第七期 104.09 Page 95-108
ISSN：2076-9474

Study of Implementation of Enterprise Database Activity Monitoring Based on Agile Project Management
運用敏捷專案管理導入企業資料庫活動監控研究

Wei-Ming Ma[1] James Lee[2]

ABSTRACT

In recent years, more and more personal information to be used as a fraud syndicate tools. In order to ensure that personal information will not be leaked by enterprises, "Personal Data Protection Act" was promulgated and implemented by Taiwan, ROC, and its purpose is to allow companies to fulfill the obligation to protect customer data, and then achieve the goal "of compliance exemption". This study is response to data audit mechanism, and combined with existing enterprise management mechanisms, personal risk assessment and implement a data-owned law advocacy and information security education and training, making the business in line with the law and regulations.

Database Activity Monitoring (DAM) tools have been implemented to capture the records from user and server connections of Application server and then compared that to user and the server side database SQL execution record. From the records, the company can determine which violates the information security policy to executive warning or blocking invasions and track events. It can be instantly and continuously monitor and analyze database activity, for violating the policy database activity can send alerts immediately. All the tracks can be recorded for later analysis, identification of end-users and accountability, and can solve enterprise database security audit and other issues. This study also confirms DAM can be reached the goal all the time to protect enterprise's data forming a layer of safety nets to protect critical assets owned by the company.

Keywords: Personal Data Protection Act, Database Activity Monitoring, Information Security Policies, Regulatory compliance

摘要

近年來越來越多的個人資訊被犯罪集團用來當成詐騙的工具。為了確保個人資料不被企業外洩，我國頒布實施「個人資料保護法」，目的在於讓企業必須善盡保護客戶資料的義務，達到『合規免責』的目標。本研究因應個人資料保護法，導入資料庫安全稽核機制，結合企業原有的管理機制、個人資料風險評估及落實個資法宣導與資安教育訓練，使得企業更加符合法規。

本研究運用敏捷專案管理導入資料庫活動監控產品工具，在不需要額外修改程式碼，也不需要改變網路架構下，擷取使用者與伺服器的連線紀錄，進而比對後端資料庫使用者與伺服器的查詢語言執行紀錄，決定哪些違反公司資訊安全政策，執行警示或阻擋的功效，以達到追蹤事件是何人所為。可即時並持續監控分析資料庫活動，針對違反資訊安全政策的資料庫活動可進行即時警示，可記錄所有軌跡供事後分析，辨識終端使用者與責任追究，並且可以解決企業資料庫安全稽核等問題。本研究證實資料庫活動監控，可達成資料庫存取之事前、事中、事後之全面保全，為企業之資料存取加上一層安全的防護網，保護公司所擁有的重要資產。

關鍵字：個人資料保護法、資料庫活動監控、資訊安全政策、符合法規

[1]作者為正修科技大學資訊管理系助理教授，Email: k3666@gcloud.csu.edu.tw
[2]作者為正修科技大學資訊管理所碩士，Email: james5592@gmail.com

1.Introduction

In this chapter the Research Background, ResearchGoal and ResearchMethod are described.

1.1 Research Background

The Taiwan Legislature passed an amendment to the Computer-Processed Personal Data Protection Act ("CPPDPA") on April 27, 2010 entitled the Personal Information Protection Act (PIPA)and itwas promulgated and implemented on October 1, 2012. PIPA applies to all public agencies, businesses, organizations, large groups and individuals, and the impact of the total coverage in Taiwanese enterprises. In response to PIPA on the way, businesses and organizations start to focus on personal data protection and information security-related issues, re-examine the assessment of the collection, utilization, marketing, processing of personal data and practices.We must meet the PIPA requirements, and then make improvements for the existing management mechanism in our enterprises. In addition, the PIPA specifically regulating personal information, when an enterprise leakage of personal data, the companies must bear the burden of proof, which is the description of the internal data protection management without negligence, in order to compensate for the losses to a minimum.

However, how can we do to give evidence did not violate PIPA, become the company's current most distressing thing. Enterprises should start to establish a correct attitude towards staff processing personal data for customer and themselves, so that each member in the enterprises can understand who is given the responsibility of safekeeping the importance of personal data, and the next is the improvement of existing data management mechanisms. The enterprise can carry out personal data inventory, develop personal data accessing policies and implement education and training, to strengthen the monitoring and management and regular auditing task. Through all procedure mentioned, it allows companies to re-examine the data protection processes, be aware of existing information security weaknesses, find a source of threat data protection, to be able to choose the right tools needed to store the track record, as well as establish the ability of enterprises' own proofs.

Mega Bank planned to destroy old computers by outsourcing in 2011, but Mega Bank's staff did not monitor the entire destruction process, resulting in some computer hard disk data outflow to the secondary market, the FSC penalty Mega Bank fined NT$ 2 million dollars, the United Daily News in Taiwan reported on June 1, 2012. Leading mobile phone industry Nokia happened a major information security incidents. Taiwanese Nokia issued statement: five Taiwanese marketing campaign website was hacker by intrusion, and estimating 1.5 million customer's data leakage, including nearly 7,000 records may contain passwords, but Nokia did not explain whether the compensation. Ministry of Justice of Taiwan referred to damage to the interests of citizen, the maximum amount of fine is up to NT$ 200 million dollars, Apple Daily reported on February 23, 2013.

