

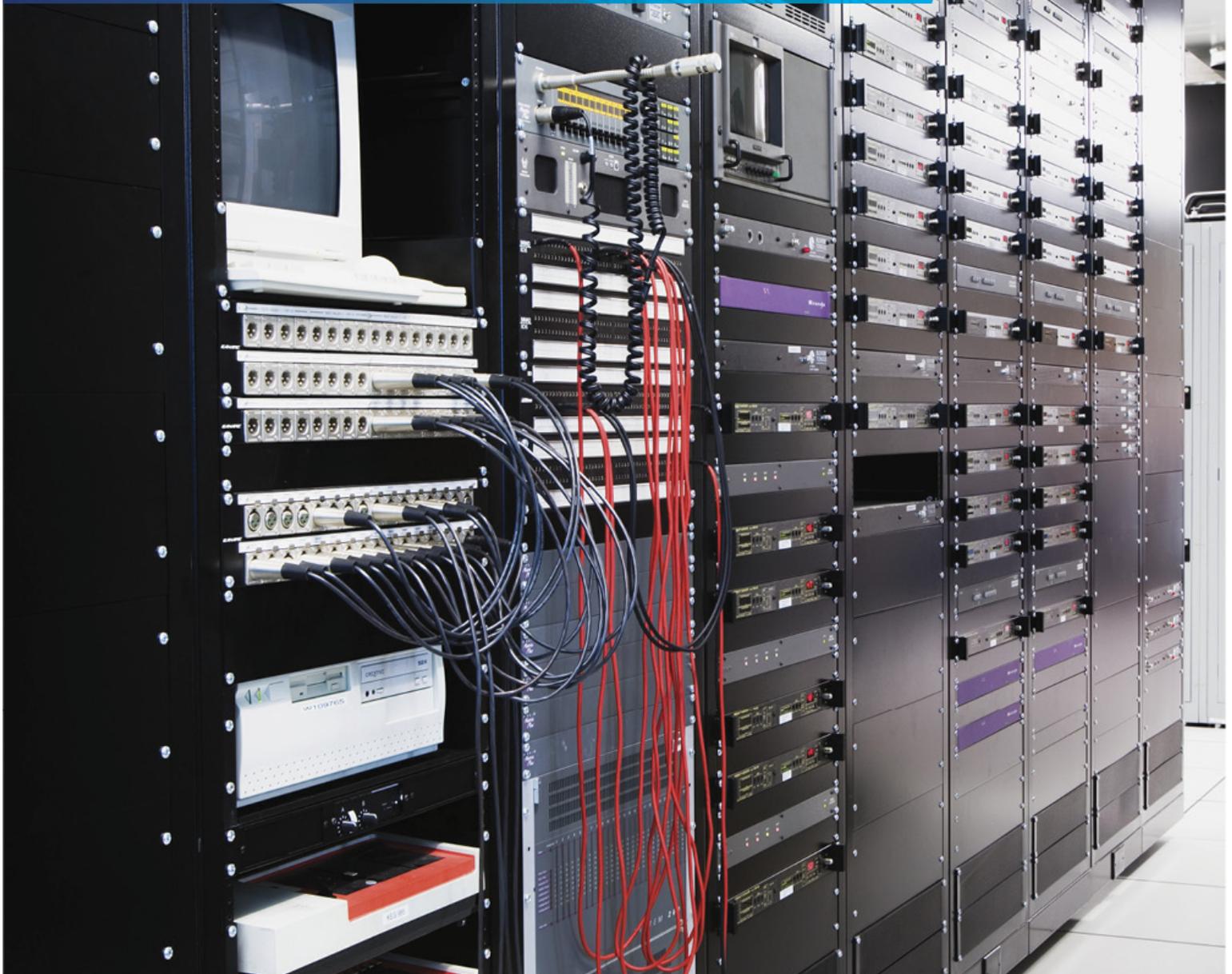


cutting through complexity™



California Statewide Automated Welfare System Consortium-IV

Report on the Description of the C-IV System and
the Suitability of the Design and Operating
Effectiveness of Controls for the Period
July 1, 2010 to June 30, 2011



**California Statewide Automated Welfare System Consortium-IV
Report on the Description of the C-IV System
and the Suitability of the Design and
Operating Effectiveness of Controls**

Contents

Section I Independent Service Auditor’s Report Provided by KPMG LLP	1
Section II Managements’ Assertions and Description of the System Provided by SAWS C-IV and Sub-Service Organizations	4
California Statewide Automated Welfare System Consortium-IV Joint Powers Authority’s (SAWS C-IV) Assertion	5
Accenture’s Assertion	7
Hewlett Packard Enterprise Services’ (HPES) Assertion	9
Managements’ Description of the System	11
Organization Overview	11
Description of Services Provided by Sub-Service Organizations	12
The Primary Sub-Service Organization, Accenture	12
The Secondary Sub-Service Organization, Hewlett Packard Enterprise Services	12
Relevant Aspects of the Control Environment, Risk Assessment and Monitoring	13
Control Environment	13
Risk Assessment	16
Monitoring	16
Information and Communication	18
Information Systems	18
General Computer Controls	18
Communication	19
Control Objectives and Related Controls	21
User Control Considerations	22
Section III Control Objectives, Related Controls and Tests of Operating Effectiveness	23
Control Objective 1 – Security Management	24
Control Objective 2 – Physical and Environmental Security	27
Control Objective 3 – System Access Management	33
Control Objective 4 – Network Security Management	39
Control Objective 5 – Operations Management	41
Control Objective 6 – Systems Development and Change Management	45
Control Objective 7 – Application and Interface Processing	49
Control Objective 8 – Communications Security	50
Control Objective 9 – Reporting	51
Control Objective 10 – Customer Support	53
Section IV Additional Information Provided by Management	56
Managements’ Response to Exceptions Noted in the Results of KPMG’s Testing	57
Disaster Recovery	59

