State of California
State Information Security Office

Guide for the Role and Responsibilities of an Information Security Officer Within State Government

October 2007

Table of Contents

Introduction 3
The ISO in State Government 4
Successful ISOs – Necessary Skills and Abilities 7
Twelve Components of an Effective Information Security Program 9
The ISO Role and Responsibilities in Each Component 11
Risk Management 12
Security Policy Management 16
Organizing Information Security 19
Asset Management and Protection 23
Human Resources Security 26
Physical and Environmental Security 29
Communications and Operations Management 32
Access Control 38
Information Systems Acquisition, Development, and Maintenance 41
Information Security Incident Management 44
Disaster Recovery Management 48
Compliance 50
Conclusion 53
Glossary 54

Introduction

Each agency must identify and implement information security policies, standards, guidelines, processes, procedures, and best practices to further strengthen its security program to protect its information assets while assuring its goals and objectives are being met. Typically, the Information Security Officer (ISO) manages an agency's information security program. The Information Security Program has five important objectives:

1. Protect the agency's information and information processing assets.
2. Manage vulnerabilities within the information processing infrastructure.
3. Manage threats and incidents impacting the agency's information resources.
4. Assure through policy the appropriate use of the agency's information resources.
5. Educate employees about their information security and privacy protection responsibilities.

The Guide for the Roles and Responsibilities of an Information Security Officer Within State Government provides a state agency and the ISO general guidance and assistance in understanding the ISO role and responsibilities in developing and maintaining an effective information security program. This Guide closely aligns with the State Information Security Office's (SISO) *Information Security Program Guide for State Agencies* and drills down into more detail about the important role of an agency ISO. Agency ISOs should become familiar with both of these Guides as it will assist them in implementing a strategy for an effective information security program.

The SISO is grateful to the many agency ISOs and other security professionals who have provided their input to shape the content of this Guide.

The ISO in State Government

All state agencies are to designate an ISO to oversee the agency's compliance with information security requirements. This section provides the authority for ISO designation, and reporting structure and level, beginning with the following outline of the policy and legal requirements for state agencies to have a designated ISO.

Applicable State Policy
State policy as stated in the State Administrative Manual (SAM) requires all state agencies to designate an ISO. Applicable SAM and Statewide Information Management Manual (SIMM) sections include:

Excerpts from SAM Section 4841.1

Executive Management–The agency director has ultimate responsibility for information technology security and risk management within the agency. On an annual basis the Director of each state agency must submit a Department Designation Letter (SIMM Section 70) designating critical personnel. See SAM Section 4845. Each year, the agency director must certify that the agency is in compliance with state policy governing information technology security and risk management by submitting the Risk Management Certification (SIMM Section 70). See SAM Section 4842 and 4845. The Director must also transmit each year an updated copy of the agency's Operational Recovery Plan or Operational Recovery Plan Certification (SIMM Section 70) to the Department of Finance. See SAM Sections 4843.1 and 4845.

Information Security Officer–The Information Security Officer (ISO) is required to oversee agency compliance with policies and procedures regarding the security of information assets. **The ISO must be directly responsible to the agency director for this purpose and be of a sufficiently high-level classification that he or she can execute the responsibilities of the office in an effective and independent manner.** It is acceptable to create this reporting relationship on a functional basis rather than reorganize the department. To avoid conflicts of interest, the ISO (for agencies other than state data centers) should not have direct responsibility for information processing, technology operations, or for agency programs that employ confidential information.

Excerpts from SAM Section 4841.2

Oversight responsibility at the agency level for ensuring the integrity and security of automated files, databases, and computer systems must be vested in the agency Information Security Officer.

Excerpts from Sam Section 4845

Designation of Information Security Officer and Operational Recovery Coordinator - Due by January 31 of each year, or as designee changes occur. The director of each agency must designate and provide contact information for the agency's Information Security Officer (ISO) and the Operational Recovery Coordinator using the Agency Designation Letter (SIMM Section 70A). Upon the designation of a new ISO and/or Operational Recovery Coordinator, the agency must submit an updated Agency Designation Letter to Finance within ten (10) business days. See SAM Section 4841.1.

Incident Follow-up Report - Each agency having ownership responsibility for the asset (SAM Section 4841.4) must complete an Agency Information Security Incident Report

(SIMM Section 65C, formerly SIMM Section 140) for each incident. The report is signed by the agency's director, **Information Security Officer,** and Privacy Officer if needed. Submit the report to the Department if Finance (Finance) within ten (10) business days from the date of notification.

Several ISO responsibilities identified in SAM further demonstrate the need for this position to be at a sufficiently high and policy influencing level. These include, but are not limited to, the following:

- Establish security policies and procedures (as inferred in SAM section 4841.7, subsection 2).
- Approval of proposals to use desktop or laptop computers to maintain or access files containing confidential or sensitive data as defined in SAM 4841.3. (SAM section 4842.2, subsection 7).
- Determine aforementioned proposals comport with all provisions of SAM information security and risk management sections (SAM sections 4840 through 4845).
- Approval for the use of alternatives to encryption for the protection of confidential, personal and sensitive information stored on portable electronic storage media and portable computing devices. (SAM section 4841.2, subsection 2, e, 7).
- Approval of any business use of peer-to-peer technologies (SAM section 4841.2, sub-section 4).

Applicable State Statutes

The California Information Practices Act (Civil Code Sections 1798 et.seq) of 1977 requires the following by state agencies:

- Establishment of rules of conduct for employees who handle individual's personal information and training on those rules (Civil Code section 1798.20).
- Establishment of appropriate administrative, technical and physical safeguards for properly securing individual's personal information (Civil Code section 1798.21).
- Designation of an employee responsible for ensuring the agency complies with all provisions of the Act (1798.22).

The latter provision is met by the designation of an ISO and/or a Privacy Officer. Some agencies designate an Privacy Officer in addition to an ISO since there are many other provisions of the act which deal with other types of individual privacy requirements (e.g., administrative procedures related to the collection, use and disclosure of personal information). For example, these other provisions include, but are not limited to the following:

- Limiting the collection of personal information (1798.14)
- Limiting access and disclosure of personal information (1798.24)
- Providing proper notice at the time of collection (1798.17)
- Ensuring proper record keeping of the source, authority and business purpose for personal information collected (1798.15 -1798.16)
- Ensuring proper record keeping of disclosures of personal information (1798.25)
- Ensuring the use of personal information is consistent with the purpose stated at the time of collection

- Ensuring appropriate information handling procedures are established and enforced (1798.20)

While there appears to be some overlap in Privacy Officer and ISO roles; an important distinction is that a Privacy Officer's emphasis is on individual privacy protection and ensuring the privacy policy requirements in Government Code 11019.9 are met; whereas, the ISO must be concerned with all aspects of security (confidentiality, integrity, and availability), not just the individual privacy (confidentiality) component.

It is also worth noting that the ISO position was specifically referenced as being required by statute (Government Code section 11771). However, this section also contained the authority creating the Department of Information Technology (DOIT). Consequently, it was repealed with the elimination of DOIT.

Reporting Structure and Level

The agency ISO must report directly to the Director. When an ISO reports outside the Director, there can be conflict when/if the ISO must take a position on security which is not aligned with his/her direct report (e.g., what is proposed is not in compliance with security laws or policies or places the organization at significant risk but direct report wants ISO to approve). If the position must report to someone other than the Director, it is recommended it be to someone at a Deputy Director level who has and will support an ISO's direct access to the Director when it is needed. Pursuant to the requirement in SAM, the position must have the ability to carry out his/her duties in an effective and independent manner.

The ISO position should be, at a minimum, equivalent to the level of the Chief Information Officer (CIO) within the organization due to the inherent conflict between these two positions. Additionally, the ISO position should not be a rank and file position (such as the information systems analyst-specialist classification), as it can be difficult to deal with confidential investigations involving employees. It is best when these two positions both have the same direct report (the Director); however, our experience is that it can work on a functional basis when the CIO reports to the Deputy Director of one Branch and the ISO reports to the Deputy Director of another Branch within the organization and both Deputy Directors of the two Branches report directly to the Director.

It is our experience, that when ISOs are placed at lower levels in the organization they cannot be effective for a number of factors, the most significant is the lack of authority and respect for the position they will need.

Successful ISOs – Necessary Skills and Abilities

Successful ISOs must have a broad range of business management and technical security skills. Possessing a background in the development and subsequent enforcement of security policies and procedures, security awareness programs, business continuity and disaster recovery plans, information technology, auditing, and applicable industry and governmental compliance issues is critical. They must be savvy in understanding the business needs of an agency and be fully supportive of its mission and goals. Some areas where an ISO must possess adequate skills and abilities include:

- **Strategic** - An agency ISO must understand the agency's program areas and business needs and their role within the activities of the agency. The ISO must keep abreast of evolving technologies to ensure appropriate security controls are implemented and maintained as agency processes change. Identifying security risks to the agency and being able to evaluate and recommend appropriate security measures, from a strategic perspective, will help management understand the risks and the need to reduce them to acceptable levels.

- **Management and communication skills** - The ability to effectively communicate, both verbally and in writing, across all levels of management and the user community cannot be understated. The need to interact with critical staff (such as executive management, the Privacy Officer, the Chief Information Officer, and the disaster recovery coordinator) and other agency business units (such as the legal, human resources, IT, procurement, business services, facilities management offices) to cooperatively achieve the goals is critical to the success of the information security program.

  The ability to write effectively, to explain information security in layperson terms, can be difficult. Security can be a dry subject and hard to understand, especially as it relates to technology. Executive management may not understand why a certain security component costs so much, or why it is important to the agency's goals. Possessing the ability to effectively develop issue papers, memorandums, letters, work plans, and other types of written communication can be invaluable in documenting security concerns and decisions, and in explaining important perspectives.

- **Technical Competence** - ISOs are required to have a certain level of technical competence to lead their organization's security initiatives. They need a general knowledge of how technical issues affect the business of the agency. It is very difficult for a security leader to be respected by their agency, regardless of size, without having a proper grasp of the technical security issues that affect it. Further, it would be difficult to garner the respect of the other technical staff within the organization without that knowledge.

Being passionate about information security is critical to the success of the program. If an ISO is not fervent about it, he or she may find that is not the right career choice for them. Those ISOs that are fanatical about it should recognize that there is sometimes a fine line between passionate and obsessive. An important function of the ISO is to not always say, "NO!" but to find secure ways to implement technologies while carefully weighing the risks against the business needs of the agency.

Training Suggestions:
The following training is recommended for new ISOs, or those security individuals wanting to enhance their existing information security skills and the effectiveness of an agency's information security program. These types of courses and certification programs are offered through a variety of training contractors/vendors/associations, many of whom specialize in information security.