Verizon data breach investigations report has pointed out that 48% of the data stolen from internal staff in 2010, such a situation would pay more attention by enterprise with the use of digital data. IDC's analysis pointed out that the number of digital data increased at twice the rate every year. The growth of sensitive information is also naturally increases with the growth of the data. IDC also found that large companies have tended to focus part by information leaked internal confrontation instead on the threat of external data leakage, while small enterprises are still the focus on the fight against external threats. Various studies report against leaking sensitive information, not only just against external hacker threats, but also pay attention to the threat of internal control and management negligence, but also underscores the importance of database security and auditing. The existing four categories of information security products are content security category, threat management category, identification and identity access management category, vulnerability assessment and Event Management category, as shown in Figure 1:

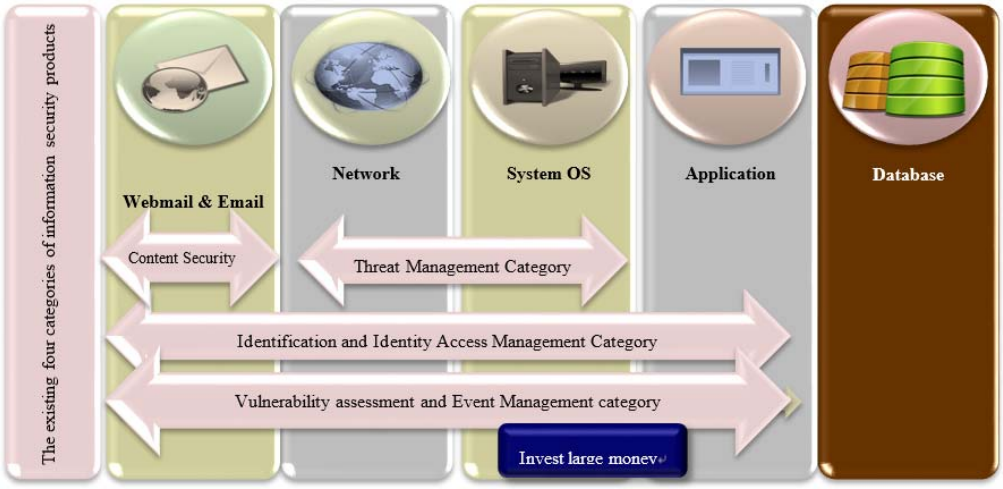

Figure1：The importance of database security

1.2 Research Goal

To fulfill PDPA regulatory requirements, how companies should reach the objectives due to compliance exemption? In this study, the agile project of database activity monitoring will be implement to verify that can meet with PIPA, in order to achieve compliance exemption for specific objectives.

On the other hand, the soft goal is to solve enterprise database security and auditing internal negligence and other issues, monitor database activity in real-time, record related tracking information, to identify the real users and the events of the time, produce audited related reports compliance with PIPA of Security Management System (ISMS) standard. When the company's information security policy violation occurred, it can immediately and automatically send an alert message to reduce the risk of information security events generated by the ability of enterprises to establish their own proof, protection and management of enterprise database without negligence in order to compensate for the losses to a minimum, audit and managers, separate responsibilities to prevent legitimate users of wanton destruction, modification, internal security alert data, inventory data taken from reached beforehand, during, after the comprehensive preservation, for the enterprise The data access with a layer of protective safety nets to protect critical assets owned by the company..

1.3 Research Method

We use empirical research method to apply ten project management knowledge and the five processes for achieving the goal of database system auditing project by following the project objectives, schedule and gradually improved to the project objectives in this study. Gartner Group surveys of the global IT project failure rate about 80%, even closed projects were over 50% with overruns or delays closed. The main reason for the project failure is lack of exploration of leadership and management capabilities of the project manager. Following the American Project Management Institute to develop agile project management methodology, in line with the five and ten knowledge areas of project processes to execute this study, in order to achieve the plan, "on scheduled", "best quality," "on the budget" purposes.

2.Literature Review

The previous studies about Personal Information Protection Act, Database Security, Database Activity Monitoring, and AgileProject Management are described and summarized briefly.

2.1 Personal Information Protection Act

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 Information Protection Act (PIPA). 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 information, 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.

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 personal information management system based on "Plan", "Do", "Check", "Act",four phases of "BS 10012 ： 2009 — personal information management system, PIMS", and presents recommendations for improvement. They study found that 64.6% of managers working at computer centers, considered organization's 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 enterprise personal information management system is at the "Plan" and "Do" phase, and a lack of control for "Check" and "Act".The Personal Information Protection Technical procedures (PIPTP) announced by Research, Development and Evaluation Commission, Executive Yuan, Republic of China, as shown in Figure 2.

