全球商業經營管理學報
第十期　107.09　page 37-48
ISSN：2076-9474

個人資訊保護的資訊安全風險管理企業架構塑模研究

Study of Enterprise Architecture Modeling for Information Security Risk Management of Personal Information Protections

馬維銘[a]　　謝孟洵[b]

摘要

隱私問題是全球企業風險所面臨的最大挑戰之一。本研究應用以企業架構為中心的卓越方法論透過專案準備、系統盤點、企業塑模、企業模型分析、審核與驗證、分析轉換等步驟，對個人資訊保護資訊安全風險管理進行塑模。本研究達到資訊安全風險管理的目標：合理配置企業資源、實現企業資訊安全高績效及降低企業資訊安全風險。

關鍵字：企業架構、塑模、資訊安全、風險管理

ABSTRACT

The privacy issue is one of the biggest challenges in the global enterprises' risks. We applied the Enterprise Architecture Center of Excellent methodology to model Information Security Risk Management of Personal Information Protection by project preparation, systems inventory, enterprise modeling, enterprise model analysis, review & verification, analysis transition. This research reached the goals of the information security risk management: appropriate allocation of enterprise's resources, high performance of enterprise's information security, and reduce risks of enterprise's information security.

Keywords: Enterprise Architecture, Modeling, Information Security, Risk Management

1. Introduction

In this section the Research Background, Research Goal and Research Method are described.

1.1. Research Background

The global major information technological risks include cyberattacks, data fraud or theft, critical information infrastructure breakdown, e.g., privacy is the key issue that need attention for the development of financial technology. The risk of loss of personal or corporate reputation and property is very high.

Enterprises usually follow a process-oriented BS 10012 personal information management system (PIMS) to solve the problem of personal information protection to reduce the risks. However, a large amount personal information is still diverted without notice, engaged in commercial marketing activities, and have personal information leaked out. The improper use of Facebook user data by Cambridge Analytica lets Russia's meddling in the U.S. 2016 presidential election, that have once again thrown a spotlight on the technology industry's inadequate privacy protections. The privacy issue is one of the biggest challenges in the global enterprises' risks.

Chao (2012) raised the five process-oriented issues: lack of structural support, organizational behavior cannot match its structure, fall into a functional orientation pattern, unable to control multiple enterprises' perspectives, and unable to demonstrate the architectural hierarchy of the enterprise.

1.2. Research Goal

The purpose of this study is to explore and practice of construct an enterprise architecture information security risk management model to solve many difficulties caused by the process-oriented approach in ISO 27001:2013 of information security

[a] 正修科技大學資訊管理系副教授 Email:k3666@gcloud.csu.edu.tw
[b] 正修科技大學資訊管理系研究生 Email:m0511110@gcloud.csu.edu.tw

risk management.

1.3. Research Method

Enterprise architecture is complex that it comprises multiple views such as strategy, version, goal, object, concept, analysis, design, implementation, structure, behavior and input/output data views. The Enterprise Architecture of Center of Excellence (EACOE) is used to compare the process-oriented project risk management and practice of the architecture-oriented model and for improving the speed of modeling.

2. Literature Reviews

The previous studies about Enterprise Architecture, Enterprise Architecture Center of Excellent, and Personal Information Protection Act are briefly described.

2.1. Enterprise Architecture

Lankhorst (2013) defined enterprise architecture as a coherent whole of principles, methods, and models that are used in the design and realization of an enterprise's organizational structure, business processes, information systems, and infrastructure." Enterprise Architecture is a blueprint describing the current and future state of an enterprise, its structure, processes, assets, and infrastructure.

Architectural documents include Enterprise architecture, business architecture, product line architecture, information system architecture. The architecture of a system (enterprise, business, product line, and so on) defines its components, the relationships between them and between the system and its environment, as well as design principles that "inform, guide, and constrain its structure and operation and future development." The enterprise architecture shows how all the components are integrated. The requirement to comply with existing architectures should be documented in the SLRs and any architectural documents that apply must be adhered to by them. Architectural documentation used as input to this meeting includes: Roles and responsibilities, Policies (business, IT, etc.), Designs, and Infrastructure.

The enterprise architecture profession requires business knowledge, technical skills, and the ability to see the big picture with a bird's-eye view. Hence the most suitable people to fill enterprise architecture positions are experienced business analysts, product managers, and product managers who gain these competencies naturally as part of their profession. Thus in small and medium enterprise, project management offices, product management teams, or a team of experienced business analysts should be responsible for evaluating and prioritizing product development/enhancement requests from all business units and ensuring the alignment of business and technical architecture. At the strategic level, successful enterprise and demand management prevent portfolio-level waste by ensuring that enterprise resources are utilized for the right product development projects that support enterprise strategies (Yayici, 2015).

Business architecture provides a blueprint that management can use to plan and execute strategies from both information technology (IT) and non-IT perspectives. Business architecture is used by organizations to guide: strategic planning, business remodeling, organization redesign, performance measurement and other transformation initiatives to improve customer retention, streamlining business operations, cost and risk reduction, the formalization of institutional knowledge, and the creation of a vehicle for businesses to communicate and deploy their business vision (IIBA, 2015).

2.2. Enterprise Architecture Center of Excellent

Enterprise Architecture also determines how the enterprise should position itself to take advantage of future innovations. Some of the more specific questions that Enterprise Architecture answers are:

- What steps should we take to position our company for future growth?
- What products should we develop to stay competitive?
- Which markets should we enter or grow to stay competitive?
- Should multiple organizations be performing the same function or processes?
- How can we quickly adapt to new legal and regulatory requirements?
- Are our business units different enough to justify multiple systems and business processes?