1. **Basic information security training** classes such as Introduction to Information Security or Security Essentials. These courses focus on security for the individual who may have basic computer skills and knowledge but is new to information technology and security.

2. **Management and leadership** classes such as leadership and management courses, security leadership essentials for managers, effective writing and communication courses, security policy and awareness, fundamentals of information security policy, security awareness training for trainers, project management, and classes that focus on the ISO/IEC 27002 (formerly ISO 17799) Framework. These types of classes help in developing skills for creating and managing security policies, implementing a solid security awareness program, and obtaining support from executive management.

3. **Legal courses in security** such as IT and information security legal issues, HIPAA implementation, contracting for data security, and laws involving fraud, misuse, and unauthorized use. These classes help an ISO understand the legal implications of information security and electronically stored and transmitted records.

4. **Technical security** classes such as hacking and network security and critical infrastructure protection. For ISOs to be effective, they need to understand the technical threats, vulnerabilities, and problems and be able to apply security solutions to mitigate those risks.

   NOTE: Any technical security courses are recommended to develop a better technical knowledge and understanding of the various facets of security. The better the knowledgebase, the better the understanding an ISO will have when dealing with or working with technical staff.

5. **Audit** classes such as IT audit and control fundamentals, meeting the minimum standards for protecting private information to aid in the fundamentals and facets of auditing, and the tools available to conduct an audit or review.

6. **Certifications** – Attaining a reputable certification, (i.e., Certified Information Systems Security Professional (CISSP), Microsoft Certified Systems Administrator (MCSA) Security+, Certified Information Systems Auditor (CISA), Certified Internal Auditor (CIA)), is an indication of the professional knowledge and self-motivation that executives appreciate in their security leaders. This is an avenue where an ISO can gain the confidence of the agency's upper level managers.

Twelve Components of an Effective Information Security Program

The *Information Security Program Guide for State Agencies* has been developed by the State Information Security Office (SISO) to assist agencies in developing an information security program or enhancing their existing program. The Guide identifies the twelve key components that should be considered when implementing, reviewing, or seeking to improve the value of its program and provides guidance to:

- Further strengthen or aid in the development of an agency's information security program needed to protect the integrity, availability, and confidentiality of agency data and safeguard information assets and resources.
- Identify processes and techniques that promotes secure communications and the appropriate protection of information among agencies.
- Establish a common information security program framework and format consistent across state agencies with different business needs.

An important component of an effective information security program is implementing an information security governance structure. This structure can be accomplished through an existing executive committee or creation of a governance body within the agency and should be comprised of business and information technology (IT) representatives. It is an essential process where the ISO informs and advises executive, business, and IT management on security plans, operations and metrics to ensure the Information Security Program adapts to the evolving business needs of the agency.

As outlined in this Guide, there are twelve key components that should be considered by an agency when implementing, reviewing, or seeking to improve the value of its information security program. These components should be reviewed for applicability to an agency's business environment and compliance with existing laws and policies, and implemented as appropriate for each agency. Some agencies may not require all components, but where a component is applicable to an agency's program, it should be assessed for adoption and implementation. The key components are:

1. Risk Management
2. Policy Management
3. Organizing Information Security
4. Asset Protection
5. Human Resource Security
6. Physical and Environmental Security
7. Communication and Operations Management
8. Access Control
9. Information Systems Acquisition, Development and Maintenance
10. Incident Management
11. Disaster Recovery Management
12. Compliance

Together these components provide a framework for developing an agency's information security program, which must be a business core value of the organization. The components provide value to an agency's business by ensuring the reliability, integrity, and confidentiality of the information used by the agency and improves the robustness of an agency's technology

infrastructure overall. A successful information security program supports business and aligns with the agency's mission, goals and objectives.

The *Information Security Program Guide for State Agencies* is available on the SISO's Web site at www.infosecurity.ca.gov/ and should be reviewed for additional details regarding the implementation of a successful information security program.

The ISO Role and Responsibilities in Each Component

This Guide identifies the twelve components of an effective information security program and the ISO's suggested role in accomplishing them. Authority, relationship and interfaces, along with a list of references and tools, are included at the end of each component section. It provides a standard structure for defining the role and responsibilities for the ISO. Four types of activities have been identified:

Planning – Identify an annual work plan to achieve security goals and objectives consistent with the agency's strategic plan.

Developing – Lead in the development of information security policies, standards, guidelines, processes, and procedures.

Managing – Conduct risk assessments, manage incidents, provide internal and external reporting, involvement in security awareness education and training, and

Oversight – Evaluate the effectiveness of ongoing security operational processes, monitor compliance for internal and external requirements (e.g., laws, regulations, statutes, state policy, etc.).

The following chart identifies the twelve information security components that should be included in an agency's Information Security Program and the ISO's role in the planning, developing, managing, and oversight of each of the components.

Information Security Program Components	**ISO Role**			
	Planning	**Developing**	**Managing**	**Oversight**
1. Risk Management	L	L	L	L
2. Security Policy management	L	L	L	L
3. Organizing Information Security	L	P	P	L
4. Asset Management and Protection	P	P	P	L
5. Human Resources Security	L	P	P	L
6. Physical and Environmental Security	P/L	P/L	P/L	L
7. Communications and Operations Management	P	P	P	L
8. Access Control	L	P	P	L
9. Information Systems Acquisition, Development and Maintenance	P	P	P	L
10. Information Security Incident Management	L	L	P/L	L
11. Disaster Recovery Management	L	P	P	L
12. Compliance	L	L	L	L

L= LEADER
P= PARTICIPANT

Note: Where the ISO is a Participant in the process, management must identify a Leader who has the appropriate skill set and program responsibility based on the structure of the organization.

Risk Management

Risk Management refers to the process of identifying risk, assessing it, and taking steps to reduce it to an acceptable level. A risk management program is an essential management function and is critical for any agency to successfully implement and maintain an acceptable level of security.

The ISO leads the planning, developing, managing, and oversight efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 1	ISO Role and Responsibility
Risk Management **Objective:** To identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the agency. • Develop and maintain a risk management program • Conduct risk assessment/analysis every two years. The resulting strategies should have a direct relationship with the disaster recovery priorities. • Mitigate security risks	**1.1 Risk Management Program:** Create a formal process to address risk through the coordination and control of activities regarding each risk. **1.2 Risk Assessment:** Conduct formal vulnerability assessments of the agency environment on a regular basis. **1.3 Risk Mitigation:** Create a formal process to mitigate vulnerabilities.

1.1 Risk Management Program

Risk management is the process of identifying risk, assessing it, and taking steps to reduce it to an acceptable level. Although the overall purpose of risk management is to identify and avoid or minimize (mitigate) the impact of threats to information and technology assets, the main goal of the program should be to protect the agency and its ability to perform its mission, not just its IT assets.

Each agency must provide for the proper use and protection of its information assets. Accordingly, agencies should assign the management responsibilities of the risk management program to a unit or individual. SAM Section 4842.2 requires that each agency provide a minimum of the following practices:

- Organizational and Management
- Personnel
- Physical Security
- Data Security
- Information Integrity
- Software Integrity
- Personal Computer Security

An effective risk management program should also mitigate risks associated with:

- Network security practices (SAM Section 4842.1)

- Threat management (SAM Section 4842)
- Disaster/operational recovery (SAM Section 4843)
- Appropriate use

In addition, the risk management program must be designed to:

- protect all IT resources and information (both electronic and paper based) from unauthorized use, access, modification, loss, or destruction, or disclosure;
- ensure the physical security of the agency's resources;
- provide and maintain a documented disaster recovery plan;
- ensure current policies and procedures are maintained regarding federal, state, and departmental mandates and guidelines;
- identify, assess, and respond to the risks associated with information assets;
- prevent misuse or loss of state agency information assets by establishing and maintaining a standard of due care; and,
- preserve the ability to meet program objectives in the event of the unavailability, loss or misuse of information assets by establishing and maintaining cost-effective risk management practices.

ISO Role

The ISO has agency-wide oversight responsibilities to ensure that policies, standards, guidelines, processes, and procedures are in place to support the risk management program. There are well documented risk management guidelines that provide the essentials for establishing an effective program.

The components of the program include risk assessment, mitigation, and evaluation. Risk assessment determines the potential threats and associated risks; risk mitigation is the process of identifying, prioritizing, evaluating, and implementing risk reduction controls; and evaluation is an ongoing and evolving process that integrates the System Development Life Cycle (SDLC) in existing and new systems. The same level of review and analysis must be applied to operational processes, in addition to existing and new application systems, because the agency's production work is performed through ongoing processes.

The ISO is responsible for the risk management program, with a primary focus on the integrity and security of automated files, databases, computer systems, and information (electronic and paper). In addition, the ISO ensures that the agency has the appropriate policies and procedures required to be in compliance with applicable laws, regulations, and state policy.

1.2 Risk Assessment

In order to have an effective risk management program, the agency must know what it is that should be protected. The risk assessment is considered one of the first processes to be performed when establishing a risk management program. The final product of the risk assessment is a report that is to be kept on file within the agency; documenting the process used and the outcome of the risk assessment; the proposed security management measures to reduce the identified risks (see risk mitigation 1.3); the resources necessary for security management; and, the amount of remaining risk to be accepted by the agency.

In order to properly perform a risk assessment, each agency must establish a risk analysis process and carry it out with sufficient regularity in order to provide a realistic response to

current risks (this action can be contracted). A critical step in this process is to identify and evaluate the risks and risk impacts, and recommend risk reducing measures. Agencies must complete the comprehensive risk analysis cycle at least every two years, or whenever there has been a significant change in the use of information technology. Included in this process are activities known as penetration and social engineering tests. The penetration activities will test the systems' (settings, versions, patches, etc.) vulnerabilities against electronic compromise efforts. Penetration testing does not constitute a risk assessment. This type of testing typically analyzes risks that can be exploited externally and does not include internal operational processes. Social engineering tests will evaluate the employee level of security awareness and adherence to established policies, procedures and processes.

ISO Role

The ISO has agency-wide oversight responsibilities to ensure that the risk assessment and analyses are thorough and complete. The risk assessments or analysis may be performed by agency staff or outsourced. The ISO oversight is essential to ensure the assessment/ analysis is performed, that senior management is provided the results along with recommended mitigation measures, that the agency determines the acceptable level of risk, and that the approved risk reduction measures are implemented. The ISO is responsible for the following:

- Coordinate the assignment of responsibilities for risk assessment with appropriate participation of executive, technical, and program management;
- Identify threats to which the information assets could be exposed;
- Participate in the assessment of vulnerabilities (i.e., the points where information assets lack sufficient protection from identified threats);
- Determine the probable loss or consequences (based upon quantitative and qualitative evaluation);
- Identify and estimate the cost of protective measures which would mitigate the vulnerabilities to an acceptable level and recommend the cost-effective measure to be implemented; and,
- Prepare and submit to the agency director and senior management a report documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining (residual) risk identified as acceptable to the agency.

