Global Information Assurance Certification Paper

GIAC Certified ISO-17799 Specialist

Practical Assignment

Version 1.1

Information Security Management System

for Intrusion Detect ion and Prevention Systems

By: Diane Wang

Submitted on: September 20, 2004

Course location: SANS 2004 Conference, Orlando

Table of contents

Abstract

This practical assignment will develop an Information Security Management System (ISMS) for Intrusion Detection and Prevention Systems (IDPS) internal to an organization with real-time alert monitoring and trending analysis capabilities over the critical information assets in a financial institution.

The organization in this case is a mortgage company that collects non-public personal information (NPI) from the customers. The data collected from the customers is very valuable to the company; and the company has the responsibility to keep the customer's information secure and private.

The organization primarily uses home-grown applications to conduct loan origination transactions. Therefore, the ability to monitor and prevent unusual and/or malicious activities against the servers hosting the applications and databases will reduce the opportunity for business interruptions from ill attempts targeting these information assets.

The IDPS will be built to protect the key assets in the organization. The key assets are defined as the application servers, database servers, and network infrastructure. In establishing the ISMS for IDPS of the financial institution, ISO-17799 principles will be utilized and specifically apply the appropriate steps in the "Plan, Do, Check, Act (PDCA)" process described in the SANS 17799 course.

Additionally, the reasons for selecting IDPS as the system for this practical assignment include:

1. Required by California privacy legislation, any business organization conducts business transactions in California that collect customer private information electronically is required to notify the affected residents in the event that security breaches occur unless encryption is utilized. Therefore, preserving evidence, such as alerts and logs, collected by an IDPS is critical in complying with the legislative requirement.

2. Regulated by the Federal Trade Commission (FTC) in their enforcement of the Gramm-Leach-Bliley Act of 1999 (GLB Act), which requires a written information security program. The IDPS is a vital component of the information security program.

1. System Definition

1.1 Introduction

This practical assignment will develop an Information Security Management System (ISMS) for Intrusion Detection and Prevention Systems (IDPS) internal to an organization with real-time alert monitoring and trending analysis capabilities over the critical information assets in a financial institution.

1.2 Scope

The scope of the proposed ISMS for IDPS includes the monitoring and response of potential intrusions to critical network segments that houses critical data assets in the organization. The personnel involvement will include senior management, business unit leaders, Internal Audit, Information Security, and various groups within Information Technology department, including Operations, Technical Services, and Network Operation Center. Since IDPS monitors the entire network, the ISMS for IDPS cover multiple locations, mainly data centers and key branches. From the technology perspective, the IDPS sensors, syslog servers, log database server, and log consolidation server are part of the scope.

1.3 Description of the Organization

The organization has approximately 5000 associates and 600 servers, which spans across about 80 branches and three data centers cross the United States. The organization is a mortgage company. The main business functions are originating and servicing mortgage loans. The organization maintains non-public personal information (NPI) from the customers as the result of business functions. The NPI data collected from the customers is very valuable to the company; and the company has the responsibility to keep the customer's information secure and private.

1.4 System Information

The organization has three (3) points of presence on the Internet and hosts its own Internet web servers. This architecture allows for network traffic load balancing for both incoming and outgoing Internet traffic. In addition, the organization has established connectivity with numerous vendors and business partners for business purposes. These entry points into the internal network are protected by firewalls and DMZ configurations.

Internally, the organization primarily uses home-grown applications to conduct loan origination transactions. Therefore, the ability to monitor and prevent unusual and/or malicious activities against the servers hosting the applications and databases will reduce the opportunity for business interruptions from ill-attempts targeting these information assets.

The business objective of the organization is to provide quality financial products and services that create value by achieving superior customer satisfaction. The

objective of the ISMS for IDPS is to help ensure a safe environment for the business operations to carry out the Company's mission statement.

The organization maintains large number of customer NPI data; thus the specific California Civil Code §1798.82 (commonly referred to as SB1386) requires the organization to notify the customers of any system security breaches. This means that it is imperative that the appropriate controls surrounding the IDPS logs are in place to help ensure the integrity of the data collected. If the event a dispute arises, the organization may need to demonstrate the integrity of the logs, which may be used for evidence purpose.

DPS will be built to protect the key assets in the organization. The key assets are defined as the application servers, database servers, and network activity log information.

1.5 Current State of Security

The organization has grown rapidly in the past few years. The primary business objective in the past has been to support the business growth. Security has not been given the necessary attention. However, various changes have been taking place from regulatory perspective. This organization is a financial institution operating in the state of California. This means that it must comply with the both federal and states regulations, such as Gramm-Leach-Bliley Act of 1999 (GLB Act) and California Civil Code §1798.82. As a result, more attention has been given to security as the organization becomes more mature.

The security culture in the organization is becoming more mature. The organization is in the process of providing more security awareness and training to all associates.

However, there are opportunities to improve the state of security. One area is the processes managing the IDPS are fragmented and there is no accountability established. There are controls in place; for example, IT Operations staff manages the devices and Information Security group determines the configuration to ensure segregation of duties. However, the controls are not systematically implemented and the effectiveness of the controls has not been determined.

