CALIFORNIA JUDICIAL BRANCH

How to Use the Information Systems Controls Framework

A Guide for the California Superior Courts

VERSION 1.3

SEPTEMBER 28, 2015

Table of Contents

1.0 INTRODUCTION

This "How to Use" guide acts as a reference for superior courts to assist them with establishing local policies and procedures based upon the Information Systems Controls Framework published by the Judicial Council. Since the framework was developed to establish a basic security approach at the branch level, this guide identifies the sections of the Information Systems Controls Framework that are most relevant to the superior courts. Superior courts are not required to implement the framework in its entirety, rather the intent is to encourage superior courts to use the framework as a template to develop security policies appropriate to their unique local business requirements. It is intended to be used as a guide, not a benchmark, of what should be done.

This guide is intended to provide a roadmap for courts and does not include all the details required for implementing specific local policies and procedures. Courts should refer to the complete framework document for specific recommendations and best practices.

2.0 INFORMATION SYSTEMS CONTROLS FRAMEWORK

2.1 SCOPE

The information systems controls framework has been developed for the establishment of a standard security approach within the Judicial Branch of California. In order to produce the framework, input was solicited from multiple courts ranging from small to large in size so that a comprehensive framework could be developed that is suitable to all entities within the judicial branch. The framework is designed to set a direction, identify and address areas of concern expressed by entities within the judicial branch, and to document policies and practices that can assist judicial branch entities with their concerns by providing a framework for creating entity-specific security policies and procedures.

The goals of the framework are:

- To suggest an overall information security policy, governance and compliance model for the judicial branch to leverage in building their security programs including roles, responsibilities, and major activities.
- To provide a holistic information security framework that the judicial branch entities can leverage in creating local policies.
- To provide guidance to all members of the judicial branch on the proper handling of sensitive information.
- To provide a basis for security training and educational awareness programs developed by judicial branch entities.

- To provide the basis for the development of implementation standards, procedures, and guidelines for each platform, operating system, application, and security device that can then be monitored and enforced against the policies defined in the framework.

2.2 ORGANIZATIONAL CHARACTERISTICS

The framework establishes how information is to be handled and secured within individual judicial branch entities, how it is exchanged between the judicial branch and local and state justice partners and with the public. Therefore, security controls (administrative and technical) related to access management are of particular importance.

2.3 DOCUMENTATION STRUCTURE

An information security program is supported by a collection of documentation capturing differing levels of detail while maintaining consistent guidance for all participants. The information security program will consist of the following categories of documents:

- **Organizational Policy** – Expresses management's expectations with regard to security and data protection. Generally limited to identification of base principles, roles and responsibilities, and the security framework. This framework provides the organizational policy for individual judicial branch entities.

- **Implementing Policy** – Further refines management's expectations; usually issued by a subordinate business or organizational unit for the purpose of interpreting the organizational policy to local entity practices. These policies will be developed as needed by the local entity.

- **Standards** – Identify specific hardware and software features and products whose use has been determined to be in support of policy. Standards may be established by local entities as needed to support policy objectives and to streamline operations.

- **Procedures** – Support standards and policy by providing step-by-step instructions for the execution of a security process. Judicial branch entities will develop and document procedures to ensure the quality and repeatability of security processes.

- **Guidelines** – Provide recommendations which can be used when other guidance has not been established. Guidelines are usually created at lower operational levels such as departments to address immediate needs until consensus is reached on broader direction.