Enterprise Architecture is "the practice of explicitly describing an organization through a set of independent, non-redundant artifacts, defining how these artifacts interrelate with each other, and developing a set of prioritized, aligned initiatives and roadmaps to create an understanding of the organization, communicate it to stakeholders, and move the organization forward to its desired state." (Ahlemann et al., 2012; Bernard, 2012; Holcman,

2013).

The Enterprise Architecture planning project is initiated by an Executive Sponsor and a Project Lead. It is started after the scope is approved and the project is funded. The following illustration shows the major inputs and outputs to each phase of the Enterprise Architecture planning project. and outputs to each phase of the Enterprise Architecture planning project. The diagram is followed by a brief description of each phase of the Six Phases, as shown in Figure 1:

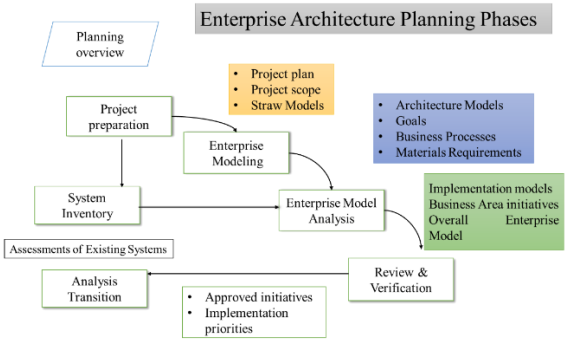


Figure 1 The Six Phases of Enterprise Architecture

Phase 1: Project Preparation includes the formation of the architecture work group, project management activities, and the creation of models and representations of the area of analysis by the Enterprise Architecture team.

Phase 2: Enterprise Modeling is to describe the current understanding of the organization and its future business vision. The enterprise modeling phase begins with the architecture orientation meeting, held to formally introduce the project, set expectations, answer questions, and plan for the enterprise modeling workshops.

Phase 3: Systems Inventory is to develop an understanding of the degree and quality of automation on in the organization as it exists and as it is currently planned. This phase focuses on assessing the systems used to (or being developed or acquired to) run the business.

Phase 4: Enterprise Model Analysis is to identify the set of projects required to transform the organization from its present state to its desired state. At the beginning of this phase, the Planning Team uses the Enterprise Architecture Models and systems inventory to develop Implementation Models.

Phase 5: Review and Verification is to build consensus on the target architecture and the resulting projects identified to move the organization from its present state to its desired state, and review and verification is to evaluate the identified projects in light of available funding, and to fund select priority projects that will have the most significant impact on the organization.

Phase 6: Analysis Transition is to ensure that the approved projects are used to implement the target architecture and result in meeting enterprise business Goals. This phase starts with educating people and communicating to them an overview of the planning process, a synopsis of the target architecture, and information about the resulting funded projects.

Quick Start Enterprise Architecture Plan of the Pinnacle Enterprise Architecture including six main stages are: Project Preparation, Systems Inventory, Enterprise Modeling Tasks, Enterprise Model Analysis Tasks, Review and Verification Tasks, and Analysis Transition Tasks.

Project Preparation includes: Project Initiation Meeting, Arrange Project Logistics, Initial (Straw) Architecture Modeling, and Pre-Technical Review. Systems Inventory include: Assemble Inventory Information, Inventory Orientation, Inventory Systems, and Document Inventory Results. Enterprise Modeling Tasks include: Workshop Orientation Session, Enterprise Model Workshop, Document Workshop Results, Workshop Review Meeting, and Prepare Implementation Models' matrices. Enterprise Model Analysis Tasks include: Develop Implementation Models, Develop Initiative Boundaries, Initial Project Documentation, Conduct Initiative Ranking Review, and Produce Final Documentation. Review and Verification Tasks includes: Introduction, Initiatives Review, Approve Initiative Rankings, and Discuss Next Steps. Analysis Transition Tasks includes: Produce Pre-Scope Documents and Conduct Post-Technical Review.

Ma (2016, 2012) studied architecture-oriented information security risk management model, effectively achieved the company's allocation of resources properly, reduce the complexity of information security risk management, and reduce risk.

2.3. Personal Information Protection Act, PIPA

The Taiwan Legislature (also known as the Legislative Yuan) passed an amendment to the Computer-Processed Personal Data Protection Act ("CPPDPA") on April 27, 2010 entitled the Personal

Data Protection Act. The scope of the Act will be broadened, and the definition of data will no longer be limited to "computer-processed data", as provided under the old CPPDPA. The Act will apply to all individuals, legal entities and enterprises that collect Personal Data, not just government agencies and designated industries under the CPPDPA. Although the Act was promulgated on May 26, 2010, it will become effective only when the Executive Yuan, the central government administrative authority, makes an official order in relation to the effective date of the Act. According to Department of Justice official, under the Executive Yuan, the Act should become effective one or one-and-a-half year from May 26, 2010.

PIPA is enacted to govern the collection, processing and use of personal information so as to prevent harm on personality rights, and to facilitate the proper use of personal information. The act has 56 articles.

Companies control, or process existing personal data should review how such data has been collected and whether a subject's consent has been obtained. If not, companies are advised to consider possible approaches to obtain consent or provide notifications, although details on how consent should be obtained still await further clarifications.

Tzou et al. (2012) investigated the present college PIMS based on "Plan", "Do", "Check", "Act", four phases of "BS 10012：2009 - PIMS, PIMS", and presents recommendations for improvement. They study found that 64.6% of managers working at computer centers, considered college reputation damage the most serious impact in the case of personal information leaking; thus, most of them also considered strengthening internal audit to avoid this from happening. At present, the major developmental progress in college PIMS is at the "Plan" and "Do" phase, and a lack of control for "Check" and "Act".

After third reading of the PIPA passed, if an organization illegally uses personal information, it will face high claims payments, criminal liability and other issues. To reduce the impact from the PIPA, organizations should begin to plan and implement relevant measures for the protection of personal information.