The organization is in the process to establish the high-level security principles, such as principle of least privilege, no back door permitted, etc. This is a long process that requires the buy-in from senior management and business unit leaders. An Information Security steering committee has been formed to take this task.

2. Plan

To plan for a successful implementation of the ISMS for IDPS, the following elements are critical:

1. Timeline/Project Plan;
2. Management Structure and Approvals;
3. Development of policies, guidelines, standards, and procedures;
4. Identification of assets to be monitored/protected;
5. Resources requirements (personnel and hardware/software/environmental resources); and
6. Risk management (including assessment, mitigation, and monitoring).

2.1 Timeline/Project Plan

To establish an effective ISMS for IDPS, planning for a realistic project plan and timeline will help ensure the availability and participation of necessary resources. The initial draft plans include the following major phases/milestones:

1. Project initiation
2. Scope determination
3. Management review and approval
4. Secure resources
5. Risk management
6. IDPS evaluation and design
7. IDPS implementation
8. Continuous monitor
9. Metrics review

The initial estimated lapse time needed for the project is about six (6) months, provided that there are no resources constraints.

2.2. ISMS Management structure

The ISMS management structure is two-folds. One is the oversight and policy establishment functions, which is fulfill by the formation of Information Security steering and sub committees. The other is the implementation and enforcement functions, which is fulfill by the Information Security, Risk Management, and Internal Audit group.

2.2.1 Information Security and Risk Management

In the organization, the Information Security group is positioned in the Information Technology department. The Information Security Manager leads the Information Security group. The Risk Management group is positioned in its own department, which directly reports to the executive management team. The Internal Audit manager reports to the Chief Risk Officer (CRO). The reporting structure is depicted in Figure 1.

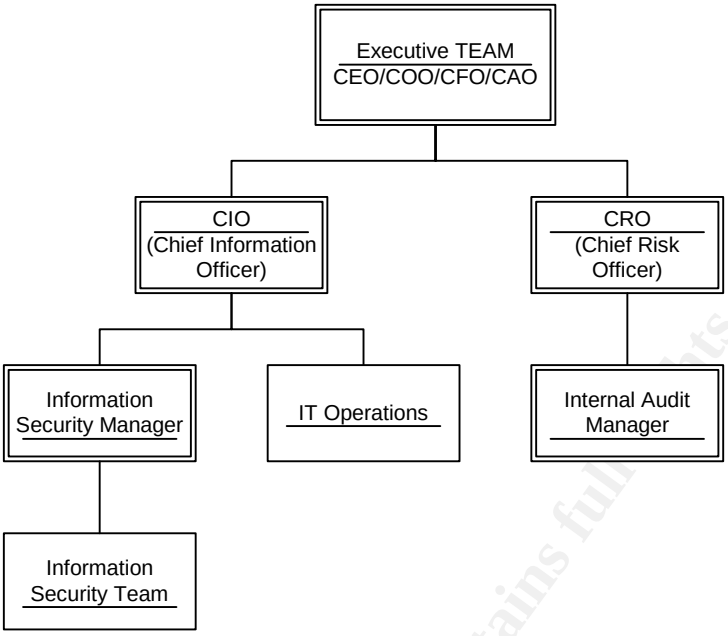

Figure 1. Information Security management structure

The Information Security Manager will drive the initiative for establishing the ISMS for IDPS project. Key members of Information Security group will participate as contributors to the project.

2.2.2 Committees

The Information Security Management System management structure is a multi-tier structure. As an oversight group, an Information Security committee comprising senior management leaders and business unit leaders will take the oversee responsibility. The Information Security committee is an existing committee that is responsible for setting the security directions for the organization. To add to existing responsibility, the committee will oversee the ISMS for IDPS and ensure that appropriate controls are in place to ensure the effectiveness of the ISMS.

In addition to the Information Security committee, various sub-committees will be formed to address specific aspect of the ISMS. The initial sub-committees formed include: Policy committee, Audit committee, Technology committee, and Risk Management committee. The committee structure is depicted in Figure 2.

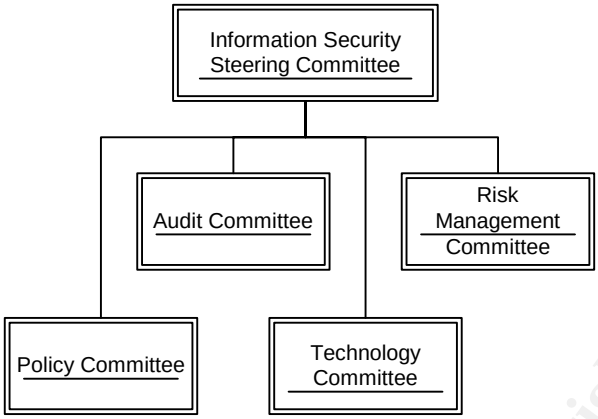

Figure 2. Information Security Committee Structure

The Information Security Manager will participate in all the committees as the facilitator. Other responsibilities of the Information Security group include the establishment of the ISMS and the identification of appropriate processes and controls to be implemented. The controls may include, but not limited to, the establishments of policies, standards, guidelines, and procedures of how IDPS will be implemented, monitored, and maintained. The Information Security group will be designated as the IDPS data owners.