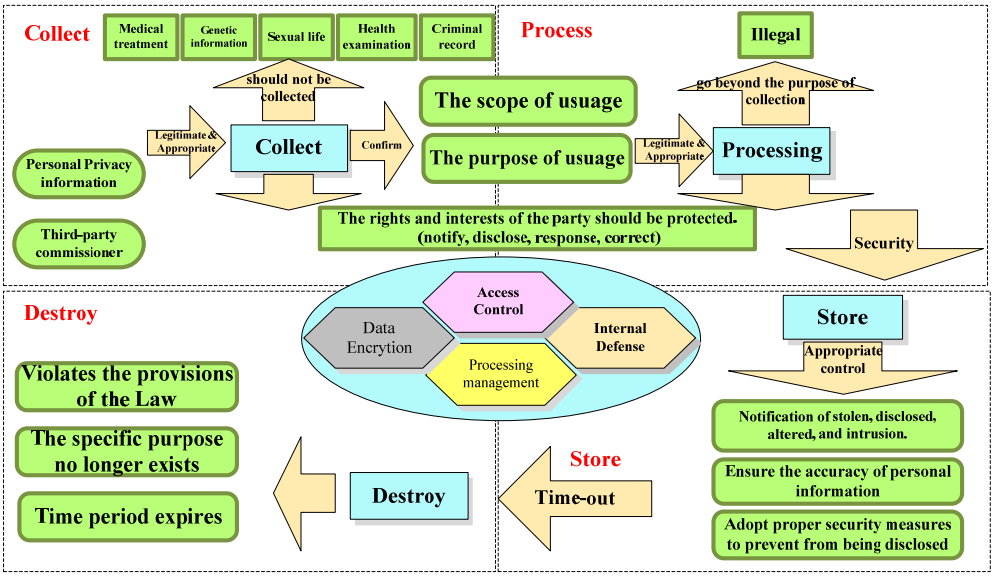

Figure2：Redraw from Research, Development and Evaluation Commission, Executive Yuan, ROC.

After carefully reading of the PIPAarticles, 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.

Chang and Hwang (2011) 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 personal information management system based on the four phases of BS 10012 such as "Plan", "Do", "Check", and "Act." They emphasized the enterprises need to strengthen personal information management system 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.

2.2 Database Security

Mogull (2012) proposed database (DB) is the most sensitive information central storage in the company, which contains a large number of customer information, financial and accounting information. For application and database administrators and other repositories for all Structured Query Language (SQL), such as accessing, modifying and deleting other activities to monitor, warning as well as blocking.

Garter (2011) proposed database security model, database security governed strategy including management, prevention and detection, etc. We will focus on the database activities detections includingdatabase activity monitoring, security information and event management,and data leakage protection, as shown in Figure 3:

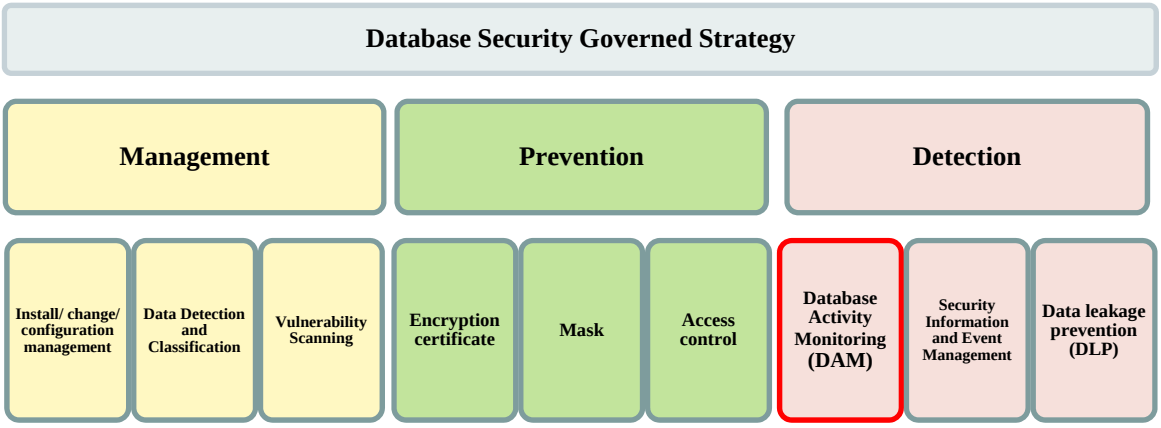

Figure3：Garter (2011) proposed Database Security Model.

2.3 Database Activity Monitoring

Database Activity Monitoring (DAM) is monitoring and analysis techniques for database, which is the source of the data to be monitored on usage of information and data leakage prevention (DLP). DAM is different from DLP, which defenses in the most peripheral businesses to avoid leakage of information. Apparently, monitoring data flow at source of the enterprise computer system is better than that information leakage is intercepted at terminal or peripherals. DAM monitors all records from the Internet and execute SQL server to decide which violates its information security policy, and thus achieve the effect of a warning or blocking SQL execution. Basic DAM tool should contain the following major functions (Cooper, 2015):

✓ Real-time monitoring SQL commands execution records between DB client-side and DB server-side.

✓ Real-time monitoring the SQL activities of DB local-side, monitoring whether the power user has abuse status.

✓ Not only track SQL executed by a DB user records, but also which is being performed by an application (AP) and AP User execution.

✓ Monitoring heterogeneous databases activities, such as Oracle, MS SQL and DB2, etc.

✓ Real-time monitoring of SQL execution records and other DML, DDL and DCL activities.

✓ SQL execution history records can be stored in a separate secure servers, managed by different departments, managers have the opportunity to avoid the DB delete, or modify audit records to cover up crimes.

Wu (2013) and Lin (2010), explored the growing importance of database system facing the high threat of information leakage, respectively.

They recommends that companies should use DAM technology "in advance", "doing" and "post" the audit objectives, acts of intimidation unauthorized access database of abused inside the enterprise to reach a "continuous", "instant" and "independence" of the database security auditing operations. Lin (2010) studied DAM related literatures and analyzed the results of case studies and industry features, providing a wider range of enterprise business applications, and allow a better understanding of the academic DAM which can be applied in the field. He made five important information must be fully recorded in the log DAM, including: Who? Which? When? Where? Why? It can help companies' accomplish internal audit and control.

Tsian (2012) proposed for the full depth of the financial industry planning a management and monitoring mechanisms for the protection of the information, in the face of technological trajectories retained audit planning mechanisms, such as: DLP, encryption, DAM, simplify archive so as to identification storage or handle large amounts of personal information systems, the design of the corresponding information security control measures, and comprehensive consideration of costs and benefits, planning the audit system tracks the retention of important information and protection mechanisms.