1.3 Risk Mitigation

Upon completion of the risk analysis, there will be a list of vulnerabilities requiring decisions that will be taken to lessen (mitigate) the impact of these vulnerabilities. Each agency should have a formal process in place to document those decisions and actions taken to mitigate vulnerabilities. These documented results demonstrate the due diligence efforts on the part of management and provide evidence required during audits that the agency is adhering to state and federal requirements.

ISO Role

The ISO has agency-wide oversight responsibilities to ensure that mitigation efforts are thorough and complete and that executive management is aware of and approves the residual risk. The ISO must be actively involved and oversee the efforts of staff involved in the mitigation efforts, even though these efforts may cross over to different units and

divisions within the agency (program services, human resources, etc.) Critical areas where the ISO should be heavily involved include, but are not limited to:

- Lead an effort to establish and coordinate an incident response plan (Refer to Section 10, Information Security Incident Management.)
- Lead the oversight efforts for disaster recovery planning and participate in the testing and documentation of issues and resolutions. (Refer to Section 11, Disaster Recovery Management.)

Authority	Relationship/Interfaces	References/Tools
• SAM Sections 4840-4842 • State FISMA	• Executive Management • Legal Office • Human Resources/Labor Relations • CIO • Equal Employment Opportunity Officer • Privacy Officer/Coordinator	• SISO's Risk Assessment Toolkit- www.infosecurity.ca.gov/tools/ • National Institute of Standards and Technology (NIST) Risk Management Program – http://csrc.nist.gov/ • ISO/IEC 27002

Security Policy Management

Policy Management refers to the practices and methods used to create and maintain security policies to translate, clarify, and communicate management's position on high-level security principles.

The ISO leads the planning, developing, managing, and oversight efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 2	ISO Role and Responsibility
Security Policy Management **Objective**: To provide management direction and support for information security in accordance with business requirements, relevant laws and regulations, and state policy. • Create, issue, and maintain security policies, standards, guidelines, processes and procedures	**2.1 Executive Communication:** Provide management advice and recommendations for the agency's information security program. **2.2 Policy Development:** Develop and maintain security policies, standards, guidelines, processes and procedures. **2.3 Policy Compliance:** Oversee the monitoring and compliance with policies, standards, guidelines, processes and procedures. **2.4 Employee Acknowledgements:** Create a security policy acknowledgement process.

2.1 Executive Communication

Security policies are the agency's core business principles that provide guidance to all employees about information security and privacy. Communication with the executive management is essential to ensure issues are elevated, discussed, and the appropriate approvals and support for policies are obtained. The agency should have in place a governance structure, such as an information security committee led by the ISO, to act as the governing body for providing advice and recommendations regarding information security policies, standards, guidelines, processes and procedures.

ISO Role

The ISO serves as the primary interface with the executive management on matters of information security and is responsible for:

- Coordinating a governance structure responsible for developing, reviewing, approving new or revised policies, standards, guidelines, processes and procedures.

- Providing updates on existing or pending laws, regulations, or statewide policies, security issues or incidents, and the potential impact to the agency.

2.2 Policy Development

Security policies should be one of an agency's core business principles that provide guidance to all employees communicates management's position on high-level security principles, and protects the agency from potential legal and civil harm. Policy management includes the development, documentation, issuance and maintenance for compliance with federal and state laws, regulations, and mandates. A successful policy must be independent of specific hardware and software decisions to adapt to changes in an agency's business environment.

To be practical and effective, specific policies should be applied to an agency's environmental and operational business and supported through standards, guidelines, processes and procedures.

ISO Role

The ISO develops, communicates, updates, and assists management in the enforcement of agency security policies. Developing and updating policy should be a joint effort with the ISO and the governance structure. The governance membership should represent key business functions across the organization. This process ensures that the agency security policies are in alignment with the core business processes. Responsibilities include, but are not limited to:

- Develop and document a formal process for creating, updating, and adopting security policies. This process should include reviews by the agency's Legal Office, Human Resources Office, Equal Opportunity Office, Privacy Officer, and the Chief Information Officer and other key stakeholders;
- Create a governance committee and develop a charter, identify roles and responsibilities, and set goals and objectives; and,
- Schedule regular meetings with the committee to discuss security policy, standards, guidelines, processes, procedures, and issues.

2.3 Policy Compliance

Compliance refers to the process of ensuring conformity to applicable federal and state statutory, regulatory, and contractual requirements and verifying adherence to statewide reporting requirements. Agencies should implement internal procedures to ensure compliance requirements are met, organizational records are protected, and controls are in place and must adhere to all applicable laws, regulations, statutes, and statewide policy.

ISO Role

The ISO oversees agency compliance with the security policies, standards, guidelines, processes, and procedures. It is important that the ISO establish cooperative relationships with management, data owners, data custodians, and information users. The ISO responsibilities include, but are not limited to:

- Review existing internal controls in place to monitor and report exceptions or violations and prepare reports of findings;

- Recommend improvements or oversee the development of controls necessary to monitor compliance;
- Provide executive management and the committee with status reports and updates regarding compliance;
- Review reports of technical violations or alerts that are recorded in logs to ensure they are appropriately addressed;
- Review and report how incidents or threats (such as unauthorized access, misuse, modification, duplication, or disclosure of information) are handled and controlled for compliance; and,
- Review the state reporting compliance requirements and ensure they are met. (See SAM Section 4845).

2.4 Employee Acknowledgements

There are various types of acknowledgements an agency should consider implementing. Agencies should implement banners on all systems, which acknowledge the expectations of use. Additionally, agencies should require all employees to sign a security acknowledgement form that notifies them of their responsibilities regarding the use of the agency's resources. Before acknowledgement forms are signed, employees should be provided security and privacy awareness training that informs them of the acceptable use policies and their responsibility to adhere to them.

The language in the acceptable use banner, displayed at logon, typically informs employees that: 1) monitoring is in place to detect unauthorized use, 2) the system being accessed is owned by the agency, 3) there should be no expectation of privacy, and 4) unauthorized access is not permitted. The employee should be required to acknowledge the banner message to continue with the logon process. Similar language should be used in the agency's employee acknowledgement form.

ISO Role

The ISO oversees agency compliance with information security acknowledgement processes and should ensure the process includes the use of acceptable use banners and an employee acknowledgement form.

Authority	Relationship / Interfaces	References / Tools
SAM 4840-4845	• Executive Management • Governance Committee • CIO • Privacy Officer/Coordinator • Human Resources/Labor Relations • Legal Office • Business Services Unit • Program Areas	• SISO's Information Security Program Guide – www.infosecurity.ca.gov/ • Sample Banner Language – www.infosecurity.ca.gov/library/ • NIST SP 800-100, 800-12, & 800-53 - http://csrc.nist.gov/ • SANS Security Policy Project – www.sans.org/resources/policies/#template • ISO/IEC 27002

Organizing Information Security

A governance structure is essential to organizing information security within and across the organization. Governance maintains balance between the value of information security, the management of security-related risks, and increased requirements for control over information.

The ISO leads the planning and oversight and participates in developing and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 3	ISO Role and Responsibility
Organizing Information Security **Objective**: Managing information security within the organization • Management commitment • Information Security Program • Governance structure • Security agreements and contract language	**3.1 Information Security Program:** Establish and implement a security program that aligns with the agency's business, mission, goals, and objectives. Establish a governance framework for communicating and coordinating security activities **3.2 Independent Reviews:** Implement a strategy for independent reviews at planned intervals. **3.3 Confidentiality or Non-Disclosure Agreements:** Oversee the development and process for the implementation of these agreements. **3.4 Third Party Agreements:** Establish security language to be included in the contracts and agreements.

3.1 Information Security Program

Management must establish a governance framework for the implementation of an effective information security program within their agency that aligns with its business, mission, goals, and objectives. Further, management should designate an individual to fulfill the role of the ISO, who is directly responsible to the agency director for this purpose, and who should possess professional qualifications, including the training and experience required to administer an information security program. This governance framework should involve cooperation and collaboration of agency representatives from applicable business areas, such as legal, human resources (labor relations), business services, equal employment opportunity, privacy officer, chief information officer, and program areas.

ISO Role

The ISO is responsible for establishing and implementing an information security program and establishing the governance structure for communicating and coordinating security activities. In some cases, the coordination may include planning, developing, managing,

and oversight depending upon the activities. The ISO coordination activities might typically include:

- Lead or participate on committees and workgroups to provide information security guidance and direction;
- Ensure that security activities are in compliance with laws, regulations, state policy, and internal information security policies;
- Ensure that processes for non-compliance exist and are functional;
- Ensure that information security training, education, and awareness is provided throughout the agency; and,
- Provide reports to management on the program's adequacy and effectiveness.

3.2 Independent Reviews

The ability to conduct independent reviews and assessments to ensure the continuing suitability, adequacy, and effectiveness of an agency's approach to managing information security is critical. Security compliance validation reviews provide an in-depth examination of the agency's security program infrastructure, policies, and procedures. Independent reviews are needed to provide individuals who are responsible for the agency's information systems, as well as executive management, with an independent assessment of the security condition of those systems. Management should support these efforts to ensure investment in information security continues to align with the agency's business program strategies and objectives.

ISO Role

The ISO should be actively involved in conducting routine independent reviews of information security. These reviews may be done in collaboration with other applicable units, such as internal auditors or other information technology management. The ISO activities may include:

- Conduct or assist in reviews and assessments on regularly planned intervals. These reviews and assessments may only apply to specific incremental changes (such as the implementation of a new system or change in the networking environment) or may be larger in scope depending upon the situation;
- Discuss mitigation strategies with appropriate staff; and,
- Provide the review results and the mitigation plan with agency management.

3.3 Confidentiality Or Non-Disclosure Agreements

In many situations, there may be a need to establish confidentiality or non-disclosure agreements with certain entities and applicable employees to protect confidential information provided to them as part of the agency's business with that entity. It is important that these agreements be established, using legally enforceable terms, to ensure the individual understands the repercussions of accidentally or purposely releasing or misusing the protected information. Typically, the content of the agreements are reviewed and approved by the agency's legal office.

ISO Role
The ISO provides guidance and oversight to the program areas that own the confidential information to ensure a formal process is in place to adequately protect the information. The ISO should assist in developing confidential or non-disclosure agreements and assist with identifying the parties that must sign them. The ISO activities may include:

- Ensure that the development and content of confidentiality or non-disclosure agreements reflects the agency's need for the protection of its information;
- Review the agreement language to ensure compliance with policy;
- Ensure management supports the utilization of the confidentiality agreements.
- Ensure the agency has the ability to audit and monitor activities of those persons that have signed the agreements; and,
- Ensure a procedure is in place to discontinue access to confidential information when an agreement is terminated, there is a change in the need for access, or a violation has occurred.