Data Asset Owners are defined as the business unit management whom has the decision-making authority over the data assets in his/her business units. The IDPS is designed to detect and/or prevent any ill attempted against these data assets. Data Assets Owners will participate in the various Information Security sub-committees.

The Information Technology Operations group will participate in the Technology committee. In addition, this group will be responsible for the technology and controls implementation. The group will also be designated as the custodian of the IDPS data assets, but not the owner.

The Internal Audit group will participate in the Audit committee and the Risk Management committee. In addition, the group will be responsible for the verification enforcement of the appropriate controls identified by the Information Security group.

2.3 Policies

To help ensure that the appropriate controls are in place for the proposed ISMS, policies and procedures must be developed so that the IDPS objectives and requirements can be clearly communicated. The followings are the initial set of policies proposed for the ISMS.

2.3.1 Access Control Policy

Policy name	Access Control Policy
Purpose	Address the need for access control of any information collected by IDPS must require authentication; and only authorized associates are permitted to work on the configurations of IDPS systems.
Audience	All associates
Areas of Standard that will be addressed	Asset classification and control Access control System development and maintenance

2.3.2 Compliance Policy

Policy name	Compliance Policy
Purpose	State that the organization must comply with regulatory requirements. Define the roles and responsibilities of departments within the organization necessary in complying with the regulatory requirements.
Audience	All associates
Areas of Standard that will be addressed	Compliance

2.3.3 Data Archive Policy

Policy name	Data Archive Policy
Purpose	Organization must maintain confidentiality and integrity of the log data that IDPS generated. The data must be kept forensically sound and free from tempering. Data must be archived on a regular basis and must be based on the Corporate Data Retention Policy for retention period.
Audience	IT associates, Information Security associates
Areas of Standard that will be addressed	Communications and Operations Management Compliance

2.3.4 Incident Response and Escalation Policy

Policy name	Incident Response and Escalation Policy
Purpose	Organization must be able to response to any security incident in a timely manner. The goal is to preserve the privacy of customer data and confidentiality of company proprietary information.
Audience	All associates
Areas of Standard that will be addressed	Communications and Operations Management

2.3.5 Traffic/Activity Monitor Policy

Policy name	Traffic/Activity Monitor Policy
Purpose	Organization must monitor the traffic collected from IDPS on regular basis to help ensure that the network is safe and sound. Organization must monitor any action taken by the intrusion prevention system on a regular basis to help ensure that the actions are appropriate and warranted.
Audience	All associates
Areas of Standard that will be addressed	Communications and Operations Management

2.3.6 Configuration Management Policy

Policy name	Configuration Management Policy
Purpose	Organization must maintain the integrity of the configurations on the IDPS devices. All configuration changes must be reviewed for the appropriateness and be tracked in the change log trail.
Audience	All associates
Areas of Standard that will be addressed	Communications and Operations Management System development and maintenance

2.3.7 Personnel Policy

Policy name	Personnel Policy
Purpose	Organization must perform background check before hiring associates into the company. Management must review the experience and skill sets of the associates before placing him/her into the position requiring specific skills. For example, system administrator has administrative level of access to many systems; therefore, background check result must satisfy the requirement of a position with access to sensitive information. Furthermore, with administrative access to mission critical systems, the system administration must possess a certain level of knowledge and know the consequence of his/her actions over the systems.
Audience	Human Resources, Management staff
Areas of Standard that will be addressed	Organizational Security Personnel Security

2.3.8 High Availability Policy

Policy name	High Availability Policy
Purpose	Organization must maintain high availability of the systems to help ensure that in the event that a system fails, the business operation disruptions are minimized.
Audience	IT Operations, Information Security, Risk Management
Areas of Standard that will be addressed	Communications and Operations Management Business Continuity Management

2.3.9 Data Center Security Policy

Policy name	Data Center Security Policy
Purpose	Organization must maintain a secure facility to protect computing resources. This policy defines roles and responsibility of IT personnel, and identifies requirements with regards to Data Center facility and environmental controls.
Audience	IT Operations, Information Security
Areas of Standard that will be addressed	Communications and Operations Management Physical and Environment Security

2.4 Identification of assets to be monitored/protected

To properly assess risks associated with the ISMS, identification of assets is an important phase. The goal of this phase is to identify assets that must be included in the system, and assets that should be excluded or optional to the systems. The steps to take consist of the following:

1. develop information flow diagram
2. based on the diagram, indicate key assets in the system
3. based on the key assets identified in step 2, inventory the physical devices associated with the key assets and document the result
4. assign sensitivity and criticality factors to the assets inventoried from step 3
5. based on the sensitivity and criticality factor, develop impact of loss or disclosure of assets.

There are four sensitivity levels: private, confidential, secret, and top secret; and there are three criticality factors: confidentiality, integrity, and availability.

Based on the steps, the initial set of assets is identified as follows.