Ma and Lee (2015) pointed out small and medium-sized enterprises and non-profit organizations are concerned about being required to prove that they have no intention or negligence related to personal information leak-out problems than organization goodwill impairment. They assessed an organizational PIMS based on the four phases of BS 10012 such as "Plan", "Do", "Check", and "Act." They emphasized the enterprises need to strengthen PIMS to enable organizations to reduce the impact of the PIPA.

The Article 9 of the PIPA referred to the appropriate security measures, security matters or the proper safety measures refers to public agencies or non-official agencies in order to prevent personal information being stolen, modified, damaged, and lost or leakage, and we should take the necessary measures in technique and organization. Necessary measures, which costs of the expenditure required to meet the appropriate proportion is limited to personal information protection purposes, shall include the following matters:

(1) Risk assessment and managerial mechanism for the personal information.
(2) Defining the scope of personal information.
(3) Information security management and personnel management.
(4) Equipment safety management.
(5) Information security audit mechanism.
(6) Established of management organizations, configuration of considerable resources.
(7) Continuous improvement of the overall security of personal information protection.
(8) Accident prevention, reporting and responsive mechanism.
(9) Cognitive advocacy and educational training.

2.4. Project Risk Management

Project Risk Management includes the processes of conducting risk management planning, risks identification, qualitative risk analysis performing, quantitative risk analysis performing, risk responses planning, risk responses implementation, and monitor risks on a project. The objectives of project risk management are to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risk to optimize the chances of project success (PMI, 2017).

Plan Risk Management process includes Tailored risk management process, Risk thresholds, Process Rules Risk Management Plan. Identify Risks includes Prompt lists, List of risks, Risk owners, Risk register, Risk reports, and Project documents updates. Perform Qualitative Risk Analysis includes Probability, Impact, Root causes, Importance, Prioritized list. Perform Quantitative Risk Analysis includes Numerical models, Combined outcomes, Confidence limit, Sensitivity analysis, and Prioritized list updates. Plan Risk Responses includes Strategies, Actions, Action owners, Time Analysis,

Project plan updated. Implement Risk Responses includes Expert judgment, Project management information system, Change requests, Project documents updates. Monitor Risks includes Status and trends, Reporting, Trends in risk exposure, and Project documents updates. Plan Risk Responses give feedback to Identify Risks, Perform Qualitative Risk Analysis, and Perform Quantitative Risk Analysis. Monitor Risks give feedback to Identify Risks and Plan Risk Responses, as shown in Figure 2:

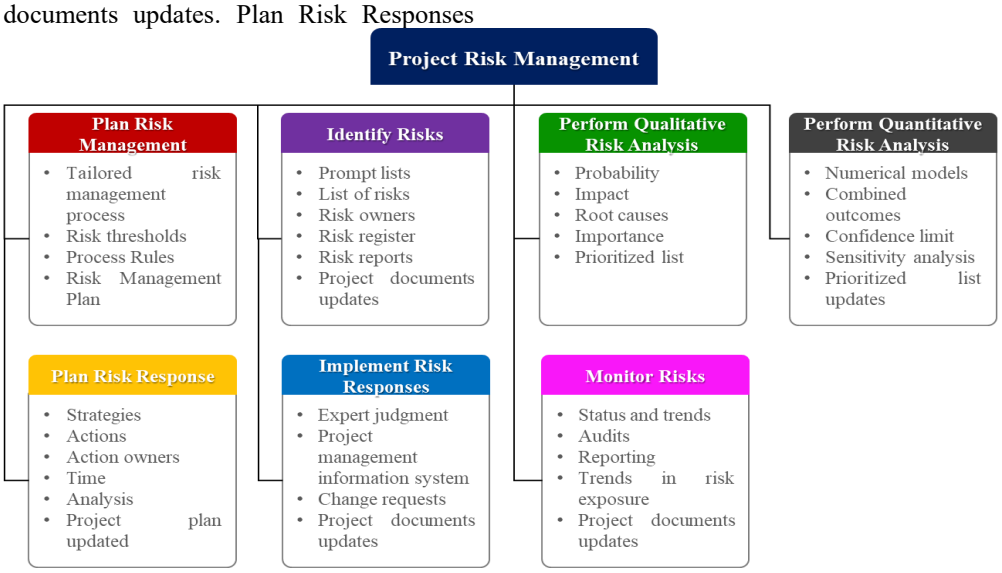


Figure 2 Project Risk Management Process Flow Diagram (PRMPFD) (Redrawn from PMI, 2017)

3. Enterprise Architecture Modeling for Information Security Risk Management of Personal Information Protections

In this section described Goal Model for Protect Personal Information of the Enterprise, Process Model for Information Security Risk Management Architecture, and Materials Model for Information Security Risk Management Architecture.

3.1. Goal Model for Protect Personal Information of the Enterprise

While nearly all enterprises build information systems, the end objective is not just an information system, but a flexible, changeable, and reusable asset that will meet current and future business needs. Few organizations today use model-driven approaches that truly separate Architecture (Engineering) from Implementation (Manufacturing). Throughout recorded history, as complexity increases, separating Architecture from Implementation becomes an imperative. Enterprise Architects will ensure that the enterprise's information technology and business systems are aligned with business goals, are capable of change in continually changing business and technology climates, can reuse enterprise systems assets, and are cost effective. Goals of Protect Personal Information are: Appropriate Allocation of Resources, High Performance of Information Security, and Reduce Risks of Information Security. Goal Model for Protect Personal Information of the Enterprise, as shown in Figure 3:

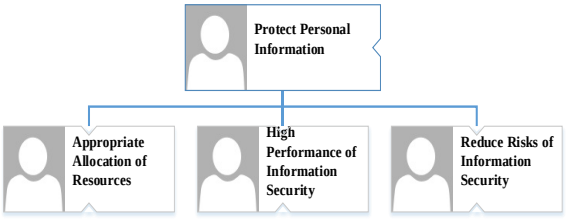


Figure 3 Goal Model for Protect Personal Information of the Enterprise

3.2. Process Model for Information Security Risk Management Architecture

Manage Information Security Risk includes Plan Risk Management, Identify Risk, Prioritize Risk, Analysis Risk, Monitor Risk, Resolve Risk, Control Risk, Assess Risk. Process Model for Information Security Risk Management Architecture, as shown in Figure 4:

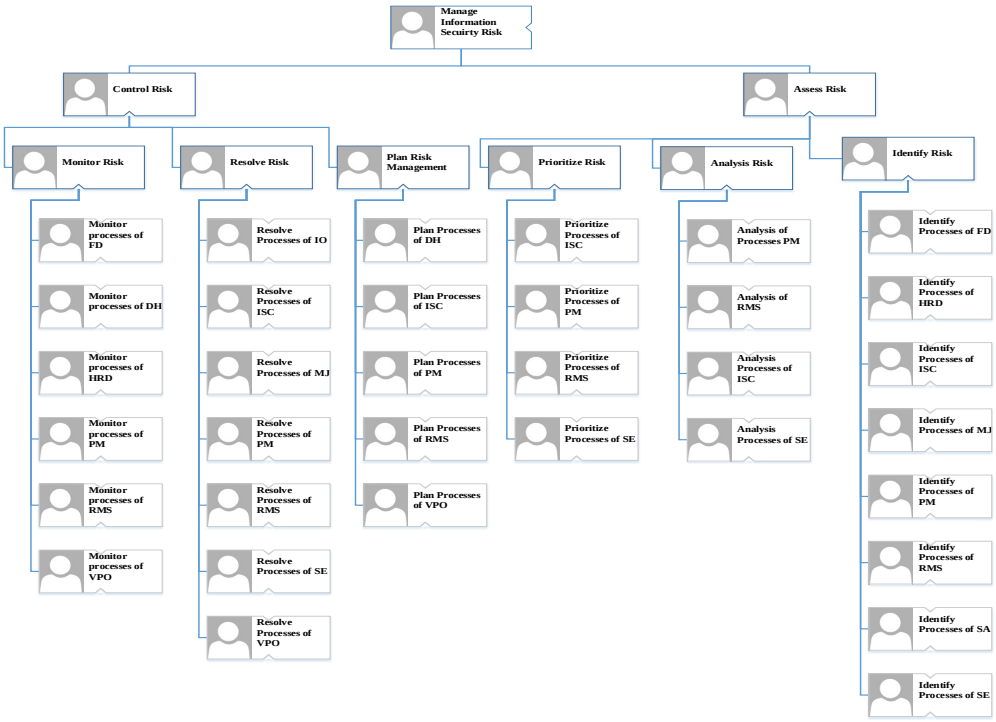


Figure 4 Process Model for Protect Personal Information of the Enterprise

3.3. Materials Model for Information Security Risk Management Architecture

There are four main materials in Protect Personal Information of the Enterprise: Personal information, Internet servers, Physical equipment, Safety equipment. Personal information materials include: Database, Email, audio-visual information, and Safety boxes. Internet servers, Web Servers, DNS, Wireless AP, Routers, and Switches. Physical equipment includes PCs, Mobile HD, Laptops, and RAID Storages. Safety equipment includes Monitoring cameras, RFID lockers, Fire extinguishers, Fire sand cans, CO2 cans, flooding alarms, and UPS Systems, as shown Figure 5:

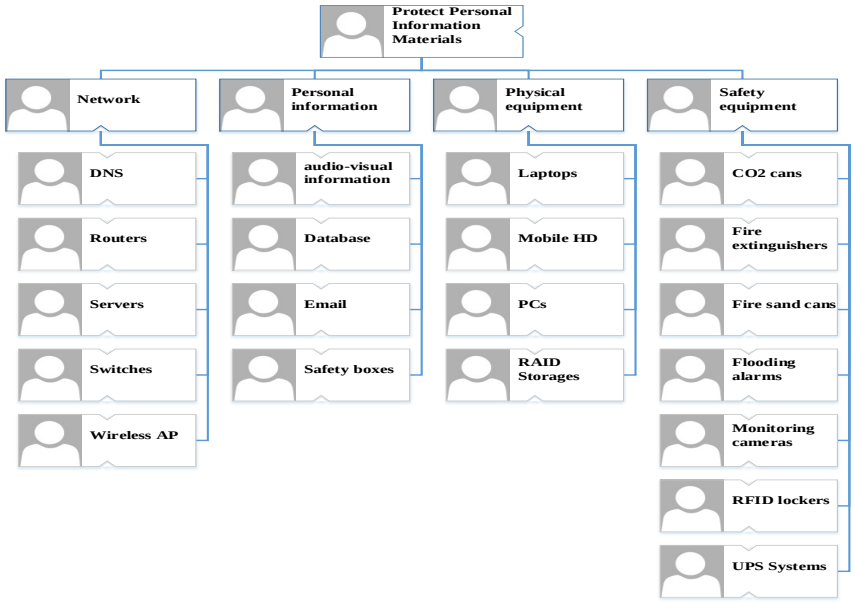


Figure 5 Material Model for Protect Personal Information of the Enterprise

3.4. Roles Model for Information Security Risk Management Architecture

There are four role layers in Protect Personal Information of the Enterprise: Management layer, Executive Layer, Supportive Layer, and Director of Information Department. Director of Information Department is a role of Executive Layer. But it is a very important role in Protect Personal Information of the Enterprise, we increase a new layer specially.

