Tapping Open Source Governance Risk and Compliance Tools to Monitor Compliance to the Data Privacy Act of 2012

Lyn De Guzman, Danny Cheng
Information Technology Department
College of Computer Studies De La Salle University
danny.cheng@dlsu.edu.ph

Abstract: There has been a growing complexity in the three disciplines: Governance, Risk, and Compliance (GRC) over the years due to an increasing number of regulations being implemented by the government both in the international and local scene, risks that organizations have to deal with if they do not comply with these regulations, and ensuring and monitoring alignment of organization's objectives to these regulations (Racz et al, 2011). Organizations need to be able to ensure compliance easily to these regulations and they go through audits in order to be certified as compliant (El Kharbili et al, 2008) and one way to ensure compliance is to monitor it and be prepared prior to audit schedule. One way of efficiently monitoring compliance is to utilize a GRC tool, which allows key proponent to create and coordinate policies and controls and map them to regulatory requirements (Lindros, 2017). However, a GRC tool can be complex to use (Eramba, n.d.) and there are several GRC tools in the market. In this study, our approach to monitor the compliance level and related projects of the DPA of 2012 is by selecting Eramba as the GRC tool and Redmine as the ticket tracker in order to be suitable for monitoring compliance with the DPA of 2012. Our study also shows how the DPA of 2012 can be embedded within the GRC tool so that it can be part of the overall organizational governance system.

Key Words: Governance Risk and Compliance, Open Source, Data Privacy, Management System Implementation

1. INTRODUCTION

The implementation of the provisions of the DPA of 2012 through the IRR is relatively new in the local setting (Mundin, 2017). Impacted companies have only complied last September 9, 2017 for the Phase 1 of DPA of 2012. With the rising need to be compliant to the DPA of 2012, it is important to monitor the compliance level and status of the implementation of the DPA of 2012 through projects before the next audit occurs. However, monitoring the compliance level and the status of the overall implementation of the regulation can be challenging prior to audit. Usually, what organizations have are the spreadsheet with list of requirements, then person-in-charge asks around relevant teams if they have everything in place and will add notes on the spreadsheet to have a view on how everything is before the audit (Eramba, n.d.). Imagine the several exchanges of email and the consolidation of spreadsheets accomplished by different business units only to have a view how much compliant an organization is to the said regulation.

As previously mentioned, one efficient way of monitoring is through the utilization of a GRC tool, which can increase efficiency and reduce complexity (Lindros, 2017). However, uploading the DPA of 2012 to a GRC tool in order to create a compliance package for monitoring can be complex as its content is too general and different compared to standards document such as the PCI-DSS, HIPAA, ISO27001, etc. that are straightforward in their directives of what needs to be performed by the organization in order to be compliant. Thus far, there are no existing studies found yet that deals about customizing a specific GRC tool such as Eramba for monitoring the compliance level and the status of projects related to the implementation of the DPA of 2012 that are tracked in a separate project management system and as to how the said regulation can be structured and uploaded in the tool. Therefore, the problem addressed in this study is how to customize Eramba and utilize it for monitoring the compliance to the DPA of 2012 and also, the implementation status of its related projects that are being tracked in a separate project management system. This GRC tool may be utilized by organizations that need to present their compliance to the Data Privacy Act to NPC.

2. OBJECTIVE OF THE STUDY

The objective of this study is to customize Eramba and utilize it for monitoring the compliance level and the status of the implementation of projects related to the DPA of 2012, and to determine the compliance level. Specifically the study included the following goals:

- To format the DPA of 2012 in order to be uploaded and accepted by Eramba;
- To create the compliance package for the DPA of 2012 in Eramba;
- To register sample assets, risks, controls, and policies in Eramba;
- To map the registered sample assets, risks, controls, and policies appropriately to the created compliance package for the DPA of 2012;
- To manage the links of related DPA projects that are being monitored in Redmine to a particular compliance requirement of and controls for the DPA of 2012 in Eramba;
- To evaluate as to how Eramba demonstrates the compliance level to the DPA of 2012 and the status of related projects

3. METHODOLOGY

3.1 Understanding Eramba architecture

This section will discuss the relevant modules of Eramba namely the Organization, Asset Management, Controls Catalogue, Risk Management, Compliance Management, and Security Operations and what modules can be mapped to each module. The illustration below provides a holistic understanding of the GRC philosophy behind the system of Eramba Fig. 1.