Assets	Sensitivity	Criticality factors	Impact of loss or disclosure
IDPS sensors	Confidential	Confidentiality Integrity	If the devices are lost, they could potentially impact the organization. However, the company can continue to operate.
Routers	Confidential	Availability Confidentiality Integrity	If the devices are lost, they could potentially impact the organization. Depending on the number lost, there may be business interruption due to a network routing failure.
Syslog servers	Secret	Confidentiality Integrity	The information within the syslog server may contain sensitive information related to the network. Information may be used to harm the organization if it is lost or disclosed.
Log consolidation servers	Secret	Confidentiality Integrity	The information within the log consolidation server may contain sensitive information related to the network. Information may be used to harm the organization if it is lost or disclosed.
Database servers (IDPS logs)	Secret	Confidentiality Integrity	The information within the database server storing IDPS logs may contain sensitive information

Assets	Sensitivity	Criticality factors	Impact of loss or disclosure
			related to the network. Information may be used to harm the organization if it is loss or disclosed.
Database servers (customer information)	Top Secret	Availability Confidentiality Integrity	If customer information is compromised, required by law the organization must notify all affected California residents. This may threaten the viability of the organization.
IT Operations associates	n/a	Availability Confidentiality Integrity	The organization may face competition or loss of knowledge base.
Information Security associates	n/a	Availability Confidentiality Integrity	The organization may face competition or loss of knowledge base.
Data Center facility	n/a	Availability Confidentiality	All critical computing devices are housed in one of the three data centers. If the organization loses one data center, the other two serve as backups. However, time and effort are required to restore the services.
Backup tapes (IDPS data)	Secret	Confidentiality Integrity	If the tapes are loss or disclosed, the impact is the same as the loss of database servers housing IDPS data.
Backup tapes (Customer information)	Top Secret	Confidentiality Integrity	If the tapes are loss or disclosed, the impact is the same as the loss of database servers housing customer information.
Device configuration files (intellectual properties)	Secret	Confidentiality Integrity	If the configurations file are lost or disclosed, the information may be used to harm the organization's IT infrastructure.
Vendor maintenance services	Secret	Availability	If the maintenance services are not available when the needs arise, the business operations may potentially be interrupted.

2.5 Resources requirements (personnel and hardware/software/environmental resources)

Resources required for the ISMS for IDPS implementation include:

1. Information Security committees – meet periodically
2. Data Assets Owners – acknowledge their assets are being monitored by IDPS
3. Information Security associates – active participate in the system
4. IT Operations associates – active participate in the system
5. Internal Audit associates – perform audit of the system periodically
6. Hardware/software – IDPS sensors, database servers, log servers, and other required software
7. Physical environment – available data center and backup data storage facility

2.6 Risk Management

The approach to risk management used here is a slight modification of a process that mirrors the Project Management Institute's *PMBOK® Guide – 2000 Edition* [2]. For the ISMS for IDPS, the Risk Management planning includes the following major steps:

1. Validate the project scope and objective
2. Identify risk environment
3. Establish approach to risk management
    a. Define risk management templates
    b. Define threshold or tolerance level
    c. Define metrics
    d. Define roles and responsibilities
    e. Define tracking methodology
    f. Define cost/budget requirements
    g. Define evaluation criteria
4. validate issues and problems
    a. Risk identification
    b. Risk qualification analysis
    c. Risk quantification analysis
5. Risk response/treatment planning
6. Risk monitoring and control

Risk is defined as the combination of threat, vulnerability, and the value of the assets. The method for risks analysis in this case uses the combination of both qualitative and quantitative to determine the risk level, which includes the combination of impact of loss assets (potential and actual values) and the likelihood of occurrence of a particular risk without any mitigation controls.

The controls referenced are the AS/NZS 7799.2 [1]. The threats and vulnerabilities used below are referenced from "Information Security Guideline for NSW Government - Part 2. Department of Commerce, Office of Information and Communications Technology [5]. Using the risk management approach stated above, initial set of risks is as follows:

2.6.1 Risk: Unauthorized Data Access

Threat: Unauthorized Data Access
Vulnerability:
- Lack of logical access controls
- Inability to authenticate requests for information
- Lack of physical security over data center facility
- Lack of physical security over data communications cabinets

Likelihood of occurrence: Medium
Risk Level: Medium
Control Description:
- 7.1.1 Physical Security Perimeter
- 7.1.2 Physical entry control
- 8.1.1 Documented Operating procedures
- 8.1.4 Segregations of duties
- 9.2.2 Privilege Management
- 9.2.3 User Password Management
- 9.2.4 Review of user access rights
- 9.4.5 Remote diagnostic port protection
- 9.5.1 Automatic terminal identification
- 9.5.2 Terminal logon procedures
- 9.5.3 User identification and authorization
- 9.5.4 Password management system
- 9.5.7 Terminal timeout
- 9.7.2 Monitoring system use
- 10.4.1 Control of operational software

Reason for selecting control:
The selected controls are specifically designed to prevent and detect unauthorized data access through the use of technologies and policies. These controls help preserve the confidentiality and integrity of the data by preventing unauthorized access.
Risk level after implementing controls: Low

2.6.2 Risk: Malicious destruction of data and facilities

Threat: Malicious destruction of data and facilities
Vulnerability:
- Lack of physical security
- Lack of logical security
- Lack of backup media storage procedures
- Lack of appropriate terminated associate procedures
- Inadequate personnel screen process
- Inadequate inventory and classification of assets