Management Layer role include: Vice-president, Chief Information Security Officer, Secretary. Executive Layer role include: Director of Planning Department, Director of Insurance Department, Director of Human Resource Department, Director of Financial Department, Director of Project Department, Director of Research and Develop Department. Supportive Layer role include: Director of Supervise Committee, Supervise Committee Member. Director of Information Department role include: Software Engineer, Hardware Engineer, Web Engineer, Internet Engineer, Database Engineer, as shown in Figure 6:

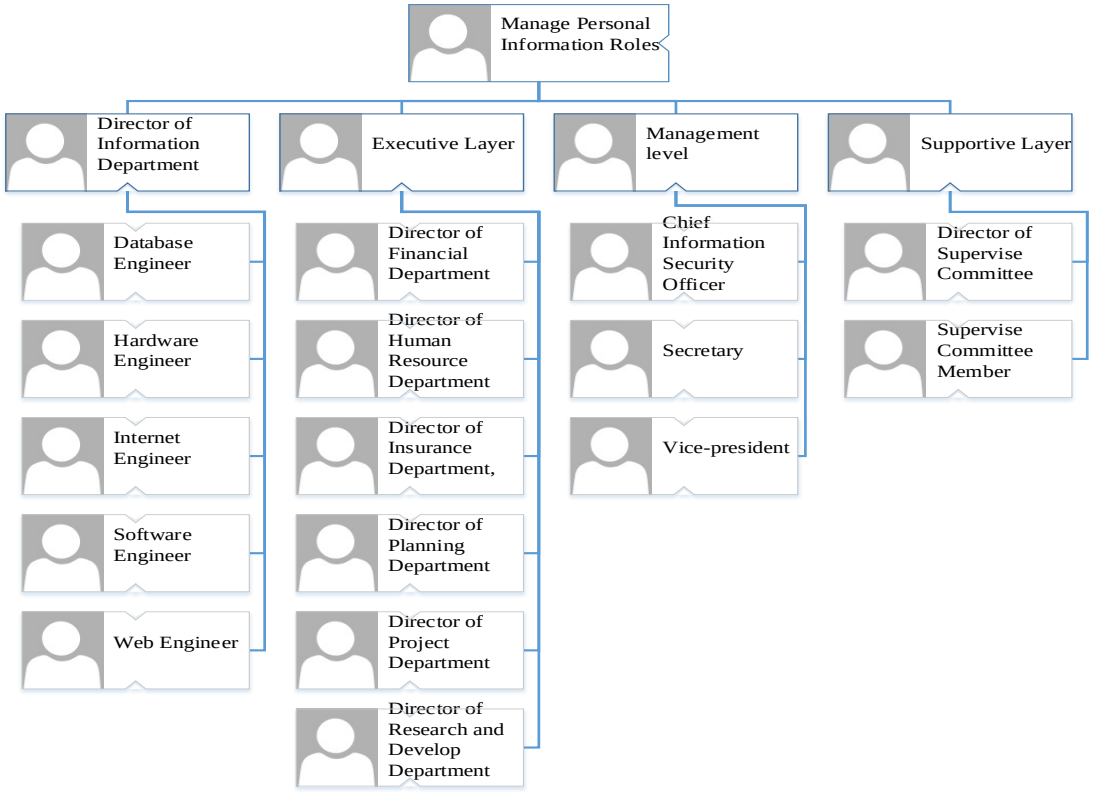


Figure 6 Role Model for Protect Personal Information of the Enterprise

3.5. Locations Model for Information Security Risk Management Architecture

There are four main locations in Protect Personal Information of the Enterprise: Physical Layer locations include: Document Storeroom, Photo-offset Room, Conference Room, Committee Office, Department Office, Security Guard Office. Computer Data locations include: Vice-president Office, Chief Information Security Office, Committee Office, Department Office, General Engineer Office, Security Guard Office, Conference Room, Secretary Office. Clouds locations include: Information Server Room, Chief Information Security Office, General Engineer Office. Conversation layer locations include: Vice-president Office, Committee Office, Conference Room, as shown in Figure 7:

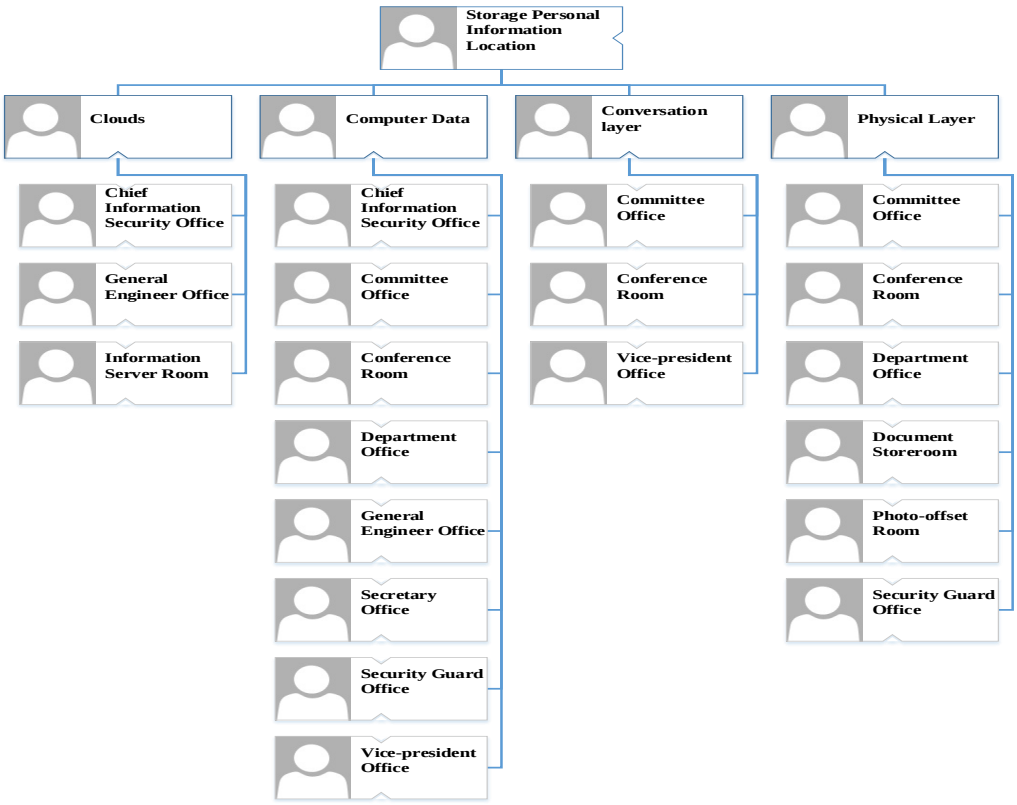


Figure 7 Location Model for Protect Personal Information of the Enterprise

3.6. Events Model for Information Security Risk Management Architecture

There are four main events in Leak Personal Information Events: Collect Layer, Process Layer, Store Layer, and Destroy layer. Input Layer events include: Unauthorized collection. Storage Layer events include: Unauthorized Storage. Use Layer events include: Employee betraying, Unauthorized Storage, Invade, System Attack. Discard layer events include: Equipment Discard and Reuse, canceled authorization, as shown in Figure 8:

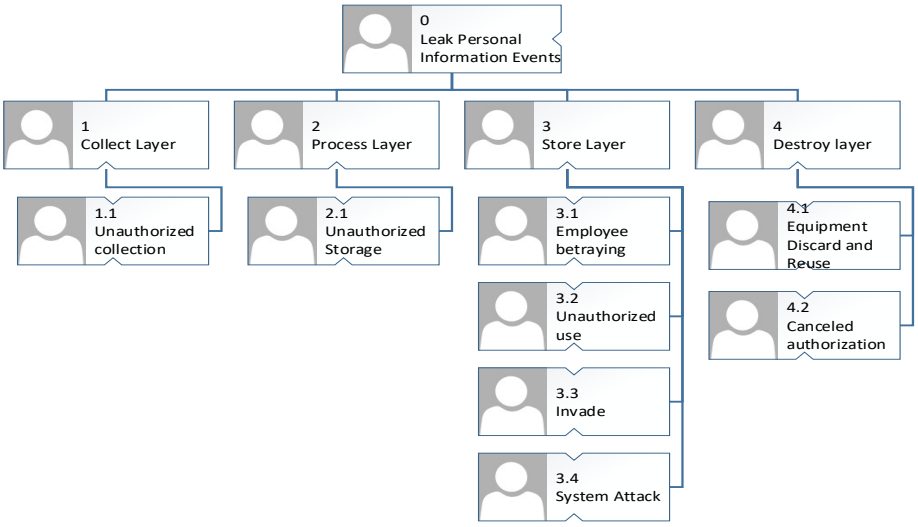


Figure 8 Event Model for Protect Personal Information of the Enterprise

3.7. Build Implementation Models

During this activity, the Planning Team and the Core Business Team create a series of Implementation Models to represent the associations of key enterprise aspects. The initial set of suggested Implementation Models are those used to represent the Processes required to support the Goals of risk management, the Materials required to support the Processes, the systems used to automate the Processes, and the Roles required for each process. Any two architecture artifacts can be related to form new insight into the organization.

The Pinnacle Enterprise Architecture Methodology suggests that Processes be used as the "anchor enterprise artifact, since most business personnel think along Process lines. The Pinnacle Methodology focuses on these fundamental relationships requited to understand the enterprise: (1) Processes support Goals (2) Processes require Materials (3) Processes are performed at Locations (4) Processes Involve Roles (5) Processes are mechanized by systems.

Building the Implementation Models for risk management is not technically difficult, but it is time-consuming and requires analytical skills. The ream will need to create the Implementation Models and assess each relationship between the artifacts. There is no tool that can do the analysis for us; it requires human thinking and recognition, though a tool “can” help you "drive through" the large number of associations and record the results of the teams' analyses. Once these analyses are completed, the essence of the enterprise will be explicitly represented.

3.8. Processes-Support-Goals Implementation Model

The first association to analyze is which Processes are required to achieve Goals. The best way to represent this Implementation Model is to create a matrix that lists the Goals along one axis and the Processes along the other. The Implementation Model Will be developed in the same manner that the Architecture Models were: The Planning Team develops the first model from traceable sources, and the refinements should be created in a working session with representatives from the Planning Team and the Core Business Team. If there are a lot of relationships, the team should form sub-teams and divide the work. The team can use post it, Hip charts, or a spreadsheet in the working session. If team members use flip charts or post it, they should capture the information in a Spreadsheet at the end of this step.

The planning Team should use the Processes from the Enterprise Architecture Models to begin work on Implementation Models. This step will also help identify updates that should be incorporated in the Enterprise Architecture Models. The team should develop both Current As-Is-State and target Desired-State models, because for example: A Process may appear in the current architecture even though the team may have eliminated it when they created the target architecture. Yet, he Implementation Model may show that the Process is still required for other reasons, as shown in Table 1:

3.9. Processes-Involve-Materials Implementation Model

The next association you will analyze determines what Materials are required for a Process to be performed. As with the previous Implementation Model, the best way to proceed is to create a matrix that lists the Processes on the axis and the Materials on the ocher. Develop the Implementation Model in the same manner as you developed the Architecture Models: The Planning Team develops the first model from traceable sources and the refinements should be created in a working session with representatives from the Planning Team and the Core Business Team. If there are a lot of relationships, the team should form sub-teams and divide the work. As with the prior Implementation Model, if the team uses sticky notes or flip charts, he information should be captured in a spreadsheet at the end, because the resulting Implementation Model will be the source for the affinity analysis later in the Methodology.