Lin (2010) pointed out that database as defined by PIPA is to collect, process and utilize phases at the core position, so the database security and auditing mechanism covering these three processes. If one's personal information is funded or collected through the Internet or the website by web firewall or original code detection program, and database security audit phase link. Thus, after personal information is removed from the database, and it can be combined with data encrypted and e-mail security protection program to ensure a flow of personal information in the whole process has been complete and thoroughly protected.

2.4 Agile Project Management

Project Management Body of Knowledge (PMBOK, 2013) enacted by the American Project Management Institute (PMI), project is defined a temporary effort to create a unique product, service or result. The project is divided into ten areas of knowledge management for how to define the field of knowledge, the development of relevant documents and implementation, monitoring, and explains the close relationship between themselves implicated. The ten knowledge areas are: Project Integration Management, Project Scope Management, Project Time Management, Project Cost Management, Project Quality Management, Project Human Resource Management, Project Communications Management, Project Risk Management, Project Procurement Management, and Project Stakeholders Management.

There are so-called ad hoc project life cycle, the purpose is to divide the project into five distinct phases. After the end of a phase, the next phase can be entered until the end of the project. All project will go through five phases or processes from start to finish. In addition to the five processes can enhance the project's performing smoothly, but also give the project managers know what are going to do in the process to promote the improvement of the project. And the five process phases, like a chain in their process, but also all the ten knowledge will be used in the field of knowledge. Five process phases of the project management process is to understand the project content, including: What are you doing? Who is responsible for doing? Why must we to do it? And after the time, cost and manpower to plan execution, while project teams are continuing to review and make changes over and over again in various processes to control effectively, and then reach the project's goals. The five process phases for project management as shown in Table 1:

Table1：The Five Process Phases of Project Management

Process Phase	Description
Initiating Phase	Those processes performed to define a new project or a new phase of an existing project by obtaining authorization to start the project or phase. Since the problem of the definition of the project will be encountered when the project began, and for the issue to formulate solutions and regulations, the project manager must be coordinated in order from an early consensus on the project.
Planning Phase	Those processes required to establish the scope of the project, refine the objectives, and define the course of action required to attain the objectives that the project was undertaken to achieve such as project resources, project schedule and risk control & management etc.

Executing Phase	Those processes performed to complete the work defined in the project management plan to satisfy the project specifications. Staff and resources must be coordinated in accordance with the integration of project management plan and execute actions.
Monitoring and Controlling Phase	Those processes required to track, review, and regulate the progress and performance of the project; identify any areas in which changes to the plan are required; and initiate the corresponding changes. If the deviation should be corrected, if it cannot make up for the reduction should also be made
Closing Phase	Those processes performed to finalize all activities across all Process Groups to formally close the project or phase.

Agile project management applied to the change of environment, needs or uncertain stakeholders. From the 1990s, agile project management is designed for software development project management practices. Agile project management is a value-oriented to create value for customers such as increased interest income, low cost, low risk, and therefore can promote the success of the project, the maximum value of output in the shortest time. Manifesto for Agile are: Individuals and interactions over processes and tools, Working software over comprehensive documentation, Customer collaboration over contract negotiation, and responding to change over following a plan (Cohn, 2005; Cockburn, 2006; Highsmith, 2009; Lyssa, 2010).

Scrum is group means football, when unilateral violation that the two sides tied for the team scrimmage. Scrum is initiated by Schwaber (2004), people-oriented methodology, which emphasizes on team role and self-organization, commonly used in software development. It is a very common agile practices, featuring lightweight and easy to understand, but difficult to digest. It is also a high frequency of iterations methodology, means activities within a short period is complete, but the content is not the same in weekly period (Shalloway et al., 2009).

Scrum framework is a guidance for project team, the content includes: Scrum practices, roles, events, artifacts and rules. Three pillars of Scrum as follows: (1) Transparency giving transparent monitoring output, so that stakeholders at a glance, get together recognized. (2) Inspection from time to time to check the progress of the project, identify the difference analysis, output continued to show to the customer for confirmation. (3) Adaptation is to adjust processes to reduce the problem, before the end of Iteration convene Retrospective meeting to adjust process work practices or amend the working agreement (Shore et al, 2007;. Cohn, 2004; Smith, 2009).

Common agile system are: Scrum is a common agile practices accounted for more than half of the users, Extreme Programming (XP), Lean Software Development (LSD), Crystal Family, Dynamic Systems Development Method (DSDM), Feature-Driven Development (FDD) six systems. Although the six systems of common Agile methodology, but the practice is often short and finally the integration of these methods, rather than adopt a purely single method. Agility is not only used to develop the software, all rapidly changing environment, customers or demand are applicable, in particular people-oriented or activity-oriented industries, such as: services and SMEs which are described in Table 2:

Table2：Comparison of Six systems of the Common Agile Methodology

System	XP	Scrum	DSDM	FDD	Crystal	Lean
Author	Beck, 1996	Sutherland, 1995	Hingsmith, 2002	Coad, 1999	Cockburn, 2007	Poppendieck, 2003
Developing	Repeatedly incremental delivery	Repeatedly incremental delivery	Repeated	Repeated	incremental delivery	Repeated
Project size	small	Any kinds	Any kinds	Complex	Any kinds; family	Any kinds