Likelihood of occurrence: Low
Risk Level: Medium
Control Description:
- 5.1.1 Inventory of assets
- 5.2.1 Classification of guidelines

5.2.2 Information labeling and handling
6.1.2 Personnel screening and policy
6.1.3 Confidentiality agreement
6.1.4 Terms and conditions of employment
7.1.1 Physical Security Perimeter
7.1.2 Physical entry controls
7.1.3 Securing Offices, rooms, and facilities
7.2.1 Equipment site/location protection
8.4.1 Information back-up
9.2.2 Privilege Management
9.2.3 Review of user access rights
9.4.1 Policy on use of network services
9.6.1 Information access restriction
9.6.2 Sensitive system isolation
9.7.2 Monitoring system use
11.1.1 Business continuity management process
11.1.2 Business continuity and impact analysis
11.1.3 Writing and implementing continuity plan
11.1.4 Testing, maintaining, and reassessing business continuity plan
12.1.1 Identification of applicable legislation
12.1.2 Safeguarding of organizational records
12.1.3 Data protection and privacy of personal information
12.3.2 Protection of system audit tools

Reason for selecting control:

The selected controls are designed prevent malicious destruction of data and facilities that are of values to the organization. If the event that the threat does occur, the selected controls are designed to address the business continuity aspect of the system. The destruction of data can be both done both physically and logically. These controls help preserve the availability and integrity of the assets.

Risk level after implementing controls: Low

2.6.3 Risk: Unauthorized changes in software and/or configurations

Threat: Unauthorized changes in software and/or configurations

Vulnerability:

Lack of documented change management policies and procedures
Lack of change management policies and procedures enforcement
Lack of backup copies of software and/or configuration files

Likelihood of occurrence: Low

Risk Level: Medium

Control Description:

8.1.1 Documented Operating procedures
8.1.2 Operational Change Control

8.1.3 Segregation of duties
8.4.1 Information back-up
8.4.2 Operator log
9.7.1 Event logging
9.7.2 Monitoring system use
10.5.1 Change control procedures
11.1.1 Business continuity management process
11.1.2 Business continuity and impact analysis
11.1.3 Writing and implementing continuity plan
11.1.4 Testing, maintaining, and reassessing business continuity plan
12.3.2 Protection of system audit tools

Reason for selecting control:

The selected controls are designed to prevent unauthorized changes in the systems. In the event that unauthorized changes do occur, the selected controls are designed to capture the changes and notify proper personnel. If the changes damage the system, the selected controls are designed to help ensure that system can be recovered to the original state.

Risk level after implementing controls: Low

2.6.4 Risk: Denial of Services/Malcode attack on the network

Threat: Denial of Services/Malcode attack on the network

Vulnerability:

Lack of appropriate anti-virus software
Inadequate virus definition update process
Lack of patch management process to keep all devices on current software
Inadequate acceptable Internet and e-mail use policies
Lack of appropriate control over corporate computers
Inadequate network management and controls of unauthorized devices connecting to the network
Lack of security alerts monitoring and notification procedures

Likelihood of occurrence: Medium

Risk Level: High

Control Description:

8.1.3 Incident management procedures
8.3.1 Control against malicious software
8.4.3 Fault logging
8.5.1 Network Controls
8.7.4 Security of Electronic e-mail
9.4.1 Policy on use of network services
9.4.2 User authentication for external connections
9.7.1 Event logging
12.1.1 Identification of applicable legislation
12.1.2 Safeguarding of organizational records

12.1.3 Data protection and privacy of personal information
12.1.4 Collection of evidence
12.1.5 Protection of system audit tools

Reason for selecting control:

The selected controls are designed to reduce the potential denial of services attack or malicious code attacks. In the event that denial of services or malcode attacks does occur, the organization has the appropriate controls in place to handle the incident.

Risk level after implementing controls: Low

3. Do

After the planning phase, gaps will be identified and analyzed. In this section, the discussion is on the mitigation strategy to close the gaps identified in order to implement and improve the ISMS for IDPS. In the following sections, the gaps (i.e. problem statements) are stated along with the actions necessary and the activities to be implemented to close the gaps.

3.1 Problem: Policies and procedures are fragmented for the ISMS for IDPS

Since there were no formal ISMS defined for IDPS, policies and procedures are not fully defined and developed. The impact of no formal policies and procedures is that ISMS cannot be formalized and processes may not be repeatable or predictable.

Action: To remediate this problem, formal policies and procedures for the ISMS must be defined and published.

Activities:

- Step 1 – Bring together members of the Information Security steering committee members and develop the high-level security policies
- Step 2 – Bring together members of the Policy sub-committee and develop the policies based on the high-level security policies identified by the Information Security steering committee (see section 2.3). The Policy sub-committee develops the policies through a series of working sessions
- Step 3 – Information Security steering committee review and approve the policies
- Step 4 – Document the approved policies and publish them
- Step 5 – Each of the operational areas (IT Operations, Information Security, and Internal Audit) writes appropriate procedures to conform to the formal policies
- Step 6 – Document the procedures and publish them within the respective departments
- Step 7 – Implement the formal policies and procedures

3.2 Problem: Security Incident Response and Handling process does not exist.

Without a security incident response and handling process, in the event that the organization is under attack by denial of services or other malicious code (worm, virus, etc.), the organization cannot respond to the incident in a timely or controlled manner. The impact of this gap on the system is that the operations may be interrupted as the result of malicious code. The result is lack of system stability, availability, and potentially compromised system integrity and data confidentiality.

