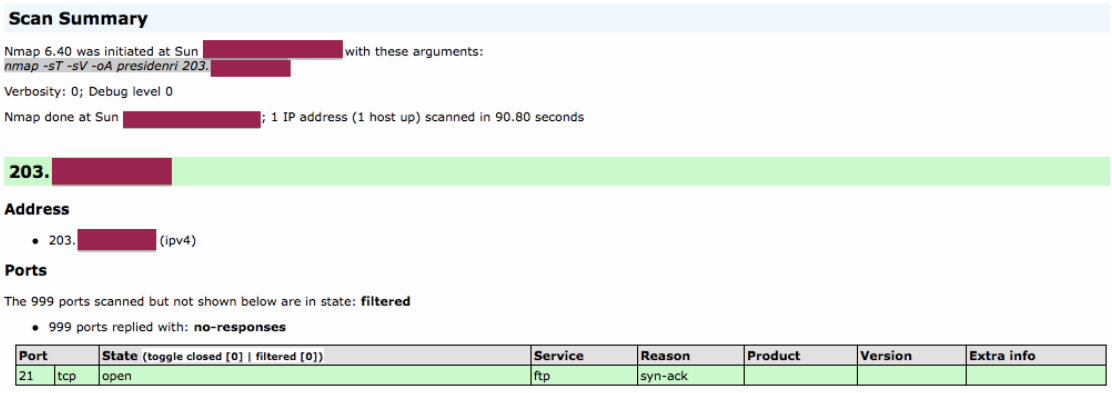


Figure 4 Nmap Scanning Result

For example 2013 internal audit report findings mentioning PHP Calendar components flaw (integer overflow) causing denial of service and others PHP vulnerability. [17] But none of those exposed to the external network. Using Acunetix tools we only found low laxity like directory traversal issues through Front End interface; which is NGINX with NAXSI Perimeter Protection (WAF).

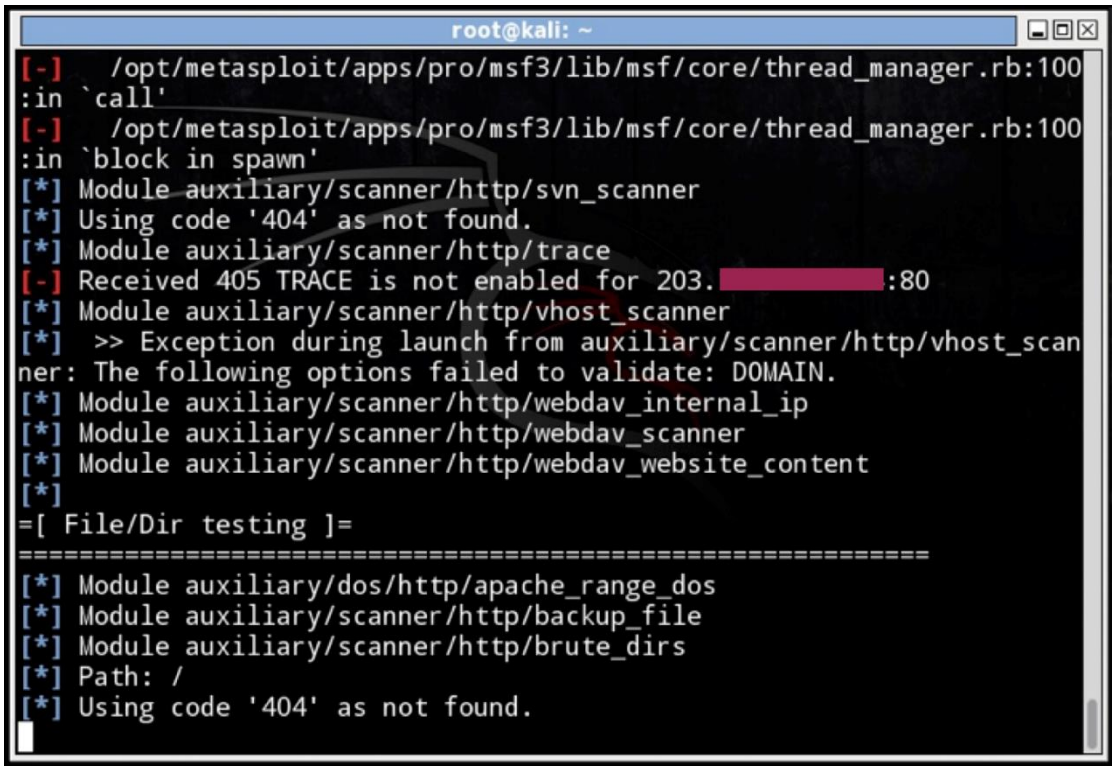


Figure 5 Metasploit comes with no result

Below explained real complete architecture implementation of Infrastructure Security Design:

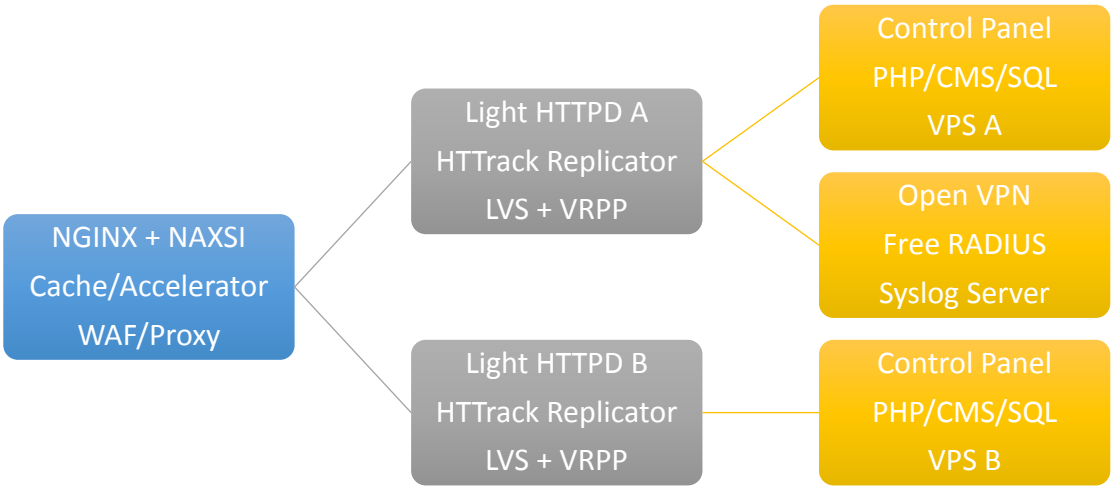


Figure 6. Architecture of Presidential Web Sites

The implementation of infrastructure design as follows, was carried on this impressive reputation:

- ***Perimeter protection***: using NAXSI from OWASP (Open Web Application Security Project) as a WAP plug in for NGINX. [4] Then combined it with SNORT IDPS (Intrusion Detection and Prevention System and OSSIM SIEM (Security Information and Event Management) – both are free, open source application. [8] [9] We also build separate Syslog Server to collect logs from all services to provide raw data for further analysis.
- ***Web accelerator***: using NGINX – a full featured, lightweight, free, open source and powerful reverse HTTP proxy. NGINX uses scalable event driven (asynchronous) architecture to handle request instead of threads based on conventional HTTP server. This mechanism will handle under load memory more efficient and helps the system to scale up for thousands request with the same resources. With the support of many third party plug in and modules, NGINX can be expanded into full-featured secure HTTP server and/or as push cache/accelerator. [6]
- ***Reverse proxy***. The basic idea of reverse proxy is to hide the existence and characteristic of the origin servers. Using NGINX as a reverse proxy, it will acts as a front end intermediary to redistributed the traffic request to its associated servers (web, application and database) – usually separated behind the internal network to prevent direct connection with the requester. The requester or the attacker may not be aware of the processes under way that may have known vulnerability or zero day. [6]
- ***Virtualization***: using XEN hypervisor engine – a free, open source x86-64 virtualization. XEN was developed by University of Cambridge (now XEN Project) – providing services allowing multiple Operating Systems to be executed in the same hardware resources concurrently and shared the server idle capacity (processors, memory and storage) efficiently. [7]
- ***Service staging***: separating all services into different Virtual Private Server (VPS): front end, web server (using Light HTTPD – a free, open source, light, high performance HTTP server), application (PHP engine and CMS) and database. It is inspired by NIST Web Service Security Standards. [1]
- ***Web replicator***: using HTTrack – a free, open source web site copier. It will allow dynamic content generated from usual web server to be converted into static HTML codes. HTTrack build identical web site structure recursively into local directory, including images and any other files from origin server. HTTrack arranges the original site's relative link-structure as a mirror so the visitor can browse the site from link to link, as if they access it directly to the origin server. HTTrack can also update an existing mirrored site by pushing static input content and reverse converted into dynamic content that are fit to the origin server format. It also have a capability to resume interrupted downloads.
- ***Load balancer***: using NGINX as an intermediary and managed by LVS (Linux Virtual Server) and VRPP (Virtual Router Redundancy Protocol) to handle traffic distribution.
- ***Access control management***: using combination of Open VPN and Free RADIUS – both are free, open source application. Provide secure (encrypted) access, auditable user authentication, IP restriction and control remote access.

7. Disadvantages

It is perfectly appropriate for a static site. For dynamic services i.e. form, forum, advanced databases query etc. which require user interaction, it needs additional separate reverse proxy configuration with push features. Sometimes each dynamic function needs to be treated specifically. [18]

It is not aimed to fix any vulnerability. Means, the weakness is still there. [17] It will not fit to small systems implementation – since more resources are required, for example servers and memory. Despite of its simplicity and robustness, in fact configuring infrastructure security are not easy. Series of commissioning test are needed to ensure stability and to record troubleshooting guiding procedures. It may costly, although it's only performed in the beginning of the project.