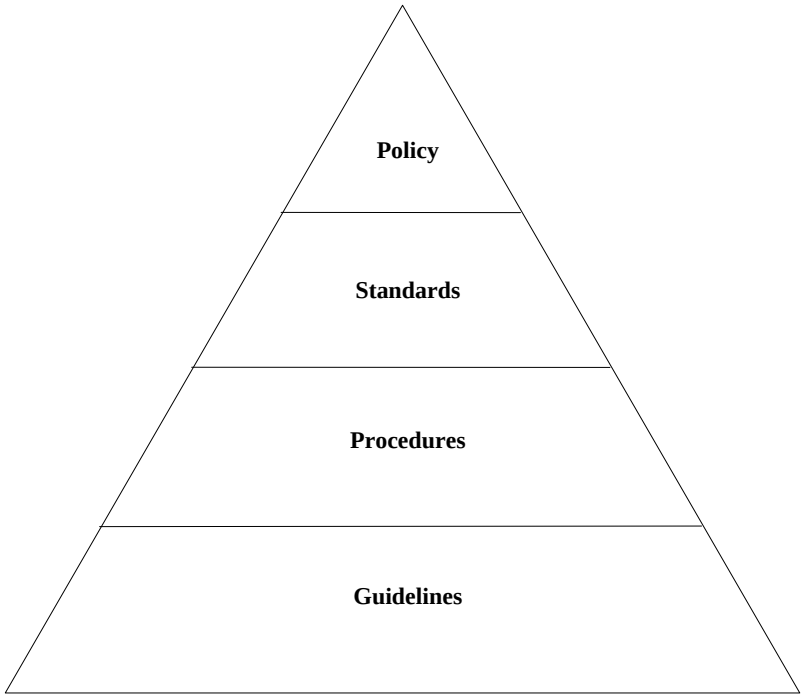

Figure 1: Security Documentation Hierarchy

3.0 PURPOSE OF INFORMATION SECURITY

Information and the supporting processes, systems, and networks are important assets. Defining, achieving, maintaining, and improving information security may be essential to maintain legal compliance, confidentiality, integrity, and availability of information and systems.

Judicial branch entities and their information systems and networks are faced with security threats from a wide range of sources, including computer-assisted fraud, espionage, sabotage, vandalism, fire or flood. Causes of damage (such as malicious code, computer hacking, and denial of service attacks) have become more common, more ambitious, and increasingly sophisticated.

Many information systems have not been designed with security in mind. The security that can be achieved through technical means is limited, and should be supported by appropriate management policies and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management requires, at a minimum, participation by all employees in the branch. It may also require participation from local and state justice partners, the public suppliers, third parties, contract labor, or other external parties. Information Security is a continually evolving area and courts are encouraged to stay informed and educated on current topics and ensure security policies are up to date. Although there is no requirement, it is also a best practice to establish an escalation path to ensure that incidents receive the proper attention based on severity and are processed in a timely manner.

4.0 INFORMATION SYSTEM CONTROLS

Information is an asset, which, like other important business assets, has value to an organization and consequently needs to be suitably protected. Judicial branch entities, as part of their on-going program to maintain adequate and effective controls, want to ensure that the Information Systems - the devices, operating systems, applications, and the sensitive and confidential information - are adequately protected from the risk of loss due to:

- Intentional acts by third-parties inside or outside the organization.
- Inappropriate access by individuals or groups untrained in correct local policies or procedures.
- Accidental loss of a portable device containing confidential information.
- Accidents, natural disasters, or other force majeure.

The document entitled Information Systems Controls Framework, published 08/12/2014 shall serve as the official information security document for the California judicial branch. This framework represents "best practices" and is recommended as a security framework to be used by all judicial branch entities.

5.0 USING THE FRAMEWORK

The Information Systems Controls Framework published by the Judicial Council provides a model that courts can leverage. Superior courts are not required to implement the recommendations contained in the framework but they are encouraged to leverage the framework as appropriate for their unique local business requirements. The framework provides context for a court's local IT security policies. The framework is designed to be modular so that courts can refer only to the sections that are relevant to them. The framework does not recommend any specific technologies that should be implemented nor is the framework of set of policies required for audit compliance.

A local court can utilize the framework and this "how to use" guide in the following manner:

1. Review this "how to use" guide and determine which of the "Recommended Controls for Superior Courts" listed in the next section are relevant to the court's local business environment.
2. The local court then decides what their local policy will be.
3. The local court identifies options for implementing the policy.
4. The local court determines if resources exist to implement the local policy.

Even if there are not enough resources to implement the local policy, steps 1-3 are still useful for documenting a roadmap and plan for when resources become available.