3.4 Third Party Agreements

Third party agreements are different from confidentiality or non-disclosure agreements. Third party agreements may include contractual language, service level agreements, operating level agreements, or memorandums of understanding with internal or external entities. It is an agreement between two or more parties that creates for each party a duty to do something (e.g., handle an agency's assets in a certain way) or a duty not to do something (e.g., divulge an agency's detailed network infrastructure design or provide access to an information system to an unauthorized individual). A party's failure to honor this agreement allows the other party or parties to bring action. Typically, the content of the agreements are reviewed and approved by the agency's legal and contract offices.

ISO Role
Working with the agency's legal and contract offices, the ISO reviews the content in the third party agreement, before it is signed, to ensure it meets applicable laws, regulations, statutes, state policies, and internal policies. The ISO may assist in identifying who will be responsible to oversee the third party compliance, and provides oversight to ensure that the:

- Existing agreements are updated, or terminated, when necessary;
- Appropriate controls protecting information that is not intended to be accessed by the applicable parties are in place;
- Stakeholder security issues are addressed; and,
- Owner of the agreement has assigned sufficient technical skills and resources to monitor the requirements of the agreement; in particular that the information security requirements are being met.

Authority	Relationship/Interfaces	References/Tools
SAM Sections 4810, 4841, & 4841. 2	• Executive Management • Legal Office • Governance Committee • Human Resources/Labor Relations	SISO's Information Security Program Guide – www.infosecurity.ca.gov/ SISO's Template Web site – www.infosecurity.ca.gov/library/

Authority	Relationship/Interfaces	References/Tools
	• CIO • Contracts Office Department of General Services (DGS)	NIST SP 800-12 - http://csrc.nist.gov/ ISO/IEC 27002

Asset Management and Protection

Asset Management and Protection refers to a process where agencies identify and inventory assets, agree upon ownership and the classification of information, and document the process of safeguarding each asset to protect against loss or theft.

The ISO leads the oversight and participates in planning, developing, and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 4	ISO Role and Responsibility
Asset Management **Objective**: To achieve and maintain appropriate protection of agency assets. • Asset inventory, ownership and acceptable use • Data classification	**4.1 Asset Protection:** Develop and maintain internal policies, standards, processes, procedures and practices that prevent and detect fraud, misuse, and abuse of state assets. **4.2 Data Classification:** Develop categories and definitions that provide guidelines used to determine the appropriate level of protection for information.

4.1 Asset Management And Protection

Asset management is a fundamental discipline that identifies a process where agencies identify all assets and inventory them. It enables improved cost control and truer understanding of an agency's business value, and can help an agency recover from a disaster. At a minimum, an inventory should include all information technology equipment, software, paper records, and confidential/sensitive information which may reside in systems (e.g., applications, database, servers, desktops, laptops, etc.) or on portable media (e.g., back-up tapes, floppy disks, flash/jump/USB drives, CDs, DVDs, etc.). As part of an asset management program, agencies must ensure:

- Assets of the agency are identified and properly accounted for.
- Data ownership and data classification is clearly established.
- Assets are periodically inventoried, on a recurring nature.
- Rules of conduct and appropriate safeguards are established to ensure the use of assets support the agency's mission and objectives, and that such use does not violate applicable laws and State policies.
- Employees are trained on such rules and their responsibilities for the proper use and maintenance of assets, and the penalties for misuse and non-compliance with rules.

ISO Role

The ISO has general oversight responsibility to ensure that policies, standards, processes, procedures, and practices are established and enforced to support the protection of assets through their proper use and prevention and/or detection of misuse or abuse. This responsibility includes that the agency has the necessary controls in place to be in

compliance with laws, regulations, statutes and state policies with respect to asset inventory, identification, classification, and use and disposition requirements. Establishing cooperative relationships with management in other functional units (e.g., business areas, human resources and labor relations, business services and procurement, information technology services and legal) is pertinent. The ISO activities may include

- Review asset inventories, ownership designations, and data classifications to make asset and information security labeling and handling recommendations, and development of policy based on risk;
- Provide implementation guidance to management in the dissemination of policies to ensure employees have been informed of their responsibility for protecting assets; and,
- Review and validate the establishment and effectiveness of asset protection policies, procedures and practices through observation, interviews, and periodic tests of safeguards.

4.2 Data Classification

Agencies must ensure that data classification procedures are implemented and the information (paper or electronic) has been adequately classified (e.g., confidential, sensitive, personal information). Data classification is the responsibility of the data owner, requiring the initial classification and periodic reviews to ensure the appropriate level of security controls are in place.

ISO Role

The ISO ensures that the agency has established policies and procedures for the classification of information and that it is in compliance with laws, regulations, statutes, state policies, and best practices. The ISO may be a participant in the classification efforts; however, the ISO's main role is to ensure the procedures are in place to support proper classification of information.

Authority	Relationship/Interfaces	References/Tools
• Government Code Sections 14740-14770 • Civil Code Section 56, 1798.3, 1798.17 (a) & (b), 1798.20, 1798.21, and 1798.29 • Health & Safety Code Sections 123100- 123149.5 • Health Insurance Portability & Accountability Act (HIPAA), 45 C.F.R. parts 160 & 164 • Penal Code Sections 311-312.7, 346, 474, 484-502.9 • SAM Sections 1602, 1666, 3693, 4841.2-4841.4, 4842.2 (7), 4846.2, 4989.3,	• Executive Management • Human Resources/ Labor Relations • Facilities Management • Equal Employment Opportunity Officer • Legal Office • CIO • Business Services Unit • Procurement Unit • IT staff • DGS	• SISO's Template Web page www.infosecurity.ca.gov/library/ • DGS - http://sam.dgs.ca.gov /TOC/default.htm • ISO/IEC 27002

Authority	Relationship/Interfaces	References/Tools
8600, 8601, 8652, 20050 & 20080		

Human Resources Security

Human Resource (personnel) Security refers to those practices, technologies, and services to ensure the employees and contractors authorized to access or maintain systems have the appropriate levels of access needed to perform their duties.

The ISO leads the planning and oversight and participates in the developing and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 5	ISO Role and Responsibility
Human Resources Security **Objective:** To ensure that employees, contractors, and third party users understand their responsibilities, that they are suitable for the roles they are considered for, and to reduce the risk of theft, fraud, or misuse of facilities by recognizing information security problems and incidents. • Screening • Management responsibilities • Security and privacy awareness training and education • Disciplinary process • Termination or change of employment • Return of assets • Removal of access rights	**5.1 Personnel Practices:** Ensure activities related to employees include the proper handling of security breaches; and creation of checklists for managers' signoff upon employee termination or change of job duties. **5.2 Awareness Training:** Coordinate training efforts for the appropriate use of information assets, including personal, sensitive or confidential information and the process to report security and privacy incidents.

5.1 Personnel Practices

Personnel security provides the policy and procedures associated with employee activities including the appropriate and fair treatment for enforcing and handling breaches of security, and the termination processes for changes in job function or departure from the agency.

ISO Role

The ISO leads in the development and enforcement of policies, standards, processes, and procedures related to personnel practices for information security management through the established governance structure. Because these actions affect the employee work environment, it is important to have representation from the agency's human resources, labor relations, legal, equal employment opportunity, and information technology offices. They include, but may not be limited to:

- Disciplinary process – development of policy and procedures that provide for appropriate and fair treatment in the enforcement and handling of security breaches.

- Termination Process – development of formal processes for asset return, and physical and computer access changes when an employee or contractor has a job assignment change or departs from the agency.

5.2 Awareness Training

Employees are the most important assets available to ensure that state business functions operate properly. Security awareness training is an essential component of an information security program and its importance cannot be overlooked. As employees are provided training for other areas of their assignments, training on their security roles and functions should be included and properly integrated. One simple aspect of security and privacy is to issue an "agency approved" identification badge to each employee and instruct them on its use and protection. While this method does not directly address the security of information, it can be readily seen that protection of the physical site is a primary requirement to ensure security. Security awareness should encompass (at a minimum) the following areas:

- Laws, regulations, statutes, and state policy regarding the protection of information (both electronic and paper based).
- Agency security policies and procedures.
- Identifying an incident, the employee's responsibility to report it, and the process for reporting it.
- Description of physical security requirements, including expected response when there is discovery of unauthorized personnel, security doors left/propped open, missing or altered equipment or data, and who the employee should contact regarding these types of security issues.
- Appropriate use of the Internet, email, instant messaging and other agency authorized resources, including the agency's monitoring policy.

Privacy training is required annually. By combining the privacy and security training, an agency can reinforce the appropriate handling of personal information and the notification process for reporting an unauthorized disclosure. Examples of personal information, which require special protections, is an individual's name and social security number or driver's license or identification card (required by many businesses), or an individual's name and bank card with pin number. Under state policy (SAM Section 4841.3.2(a) Classification of Information) this type of information requires protection from unauthorized disclosure. There are constitutional rights and laws that address access, handling, use, and notification for unauthorized disclosure of personal information, including, but not limited to:

- California Constitution Article 1 Declaration Of Rights
- California Information Practices Act (Civil Code 1798 et. seq)
- Health Insurance Portability and Accountability Act (HIPAA)
- Family Educational Rights and Privacy Act of 1974 (FERPA)

ISO Role

The ISO oversees agency compliance with policies, standards, guidelines, processes and procedures regarding the protection of information assets and ensures all employees (including contractors) have been appropriately trained to understand their role and responsibility for information security, the rules of conduct for use of information assets, information access and handling, and the consequences of failure to comply with those rules. The ISO (in coordination with the agency's privacy officer and training office) should

coordinate the security awareness training with privacy training as much as possible, as these two areas overlap. In addition to formal training, there are other methods available to promote security and privacy awareness, such as newsletters, articles on specific topics, or awareness tips. It is important that new employees are made aware of the requirements at the onset of employment with the agency so they understand and follow agency policy

Based on an agency's size, the ISO may work collaboratively with the training office to create the awareness material and provide training. In other situations, it may be the ISO who creates the materials and provides training. There are a large number of resources readily available that provide awareness material which can be easily modified to fit an agency's environment. Good resources include the SISO's Web site at www.infosecurity.ca.gov/ or by contacting other agencies who have already developed a training program and request a copy of their materials.