Iteration	1-3 weeks	2-4 weeks	Spent 20% of total time to solve the 80% of problems	2 days-2 weeks	Family style	2 weeks
members	1<20 people; small team	Any size (Scrum of Scrums concept)	Any size; independence	Members; >1 team	Any size; family	Members; >1 team
Communication methods	Informal; daily standup	Informal; daily standup	Documentation	Documentation	Informal; face to face	Frequently communicate, Non document
Customer participation	Customer fully participation	Through P.O.	Through frequent release	Through reports	Through incremental release	Frequent communication
Documentation	Only the basic document	Only the basic document	Documentation is necessary	Documentation is necessary	Only the basic document	Only the basic document
Specific methods	TDD, user story, reconfigure	Sprint product and Sprint backlog, planning poker, Scrum Master	Prototyping	UML diagrams	Adaptive methods; depending on the number of ad hoc and scheduled	Extending from manufacturing Lean Production method
Advantage	Open working space, customers as a team member, the best example well-defined, feedback	high level of communication and cooperation	Require prioritization and effective project management	Reports and documents to enable multi-tasking	adjusted method according to the project type and size	Eliminate waste, enhance learning, defer decisions, fast delivery, team empowerment, build a complete and holistic view
disadvantage	Less emphasis on document, lack of regulation, existence of customer mandatory	Less emphasis on the documentation, poor control of the project	Complex documents	Individual code ownership, NA Small Project	Larger teams are required to play an effective collaboration	Not belong to a agile method

3.Planning and Execution Database Activity Monitoring Project

his chapter illustrates the Project Goals, Project Scope Statements, the Project Requirement Analysis, Database Activity Monitoring Architecture, and Database Activity Monitoring Deployment.

3.1 Project Goals

Traditional database auditing uses the built-in database auditing function, and this approach can meet the basic database auditing operations. The most situation consumes 20% to 40% of system resources, making the system administrator must trade-offs the facing difficulties, and difficulty of the implementation of the enterprise database auditing.

The main objective of this agile project is to build a database activity monitoring system, which network architecture is suitable for multi-level architecture, master-slave architecture, centralized system architecture framework and other applications without changing existing enterprise network infrastructure.There is no need to modify any application code andit can change in response to enterprise network environment architecturewith elastic expansion of capacityfor the future applications. If the large number of company'sDB server included in the scope of monitoring, database auditing system can employ hierarchical architecture to centrally management in which all administrations will be handled by a host system to improve overall system performance and data processing capabilities.

Database activity monitoring system to operate independently outside the database management system (DBMS) without relying on the built-in database audit mechanismfor monitor database activity tracking purposes.The system has clearly defined roles and different authorities in accordance with company policy mandate operations and

achieving independent audit of non-repudiation.

In addition to the standard operating procedures database auditing, will present the company's information security policies, such as: sensitive information accessing protection, off-peak hourssuspicious accessing continuously and real-time DAM in accordance with policies and PIPA regulations providing auditing reports. Establishing a fully automatic mechanism improve information security monitoring, auditing and protection.

3.2 Project Scope Statements

The agile project will implement continuous and real-time DAM in response to PIPA regulations to provide database servers and application server data access behavior ensuring that all data access tracks, which are included in the scope of information security audit tracking, project scope statement. The project scope are establishing management organization and allocating enough resources, defining the scope of personal information, Prevention of security accidents, Notification and response mechanism, Device Security Management, Information security audit mechanism, and Retain evidence necessary for using records and trackinginformation.

3.3 Project Requirement Analysis

DAM agile project is a set of IT security solutions, which is integratedsoftware and hardware for information security by tracking and monitoringfive dimensions: who, which, when, where, whatdatabase activities with a closed system in line with the principle of an independent auditing.In addition to all audit records have been key encrypted, we cannot directly access the data to be modified, which effective prevents information from stolen and modification.

DAM agileproject offers three modules, namely user login application servers access behavior, data processing and audit monitoring and management center, collecting local database activity, and selected the desired elasticity module according to security needs.

Using sniffing to collect the contents of the packet fromnetwork layer transmitted to analyze packet, and then through innovative packet matching techniques to identify the real user through the application access database behavior, which is full automatic monitoring and analysis of database activities.

When the system implements enterprise information security policies and provide many different types of sample auditing reports, companies can be directly applied to scheduled reports, and it can also be through the built-in wizard to customize reports greatly simplifies the setting burden. In addition, the system has many default security alert conditions, as long as the databasegenerating suspicious behaviors or policy violations. The system will immediately send an alert message to notify the administrator.

If leaking personal information incident occur in the enterprise, it needs to make the relevant supporting evidence to confirm the security management of the enterprise itself is no mistake. The variety of PIPA compliance reports from auditing and monitoring and management information processing center including direct output statements to reduce complicated procedure of proof processes.

3.4 DAM Architecture

DAM architecture includes: user, network switch, web application (AP) servers, DB server, DB Local Agent, auditing storage, auditingAppliance and DAM Server and so on.

Under the unchanged setting of DAM system, which collected information database access activity through an encrypted network, and then the information is transmitted to the centralized information auditing server to control and analysis. All the information are stored in a separate device in order to further independent database auditing operations. The auditors did not require database administrator's permission to conduct sensitive information setting, classification of auditing subject, and auditing policy development.

