# EXECUTIVE SUMMARY

The State Administrative Manual (SAM) requires each state agency to conduct a comprehensive risk assessment of its information assets every two years and or when ever there is significant change in the agency’s use of information technology. To comply with this requirement, the <DEPARTMENT'S NAME> formed a committee to assess the risk management practices of <DEPARTMENT'S NAME> information assets. The risk assessment was conducted from MONTH/DAY/YEAR to MONTH/DAY/YEAR using the Facilitated Risk Analysis Process.

In conducting the risk assessment, the committee and the participants reviewed and assessed the organizational and management practices, personnel practices, data security practices, information integrity practices, software integrity practices, and personal computer practices of each of the <DEPARTMENT'S NAME>. The committee and the participants noted the following general weaknesses in the department's risk management practices.

## Organizational and Management Practices:

Problem: Most of the branches of the <DEPARTMENT'S NAME> do not have information security policies and procedures for their databases. This has a potential threat of unauthorized access to the department’s databases and improper dissemination of confidential and or sensitive information. Such access and dissemination of confidential and sensitive information could result in lawsuits, increased complaints from the insurance consumers, producers and employees.

Recommendation: To protect <DEPARTMENT'S NAME> information assets, each branch should develop policies and procedures for accessing its databases and disseminating confidential and or sensitive information assets.

## Personnel Practices:

Problem: Employees do not sign any acknowledgement, which deals with security policies, and procedures for new, transferred and terminated employees. Further, employees of the department have not received the annual training in information security and privacy risk management practices. Because employees have not been trained in <DEPARTMENT'S NAME> risk management practices and do not sign acknowledgement of security policies and procedures, they may not be held accountable for any improper actions. Untrained staff may also make incorrect changes to the databases.

Recommendation: To correct the above weaknesses, each <DEPARTMENT'S NAME> branch should provide training in information security and privacy policies and procedures for its databases. The training can be provided by the Information Security Officer and coordinated with the Branch. Additionally, each employee should sign an acknowledgement of the receipt of <DEPARTMENT'S NAME> security policies and procedures.

## Physical Security Practices:

Problem: While there is an adequate physical security for entry to the work areas of most branches, physical security for entry into the work areas of a few branches is not adequate. As a result, the equipment as well as the databases of these branches is not adequately protected from potential theft, damage or destruction.

Recommendation: To protect the equipment, these branches should install electronic keylock entry system. Ideally a centralized security system housed in Sacramento with decentralized administration within the three main department sites will address this situation and provide reports to management. Such a system will range from $250,000 or more to implement.

## Data Security Practices:

Problem: User passwords are not periodically changed. E-mail messages and attachment are not secure and employees are not aware that their E-mails are not secure. The H:\ (“personal”) network drive for each employee is accessible to unknown number of persons at the IT Branch without a known tracking system.

The loss of E-mail messages could result in loss of productivity and loss of access to incoming and outgoing mail. Without a tracking system, a number of IT Branch personnel could gain access to the branch’s database without a record of the event on who gained access.

Recommendation: The department should implement policies and procedures that require changing passwords at least quarterly. The department should also develop and implement policies and procedures delete generic”/guest” passwords, inform employees about lack of security inherent in E-mails and provide alternative means of communicating confidential and sensitive information. A tracking system should be developed to record access of IT Branch personnel to the “H” drive of the users.

## Information Security Practices:

Problem: Some of the branches do not have established policies and procedures to control data input and output and users of the databases are not provided training in quality control. Further, these branches do not have a central library for reports and data. As a result the following range of problems may occur: (a) lack of uniformity of data, (b) incomplete data or redundancy of data, (c) potential loss of funding due to dissemination of inaccurate data, and (d) faulty data may result in erroneous analysis of the data.

Recommendation: To address these deficiencies, each branch should develop and implement data quality policies and procedures, and a user’s guide on data quality assurance. Finally, each branch should maintain a central library for its reports.

## Software Integrity Practices:

Problem: Some of the branches do not provide adequate training in software integrity practices. In addition, some branches do not have appropriate documentation for their software packages to enable their staff to fully utilize the software. Further, there is a potential for unlimited access where users can change databases tables and functions. These deficiencies can result in loss or corruption of data, damage to database functionality; and loss of time and resources while reconstructing the database.

Recommendation: To correct the deficiencies, the IT Branch should provide a developer’s kit for the programmers or allow a client server platform upon which to run the program. Each branch should provide training in software integrity practices and appropriate documentation for their software packages to enable their staff to fully utilize the software.

## Personal Computer Practices:

Problem: <DEPARTMENT'S NAME> branches do not have established policies and guidelines for password protocol. This protocol requires periodic changes to password and employees to turn off their computers at the end of every day. Additionally, the guidelines can address regulating the storage of highly classified (on the network or local drive) or confidential information. Finally, the branches do not provide training or highlight the consequences for downloading information or programs from the Internet.

The range of threats noted above are: (a) unauthorized access to the database, (b) manipulation or loss of data; (c) compromise of password security allowing access to the computer as well as confidential and sensitive data, (d) download of information to the network or local drive could contain a virus and infect the entire network.

Recommendation: To correct the above deficiencies, each branch should develop a training plan regarding password protection and system vulnerabilities. That plan can address the consequences of downloading information or programs from the Internet. Ideally the IT Branch network administrators should have a tool that monitors what information is downloaded and what programs are on the local drive of the users. To implement this type of monitoring system will cost $120,000 or more depending on the site license agreement.