The Compliance Analysis submodule that is under the Compliance Management module is where the projects, assets, security services (controls), policies, and risks are being mapped to their appropriate compliance requirement. The compliance requirements are created in the system by creating a package in the Compliance Package submodule under the Compliance Management module as well. However, before one can create a Compliance Package, the name of the regulation must be created in the Third Parties submodule under the Organization module first.

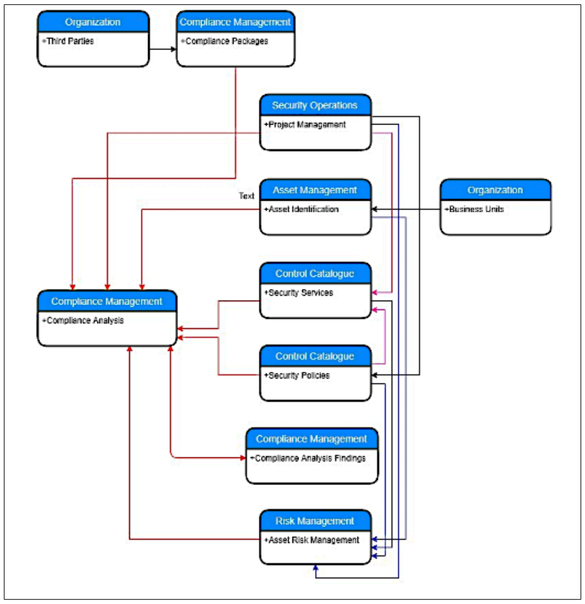


Figure 1. GRC Philosophy of Eramba System

Assets are registered in Assets Identification submodule under Asset Management module. Business units own these assets and Business units are defined in Business Units submodule under the Organization module. Projects are registered in Project Management submodule under Security Operations module. Security Services, also known as controls, are created in Security Services submodule un-der Control Catalogue module. Policies are also considered as controls but Eramba made a separate submodule for it and are registered in the Security Policies submodule under the Control Catalogue module. Risks are created in Asset Risk Management submodule under Risk Management module. Statements from auditors are created in the Compliance Analysis Findings submodule un-der the Compliance Management module and mapped to the affected requirement in the Compliance Analysis submodule.

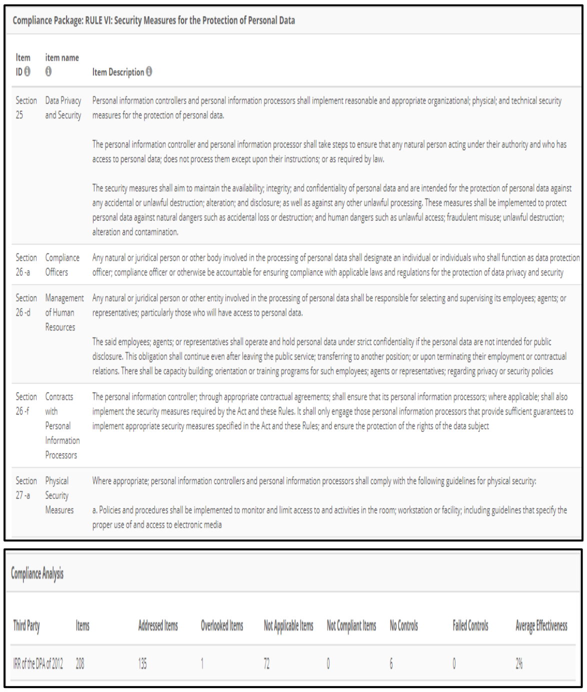
Assets are owned by business units and are prone to threats and have inherent risks, which controls should be applied to. Looking further, assets are directly connected to the Business Units but the assets and business units are not directly connected to controls and vice versa. The relevant modules and submodules and how they are connected shows that the program of Eramba enforces the relationship of Governance, Risk, and Compliance.

3.2 Incorporating DPA within Eramba

Eramba being configurable to multiple requirements allows for the uploading of the requirements as a Compliance Package. The Compliance Package cannot be created without creating the Third Party for DPA of 2012 first. It is required in batch uploading the Compliance Package and in creating the same one by one. Third Parties may be the suppliers, customers, or regulators. In this study, regulators shall be selected for the DPA of 2012. The DPA of 2012 in CSV file using the "Import" feature of Compliance Package was successfully uploaded in Eramba after applying the format of GDPR that was based on the documentation of Pre-Compiled Compliance Packages in the website of Eramba.

However, when one analyzes the Compliance Analysis sub-module under Compliance Management module Fig. 2 and view it in the Health sub-module under Program module, it does not provide a comprehensive details on how much an organization is compliant so far to the DPA in terms of requirements including the program controls, and implementation of projects related to the said regulation. With this, the second format was developed.