Action: To remediate this problem, the following policies and procedures will need to be developed and implemented.

Activities:

- Step 1 – Bring together members of the Policy sub-committee to develop a Security Incident Response and Handling policy
- Step 2 – Information Security steering committee to review and approve the policy
- Step 3 – Identify required members of the incident response team
- Step 4 – Assemble the team to develop incident response and escalation procedures
- Step 5 – Document the procedures
- Step 6 – Communicated the policies and procedures to associates who are part of the security incident response and handling team (primary and backup)
- Step 7 – Test the procedures on a regular basis

3.3 Problem: Compliance policy is not up to date to include the new regulatory requirements.

Numerous new privacy laws are being passed at both federal and state level. The organization is aware of the new laws and is in the process to update internal policy and procedures in order to comply with the law. Specifically, California Civil Code §1798.82 requires the organization to notify all affected California residents after a security breach. Without appropriate policy and procedures, the organization may not store the IDPS logs in a way to be forensically sound and free from tempering, potentially interfering with the organization's ability to identify or respond to an incident.

Action: To remediate this problem, the following policy and procedures will be need to be developed and implemented.

Activities:

- Step 1 – Bring together members of the Policy sub-committee to develop a data archive policy
- Step 2 – Information Security steering committee to review and approve the policy
- Step 3 – Identify the responsible associates, such as IT Operations and Information Security, to gather requirements for necessary procedures for data archive
- Step 4 – Develop and document the procedures to conform to the data archive policy
- Step 5 – Communicate the policy and procedures to the associates working the these data
- Step 6 – Test the procedures on a regular basis to help ensure the data are being archived (backup and store) appropriately

Step 7 – Test the restore procedures on a regular basis to help ensure that data can be restored if necessary

3.4 Information Security sub-committees are not fully formed

Although the organization has the Information Security steering committee established, not all the sub-committees are fully formed with appropriate participants from the senior management and business units' representatives.

Action: To remediate this problem, the following steps must be implemented.

Activities:

Step 1 – Bring together members of the Information Security steering committee
Step 2 – Identify the sub-committees to be formed
Step 3 – Identify the functions of sub-committees
Step 4 – Recommend appropriate sub-committee members
Step 5 – Obtain buy-in from the senior management and solidify the availability of recommended sub-committee members
Step 6 – Bring together members from each of sub-committees (separate meeting)
Step 7 – Share with them the overall Information Security committee mission statement
Step 8 – Develop mission statement for each of the sub-committees
Step 9 – Have the committee members meet on a regular basis, depending the need of overall information security program

3.5 Statement of applicability for an applicable control

Standard 9.7 Monitoring system access use

Control 9.6.1 Event logging

By definition, IDPS monitors the network activity, and generates appropriate alerts or takes appropriate actions when suspicious network activity detected. Therefore, it is imperative that events taking place are being logged as audit trails. In the event that it is necessary to review what had taken place on the network, event logs can be reviewed and provides the ability to re-construct the sequence of events took place. Therefore, this control is very applicable to the ISMS for IDPS.

3.6 Statement of applicability for a not applicable control

Standard 10.2 Security in Application Systems

Control 10.2.1 Input data validation (not applicable)

This control is to design to ensure that data input to application system is validated to ensure that it is correct and appropriate. This control is not applicable to the intrusion detection and prevention system. The implementation of IDPS does not take input; but rather, the system listens on the network to monitor the activities. Therefore, this control does not apply in the ISMS for IDPS.

4. Check

As part of the PDCA cycle, an audit checklist is developed to be used to audit the ISMS for IDPS against the relevant criteria from the standard. The following tables describe selected controls from the standard, the control objective for each selected controls, reason for audit the controls, the audit steps for these controls, and the frequency to perform the audit of controls. The sections and control numbers referenced are from the AS/NZS 7799.2

4.1 Communications and Operations Management domain

4.1.1 (8.1) Operational Procedures and responsibilities

4.1.1.1 (8.1.1) Documented Operating Procedures

Control Objective	Security operating policies and procedures have clearly identified and documented
Reason for audit	Without documented operating policies and procedures, process cannot be formalized and associates may not perform their operation duties in a consistent manner. This may increase of the risks that the systems may become inconsistent leading to data integrity problems.
Tests to be performed	• Review documented policies and procedures • Inquire of operation associates on how they perform tasks • Observe the operation associates on how they perform tasks • Verify that the answers to inquiries and observation results are consistent with the documented policies and procedures The tests should be performed at the minimum on an annual basis.

4.1.1.2 (8.1.2) Operational Change Control

Control Objective	All programs running on the IDPS production systems are subject to change control process, and any changes are subjected to change control authorization.
Reason for audit	Formal change control process help ensure the integrity of the production systems by obtaining proper reviews and authorizations prior to any changes to the systems.
Tests to be performed	• Review the documented change policy and procedures • Inquire of operation associates on the process for applying changes to the systems • Select a sample system and review the change control history documentation (e.g. change log, change activity submissions, etc.) on this system and compare

	against the baseline configuration previously attained • Observe the change control process by sitting in the change control meeting The tests should be performed at the minimum every six months.