Here is a non-IT example of how the framework could be used:

Domain: Physical Security		
	Recommendation	Source of Recommendation
Step 1: Determine relevant control	Court facilities should be secure	Framework
Step 2: Set local policy	Non-public accessible areas can only be entered through a locked entrance	Local court
Step 3: Identify implementation options	Option 1: Install locks with physical keys Option 2: Install keypad lock Option 3: Install locks with card key readers	Local court
Step 4: Determine available resources	Available resources can only support Option 1.	Local court

Here is an IT example of how the framework could be used:

Domain: Access Control for Mobile Devices		
	Recommendation	Source of Recommendation
Step 1: Determine relevant control	Establish mobile device security policy	Framework
Step 2: Set local policy	▪ Mobile devices must enforce a lock screen PIN. ▪ Only email and calendar synchronization allowed. ▪ Direct access to court network and other court applications prohibited.	Local court
Step 3: Identify implementation options	Option 1: Court IT configures court mobile devices per policy Option 2: Software and configuration settings downloaded by end-user Option 3: Mobile device management software manages device remotely	Local court
Step 4: Determine available resources	No resources available to implement at this time.	Local court

6.0 RECOMMENDED CONTROLS FOR SUPERIOR COURTS

The following chart summarizes the sections of the Information Systems Controls Framework (ISCF) that are most relevant to the superior courts. Courts are encouraged to review the entire framework to determine if other sections could apply to their local business environment.

Each section has been categorized to indicate the primary focus for each section:

- Process – this item generally involves the implementation of a business process if one does not already exist
- Policy – this item generally involves the creation of a policy if one does not already exist
- Technical – this item generally involves the implementation or configuration of technology

Some sections may involve multiple categories of activity. In those cases, the section has been categorized based upon the primary focus for that area.

When creating a set of local IT policies, courts can decide if they prefer to have a single document that contains all the selected sections relevant to their local environment or if they prefer to publish individual policy documents for a particular section or group of sections. Individual documents may make it easier to update a particular section without the need to republish the entire policy document while a single document can used as an all-inclusive publication.

ISCF Section	Title	Summary	Category
Program Management			
4.2	Senior Information Security Officer	Identify someone in the organization that has responsibility for IT security.	Process
4.5	Information System Inventory	Maintain an inventory of information systems.	Process
4.8	Critical Infrastructure Plan	Document critical IT infrastructure and key resources.	Process
4.15	Contacts with Security Groups and Associations	Establish contact with the security community.	Process
Access Control			
5.1	Access Control Policy and Procedures	Document an access control policy.	Policy
5.2	Account Management	Identify account managers and create, modify, and disable system accounts based on authorized access	Process
5.3	Access Enforcement	Enforce system access	Process
5.4	Information Flow Enforcement	Manage the flow of information between systems	Technical
5.6	Least Privilege	Provide only necessary access	Process

5.7	Unsuccessful Logon Attempts	Enforce a limit of invalid logon attempts when appropriate	Technical
5.8	System use Notification	Display logon message that displays privacy and security notices	Technical
5.9	Concurrent Session Control	Limit the number of concurrent session when appropriate	Technical
5.10	Session Lock	Automatically lock session after a defined period	Technical
5.11	Session Termination	Automatically terminate session when appropriate	Technical
5.12	Permitted Actions Without Identification or Authentication	Document actions that can be performed without identification or authentication	Technical
5.13	Remote Access	Establish remote access security policy	Policy
5.14	Wireless Access	Establish wireless access security policy	Policy
5.15	Access Control for Mobile Devices	Establish mobile device security policy	Policy
5.16	Use of External Information Systems	Establish policy for accessing non-Court systems	Policy
5.17	Information Sharing	Establish information distribution rules (e.g. confidential, public, etc.)	Policy
5.18	Publicly Accessible Content	Determine who can publish publicly accessible information	Policy
Awareness and Training			
6.1	Security Awareness and Training Policy and Procedures	Determine how to provide security training and information to personnel	Process
Audit and Accountability			
7.1	Audit and Accountability Policy and Procedures	Determine policy for managing audit information	Policy
7.2	Audit Events	Identify key audit data (e.g. log files)	Technical
7.3	Content of Audit Records	System should generate audit information when appropriate	Technical
7.4	Audit Storage Capacity	Ensure enough capacity for storing audit data	Technical
7.5	Response to Audit Processing Failures	Ensure system audit function is performing	Technical
7.6	Audit Review, Analysis, and Reporting	Review audit data regularly	Process
7.7	Audit Reduction and Report Generation	Ensure ability to generate audit reports	Technical
7.8	Time Stamps	Ensure audit records are time stamped	Technical
7.9	Protection of Audit Information	Ensure authorized access to audit records	Technical
7.10	Non-Repudiation	Ensure validity of audit data cannot be challenged	Technical
7.11	Audit Record Retention	Determine retention period for audit records	Policy