In doing the second format Fig. 3, the pattern of the Five (5) Pillars of Data Privacy Accountability and Compliance was applied. In this type of format, the Five (5) Pillars were created in a separate Third Party while the components of each pillar were the Compliance Packages and the requirements to accomplish each component were the items that need to be addressed in order to say that compliance to a particular pillar is complete.



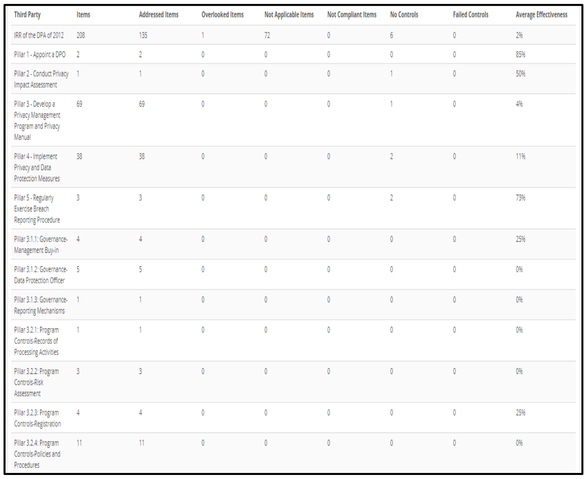
Compliance Package: RULE VI: Security Measures for the Protection of Personal Data

Item ID	item name	Item Description
Section 25	Data Privacy and Security	Personal information controllers and personal information processors shall implement reasonable and appropriate organizational; physical; and technical security measures for the protection of personal data. The personal information controller and personal information processor shall take steps to ensure that any natural person acting under their authority and who has access to personal data; does not process them except upon their instructions; or as required by law. The security measures shall aim to maintain the availability; integrity; and confidentiality of personal data and are intended for the protection of personal data against any accidental or unlawful destruction; alteration; and disclosure; as well as against any other unlawful processing. These measures shall be implemented to protect personal data against natural dangers such as accidental loss or destruction; and human dangers such as unlawful access; fraudulent misuse; unlawful destruction; alteration and contamination.
Section 26 -a	Compliance Officers	Any natural or juridical person or other body involved in the processing of personal data shall designate an individual or individuals who shall function as data protection officer; compliance officer or otherwise be accountable for ensuring compliance with applicable laws and regulations for the protection of data privacy and security
Section 26 -d	Management of Human Resources	Any natural or juridical person or other entity involved in the processing of personal data shall be responsible for selecting and supervising its employees; agents; or representatives; particularly those who will have access to personal data. The said employees; agents; or representatives shall operate and hold personal data under strict confidentiality if the personal data are not intended for public disclosure. This obligation shall continue even after leaving the public service; transferring to another position; or upon terminating their employment or contractual relations. There shall be capacity building; orientation or training programs for such employees; agents or representatives; regarding privacy or security policies
Section 26 -f	Contracts with Personal Information Processors	The personal information controller; through appropriate contractual agreements; shall ensure that its personal information processors; where applicable; shall also implement the security measures required by the Act and these Rules. It shall only engage those personal information processors that provide sufficient guarantees to implement appropriate security measures specified in the Act and these Rules; and ensure the protection of the rights of the data subject
Section 27 -a	Physical Security Measures	Where appropriate; personal information controllers and personal information processors shall comply with the following guidelines for physical security: a. Policies and procedures shall be implemented to monitor and limit access to and activities in the room; workstation or facility; including guidelines that specify the proper use of and access to electronic media

Compliance Analysis

Third Party	Items	Addressed Items	Overlooked Items	Not Applicable Items	Not Compliant Items	No Controls	Failed Controls	Average Effectiveness
IRR of the DPA of 2012	208	135	1	72	0	6	0	2%