Authority	Relationship / Interfaces	References / Tools
• SAM 4840 – 4845, 4819.31(6), 4840, 4841, 4842 • HIPAA • Civil Code Section 1798 et seq (Information Practices Act of 1977)	• Executive Management • Legal Office • Human Resources/Labor Relations • Equal Employment Opportunity Officer • CIO • Privacy Officer • Training Office • Department of Personnel Administration (DPA) • CA Office of Privacy Protection (COPP) • CA Office of HIPAA Implementation (CalOHI)	• SISO - www.infosecurity.ca.gov /Library/Awareness/ • DPA - www.dpa.ca.gov/ • COPP - www.privacy.ca.gov/ • CalOHI - www.calohi.ca.gov/ • NIST SP 800-50 - http://csrc.nist.gov/

Physical and Environmental Security

Physical and Environmental Security refers to those practices, technologies and services used to address the threats, vulnerabilities, and counter measures utilized to protect information assets and the premises in which they reside.

The ISO leads the oversight and participates in the planning, developing, and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 6	ISO Role and Responsibility
Physical and Environmental Security **Objective:** To prevent unauthorized physical access, damage, and interference to the agency's premises and information. • Physical security perimeter and controls • Protecting against external and environmental threats • Working in secure areas • Equipment security • Secure disposal or re-use of equipment • Secure disposal / destruction of confidential and sensitive information (paper and media)	**6.1 Physical and Environmental Security:** Lead or participate in the development and maintenance of internal policies, standards, processes, and procedures that prevent unauthorized physical access to state assets, damage from man-made or natural disasters, and conduct internal and external threat assessments.

6.1 Physical And Environmental Security

Physical and environmental security encompasses site design and layout, environmental components (e.g., heating, water, and air), emergency response readiness, access barriers and controls, and power and fire protection. The state has defined physical security as “the protection of information processing equipment from damage, destruction or theft; information processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.”

In conjunction with physical security, agencies must ensure that equipment is identified with a property identification tag, properly accounted for and secured from loss, theft, damage and interference until the end of its lifecycle (see Asset Management and Protection section). This includes, but is not limited to, establishing policies, standards, processes, procedures and practices related to the placement and/or location of critical assets, and use of locks, device alarms, cable traps, and switch and port controls. Further, once information and equipment have reached the end of their useful lifecycle, agencies must ensure their internal policies and procedures support proper trade-in, lease, sale, transfer, reuse and/or disposal of equipment and the secure destruction of personal, confidential and sensitive information. Information Technology equipment, such as servers, routers, desktops, laptops, and flash drives may contain software with specific software license restrictions and information of a confidential or sensitive nature. Physical equipment, such as desks, lockers, and storage cabinets may contain paper documents of a confidential or sensitive

nature. Thus, appropriate disposal and destruction methods must be implemented and enforced.

Disposal of equipment and destruction of personal, confidential and sensitive information (paper or electronic) must be a defined business process that provides auditable evidence of proper disposal and destruction in accordance with state policy and applicable laws.

ISO Role

The ISO recommends and participates in the selection and development of physical and environmental controls to ensure the protection of state assets and evaluates the effectiveness of such controls. The ISO ensures that policies, standards, processes, procedures, and practices are in place to prevent unauthorized physical access, damage, and interference to the agency's premises, equipment and information assets. Additionally, this role involves establishing cooperative relationships with business and facility management across the agency and responsibilities may include, but are not limited to:

- Lead or participate in the development of policies and procedures in compliance with applicable laws and state policies, for the proper physical security perimeter and controls in state-owned or leased facilities and other facilities where the agency's information assets are used, stored and/or maintained;
- Participate in the development and approval of policies which limit access to state assets to authorized personnel requiring access in the performance of their assigned duties. This may include the placement of physical barriers, manned reception areas, and other means to control or restrict physical access;
- Participate in the development and approval of policies which provide for the proper disposal of information and equipment at the end of their lifecycle;
- Participate in the development and approval of policies which provide for the necessary environmental controls (e.g., backup power to facilitate proper shut down, uninterruptible power supply (UPS), fire detection, humidity controls, and water damage detection) and proper placement of critical documents and systems to minimize damage and disruption to services;
- Perform or participate in the review of facility risk assessments and make recommendations in the prevention of unauthorized physical access, damage and interference to state-owned or leased facilities and operations. This may include analysis of a wide variety of external and environmental factors and evaluating and recommending security products and controls; and,
- Conduct periodic review and evaluation of the effectiveness of such policies through observation, interviews, and examination of requests for access to secure areas and the testing of software used to wipe media prior to the transfer, sale, reuse or disposal of equipment.

Authority	Relationship/Interfaces	References/Tools
Government Code Sections 13403, 14615(a) & (b), 14673-14675, &14685(c)(1), 15675 Vehicle Code Section 2400 (g)	• Executive Management • CIO • Privacy Officer • Facilities Management • Security guards • Service contractors	• CHP Handbook Pub. HPH 100.5, Security Recommendations - www.chp.ca.gov/ • International Crime Prevention through Environmental Design (CPTED) Association

Authority	Relationship/Interfaces	References/Tools
SAM Sections 1326, 1452.2, 1671, 1673, 2580-2580.1, 3693, 4800, 4840.4, 4841.1, 4841.3, 4841.5, 4842.2 (3), 4845, 4900.2, 5100, 5900- 5953, 6841, 6850, 6899, 8633, 8640-8643, 8650 & 20050	• DGS • California Highway Patrol (CHP) • Fire Department	• SISO Monthly Newsletters - www.infosecurity.ca.gov/Library/Awareness/ • Standards for the Professional Practice of Internal Auditing (SPPIA) issued by the Institute of Internal Auditors • www.security.org - locks, safes,& security • NIST SP 800-12 and 800-53 - http://csrc.nist.gov/ • ISO/IEC 27002

Communications and Operations Management

System communications protection refers to the key elements used to assure data and systems are available, and exhibit the confidentiality and integrity expected by owners and users to conduct their business. Operations management refers to implementing appropriate controls and protections on hardware, software, and resources; maintaining appropriate auditing and monitoring; and, evaluating system threats and vulnerabilities.

The ISO leads the oversight and participates in the planning, developing, and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 7	ISO Role and Responsibility
Communications and Operations Management **Objective:** To ensure the correct and secure operation of information processing facilities. • Documented operating procedures • Change management • Segregation of duties • Separation of development, test, and operational facilities • Protection against malicious and mobile code • Backup functions • Network security management • Media handling • Exchange of information • Electronic messaging • Electronic commerce services • Monitoring • Protection of logs	**7.1 Operational Procedures:** Lead in the development and documentation of operating procedures, including change control and separation of duties. **7.2 Protecting Against Malicious Code:** Activities required for the prevention and detection of malicious code, which could cause a disruption in business. **7.3 Backup Functions:** Activities required for the integrity and availability of information and systems. **7.4 Network Security Management:** Activities required for the protection of networks and supporting infrastructure. **7.5 Media Handling:** Activities for the prevention of unauthorized disclosure, modification, removal or destruction of assets. **7.6 Exchange of Information:** Lead in the development and implementation of a formal information and application exchange with internal and external entities. **7.7 Electronic Messaging:** Lead in the development of policies and procedures needed to protect electronic messages and systems.

Component 7	ISO Role and Responsibility
	7.8 Electronic Online Services: Lead in the development and implementation of security measures to ensure the integrity and confidential of information while accessing electronically. **7.9 Monitoring:** Ensure that agency operational policies and procedures are being followed. Periodically, or on request, monitor the controls in place in support of agency policies and procedures.

7.1 Operational Procedures

Agencies must have documented up-to-date operational procedures in place to ensure the correct and secure operation and management of information processing systems. Segregation of duties should be implemented to reduce the risk of negligent or deliberate system misuse. Based on the size, some agencies may find segregation of duties difficult to achieve, but the principle should be applied as much as possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision should be considered. It is important that security monitoring and reporting remains independent.

ISO Role

The ISO oversees agency compliance with state policies, standards, guidelines, processes and procedures regarding network security management, documented operational procedures, change controls, proper segregation of duties, and protected production environment. The development and maintenance of operational procedures are typically the responsibility of the information technology staff; however, the ISO has oversight responsibilities to ensure that they are in place. Additionally, the ISO ensures that the managed assets include baseline change control information that can be monitored and that there are appropriate audit trail reports or alerts produced to identify all changed elements. The responsibilities may include, but are not limited to:

- Verify procedures have been documented for system activities associated with information processing and communication facilities, such as IT equipment start-up and close-down procedures, backup, equipment maintenance, media handling, computer room and mail handling management, and safety.
- Verify operating procedures have been documented, maintained, and made available to employees who have a business need for them;
- Participate in the change management process to assess potential security impacts of the proposed changes;
- Review and monitor operational procedures to ensure they support and identify that segregation of duties exist and are in compliance with agency policies and procedures, to reduce the risk of negligent or deliberate system misuse;

- Identify, review, and recommend areas of responsibility that should be segregated to ensure no single person can access, modify, or delete assets with authorization or detection; and,
- Verify and monitor to ensure sufficient separation of development, test, and operational facilities exist to reduce the risks of unauthorized access or changes or to prevent operational problems or disruptions to the operational systems.

7.2 Protecting Against Malicious Code

Agencies must take appropriate steps to prevent unauthorized or malicious code that could allow access or corruption of its information assets. Precautions and controls are required to prevent and detect the introduction of malicious or unauthorized code.

ISO Role

The ISO oversees internal policies, standards, guidelines, processes and procedures regarding network security management to ensure that controls are in place to prevent and detect malicious code from corrupting information assets or disrupting agency or state services. The responsibilities may include, but are not limited to:

- Validate controls and/or security tools are in place to proactively scan production code and compare to approved baseline code to protect against malicious code;
- Review and recommend, where appropriate, additional controls to prevent, detect, and remove malicious code; and,
- Review and recommend that Internet web servers have in place controls and protection to detect and prevent the introduction of malicious code.

7.3 Backup Functions

Agencies must be in compliance with applicable laws, regulations, statutes, and state policies regarding sufficient backup and recovery procedures necessary to preserve and protect information assets and maintain the integrity and availability of information and information processing systems.

ISO Role

The ISO oversees internal policies, standards, guidelines, processes and procedures regarding network security management regarding backup and recovery of agency information assets. The responsibilities may include, but are not limited to:

- Monitor and validate regular scheduled backup and restore processes;
- Monitor regular testing using back-up copies of information and software to validate the backup policy; and,
- Validate adequate back-up facilities are provided to ensure that all essential information systems, applications, and data can be recovered following a disaster, disruption of business, or media failure.

7.4 Network Security Management

The secure management of networks, which may span organizational boundaries, requires careful consideration to legal implications, monitoring, and protection. Additional controls

must also be in place to protect sensitive or confidential information passing over public networks and to ensure the protection of the supporting infrastructure.

ISO Role
The ISO oversees internal policies, standards, guidelines, processes and procedures regarding network security management. The responsibilities may include the following:

- Monitor and oversee that scheduled network security testing and controls are in place to alert management of unauthorized attempts;
- Monitor and work with network managers to implement controls to ensure the security of information in networks and the protection of connected services from unauthorized access; and,
- Monitor and ensure that appropriate logging and monitoring controls are in place to enable recording of relevant events and alerts.