Table 1 Processes-Support-Goals Implementation Model

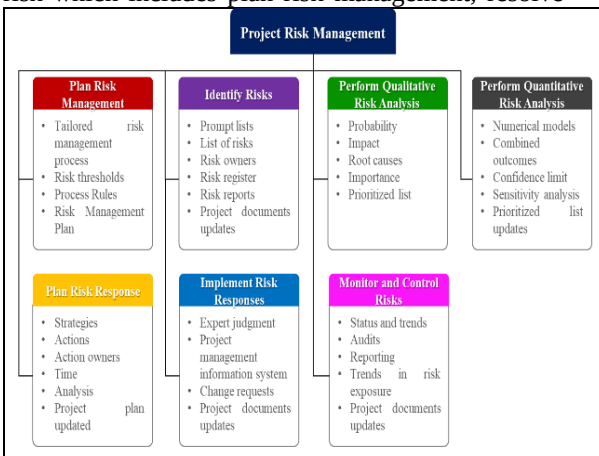
0 Protect personal Information				
	Processes \ Goal	1 Appropriate Allocation of Resources	2 High Performance of Information Security	3 Reduce Risks of Information Security
1	Control Risk			
1.1	Monitor Risk			
1.1.1	Monitor processes of PM	X	X	X
1.1.3	Monitor processes of DH	X	X	X
1.1.4	Monitor processes of FD	X		X
1.1.5	Monitor processes of HRD	X		X
1.1.6	Monitor processes of RMS	X		X
1.2	Resolve Risk			
1.2.1	Resolve Processes of SE		X	X
1.2.2	Resolve Processes of VPO	X	X	X
1.2.3	Resolve Processes of PM	X	X	X
1.2.4	Resolve Processes of MJ			X
1.2.5	Resolve Processes of IO			X
1.2.6	Resolve Processes of ISC			X
1.2.7	Resolve Processes of RMS	X		X
1.3	Plan Risk Management			
1.3.1	Plan Processes of PM	X	X	X
1.3.2	Plan Processes of VPO	X	X	X
1.3.3	Plan Processes of DH		X	X
1.3.4	Plan Processes of ISC			X
1.3.5	Plan Processes of RMS	X		X
2	Assess Risk			
2.1	Prioritize Risk			
2.1.1	Prioritize Processes of SE		X	X
2.1.2	Prioritize Processes of PM		X	X
2.1.3	Prioritize Processes of ISC			X
2.1.4	Prioritize Processes of RMS	X		X
2.2	Analysis Risk			
2.2.1	Analysis Processes of SE		X	X
2.2.2	Analysis of Processes PM		X	X
2.2.3	Analysis Processes of ISC			X
2.2.4	Analysis of RMS	X		X
2.3	Identify Risk			
2.3.1	Identify Processes of SA		X	X
2.3.2	Identify Processes of SE		X	X
2.3.3	Identify Processes of PM		X	X
2.3.4	Identify Processes of FD			X
2.3.5	Identify Processes of HRD	X		X
2.3.6	Identify Processes of MJ			X
2.3.7	Identify Processes of ISC			X
2.3.8	Identify Processes of RMS	X		X

4. Comparison Between Project Risk Management Process and the EA Risk Model

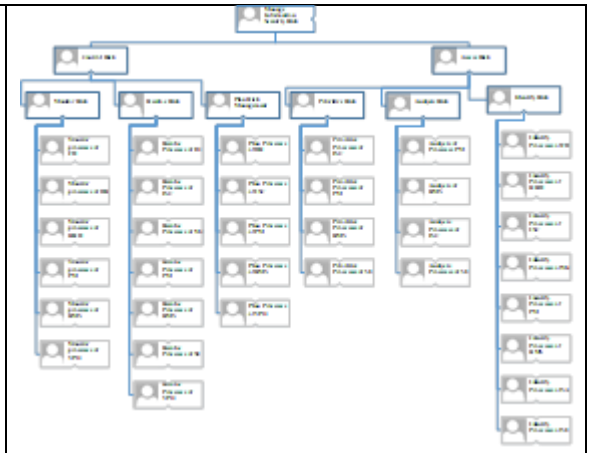
EACOE Process Model for Protect Personal Information of the Enterprise Architecture is compared with Project Risk Management Process model.

Project Risk Management Process includes the processes of conducting risk management planning, identification, analysis, response planning, response implementation, and monitoring risk on a project. The objectives of project risk are to increase the probability and/or impact of positive risks and to decrease the probability and/or impact of negative risks, to optimize the chances of project success. EACOE Process Model for Protect Personal Information of the Enterprise includes controlling risk which includes plan risk management, resolve risk, and monitoring risk; assessment risk which includes identification risk, analysis risk, and prioritize risk. We can see the units in the organizations for responsible processes.

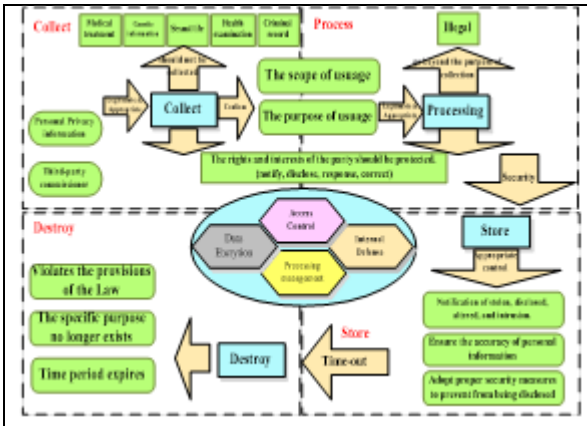
The Personal Information Protection Technical procedures (PIPTP) announced by Research, Development and Evaluation Commission, Executive Yuan, Republic of China in 2012, as shown in Figure.