Figure 2. Health monitoring of compliance to DPA first attempt

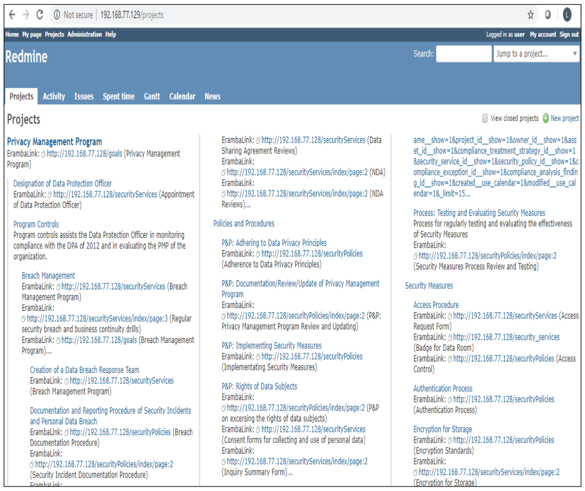


Third Party	Items	Addressed Items	Overlooked Items	Not Applicable Items	Not Compliant Items	No Controls	Failed Controls	Average Effectiveness
IRR of the DPA of 2012	208	135	1	72	0	6	0	2%
Pillar 1 - Appoint a DPO	2	2	0	0	0	0	0	85%
Pillar 2 - Conduct Privacy Impact Assessment	1	1	0	0	0	1	0	50%
Pillar 3 - Develop a Privacy Management Program and Privacy Manual	69	69	0	0	0	1	0	4%
Pillar 4 - Implement Privacy and Data Protection Measures	38	38	0	0	0	2	0	11%
Pillar 5 - Regularly Exercise Breach Reporting Procedure	3	3	0	0	0	2	0	73%
Pillar 3.1.1: Governance-Management Buy-in	4	4	0	0	0	0	0	25%
Pillar 3.1.2: Governance-Data Protection Officer	5	5	0	0	0	0	0	0%
Pillar 3.1.3: Governance-Reporting Mechanisms	1	1	0	0	0	0	0	0%
Pillar 3.2.1: Program Controls-Records of Processing Activities	1	1	0	0	0	0	0	0%
Pillar 3.2.2: Program Controls-Risk Assessment	3	3	0	0	0	0	0	0%
Pillar 3.2.3: Program Controls-Registration	4	4	0	0	0	0	0	25%
Pillar 3.2.4: Program Controls-Policies and Procedures	11	11	0	0	0	0	0	0%

Figure 3. Health monitoring of compliance to DPA second attempt

Once the packages have been uploaded to the Eramba, the rest of the modules can be used in accordance with the regular GRC process. However, since Eramba is mainly a GRC tool, it does not have extensive support for project management or ticket tracking in order to allow for granular monitoring of progress of the compliance program. As such, a dedicated project management ticketing system was used in the form of Redmine which is also open source.

In order for both to integrate and link seamlessly, the projects in Redmine were configured to match the compliance package that was uploaded to Eramba as can be seen in Fig. 4. The reference from Eramba to Redmine is placed as a URI as part of the comment section of the specific item that requires further work. It allows Eramba to link to Redmine to allow for tracking of the actual work conducted as well as the history of what transpired for that item before it was closed. This would normally refer to a control or a risk as defined in Eramba (Fig 5). To link back from Redmine to Eramba, the link to the actual module in Eramba is placed as part of the description of a project in Redmine as see on Fig. 6.



Projects

Privacy Management Program
ErambaLink: http://192.168.77.128/goals (Privacy Management Program)

Designation of Data Protection Officer
ErambaLink: http://192.168.77.128/securityServices (Appointment of Data Protection Officer)

Program Controls
Program controls assists the Data Protection Officer in monitoring compliance with the DPA of 2012 and in evaluating the PMP of the organization.

Breach Management
ErambaLink: http://192.168.77.128/securityServices (Breach Management Program)
ErambaLink: http://192.168.77.128/securityServices/index/page:3 (Regular security breach and business continuity drills)
ErambaLink: http://192.168.77.128/goals (Breach Management Program)...

Creation of a Data Breach Response Team
ErambaLink: http://192.168.77.128/securityServices (Breach Management Program)

Documentation and Reporting Procedure of Security Incidents and Personal Data Breach
ErambaLink: http://192.168.77.128/securityPolicies (Breach Documentation Procedure)
ErambaLink: http://192.168.77.128/securityPolicies/index/page:2 (Security Incident Documentation Procedure)
ErambaLink:

ErambaLink: http://192.168.77.128/securityServices (Data Sharing Agreement Reviews)
ErambaLink: http://192.168.77.128/securityServices/index/page:2 (NDA)
ErambaLink: http://192.168.77.128/securityServices/index/page:2 (NDA Reviews)...