DAM system is a role-based system to use and take separation of powers and responsibilities of the operation and management strategies. DAM gives each user a different roles with the corresponding system operating authority. For reports may involve sensitive information, such as using public key encryption mechanism and the common key keepers to decipher key password, while query personal sensitive information. Compliance to PIPA, enterprises can audit accessing database activities, such as: accessingsensitive personal information behavior, DML, database user accounts, user roles, DCL, database schema changes (DDL) etc. DAM can retrieve record of user connection with web application server (URL log), and then compare to SQL log of execution the back-end DB Server and Client to track who's events, as shown in Figure 4:

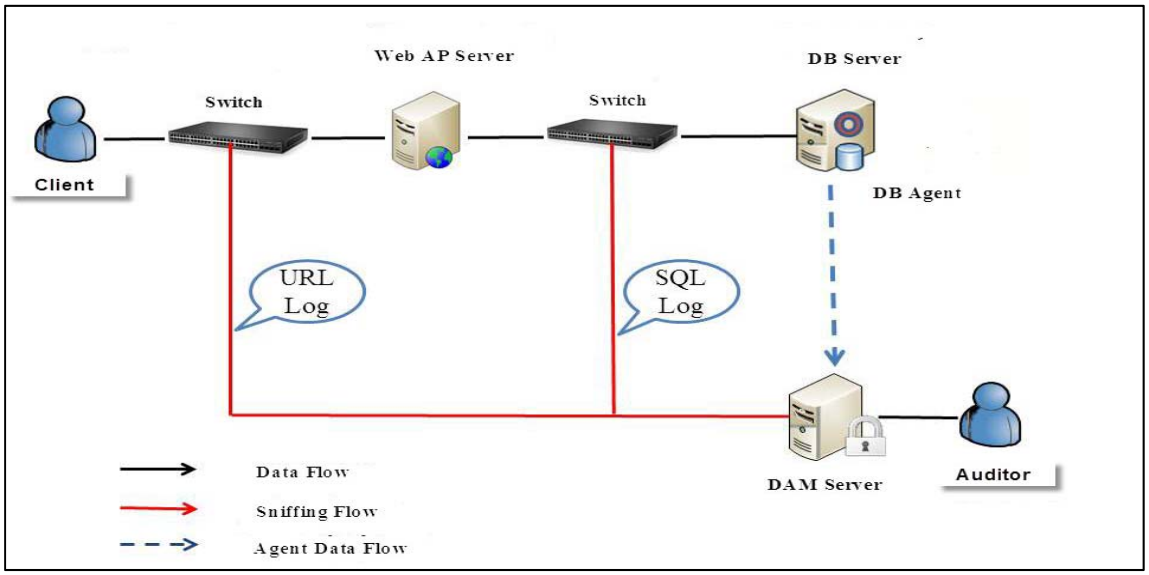

Figure4：DAM Network Architecture Diagram

3.5 Database Activity Monitoring Deployment

The network traffic entering into the web application server and DB server is collected by a sniffer, which is sent to auditing DAM server management center. Most companies front-end web application server is a common account to access the database, so if only record database account cannot be traced to the front end user, and monitor network behaviors between users andweb application server through comparing packets to confirm the identity of users. The enterprises do not need to modify the application of the risk, but also to achieve accurate recognizable.

Although, SQL has been recordedcompletely between DB Client and SQL DB Server, today's AP software architecture that provides front-end AP different user operations, but SQL commands on the back-end all which uses the same set of DB Client account tocommunicate DB Server. This design resulted in even know SQL dangerous commands sending from DB Client, but due to numerous user of the front of the AP, and it is difficult to distinguish who is committed.

The system capturesrecords that connectbetween AP user and AP server, the use of AP user and AP server connection records (URL log), and then compared to the backend DB Client and DB Server SQL execution record (SQL log) to track events whomever did them. In addition, installed on the database server DB Local Agent automatically collected by the native login access to the database server, which sent to DAM Server audit management center, database activities are recordedthe concept of who, which,when, where and what t, providing immediate and complete track recordsof database behavior.

4.ImplementingAgile Project and Verification

This chapter explains how to implement agile project and verify the works of the agile project.

4.1 Implementing Agile Project

This DAM agile project follows environmental assessment framework, data inventory, setup system, the report definition and warnings of models to facilitate the companycomprehensive scope of auditingto access sensitive digital data to ensure an appropriate level of business database security auditing operations, as shown in Figure 5:

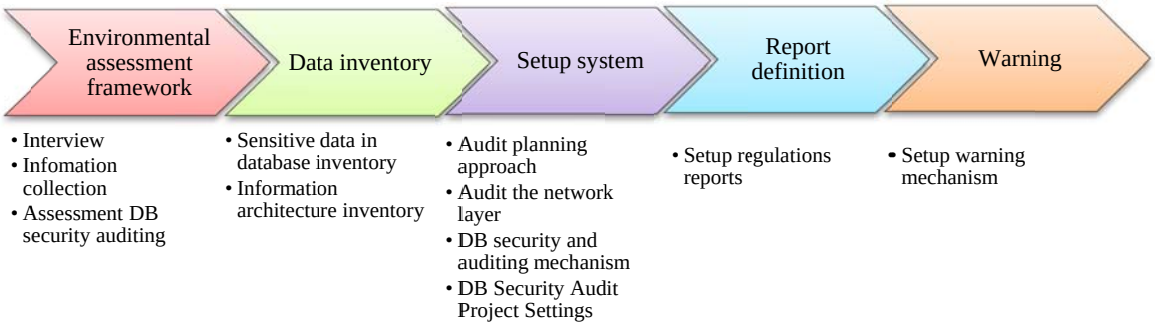

Figure5：The DAM Agile Project Flow

EstablishingPIPA regulationsreports, in addition to pre-defined in the ISO standard and PIPA related reports,it can also be audited in accordance with the enterprises'security policy, and build customized reports, except that the responsible staffs may query report in the auditing systemat any time, and the system automatically generates regular reports such as daily, weekly, monthly reports and other related reports, reduce the burden on each person who is responsible for the system, as shown in Figure 6:

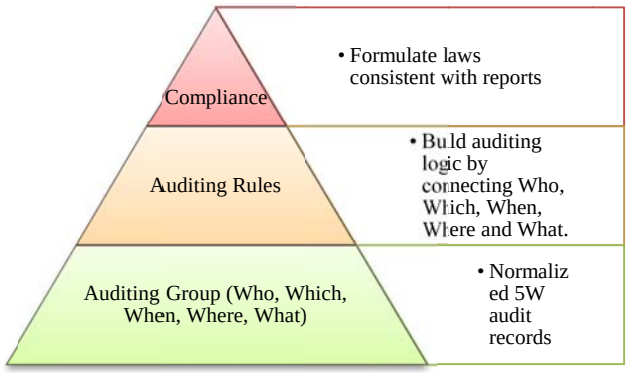

Figure6：EstablishRegulations ReportingClassificationDiagram

Free software MeisterTask and MindMeister have been used as an electronic Kanban to visualize the workflow, limit work in progress, and measure the lead time.The DAM agile project has 7activities: Establishing management organization and Allocating enough resources, Defining the scope of personal information, Prevention security events, Notification and response mechanism, Device Security Management, Information security audit mechanism, Retain evidence for using records and track data, as shown in Figure 7:

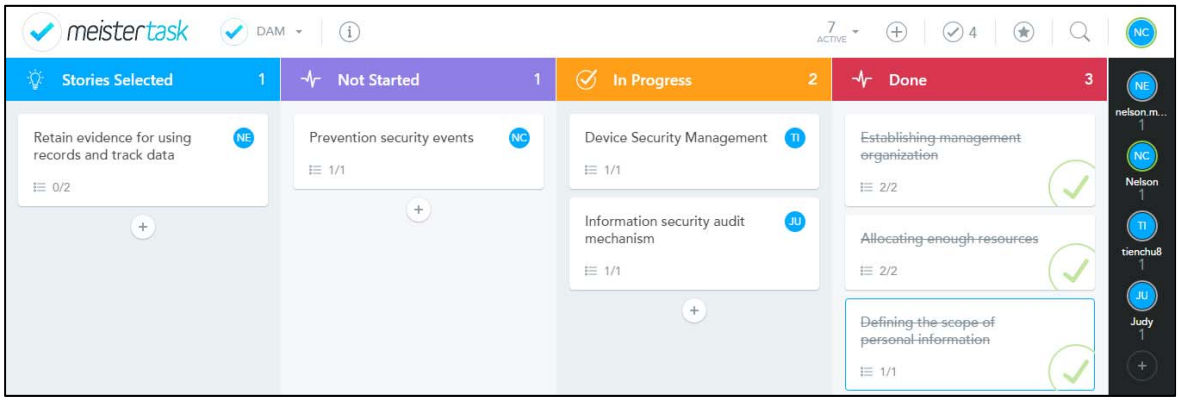

Figure7：Electronic Kanban as an Information Radiator to Show the Agile Project Processes

4.2 Project Verification

After the completion of the overall database auditing system setup, it is the time to perform functional verification, simulation simplescenarios to verify the implementation of the relevant rules of Article XII of PIPA, and validated results of this project, as described in Table 4:

Table4：ProjectVerifiedResults

Items	Verification description	Verified Results	
Establishing management organization, and allocating enough resources	Role separation, division of responsibilities	create an account on interface, groups according to the staff of different ownership (auditors, system administrators, security control administrator), different operating authority granted	Confirmative
Defining the scope of personal information	Personal information inventory	Provide personal information inventory function	Confirmative
Prevention of events, notification and response mechanism	Sensitive information protection management	Exception management reports, data access exception automatic alarm alert	Confirmative
Device Security Management	Backup and restore management	Device safety management, data backup & restore management, backup encryption support Set the schedule for backup and purge audit log Set log on a regular basis to backup, Send data directly back to auditing equipment on management interface, eliminate the need for third-party devices, restore, provide access to information	Confirmative
Information security audit mechanism	Database activity monitoring	Provide continuous and real-time database activity monitoring, the activities of operating system audit, conducted by recording personnel	Confirmative
It is necessary to retain evidence for using records, and track data	Prevent tampering with audit records modification, non-repudiation	Monitoring detailed audit information, and then stored in a secure external hardware storage device can be read only by way of accessing. traceability database activity generated by users	Confirmative

5.Conclusions and Recommendations

We conclude the study, implications of information security management, and finally give recommendations.

5.1 Conclusions

This study responds to PIPA and implementDAM agile project, couples with the existing enterprise management mechanisms, assesses riskand personal information, advocate to strengthen the implementation of cognitive education and training, and making it more in line with PIPA regulations.The use of DAM toolswhich do notneed to modify in the code, and it do not need to change the network architecture to continuously monitor and analyze database activityin real-time.Violating the policy of database activity can instantly alert, record all tracks for later analysis.Three main functions of DAM providing benefits for enterprise information security:

(1) DAM provides complete network and database activity monitoring: DAMcompiles with corporate auditing system, in addition to assisting the implementing of various standards, and to strengthen the overall information security prevention capabilities in the database-end, regardless authority to take any action, any time, via any pipeline, take any action can be fully recorded.

(2) Build an easy to learn reporting system: database auditing system is an easy to usemanagement system, whether it is after the build process, or during operation of the system with user-friendly operation, and auditors can easily use. The concept of 5 W's to establish compliance with PIPA auditing reports.