7.12	Audit Generation	Ensure systems generate audit records when required	Technical
Security Assessment and Authorization			
8.3	System Interconnections	Document connections to other systems	Technical
Configuration Management			
9.1	Configuration Management Policy and Procedures	Document roles for managing system configuration	Process
9.2	Baseline Configuration	Document baseline configuration	Process
9.3	Configuration Change Control	Document changes to the system	Process
9.4	Security Impact Analysis	Determine if system changes will impact security	Process
9.5	Access Restrictions for Change	Determine how to restrict system changes	Process
9.6	Configuration Settings	Document key configuration settings	Technical
9.7	Least Functionality	Configure system to provide only essential capabilities	Technical
9.8	Information System Component Inventory	Develop information systems inventory	Process
9.10	Software Usage Restrictions	Ensure software use is consistent with use contract	Process
9.11	User-Installed Software	Establish policy for user-installed software	Policy
Contingency Planning			
10.1	Contingency Planning Policy and Procedures	Document policy for maintaining contingency plan	Policy
10.2	Contingency Plan	Document information system contingency plan (e.g. Continuity of Operations Plans, COOP)	Process
10.3	Contingency Training	Provide contingency training	Process
10.4	Contingency Plan Testing	Test the contingency plan	Process
10.5	Alternate Storage Site	Establish alternate storage site for system backups	Process
10.7	Telecommunications Services	Establish alternate telecommunications services if possible	Technical
10.8	Information System Backup	Conduct system backups	Technical
10.9	Information System Recovery and Reconstitution	Ensure ability to restore from backup	Technical
Identification and Authentication			
11.1	Identification and Authentication Policy and Procedures	Establish identification and authentication policy	Policy
11.2	Identification and Authentication (Organizational Users)	System uniquely identifies and authenticates users acting on behalf of the court	Technical
11.3	Device Identification and Authentication	System uniquely identifies and authenticates devices	Technical
11.4	Identifier Management	Manage device and user names	Technical

11.5	Authenticator Management	Manage authenticators (e.g. passwords, tokens)	Technical
11.6	Identification and Authentication (Non-Organizational Users)	System uniquely identifies and authenticates users who do not act on behalf of the court	Technical
Media Protection			
14.1	Media Protection Policy and Procedures	Establish system media protection policy (e.g. tape, disc)	Policy
14.2	Media Access	Determine who has access to system media	Process
14.3	Media Marking	Mark media for identification and protection	Process
14.4	Media Storage	Protect and store media	Process
14.5	Media Transport	Protect and track media during transport	Process
14.6	Media Sanitization	Sanitize media prior to disposal	Technical
14.7	Media Use	Identify any prohibited media (e.g portable storage)	Policy
Physical and Environmental Protection			
15.1	Physical and Environmental Protection Policy and Procedures	Establish policy for physical environment where information systems are located	Policy
15.2	Physical Access Authorizations	Develop list of individuals who have authorized physical access to information systems	Process
15.3	Physical Access Control	Ensure physical access to information systems is controlled	Technical
15.4	Access Control for Transmission Medium	Ensure physical access to data transmission systems is controlled	Technical
15.6.	Monitoring Physical Access	Enable physical access monitoring	Technical
15.7	Visitor Access Records	Document visitor access to facilities where information systems reside	Process
15.8	Power Equipment and Cabling	Protect power equipment and cabling from damage	Process
15.9	Emergency Shutoff	Provide the capability of shutting off power in emergency situations	Technical
15.13	Temperature and Humidity Controls	Maintain appropriate temperature and humidity levels at information systems facilities	Technical
15.15	Delivery and Removal	Control delivery and removal of information system components to and from the facility as appropriate	Process
15.16	Alternate Work Site	Document information systems requirements, if any, when an alternate work site is used during contingency operations	Process
15.17	Location of Information System Components	Place information systems to minimize potential damage	Process
System and Information Integrity			
21.3	Malicious Code Protection	Employ malicious code protection (e.g. anti-virus)	Technical
21.4	Information System Monitoring	Monitor information systems	Technical

21.5	Security Alerts, Advisories, and Directives	Receive information system security alerts	Process
21.6	Security Function Verification	Control ability to startup, shutdown, and restart systems	Technical
21.8	Spam Protection	Employ spam protection mechanism	Technical
Policy Exceptions			
22.1	Policy Exceptions	Exceptions to published local policies at the discretion of the court CIO or equivalent.	Process