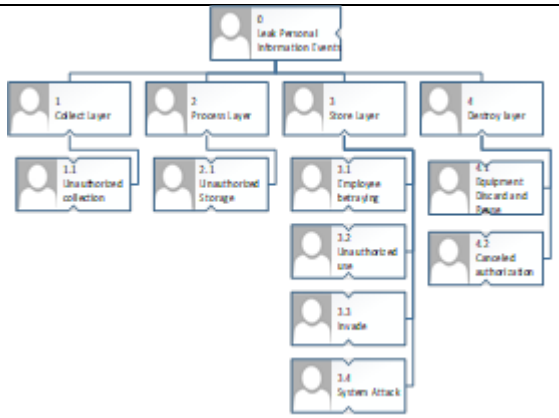
Project Risk Management Process Model (PMI, 2017)



EACOE Process Model for Protect Personal Information of the Enterprise



PIPTP Redraw from Research, Development and Evaluation Commission, Executive Yuan, ROC.



EACOE Event Model for Protect Personal Information of the Enterprise

PIPTP only provides the processes for collection, processing, store, and destroy personal information, however, no any information provided to units in the organization to execute the processes and responsible to the events. But the EACOE Event Model for Protect Personal Information of the Enterprise provides the personal information leakage due to improper processes the personal information.

5. Conclusions and Recommendations

EACOE model refers to a visual representation of information, both structures and behaviors of the enterprise architecture that operates under a set of guidelines in order to efficiently arrange and convey a lot of information in a concise manner. Enterprise architecture models are helpful to find gaps in structures and behaviors and to identify extraneous information. Enterprise architecture models provide

context to better understand and more clearly convey information about the enterprise. When an appropriate enterprise architecture model is applied, analysis becomes simple relative to analyzing the information in pure text form, because the models help visualize and summarize complex information of enterprise architecture.

References

1. Ahlemann, Frederik, Eric Stettiner, Marcus Messerschmidt & Christine Legner, (2012), Strategic Enterprise Architecture Management: Challenges, Best Practices, and Future Developments, *New York,* Springer*,* 314.
2. Bernard, Scott A., (2012), An Introduction to Enterprise Architecture, 3rd Ed., Bloomington, IN, Author House.
3. Chao, William S., (2012), Systems Architecture: SBC Architecture at Work, Taipei, LAP LAMBERT Academic Publishing, 344.
4. Chao, William S., (2016), Systems Architecture of Smart Healthcare Cloud Applications and Services IoT System: General Architectural Theory at Work, Amazon Digital Services LLC, 116.
5. Chao, William S., (2014), SBC View Model, Available at: https://sites.google.com/site /sbcar itecture/home/sbc-view-model. Accessed March 30, 2018.
6. Chao, William S. (2016), Systems Architecture of Smart Home Security Cloud Applications and Services IoT System: General Architectural Theory at Work, Amazon Digital Services LLC, 120.
7. Holcman, Samuel B., (2013), Reaching the Pinnacle, Pinnacle Business Group.
8. IIBA, (2015), A Guide to the Business Analysis Body of Knowledge, BABOK Guide, International Institute of Business Analysis.
9. ISO 27001: (2013), Information Technology-Security Techniques-Information Security Management System, Available at: http://www.iso.org/, Accessed March 30, 2018.
10. ISO 27000: (2014), Information Technology-Security Techniques-Information Security Management System, Available at: http://www.iso.org/, Accessed March 30, 2018.
11. Lankhorst, Marc, (2013), Enterprise Architecture at Work: Modeling, Communication and Analysis, 3rd ed., New York, Springer,364.
12. Li, Fu-Shiau, Wei-Ming Ma, & Architect Chao, (2008), Architecture Centric Approach to Enhance Software Testing Management, Eighth International Conference on Intelligent Systems Design and Applications, 654-659.
13. Ma, Wei-Ming, (2010), Study on Architecture-Oriented Information Security Risk Assessment Model, Proceedings, Springer-Verlag Berlin Heidelberg, Second International Conference on Computational Collective Intelligence Techno-logies and Applications,Vol.6423 /2010, 218-226.
14. Ma, Wei-Ming & Cheng-Fu Tsai, (2012), Study of Implementation of the Personal Information Protection Act Architecture on CSU Campus, 2012 Symposium on Global Business Operation and Management, Kaohsiung, Taiwan (ISBN 978-986-7339-71-3).
15. Ma, Wei-Ming,(2013), Study on Enterprise Architecture Development, Journal of Global Business Operation and Management (ISSN: 076 -9474).
16. Ma, Wei-Ming & James Lee, (2015), Study of Implementation of Enterprise Database Activity Monitoring Agile Projects, *Journal of Global Business Operation and Management*,7,95-108.
17. Ma, Wei-ming, (2016), A comparative study of information security risk management Enterprise architecture and architecture-oriented model, 2016 International Conference on Business and Information, Osaka, Japan.
18. Ma, Wei-ming,(2017), Systems Architecture of Information Security Applications and Services IoT System General Architectural Theory at Work, BAI Winter 2017, Bangkok, Thailand 105-133.
19. PMI, (2017) A Guide to the Project Management Body of Knowledge PMBOK Guide,6th Ed., 396.
20. Research, Development & Evaluation Commission, Executive Yuan, ROC, (2012), The Personal Information Protection Technical procedures.
21. Tzou, Wan-Lian, ming-da Hwang, (2012), A study of introducing college personal information management system based on BS 10012, Computer Audit, 25, 72-88.
22. Yayici, Emrah, (2015), Business analysis methodology book, *Emrah* Yayici.