A large blue diagonal graphic that starts from the top-left corner and extends towards the bottom-right corner, creating a split background of blue and white.

Section I
Independent
Service Auditor's
Report Provided
by KPMG LLP



KPMG LLP
Suite 1400
55 Second Street
San Francisco, CA 94105

Independent Service Auditors' Report

The Board of Directors

California Statewide Automated Welfare System Consortium-IV Joint Powers Authority (SAWS C-IV):

Scope

We have examined California Statewide Automated Welfare System Consortium-IV Joint Powers Authority's (SAWS C-IV) (the service organization) and Accenture's and Hewlett Packard Enterprise Services' (HPES) (the sub-service organizations) description of the C-IV System for processing user entities' transactions throughout the period July 1, 2010 to June 30, 2011 (the description) and the suitability of the design and the operating effectiveness of SAWS C-IV's, Accenture's, and HPES' controls to achieve the related control objectives stated in the description. Accenture and HPES are independent service organizations that provide security management, physical and environmental security, system access management, network security management, operations management, systems development and change management, application and interface processing, communications security, reporting, and customer support services to SAWS C-IV. SAWS C-IV's description includes a description of Accenture's and HPES' services used by SAWS C-IV to process transactions for its user entities, as well as relevant control objectives and controls of Accenture and HPES. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of SAWS C-IV's, Accenture's and HPES' controls are suitably designed and operating effectively, along with related controls at the service organization. We have not evaluated the suitability of the design or the operating effectiveness of such complementary user entity controls.

The information in Section IV of management's description of the system, "Other Information Provided by Management" that describes managements' responses to exceptions noted and disaster recovery, is presented by management of SAWS C-IV, Accenture and HPES to provide additional information and is not a part of SAWS C-IV's, Accenture's and HPES' description of its system made available to user entities during the period July 1, 2010 to June 30, 2011. Information about managements' responses to exceptions noted and disaster recovery have not been subjected to the procedures applied in the examination of the description of the system and of the suitability of the design or operating effectiveness of controls to achieve the related control objectives stated in the description of the system, and, accordingly, we express no opinion on it.

Service organization's responsibilities

In their description, SAWS C-IV, Accenture and HPES have provided their assertions about the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description. SAWS C-IV, Accenture and HPES are responsible for preparing the description and for the assertions, including the completeness, accuracy, and method of presentation of the description and the assertions, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks



that threaten the achievement of the control objectives, selecting and using suitable criteria, and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Service auditor's responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description, the suitability of the design and the operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is fairly presented, the controls were suitably designed and the controls were operating effectively to achieve the related control objectives stated in the description throughout the period July 1, 2010 to June 30, 2011.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and the operating effectiveness of those controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described in managements' assertions. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent limitations

Because of their nature, controls at a service organization or subservice organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or subservice organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in SAWS C-IV's, Accenture's and HPES' assertions, (1) the description fairly presents SAWS C-IV's C-IV System and Accenture's and HPES' services used by SAWS C-IV to process transactions for its user entities that were designed and implemented throughout the period July 1, 2010 to June 30, 2011, (2) the controls related to the control objectives of SAWS C-IV, Accenture and HPES stated in the description were suitably designed to provide



reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2010 to June 30, 2011, and (3) the controls of SAWS C-IV, Accenture and HPES that we tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description in Section III were achieved and operated effectively throughout the period July 1, 2010 to June 30, 2011.

Description of tests of controls

The specific controls and the nature, timing, extent, and results of the tests are listed in Section III.

Restricted use

This report, including the description of tests of controls and results thereof in Section III, is intended solely for the information and use of SAWS C-IV, user entities of SAWS C-IV's C-IV System during some or all of the period July 1, 2010 to June 30, 2011, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

KPMG LLP

September 15, 2011
San Francisco, California

Section II

Managements'
Assertions and
Description of the
System Provided
by SAWS C-IV and
Sub-Service
Organizations



California Statewide Automated Welfare Systems (SAWS)

C-IV Project

11290 Pyrites Way, Suite 150
Rancho Cordova, CA 95670-4481

California Statewide Automated Welfare System Consortium-IV Joint Powers Authority's (SAWS C-IV) Assertion