(3) Flexible system configurations: we can build the auditing system based on the business'needs,rolesandthe position of the elastic configuration auditing systems. It can simultaneously monitor user activities frommultiple databases, focused on a single management interface, and itself provides a good backup mechanism to comply with PIPA long-term preservation of information access records.

5.2 Implications on Information Security Management

When companies build theinternal PIPA system, top managers must support and devote sufficient resources to support and assign an appropriate person responsible for the overall planning and execution, and fully mobilizepersonal to success. When an enterprise performs protectionpersonal information, it isrequired to inventory of storage and business personal information patterns. It is recommended Small-Medium enterpriseto adopt classification of departments, large enterprises can adopt the information flows to distinct between information gathering, processing and utilization of the different stages to classify.

Based on enforcement rules of the PIPA: the prevention of events, the notification and response mechanisms, and enterprises must establish smooth pipeline.If an event resulting in personal information leakage, companies must identify an appropriate manner to notify the parties. Enterprises must establish personal data collectionin weekdays, processing and use of relevant internal management procedures, information security management, personnel and equipment safety management, as well as advocacy and awareness education. Through internal management procedures and records, regardless of paper or electronic files, there are required to be kept, and the ongoing improvement work to fulfill the responsibility of protection. The keys to proposepowerfuldigital evidence is whether companies can achieve authentication, correctness, and to ensure that evidence is not polluted.

An administrator has right to access a host system, and it is possible to turn off the agent, then the subsequent behavior will not be able to verify. Although the product is designed to do once management center cannot detectthe agent, and then the alert notification will release to the person in charge, but the window period may indeed exist. Therefore, more importantly the business must be done in the attribution of responsibility on decentralization, if DBA and audit manager is a same person, even in conjunction with system management and information security control manager who is the same person, they are facing the players and the referee dilemma situation.

5.3 Recommendations

Because establishedenterprises'private cloud systemsis popular, it is recommended interested in implementing DAM project or audit-related research project to know enterprise private cloud systems infrastructure cognitive, and then deeply study and analysis contentsbased on the information patternsstored in a database.Enterprise carefully auditing can prove the responsibility to fulfill security management, anda variety of tracks and digital evidence aremaintained.

References

1. Coad, Peter, Lefebvre E. and De Luca J., 1999, Java Modeling In Color with UML: Enterprise Components and Process, Prentice Hall International.
2. Cobrasonic, 2015, Database Activity Monitoring.
3. Cockburn, Alistair, 2007, Agile Software development: The cooperative game, 2nd ed., Reading, MA: Addison-Weslley.
4. Cohn, Mike, 2005, Agile Estimating and Planning. 1 Ed., New Jersey: Prentice Hall, p. 368.
5. Gartner, Inc. Jeffrey Wheatman, 2011, Establishing a Strategy for Database Security Is No Longer Optional.
6. Highsmith, Jim, 2009, Agile Project Management: Creating Innovative Products. 2nd Ed., Addison-Wesley Professional, pp. 432.
7. IDC, 2013, M2M in CEE and MEA: Results from IDC's Enterprise Communications Survey.
8. Lin,I-Cheng,2010,Information security assurance and audit database,Journal of Information Communication and Technology Auditing, Computer Audit Association, No. 22, p.118-127.
9. Lin, Yin-Fong,2010, New Trends of Audit database technologies - Database Activity Monitors, Journal of Information Communication and Technology Auditing, Computer Audit Association, No. 22,p.131- 135.
10. LRDROC, 2012, Laws & Regulation Database of the Republic of China, Enforcement Rules of the Personal Information Protection Act.
11. Lyssa, Adkins, 2010. Coaching Agile in a Teams: A Companion for Scrum Masters, Agile Coaches, and Project Managers in Transition, New York: Addison-Wesley Professional, pp. 352.
12. Mogull, Rich, 2012, Understanding and Selecting a Database Activity Monitoring Solution, SANS Institute, https://securosis.com/assets/library/reports/DAM-Whitepaper-final.pdf
13. PMI, 2015, PMP PMBOK, http://www.pmi.org, browsed on March 18, 2015.
14. Poppendieck, Mary, 2003. Lean Software Development: An Agile Toolkit, New York: Addison-Wesley Professional.
15. RDECEYROC, Research & Development and Evaluation Commission, Executive Yuan, ROC, the process-oriented model Personal Information Protection Technical procedures (PIPTP), 2012.
16. Schwaber, Ken, 2004. Agile Project Management with Scrum. Redmond: Microsoft Press, pp. 192.
17. Shalloway, Alan, Guy Beaver, and James R. Troa, 2009, Lean-Agile Software Development: Achieving Enterprise Agility, New York: Addison-Wesley Professional, pp. 304.
18. Sutherland J. and Schwaber K., 1995, Business object design and implementation, OOPSLA'95 Workshop Proceedings, University of Michigan, p. 118.
19. Tseng, Yun, 2012,Impact on Personal Information Protection Actwith respect to the impact of the financial industry's response measures, Finance Information Quarterly, No.71.
20. Apple Daily News, 2013, http://www.appledaily.com.tw/appledaily/article/headline/20130223/34847564/, browsed on March 18, 2015.
21. United Daily News, 2012, http://money.udn.com/fund/storypage.jsp?f_ART_ID=265457, browsed on March 18, 2015.
22. Verizon data breach investigations report, 2010, http://www.verizonenterprise.com, browsed on March 18, 2015.