4.1.1.3 (8.1.3) Incident Management Procedures

Control Objective	Incident management procedures exist and address: incident management responsibilities; different types of incidents; audit trails and logs maintenance; and proactive actions to prevent incident reoccurrence.
Reason for audit	Formal incident management procedures are imperative for IDPS because the purpose of the system is to detect and prevent security intrusions. Without the formal procedures, the organization may not be able to effective respond to incident in a timely manner, which may lead to business interruption or security breaches that have bottom line impact to the organization.
Tests to be performed	• Review the documented incident management policy and procedures to determine if the documentation includes responsibilities, different type of incidents, log maintenance, and response procedures • Inquire of operation associates the incident response and escalation process • Inquire of management to determine if adequate incident management procedures have be implemented • Review the incident management related documentation, such as history logs, incident reports, etc. The tests should be performed at the minimum every three months.

4.1.1.4 (8.1.4) Segregation of Duties

Control Objective	Duties and areas of responsibilities are clearly defined and segregated to reduce opportunities for unauthorized modification or misuse of information or services.
Reason for audit	Segregation of duties helps ensure the probability of unauthorized changes and misuse of information/services is reduced. There are certain trust levels in the systems administrators; however, this control is a check-and-balance measure.
Tests to be performed	• Review the documented roles and responsibilities for the positions responsible for IDPS • Inquire of operations associates to their responsibilities

	• Observe operations associates on how they perform their tasks • Review the systems configuration and access privileges to ensure check and balances are in place • Select a sample set of audit logs of activities occurs on the systems to determine if any unusual activities took place The tests should be performed at the minimum every three months.

4.2 Access Control domain

4.2.1 (9.2) User Access Management

4.2.1.1 (9.2.1) User Registration

Control Objective	Formal user registration and removal procedures exist for granting access to the systems.
Reason for audit	Formal user registration and remove procedures help ensure that only users authorized have the ability to access the systems. Without the procedures, there is increased in risks that unauthorized may have access to the systems due to reasons such as termination, change in position, or addition without appropriate authorization. This may jeopardize the confidentiality, reliability, and integrity of the systems.
Tests to be performed	• Review the documented user registration and removal procedures • Inquire of responsible associates the process they use for user registration/de-registration • Observe the responsible associates on how they register and de-register users • Review documentation on user registrations/de-registration, such as forms and system audit trails. • Select a sample set of users (active and terminated) and compare against active user account in the system(s) The tests should be performed at the minimum every six months

4.2.1.2 (9.2.2) Privilege Management

Control Objective	Formal authorization process exists for the allocating privileges in the systems. Allocation and use of privileges in the systems are restricted and controls based on need to use basis.
Reason for audit	Sensitive information within the systems must be maintained to help ensure the confidentiality and integrity. Specifically, the information in IDPS may be used to prove or disprove

	security breaches, which may have regulatory compliance implications; therefore, it is imperative that only authorized personnel have access to the information and the systems.
Tests to be performed	• Review documented policies and procedures for allocating privileges in the system • Review the authorization matrix for granting privileges in the system • Inquire of management and associates to determine if the documented policies and procedures are being followed • Select a sample of users with privileges and review supporting documentation (e.g. authorization evidence, documented business reasons for allocation privileges, period review for the applicability of privileges) The tests should be performed at the minimum every six months

4.2.1.3 (9.2.3) User Password Management

Control Objective	Allocation and reallocation of passwords are controlled through a formal management process. Users must acknowledge the passwords are to be kept confidential.
Reason for audit	Passwords often are the first level of protection for getting into the systems. Therefore, it is imperative that the confidentiality of passwords is preserved. Furthermore, the passwords must not be easily guessed.
Tests to be performed	• Review documented policy and procedures on user password management • Inquire of personnel the passwords usage practices • Observe the personnel of the password usage practices • Run password-cracking tools to verify that only strong passwords are used • Review system configuration to ensure strong password policy is implemented, such as password expiration, minimum length, combination of alpha-numeric, etc. The tests should be performed at the minimum every three months

4.2.1.4 (9.2.4) Review of User Access Rights

Control Objective	Formal process exists for reviewing of user access rights on regular basis.
Reason for audit	Due to the sensitivity of the information within the systems, only authorized users should have access to the information. However, the access rights of the users may not always stay

	the same for reasons such as changes of position, changes in the organization, changes in the policies, change in position status, etc. Therefore, periodic review the user access rights help ensures that systems access remains on need to have basis.
Tests to be performed	• Review documented policies and procedures on user access rights review process. • Inquire of personnel how frequent user access is reviewed and for what systems • Review user access review supporting documentation from the past review • Review the existence of user access rights matrix for reasonableness • Randomly select a sample set of users and review their access rights against the access matrix The tests should be performed at the minimum every month.