Policies and Procedures

P&P: Adhering to Data Privacy Principles
ErambaLink: http://192.168.77.128/securityPolicies (Adherence to Data Privacy Principles)

P&P: Documentation/Review/Update of Privacy Management Program
ErambaLink: http://192.168.77.128/securityPolicies/index/page:2 (P&P: Privacy Management Program Review and Updating)

P&P: Implementing Security Measures
ErambaLink: http://192.168.77.128/securityPolicies (Implementating Security Measures)

P&P: Rights of Data Subjects
ErambaLink: http://192.168.77.128/securityPolicies/index/page:2 (P&P on excersing the rights of data subjects)
ErambaLink: http://192.168.77.128/securityServices (Consent forms for collecting and use of personal data)
ErambaLink: http://192.168.77.128/securityServices/index/page:2 (Inquiry Summary Form)...

ame__show=1&project_id__show=1&owner_id__show=1&asset_id__show=1&compliance_treatment_strategy_id__show=1&security_service_id__show=1&security_policy_id__show=1&compliance_exception_id__show=1&compliance_analysis_finding_id__show=1&created__use_calendar=1&modified__use_calendar=1&_limit=15...

Process: Testing and Evaluating Security Measures
Process for regularly testing and evaluating the effectiveness of Security Measures
ErambaLink: http://192.168.77.128/securityPolicies/index/page:2 (Security Measures Process Review and Testing)

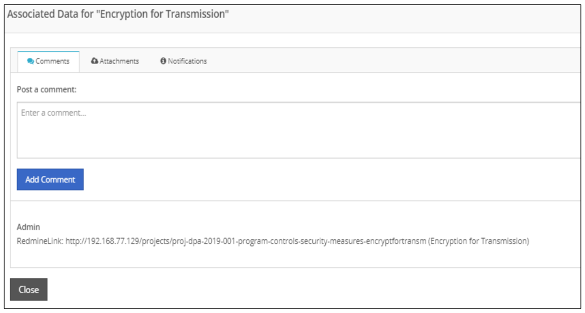
Security Measures

Access Procedure
ErambaLink: http://192.168.77.128/securityServices (Access Request Form)
ErambaLink: http://192.168.77.128/security_services (Badge for Data Room)
ErambaLink: http://192.168.77.128/securityPolicies (Access Control)

Authentication Process
ErambaLink: http://192.168.77.128/securityPolicies (Authentication Process)

Encryption for Storage
ErambaLink: http://192.168.77.128/securityPolicies (Encryption Standards)
ErambaLink: http://192.168.77.128/securityServices/index/page:2 (Encryption for Storage)

Figure 4. Redmine project structure



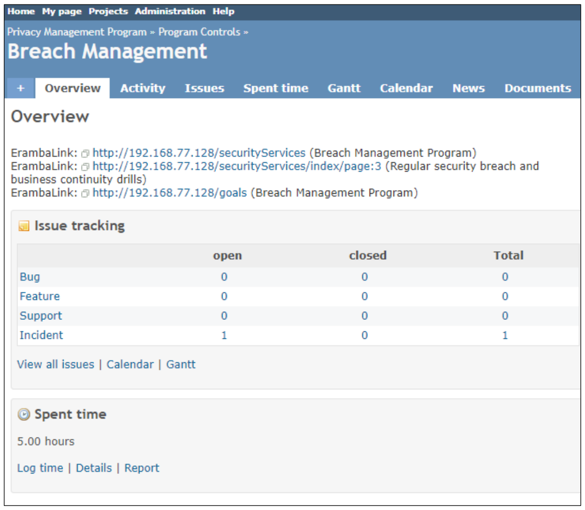
Associated Data for "Encryption for Transmission"

Post a comment:

Enter a comment...

Admin
RedmineLink: http://192.168.77.129/projects/proj-dpa-2019-001-program-controls-security-measures-encryptfortransm (Encryption for Transmission)

Figure 5. URI link from Eramba to Redmine



Privacy Management Program » Program Controls »

Breach Management

Overview

ErambaLink: http://192.168.77.128/securityServices (Breach Management Program)
ErambaLink: http://192.168.77.128/securityServices/index/page:3 (Regular security breach and business continuity drills)
ErambaLink: http://192.168.77.128/goals (Breach Management Program)