7.5 Media Handling

Controls to prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities must be in place to protect the information.

ISO Role
The ISO oversees internal policies, standards, guidelines, processes and procedures regarding media handling. The responsibilities may include, but are not limited to:

- Validate that formal procedures for the secure disposal of media are in place to minimize the risk of sensitive or confidential information leakage;
- Validate that secure industry standard erasure tools are used for media containing sensitive or confidential information prior to reuse or disposal;
- Validate that media is disposed of securely and safely, e.g. by incineration, shredding, degaussing, or erasing data;
- Validate that controls are in place for the management of removable media; and,
- Validate that controls are in place for media removed from the agency and that records of such removals are kept in order to maintain an audit trail.

7.6 Exchange Of Information

Formal internal exchange policies, procedures, and controls should be in place to protect the exchange of information through all types of communication facilities.

ISO Role
The ISO oversees internal policies, standards, guidelines, processes and procedures regarding secure information exchange. The responsibilities may include, but are not limited to:

- Monitor to ensure controls are in place to report information exchange processes;
- Monitor that state-mandated cryptographic (encryption) techniques are in use to protect sensitive and confidential information exchanged between agencies or business partners;

- Ensure that agreements are established for the exchange of information and software between the agency and applicable government entity or business partner; and,
- Monitor security awareness, policy, and procedures to ensure the use of information exchange facilities are in place to avoid compromise or leakage (such as, discussion overheard on a mobile phone in a public place, misdirection of an electronic mail message, sensitive voicemail messages being overheard, unauthorized access to voicemail systems, or accidentally sending facsimiles to the wrong telephone number).

7.7 Electronic Messaging

Electronic messaging, including email and instant messaging, play an increasingly important role in business communications. Electronic messaging has different risks than paper-based communications and must be protected.

ISO Role

The ISO oversees internal policies, standards, guidelines, processes and procedures regarding electronic messaging. The responsibilities may include, but are not limited to:

- Assist in the development and implementation of policies and procedures to protect information associated with the interconnection of business information systems.
- Assist in the development and implementation of policies and procedures that reflect the business needs of the agency regarding retention and back-up of electronic messages.
- Monitor to ensure controls are in place to protect electronic messages from unauthorized access, modification, or denial of service.
- Ensure that authorization and approval processes are in place for using external public services, such as instant messaging or file sharing, and that they are required in support of agency business, or they are disabled.

7.8 Electronic Online Services

There are security implications associated with using electronic online services, including on-line transactions that require a higher level of security controls for their use. Therefore, the integrity and availability of information processed through these systems must be addressed.

ISO Role

The ISO oversees internal policies, standards, guidelines, processes and procedures regarding electronic online services to protect from fraudulent activity and unauthorized disclosure or modification. The responsibilities may include, but are not limited to:

- Monitor to ensure controls are in place to support authorized electronic online services.
- Monitor to ensure controls are in place to ensure that transactions are in full compliance with laws, rules, and regulations.

7.9 Monitoring

Information security events should be recorded and systems must be monitored to detect unauthorized activities. Operator logs and fault logging should be used to ensure information system problems are identified. System monitoring is required to check the effectiveness of controls adopted, to verify conformity to state and agency policies, and to ensure that all relevant legal requirements for monitoring and logging of activities are met. Event logs help manage and protect systems by providing audit information to identify and resolve system incidents or problems. Logging facilities and information are extremely important information assets that must be protected against tampering and unauthorized access.

ISO Role

The ISO oversees internal policies, standards, guidelines, processes and procedures regarding agency approved monitoring. The responsibilities may include, but are not limited to:

- Ensure that only approved monitoring tools or capture processes are being used in compliance with existing information and privacy policies, standards, guidelines processes and procedures;
- Monitor to ensure that audit logs record user activities, exceptions, and information security events and are kept for an agreed period of time;
- Monitor to ensure that audit logs containing confidential personal information are appropriate and have the appropriate security and privacy protection measures in place;
- Monitor to ensure that the proper security settings regarding the capture and storage of events are in compliance with incident reporting procedures; and,
- Monitor to ensure that security event logs are protected to prevent inadvertent or malicious destruction or modification.

Authority	Relationship/Interfaces	References/Tools
SAM 4841	• CIO • Network Manager • Operations Manager • Applications Manager • Business Services Unit • DGS Records Management Program	• SISO - www.infosecurity.ca.gov/tools/ • DGS - www.osp.dgs.ca.gov/recs/default.htm • NIST SP 800-12, 800-41, 800-45, 800-83, 800-88 - http://csrc.nist.gov/ • ISO/IEC 27002

Access Control

Access Control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of the agency's information assets. Key components include identification, authentication, and authorization. They apply to people, process, and technology devices.

The ISO leads the planning and oversight and participates in the developing and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 8	ISO Role and Responsibility
Access Control **Objective:** To control access to information. • Access control policy • User access management • User responsibilities • Unattended user equipment • Clear desk/screen policy • Network access controls • Operating system access control • Application and information access control • Mobile computing and teleworking	**8.1 Access Control:** Review procedures for applying the appropriate rules and rights for each user or group. **8.2 User Access Management:** Review privilege and passwords rules and processes and user registration and de-registration procedures for granting and revoking access to information systems and services. **8.3 User Responsibilities:** Ensure users are made aware of their responsibilities in accessing, protecting, and using information assets. **8.4 Application and Information Access Control:** Review procedures to prevent unauthorized access to restricted systems, applications, and information. **8.5 Sensitive System Isolation:** Ensure the identification and separation of systems, applications, and information based on criticality and sensitivity.

8.1 Access Control

Agencies must maintain a policy to control access to networks, information systems and information processing areas to prevent unauthorized access or malicious attacks.

ISO Role

The ISO ensures that access controls are in place, the appropriate rules and rights for each user group are clearly stated in an access control policy, and that users are made aware of the policy. The responsibilities may include, but are not limited to:

- Ensure access controls provide for all points of ingress and egress of the agency's network infrastructure and computer systems.
- Ensure access controls are both logical for logon or access authentication and physical for access to a specified rooms or areas and are considered together.

8.2 User Access Management

Agencies must control and manage access to their information technology assets to ensure that only authorized devices/persons have access as is appropriate in accordance with the agency's policies and business needs. A formal process must be developed to cover all stages of access from the initial request to the termination of access when the employee has a change in job duties or leaves the agency.

ISO Role

The ISO ensures that internal policies, standards, guidelines, process and procedures are in place to allow access of information to those individuals authorized to have it. The ISO should periodically verify compliance to ensure that authorizations are current. The responsibilities may include, but are not limited to:

- Ensure devices permanently or intermittently connected to the network have approved password-based access controls in place;
- Ensure only authorized users are granted access to the agency's information systems;
- Ensure the principle of "least privilege" is used and is enforced;
- Ensure job duties are separated as appropriate to prevent any single person or user from having access not required by their job function;
- Verify that the physical surroundings of the assets (buildings, files, rooms, etc.) are covered with the appropriate physical controls to deter unauthorized admittance; and,
- Verify user authorization for both logon and physical access is appropriately modified upon job change or transfer from agency.

8.3 User Responsibilities

Employees should be made aware of their responsibilities in accessing and using information assets. This awareness ensures they understand information sensitivity issues, levels of confidentiality, and the mechanisms in place to protect the information. Employees should understand their authorization levels and any policies and guidance in place regarding their access. They should also be informed that violations of the policy may result in disciplinary action against them.

ISO Role

The ISO should ensure that the agency's training materials cover the employee's responsibility for protecting systems and information and that they are aware of the security requirements and procedures. At a minimum, employees should be informed to:

- Properly store confidential, sensitive or critical business information (whether it be paper or electronic) when away from desk;
- Terminate active sessions when finished, unless they can be secured by an appropriate locking mechanism, such as a password protected screen saver;

- Log off or protect with password protected screen saver when computers or devices are unattended;
- Provide for a secure method of receiving or sending mail and faxes containing confidential or sensitive information;
- Properly use photocopiers or other reproduction technology; and,
- Pick up documents containing sensitive or classified information from printers and faxes immediately.

8.4 Application and Information Access

Agencies must establish controls for individuals whose job function requires them to have system administrators' access that provides them the ability to override or bypass safeguards for the regular user. These access privileges should be removed immediately if there is a change in the employee's job function or departure from the agency.

ISO Role

The ISO ensures employees have the appropriate access required for their job function. Periodic review of the system administrator privileges will ensure that access to agency information, systems, and applications are made by authorized personnel only. Additionally, the review should ensure an audit trail is maintained and reviewed.

8.5 Sensitive System Isolation

Agencies should determine if they have systems that contain sensitive applications or critical information that would require a dedicated (isolated) computing environment.

ISO Role

The ISO ensures that systems, applications, and information classified as critical, sensitive or confidential is isolated in the appropriate manner. The responsibilities may include, but are not limited to:

- Ensure critical, sensitive or confidential systems, applications, and information are identified;
- Verify that access control to the isolated environment are provided to those individuals designated as having a business need; and,
- Validate that when a sensitive system or application runs in a shared environment, the risks are identified and accepted by the owner.

Authority	Relationship/Interfaces	References/Tools
SAM 4842	• Executive Management • Human Resources • Legal Office • Facility Management • System Administrators • System Owners	• NIST SP 800-12 and 800-100 http://csrc.nist.gov/ • ISO/IEC 27002

Information Systems Acquisition, Development, and Maintenance

Agencies should ensure that security is an integral part of information systems, which include operating systems, infrastructure, applications and off-the-shelf products, services, and user-developed applications.

The ISO leads the planning and oversight and participates in the developing and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 9	ISO Role and Responsibility
Information Systems Acquisition, Development, and Maintenance **Objective:** To ensure that security is an integral part of information systems. • Security requirements analysis and specification • Corrective processing in applications • Input data validation • Control of internal processing • Message integrity • Output data validation • Cryptographic (encryption) controls • Security of system files • Security in development and support processes • Technical vulnerability management	**9.1 Security Requirements:** Participate in the development and maintenance of internal policies, standards, guidelines, processes, and procedures for the collection of security requirements, approval of project-related documents, change control, technical review, independent application testing, developer security testing, and the protection of system test data and program source code.