4.3 Checks for System Improvement

The checklist is used to determine the effectiveness of the system by measuring if the control objectives are met. The test procedures for each of the control objectives are designed to help demonstrate the effectiveness. If any of the test procedures fails, then the control will be reviewed by the Information Security group to ascertain to reason why it failed. By determining the root causes, the policies and/or procedures can be refined to meet the control objectives, thereby improving the system. Additionally, metrics will be developed to help quantify the efficacy of any improvements.

5. Act

The ISMS for IDPS is a continuous process, which it is constantly going through the process life cycle including assessment, establishment, monitoring and measurement, and improvement.

The ISMS has a built-in communication/feedback process where if an incident occurs, the associate who identifies the incident has the communication channel to report the incident to the Information Security group. The Information Security group is in constant communication with the Information Security committee, Risk Management group, and IT Operations group.

The Internal Audit group is responsible for the internal audit of the effectiveness of the ISMS for IDPS on a periodically basis. Ideally, internal audit should be performed every six months. The external audit will be performed by a third party vendor on an annual basis.

The following table describes the steps in maintaining and improving the ISMS developed.

Group	Responsibilities
Information Security steering committee	• Meets periodically (at minimum every quarter) to discuss the effectiveness of the existing ISMS and identify if any new/emerging issues arise • Review and address any feedback received on the ISMS since the last meeting • Review proposals and suggestions, if any, from the Information Security sub-committees; and act accordingly • Delegate new tasks, if any, as appropriate to the Information Security sub-committees • Discuss if any new committee should be formed and/or existing committees should be review of their purpose • Review results from both internal and external audits of ISMS. Assigned tasks force to address any controls that failed the audit
Information sub-committees	• Meets periodically (at minimum every 2 months) to discuss the any issues arise in the implemented ISMS • Review action items from the last meeting and determine if any new items are necessary • Review incidents/activities related to the ISMS occurred from the last meeting and identify improvement opportunities • Make appropriate recommendations on as needed

	basis to Information Security steering committee and Information Security group
Information Security Manager	• Continue to monitor the progress of ISMS • Facilitate committee meetings as appropriates • Prepare overall progress report of ISMS • Facilitate the implementation of mitigation steps, if any, identified in internal and external audits
IT Operations associates	• Report any incidents to the Information Security manager • Ensure appropriate policies and procedures are followed • Work on audit findings, if any, to improve the effectiveness of ISMS
Internal Audit Manager	• Work closely with Information Security Manager and IT Operation associates to test the audit controls for the controls within ISMS • Report to the Information Security steering committee on the audit result
Data Owners	• Receive reports from Information Security steering committee • Provide suggestions to the Information Security steering committee

An example of process for improvement opportunity:

1. Internal Audit reviews the user access rights and identifies exceptions in access privilege to the IDPS log repository.
2. Internal Audit prepares a report, including the audit finding and recommended mitigation steps, including increase the frequency of the user access rights review, reduce the number of administrators who can grant access privilege, and ensure supporting documentation for the privilege access requests are maintained.
3. The report is reviewed by the Audit committee for validation and then forwarded to Information Security steering committee.
4. Information Security steering committee assigns the tasks to Information Security Manager to implemented the mitigation steps.
5. Information Security Manager works the IT Operations associates in implementing the mitigation steps.
6. Information Security Manager verifies the implementation of improved process and reports back to the Information Security steering committee.
7. Information Security steering committee assigned a task to Internal Audit to perform an audit to verify the audit finding is indeed closed.
8. Internal audit to report the results back.

6. Conclusion

The main goal of this exercise is to establish a repeatable process so that other systems can be added to the overall organization's ISMS. The same process used to develop the ISMS for IDPS can be extended to other areas of the organization.

This practical assignment described the steps in the process used to develop ISMS for IDPS:

1. Define the scope of system and relevance
2. Establish a high level project plan/timeline
3. Identify ISMS management structure
4. Develop high level policies
5. Identify and classify assets
6. Establish risk management cycle
7. Identify gaps
8. Remediate gaps
9. Establish checks for the system
10. Perform continuous monitoring and improvements

The next step for the organization is to apply the process to other systems and establish controls so that the Information Security Management System can cover the critical information assets. The ultimate goal is for the organization is to be ISO17799 compliant.

Appendix A – Acronyms

CAO	Chief Administration Officer
CEO	Chief Executive Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
COO	Chief Operations Officer
CRO	Chief Risk Officer
DMZ	De-militarized Zone
FTC	Federal Trade Commission
GLBA	Gramm-Leach-Bliley Act of 1999 (also known as Financial Modernization Act of 1999)
IDPS	Intrusion Detection and Prevention Systems
ISMS	Information Security Management System
IT	Information Technology
NPI	Non-public personal information
PDCA	Plan, Do, Check, Act

Appendix B – References

1. SANS Institute Track 11 – SAN 17799 Security and Audit Framework course material.

2. Carl L. Pritchard. Risk Management Concept and Guidance, Virginia: ESI International, 2001.

3. UCI Extension. Project Risk Management MGMT X474.1 course material.

4. A Guide to the Project Management Body of Knowledge (PMBOK Guide) -- 2000 Edition. Project Management Institute.

5. Information Security Guideline for NSW Government - Part 2. Department of Commerce, Office of Information and Communications Technology.