Issue tracking

	open	closed	Total
Bug	0	0	0
Feature	0	0	0
Support	0	0	0
Incident	1	0	1

Spent time

5.00 hours

Figure 6. Link from Redmine back to Eramba

4. RESULTS AND DISCUSSION

Eramba has exhibited in this study that it is an integrated Governance, Risk, and Compliance (GRC) tool that can be used for compliance monitoring in terms of the DPA of 2012. The tool was customized for the purpose of utilizing it in monitoring compliance to the DPA of 2012 including the implementation status of related projects. It was found that the first activity to be performed is to identify all the assets that will be impacted by the DPA of 2012 and the privacy-related risks inherent to each identified asset. Once done identifying the assets and risks, look at the organization's available controls and policies. From there, create the identified assets, risks, and controls in Eramba. The Security Services (controls) and Asset Management are not directly connected in the system, but the controls and Risk Management are. With this, the controls are connected to Asset Management through the Risk Management wherein risks identified here are asset-based risks, thus, this can be used in the Privacy Impact Assessment of each business unit when evaluating their assets for privacy risks. When navigating the Asset Risk Management module, all the risks identified there shall provide information on which assets are affected by the identified risk including the status of the assets, what controls are utilized for the treatment and its status, and the policies and procedures that contain the plan to address the risk. However, since the assets and business units are not directly connected to controls, indicating the name of business unit in the asset name and control name will be useful. With this, the user shall be able to visualize the business units that own these assets and the controls that they already have in place. These business units with the assistance of Information Technology and Information Security Groups shall confirm if these controls and policies are being applied, tested, and maintained well to ensure their effectiveness in protecting their assets from threats and vulnerabilities. Therefore, the organization is able to monitor their compliance at controls level. Another way to monitor at a controls level is by mapping appropriate assets, controls, risks, and policies to the compliance requirements for the Program Controls, which is one of the components of Pillar 3: Develop a Privacy Management Program and Privacy Manual.

After all the identification and mapping between risks, assets, controls, and policies in Eramba, the compliance package of the DPA of 2012 shall be created using the requirements defined in NPC's Five (5) Pillars of Data Privacy Accountability and Compliance Checklist and the stages indicated in

Program Controls of the Privacy Management Program. Basically, complying with the requirements stated in the checklist and in the Program Controls already addresses the Pillar 1: Appoint a DPO, Pillar 2: Conduct Privacy Impact Assessment, and Pillar 5: Regularly Exercise Breach Reporting Procedure. The DPA of 2012 is broad and non-instructional on what to really have and execute in order to be compliant to the DPA of 2012 compared to the requirements stated by the Five Pillars. Having an individual Compliance Package for each requirement of the Pillar provides a detailed view on how much compliant an organization is and what else needs to be addressed to as soon as possible.

5. CONCLUSIONS

This study was able to demonstrate how open source tools can be used to aide in the to reduce the barriers in the compliance efforts of an organization to the DPA of 2012. Furthermore, due to the manual encoding of Redmine Links in Eramba sub-modules through the "Comment" section that was performed in this study, it recommends conducting a new study that focuses on automating the connection between Eramba and Redmine and to look at Robotic Automated Processing (RPA) for automating other manual processes found in using the system. Finally, this study opens an opportunity to conduct a separate study on utilizing Eramba with other regulations or standards that will create interest from GRC professionals and organizations that are planning to utilize a tool for compliance monitoring.

6. REFERENCES

Curiae, A., & Buan, N. E. (2016, September 01). National Privacy Commission promulgates IRR of Data Privacy Act of 2012. Retrieved from http://www.bworldonline.com/content.php?section=Opinion&title=national-privacy-commission-promulgates-irr-of-data-privacy-act-of-2012&id=132723

El Kharbili, M., Stein, S., Markovic, I., & Pulvermüller, E. (2008). Towards a framework for semantic business process compliance management. Proceedings of GRCIS, 2008.

Eramba, (n.d.). Eramba: Open Source IT GRC. Retrieved from http://www.eramba.org/

Implementing Rules and Regulations of the Data Privacy Act of 2012. (n.d.). Retrieved from https://privacy.gov.ph/implementing-rules-regulations-data-privacy-act-2012/

Lesyuk, A. (2013). Mastering Redmine. Packt Publishing Ltd.

Lindros, K. (2017, July 11). What is GRC and why do you need it? Retrieved from https://www.cio.com/article/3206607/compliance/what-is-grc-and-why-do-you-need-it.html

Mundin, M. (2018, May 15). Implementing Rules and Regulations of the Philippines Data Privacy Act (RA 10173). Retrieved from https://www.cpomagazine.com/2017/06/23/implementing-rules-regulations-philippines-data-privacy-act-ra-10173/

Racz, N., Weippl, E., & Seufert, A. (2010, May). A frame of reference for research of integrated governance, risk and compliance (GRC). In IFIP International Conference on Communications and Multimedia Security (pp. 106-117). Springer, Berlin, Heidelberg.