9.1 Security Requirements

Agencies must ensure that security properly integrates with the system and software development lifecycle, including assurance that security requirements are appropriately addressed during the requirements analysis phase and that systems are developed or selected in accordance with applicable security standards. Agencies must identify security objectives (confidentiality, integrity, and availability) and ensure implemented solutions are developed and designed to meet those objectives, which may include:

- Security requirements analysis and specification
- Correct processing in applications (input and output validation, control of internal processing and message integrity)
- Cryptographic controls (encryption policy and key management)
- Security of system files (control of operational software, protection of system test data, and access control to program source code)
- Security in development and support processes (change control procedures, technical review of applications after operating system changes, restrictions on changes to software packages, information leakage, outsourced software development)

- Technical vulnerability management

ISO Role
The ISO ensures that policies, standards, guidelines, processes, and procedures are in place to support security requirements for the acquisition, development and maintenance of information systems throughout their lifecycle. Additionally, this role involves establishing cooperative relationships with business, information technology and systems development management and staff within the organization and externally affected parties. The responsibilities may include, but are not limited to:

- Participate in the development of feasibility studies, request for proposals, and other project-related documents to ensure security is addressed appropriately;
- Identify, define, and document security requirements for information systems at the requirements phase;
- Validate security requirements by identifying and documenting where a security requirement is not met, the risk associated with the lack of conformity, and management's decision to reject, transfer, mitigate or accept the risk;
- Provide validation guidance into data validation processes. These reviews may include:
    - review add, modify and delete functions
    - review procedures to prevent data errors as a result of system failure, program failure recovery programs, and mitigation strategies for known threats and attack vectors (e.g., buffer overflows)
    - inspect hardcopy input documents for unauthorized changes and the review of content in key fields or data files to validate integrity, plausibility checks, reconciliation counts and creating a log of activities
- Conduct or guide an assessment to determine if message integrity is required and recommend appropriate security methods;
- Develop or participate in the development of a policy that guides the use of cryptographic (encryption) controls. The policy should address security objectives (confidentiality, integrity/authentication, and non-repudiation) and a key management approach;
- Develop or participate in the development of policies that guides the use and control of operational software, the protection of system test data, and strictly controls and restricts access to program source code;
- Develop or participate in the development of formal change control procedures. These procedures should include a risk assessment, analysis of the impact of changes, and identification of security controls and should provide for the maintenance of change documentation, authorized approvals, and version controls;
- Conduct or facilitate technical reviews of applications following operating system changes to ensure they have not been compromised;
- Develop or participate in the development of a policy that guides outsourced software development and restrictions to changes in commercial-off-the-shelf (COTS) software packages. The policy should address the risks and impact to the agency when making changes to COTS software packages (e.g., vendor consent, compromise of built in integrity controls, impact on future updates) and ensure that outsourced software development is closely supervised and monitored (e.g., contractual requirements are documented and met, certifications of product quality and accuracy are obtained, and independent testing for malicious, Trojan, and/or backdoor code before installation is performed);

- Review contracts made with vendors and suppliers in support of information systems to ensure security requirements are defined and are addressed;
- Develop or participate in the development of policy and/or procedures that guide technical vulnerability management. The policy and procedures should identify roles and responsibilities for monitoring, assessing, patching and tracking assets. The policy and procedures should also establish acceptable response timelines and integrate change management controls and processes;
- Monitor technical vulnerability alerts to make timely and appropriate recommendations to address the associated risk. Note: In order to effectively carry out this role the ISO may need a complete and accurate inventory of current assets including software vendor, version number and current state of deployment (e.g., what software is installed on what systems);
- Guide and/or participate in the evaluation, selection, and approval of vulnerability tools and independent testing plans and tests; and,
- Conduct or guide the efforts of vulnerability assessments to identify security weaknesses and develop remediation plans.

Authority	Relationship / Interfaces	References / Tools
• Civil Code Sections 1633.1 to 1633.17, & 1798.29 • SAM Sections 4800-5180; emphasis on Sections 4840-4841.2, 4846-4846.2, & 5100-5175.2	• Executive management • CIO • Project Management Office • System developers • Programmers • System analysts • System administrators • System owners • System custodians • System users • Data owners • Auditors • Department of Finance (DOF) • Office of the State Chief Information Office (SCIO)	• SISO - www.infosecurity.ca.gov/ • DOF – www.dof.ca.gov/ • SIMM 120 and 160 • SCIO - www.cio.ca.gov/ • FIPS Documents: 113, 140-2, 186-2, 190, 196 – 198, 200 • NIST Documents: SP 800-23, SP 800-36, SP 800-38 (A-C), SP 80-45, SP 800-49, SP 800-53, SP 800-63, SP 800-64, SP 800-78 http://csrc.nist.gov/ • US Department of Homeland Security – Build Security In – https://buildsecurityin.us-cert.gov/daisy/bsi/home.html • ISO/IEC 27002

Information Security Incident Management

Information Security Incident Management refers to the processes and procedures agencies implement for identifying, responding to, and managing information security incidents. It includes the development, documentation, and implementation of an information security incident response plan that provides the framework for an agency to proactively manage incidents when they occur.

The ISO leads the planning, developing, and oversight and may either lead or participate in the managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 10	ISO Role and Responsibility
Information Security Incident Management **Objective:** To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken. • Reporting information security events • Management of information security incidents and improvements	**10.1 Incident Management:** Establish a formal procedure for internally reporting and tracking security incidents, ensure incident response and escalation procedures are followed, and inform all employees, contractors and third party users of their responsibility to report security incidents. **10.2 Incident Handling:** Participate and/or oversee in the investigation and management of information security events and policy violations and track to conclusion. **10.3 Incident Notification and Reporting:** Follow state policy for the notification and reporting of incidents immediately upon discovery. **10.4 Lessons Learned:** Develop and document corrective action plans and implement lessons learned to mitigate recurrence.

10.1 Incident Management

Agencies must ensure that information security incidents, events, and weaknesses of information systems are communicated and addressed in a timely manner. Formal reporting, investigation, and escalation procedures should be established to handle security incidents. As part of the agency's security awareness and training program, employees should be trained to identify an incident and know where to report it.

Examples of information security incidents include, but are not limited to the following suspected or actual events:

- State data (includes electronic, paper, or any other medium)
  - Theft, loss, damage, unauthorized destruction, unauthorized modification, or unintentional or inappropriate release of any data classified as confidential, sensitive or personal. (See SAM Section 4841.3)
  - Possible acquisition of notice-triggering personal information by unauthorized persons, as defined in Civil Code 1798.29.
  - Deliberate or accidental distribution or release of personal information by an agency, its employee(s), or its contractor(s) in a manner not in accordance with law or policy.
  - Intentional noncompliance by the custodian of information with his/her responsibilities. (See SAM Section 4841.6)
- Inappropriate Use & Unauthorized Access - This includes actions of state employees and/or non-state individuals that involve tampering, interference, damage, or unauthorized access to state computer data and computer systems. This includes, but is not limited to, successful virus attacks, web site defacements, server compromises, and denial of service attacks.
- Equipment - Theft, damage, destruction, or loss of state-owned IT equipment, including laptops, tablets, integrated phones, personal digital assistants (PDA), or any electronic devices containing or storing confidential, sensitive, or personal data.
- Computer Crime - Use of a state information asset in commission of a crime as described in the Comprehensive Computer Data Access and Fraud Act. See Penal Code Section 502. See SAM Section 4840.4, for a definition of an information asset.
- Any other incidents that violate agency policy.

California law (Civil Code Sections 1798 – 1798.78 - Information Practices Act of 1977) requires notification to impacted individuals when specific personal information is lost or stolen. Notice-triggering information includes an individual's name plus Social Security Number, driver's license/California identification card number, or financial account number. There are additional federal laws that may require notification as well. In some cases, it may be appropriate to notify affected individuals based solely upon due diligence.

ISO Role

The ISO develops and implements the agency policies, standards, guidelines, processes and procedures required for full compliance with applicable California and federal laws, regulations, statutes, and state policy regarding the reporting and notification of information security incidents. The responsibilities may include, but are not limited to:

- Obtain management approval for successful implementation of an incident response plan;
- Work within the governance structure to develop policies, standards, guidelines, processes, and procedures for reporting incidents;
- Develop and disseminate instructional and awareness material to employees and contractors on the procedures for reporting an incident to the appropriate contact person;

- Ensure incident reporting and notification requirements are included in contracts and interagency agreements;
- Ensure incidents are logged and tracked to conclusion; and,
- Ensure lessons learned and corrective action plans are documented and implemented to mitigate further risk.

10.2 Incident Handling

Agencies are responsible for promptly investigating security incidents and events. Agencies should develop and implement processes and procedures to identify the actions to be taken upon discovery of an incident, including notification to executives, legal, public information officers, and other appropriate staff. The formal reporting process and procedures should include reporting forms and a feedback mechanism.

ISO Role

The ISO serves as the primary point of contact for employees and contractors to report incidents. The ISO ensures management is made aware of the incident, that it is documented, including its impact, corrective actions taken, lessons learned, and those correction actions that were implemented. Additionally, the ISO may responsible for:

- Reporting incidents to the appropriate external organizations (e.g., law enforcement, other State or local government affiliates);
- Investigating the incident and documenting the events. In cases where staff within the agency is assigned responsibility for investigating incidents, the ISO should be immediately notified of the incident and provided the information necessary to complete the appropriate reporting; and,
- Working with the agency's legal office and privacy officer to draft notification letters to the affected individuals when the incident involves a breach of notice triggering personal information.

10.3 Incident Notification and Reporting

Per SAM section 4845, agencies are required to notify appropriate state agencies when an incident has occurred. This notification must be made upon discovery of the incident.

ISO Role

The ISO ensures the appropriate state agencies are notified when an incident has occurred. The responsibility may include, but is not limited to:

- Report the incident as outlined in SAM 4845 to the CHP and the SISO.
- Complete the incident report and submit it within 10 business days to the SISO.

Authority	Relationship / Interfaces	References / Tools
• SAM 4845 • HIPAA • Civil Code Section 1798 et al (Information Practices Act of 1977) • Penal Code Section 502 • Civil Code 178.29	• Executive Management • Legal Office • Human Resources/Labor Relations • CIO • SISO • COPP • CHP	• SIMM 65C • SISO - www.infosecurity.ca.gov /incidents/ • CHP - www.chp.ca.gov/ • CalOHI - www.calohi.ca.gov/ • COPP - www.privacy.ca.gov/ • ISO/IEC 27002 • NIST SP 800-61, NIST Computer Forensics Guidance - http://csrc.nist.gov/

Disaster Recovery Management

Agencies must ensure that a disaster recovery plan (also referred to as an operational recovery plan) is in place and routinely tested. The purpose of this plan is to provide for the continued IT support of critical business functions by developing a recovery strategy and procedures that ensures timely resumption of essential IT operations, the recovery of critical applications and information, and the delivery of the services to the workforce and customers.