8. Conclusions

Nowadays common security approach i.e. maintenance, inspection, patches are often could not be held regularly due to resource uncertainty. For example budget reducing, limited skills and knowledge, even lack of policy and procedures. Increasing complexity of the threat and always-evolving attack cannot be encountered by conventional security approach that is only focused on the effort to improve system weakness. Complexity is the enemy of security and its always evolving. Not possible to handle dynamic threat while managing dependencies factors at the same time.

This paper proposes different approach – that is rarely used, to enhance web security through an infrastructure design improvement. It was proven in many high profiles and heavy load web sites in Indonesia. For example President and Vice President web sites. [10] It will effectively avoid the lack of periodic security assessment and zero day vulnerability. It may helps system administrator, which have limited resources and security knowledge (updates) to defend its services.

References

[1] Anoop Singhal, Theodore Winograd and Karen Scarfone. Guide to Secure Web Services. *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-95. Gaithersburg, MD 20899-8930: Computer Security Division, Information Technology Laboratory – National Institute of Standards and Technology – United States Department of Commerce; September 2007

[2] Miles Tracy, Wayne Jansen, Theodore Winograd and Karen Scarfone. Guidelines on Securing Public Web Servers. *Recommendations of the National Institute of Standards and Technology*. NIST Special Publication 800-44 Version 2. Gaithersburg, MD 20899-8930: Computer Security Division, Information Technology Laboratory – National Institute of Standards and Technology – United States Department of Commerce; September 2007

[3] J.D. Meier, Alex Mackman, Michael Dunner, Srinath Vasireddy, Ray Escamilla and Anandha Murukan. Improving Web Application Security: Threats and Countermeasures. Microsoft Corporation; June 2003, Chapter 4

[4] OWASP https://www.owasp.org/index.php/Main_Page

[5] NAXSI https://www.owasp.org/index.php/OWASP_NAXSI_Project

[6] NGINX http://wiki.nginx.org/Main

[7] XEN http://www.xenproject.org/

[8] SNORT http://www.snort.org/

[9] OSSIM http://www.alienvault.com/open-threat-exchange/projects

[10] http://www.presidenri.go.id and http://www.wapresri.go.id

[11] http://www.pajak.go.id and https://www.mahkamahagung.go.id/

[12] Incident http://techno.okezone.com/read/2013/12/13/55/911757/diretas-pocong-warnai-situs-pajak-go-id
Incident http://www.tempo.co/read/news/2011/03/31/063324282/Situs-Mahkamah-Agung-Diretas

[13] Distributed nationwide intranet web system http://komdanas.mahkamahagung.go.id/
[14] Request for Id-SIRTII/CC Website Defacement Analysis Report 2013 http://www.idsirtii.or.id/
[15] Recurrence event http://nasional.kompas.com/read/2013/07/31/1323336/Situs.Bareskrim.Polri.Diretas
Recurrence event http://news.okezone.com/read/2013/05/11/337/805346/redirect/large
[16] Previous incident http://techno.okezone.com/read/2011/06/03/55/464249/pesan-hacker-di-situs-kemenpora/large
[17] CVE-2013-4635 http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2013-4635
[18] Interraction http://search.presidenri.go.id:8000/cgi-bin/namazu.cgi?query=&max=10&result=normal&submit=GO

Annual Conference on Management and Information Technology 2014

Development of Intelligent Filter for RSS-based Radio Tracking and its Application

Legowo Budianto

Master of Information Technology Department, Swiss German University,

Edu Town BSD City, Tangerang 15339, Indonesia

legowo.budianto@gmail.com

Abstract

Indoor positioning system (IPS) boosts numerous applications in mobile computing. Google and Microsoft recently add IPS to their map solution. IPS is a cheap solution to replace Global Positioning System (GPS), which is inaccurate for indoor environment. The system provides a new layer of automation called automatic object location detection. Real world applications depending on such automation are many. To name a few, one can consider the location detection of products stored in a warehouse, location detection of medical personnel or equipment in a hospital, location detection of firemen in a building on fire, detecting the location of police dogs trained to find explosives in a building, and finding tagged maintenance tools and equipment scattered all over a plant. To make an IPS a reality there are numerous consideration and challenges to justified and tackle. This paper highlight some of the issues and make some suggestion to tackle it

Indoor Positioning System; Finger Printing; Received Signal Strength Based

SWISS GERMAN UNIVERSITY
MASTER OF INFORMATION TECHNOLOGY
Kavling EduTown II.1
BSDCity Tangerang 15339
Telp. 021 3045 0045, Ext 1501-1505
mit@sgu.ac.id | sgu.ac.id

ISSN : 977-2355-020-149