The ISO leads the planning and oversight and participates in the developing and managing efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 11	ISO Role and Responsibility
Disaster Recovery Management **Objective:** To counteract interruptions to business activities, protect critical business processes from the effects of major failures of information systems or disasters, and ensure their timely resumption. • Disaster Recovery Management – documenting, testing, maintaining, and reassessing recovery plans	**11.1 Disaster Recovery:** Lead in the planning efforts for the agency's disaster recovery plan and provide oversight to ensure it is maintained. Participate in the testing and management of the plan.

11.1 Disaster Recovery

Agencies are required to have a functional and tested disaster recovery plan in place, as outlined in SAM 4843 and 4843.1. The plan provides the agency a systematic and orderly resumption of all computing services should when a disaster or an event that results in an unplanned disruption occurs.

ISO Role

The ISO ensures the agency has in place policies and procedures necessary for the continued operations of IT systems in the event of a disaster or unplanned disruption. The ISO ensures the plan has:

- Met the component requirements outlined in SIMM 65A;
- Been tested on an annual basis and the issues are documented and mitigated;
- Identified supporting utilities required for restoration of those services; and,
- Verified that all Uninterruptible Power Supplies (UPS) and back-up capabilities have been addressed.

Authority	Relationship/Interfaces	References/Tools
SAM 4843, 4843.1	• Executive Management • CIO • Operational/Disaster Recovery Coordinator	• SIMM 65A • SISO - www.infosecurity.ca.gov /ORP/ • OES - www.oes.ca.gov/

Authority	Relationship/Interfaces	References/Tools
	• COOP/COG Coordinator • Office of Emergency Services (OES)	• Disaster Recovery Institute International (DRII) www.drii.org/

Compliance

Compliance refers to the process framework for ensuring conformity to applicable federal and state statutory, regulatory, and contractual requirements and verifying adherence to statewide reporting requirements.

The ISO leads the planning, developing, managing, and oversight efforts. The following table provides the minimal role and responsibility of the ISO that may include, but is not limited to, the activities listed.

Component 12	ISO Role and Responsibility
Compliance **Objective:** To avoid breaches of any law, statutory, regulatory, or contractual obligations, and state requirements. • Identify applicable laws, regulations, statutes and state requirements • Protect organizational records • Protect personal, sensitive and confidential information • Enforce policy, standards, and technical compliance • Validate technical compliance • Conduct information system audits	**12.1 Internal Compliance:** Implement internal procedures to ensure compliance requirements are met, organizational records are protected and controls are in place. **12.2 External Compliance:** Ensure agency is adhering to all applicable laws, regulations, statutes and SAM requirements

12.1 Internal Compliance

To avoid breaches of any law, statutory, regulatory or contractual obligations, and security requirements, all relevant requirements and the agency's approach to meeting those requirements should be defined, documented, and routinely updated. Some examples of these requirements include:

- Software should only be acquired through known and reputable sources, to ensure that copyrights are not violated.
- Storage and handling procedures should be implemented to prevent the loss, destruction, or falsification of important records. Guidelines should be issued on the retention, storage, handling, and disposal of records and information.
- An organizational data protection and privacy policy should be developed and implemented.
- The security of information systems should be regularly reviewed. Managers should regularly review the compliance of information processing within their area of responsibility with the appropriate security policies, standards, and any other security requirements. Audit activities involving checks on operational systems should be carefully planned to measure against compliance requirements.

ISO Role
The ISO ensure compliance requirements are met. The responsibility may include, but is not limited to:

- Develop policy for maintaining software license conditions and disposing of or transferring software to others;
- Develop guidelines for storage and handling of records; including but not limited to databases and accounting records;
- Participate in the development the agency's data protection and privacy policy;
- Ensure the information security program work plan is updated annually and tasks are executed as planned;
- Determine and implement corrective action plans for non-compliance; and,
- Conduct periodic reviews and evaluations of compliance with security policies and standards.

12.2 External Compliance

Agencies must adhere to all applicable laws, regulations, statutes and state requirement, including but not limited to:

- Health Insurance Portability and Accountability Act (HIPPA)
- California Civic Code Section 198 et al (Information Practices Act of 1977)
- California Government Codes, such as 11019.9 (enact and maintain a permanent privacy policy) and 6250-6270 (California Public Records Act)
- Payment Card Industry Data Security Standards (PCI DSS)
- California Financial Integrity and State Manager's Accountability Act
- Family Educational Rights and Privacy Act (FERPA)
- State Administrative Manual (SAM)

ISO Role
The ISO provides oversight to ensure the agency has documentation of its statutory, regulatory and contractual requirements. The applicability of these may vary among agencies. For example, some agencies may be required to comply with PCI DSS if they support online payment applications; others may be required to comply with the HIPAA rules if they support the handling of health-related or health care operations information. This role requires establishing cooperative relationships with staff in the legal, internal audit, privacy, accounting, business services, and information systems areas. The responsibilities may include, but are not limited to:

- Participate in the identification of legal, statutory, regulatory, and state requirements;
- Participate in the development of procedures to ensure compliance with legislative, regulatory, contractual, and state requirements; and,
- Complete and file compliance certifications, such as the annual Agency Designation Letter (SIMM 70A) and the Agency Risk Management and Privacy Program Compliance Certification (SIMM 70C).

Authority	Relationship/Interfaces	References/Tools
SAM 4845	• Executive Management • Technical support staff • Legislative Office • Legal Office • Human Resources/Labor Relations • Training Office • Records Management Office • CIO • DGS • CalOHI • DOF - Office of State Audits and Evaluation	• SISO - www.infosecurity.ca.gov/policy/ • DOF - www.dof.ca.gov/FISA /OSAE/OSAEOverview.asp • DGS - http://sam.dgs.ca.gov/default.htm • CalOHI - www.calohi.ca.gov/ • PCI - https://www.pcisecuritystandards .org/tech/ • NIST SP 800-66 - http://csrc.nist.gov/ • ISO/IEC 27002

Conclusion

The ISO plays a critical role in ensuring an agency's information and it information assets are properly protected, managing vulnerabilities within the infrastructure, managing threats and incidents impacting resources, ensuring policies are in place and employees comply with them, and educating employees about their information security an privacy protection responsibilities.

The position must be strategically placed within the agency and visibly supported by management while carrying out the duties in an effective and independent manner. Possessing both a broad range of business management and technical security skills, and a clear understanding of the agency's business is critical to an ISO's success.

The twelve key components identified in the *Information Security Program Guide for State Agencies* were used in this Guide to support ISOs with their role of proper planning, development, management and oversight of an information security program.

There is no easy solution to implementing an effective information security program within an agency. An effective program cannot be established overnight and will be a continuous ongoing function once established. Appointing a skilled ISO who has the full support of executive management is the first important step necessary to implementing the program.

Glossary

Agency – When used lower case (agency), refers to any office, department, board, bureau, commission or other organizational entity within state government. When capitalized (Agency), the term refers to one of the state's super agencies such as the State and Consumer Services Agency or the Health and Human Services Agency.

Availability - Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]

Biometrics – a technology that measure and analyze human physical and behavioral characteristics for authentication purposes. Examples of physical characteristics include fingerprints, eye retinas, and hand measurements, while examples of behavioral characteristics include signature and typing patterns.

CCTV – an acronym for closed-circuit televisions used for surveillance.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]

Continuity of Operations Plan (COOP) /Continuity of Government (COG) - ensures the continuity of essential functions through a wide range of emergencies and disasters.

Cryptography - a discipline of mathematics and computer science concerned with information security issues, particularly encryption and authentication use in access control.

Demilitarized Zone (DMZ) - a network area that sits between an organization's internal network and an external network, usually the Internet.

Firewall - a piece of hardware and/or software which functions in a networked environment to prevent communications forbidden by the security policy.

Federal Information Processing Standards (**FIPS**) - publicly announced standards developed by the federal government for use by all non-military government agencies and by government contractors**.**

Guideline - a recommended course of action. Guidelines support the policy and the standards.

Health Insurance Portability and Accountability Act (**HIPAA**) **-** requires the establishment of national standards for electronic health care transactions and national identifiers for providers, health insurance plans, and employers.

HVAC - an acronym for "heating, ventilation and air-conditioning," also referred to as climate control.

IDS/IPS - an Intrusion Detection System (IDS) is any device that generally detects unwanted manipulations to systems. An Intrusion Prevention System (IPS) is any device which exercises access control to protect computers from exploitation.

Incident - An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [44 U.S.C., SEC. 3542]

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

Information Security Officer (ISO) – a position that focuses on information security within an organization. Required in state government as defined in SAM Section 4841.

ISO/IEC 27002 (formally 17799v2005) – an information security standard published in July 2007 by the International Organization for

Standardization (ISO) and the International Electrotechnical Commission (IEC).

Malicious Code (Malware) – a program written to deliberately cause an unexpected and/or unwanted event on a computer or network, such as keystroke loggers, spy ware, viruses, worms, Trojan horses.

National Institute of Standardization and Technology (NIST) – The mission of Federal NIST's Computer Security Division is to improve information systems security by raising awareness and conducting research for IT vulnerabilities; developing standards, metrics, tests and validation programs; and developing guidance to increase secure IT planning, implementation, management and operation.

Payment Card Industry Data Security Standards (PCI DSS) – a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

Policy – a broad statement authorizing a course of action to enforce an agency's guiding principles for a particular control domain. Policies are interpreted and supported by standards, guidelines, and procedures.

Procedure - provides instructions describing how to achieve a policy or standard. A procedure establishes and defines the process whereby a business unit complies with the policies or standards of the agency.

Process – a series of actions or operations conducing to an end; *especially* a continuous operation or treatment.

Supervisory Control and Data Acquisition Systems (SCADA) - a large-scale, distributed measurement and control system with processes based industrial, infrastructure or facility.

State Administrative Manual (SAM) - a State of California reference source for statewide policies, procedures, regulations and information developed and issued by authoring agencies such as the Governor's Office, Department of General Services (DGS), Department of Finance (DOF), and Department of Personnel Administration.

State Information Security Office (SISO) - has statewide responsibility and authority over the information security policy identified in SAM Sections 4840 through 4845.

Statewide Information Management Manual (SIMM) -contains instructions, forms and templates that State agencies must use to comply with Information Technology (IT) policy.

Smart Card – a pocket-sized card with embedded integrated circuits used for authentication purposes.

Systems Development Life Cycle (SDLC) – a process used to develop an information system, including requirements, validation, training, and user ownership through investigation, analysis, design, implementation, and maintenance.

Spyware – a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user.

Standard – applies to any definite rule, principle, or measure established by authority.

TCP/IP – an acronym for Transmission Control Protocol/Internet Protocol which is the Internet protocol suite of communications protocols that the Internet and most commercial networks run.

Token – a physical device that an authorized user of computer services is given to aid in authentication.

UPS – an acronym for Uninterruptible Power Supply, and a device or system that maintains a continuous supply of electric power to certain essential equipment that must not be shut down unexpected.