We have prepared the description of California Statewide Automated Welfare System Consortium-IV Joint Powers Authority's C-IV system (the C-IV system or the system) for user entities of the system during some or all of the period July 1, 2010 to June 30, 2011, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a) The description fairly presents the C-IV system made available to user entities of the system during some or all of the period July 1, 2010 to June 30, 2011 for processing their transactions. SAWS C-IV uses Accenture to perform aspects of its security management, physical and environmental security, system access management, operations management, systems development and change management, application and interface processing, communications security, reporting and customer support and Hewlett Packard Enterprise Services (HPES), as a subcontractor to Accenture, to perform aspects of security management, physical and environmental security, system access management, network security management, operations management, and customer support. The description includes both the controls and related control objectives of SAWS C-IV and the control objectives and related controls of Accenture and HPES. The criteria we used in making this assertion were that the description:
 - i. Presents how the system made available to user entities of the C-IV system was designed and implemented to process relevant transactions, including:
 - The types of services provided, including, as appropriate, the classes of transactions processed;
 - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
 - The related accounting records, supporting information and specific accounts that were used to initiate, authorize, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities;
 - How the system captured and addressed significant events and conditions, other than transactions;
 - The process used to prepare reports or other information for user entities;
 - Specified control objectives and controls designed to achieve those objectives;
 - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.
 - ii. Does not omit or distort information relevant to the scope of the C-IV system being described, while acknowledging that the description was prepared to meet the common needs of a broad range of user entities and their financial statement auditors and may not, therefore, include every aspect of the C-IV system that each individual user entity and its auditors may consider important in its own particular environment.
- b) The description includes relevant details of changes to the C-IV system during the period covered by the description.

- c) The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2010 to June 30, 2011 to achieve those control objectives. The criteria used in making this assertion were that:
- i. The risks that threatened achievement of the control objectives stated in the description were identified;
 - ii. The controls identified in the description would, if operated as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
 - iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

A handwritten signature in blue ink, appearing to read 'John Boule', is written over the text of the third list item.

John Boule
Project Director
September 15, 2011



Accenture's Assertion

We have prepared the description of Accenture's services used by California Statewide Automated Welfare System Consortium-IV Joint Powers Authority (SAWS C-IV) and user entities of SAWS C-IV's C-IV system (the C-IV system or the system) during some or all of the period July 1, 2010 to June 30, 2011, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a) The description fairly presents Accenture's services used by SAWS C-IV and user entities of the C-IV system during some or all of the period July 1, 2010 to June 30, 2011 for processing their transactions. The criteria we used in making this assertion, with regard to Accenture's services provided to SAWS C-IV and user entities of the C-IV system, were that the description:
 - i. Presents how the system made available to user entities of the C-IV system was designed and implemented to process relevant transactions, including:
 - The types of services provided, including, as appropriate, the classes of transactions processed;
 - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
 - The related accounting records, supporting information and specific accounts that were used to initiate, authorize, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities;
 - How the system captured and addressed significant events and conditions, other than transactions;
 - The process used to prepare reports or other information for user entities;
 - Specified control objectives and controls designed to achieve those objectives;
 - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.
 - ii. Does not omit or distort information relevant to the scope of Accenture's services, while acknowledging that the description was prepared to meet the common needs of a broad range of user entities and their financial statement auditors, and may not, therefore, include every aspect of Accenture's services that each individual user entity and its auditor may consider important in its own particular environment.
- b) The description includes relevant details of changes to Accenture's services during the period covered by the description.
- c) Accenture's controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2010 to June 30, 2011 to achieve those control objectives. The criteria we used in making this assertion, with regard to Accenture's services provided to SAWS C-IV and user entities of the C-IV system, were that:

- i. The risks that threaten the achievement of the control objectives stated in the description were identified;
- ii. The controls identified in the description would, if operating as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
- iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Daniel P. Dean
Senior Executive, Client Service Delivery Lead
September 15, 2011



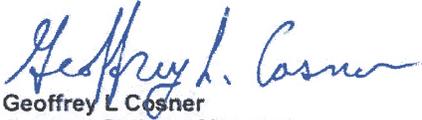
HP Enterprise Services, LLC
181 West Huntington Drive
Suite 101
Monrovia, CA 91016
USA

Hewlett Packard Enterprise Services' (HPES) Assertion

We have prepared the description of Hewlett Packard Enterprise Services' (HPES) services used by California Statewide Automated Welfare System Consortium-IV Joint Powers Authority (SAWS C-IV) and user entities of SAWS C-IV's C-IV system (the C-IV system or the system) during some or all of the period July 1, 2010 to June 30, 2011, and their user auditors who have a sufficient understanding to consider the description, along with other information, including information about controls operated by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that:

- a) The description fairly presents HPES' services used by SAWS C-IV and user entities of the C-IV system during some or all of the period July 1, 2010 to June 30, 2011 for processing their transactions. The criteria we used in making this assertion, with regard to HPES' services provided to SAWS C-IV and user entities of the C-IV system, were that the description:
 - i. Presents how the system made available to user entities of the C-IV system was designed and implemented to process relevant transactions, including:
 - The types of services provided, including, as appropriate, the classes of transactions processed;
 - The procedures, within both automated and manual systems, by which those transactions were initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports prepared for user entities;
 - The related accounting records, supporting information and specific accounts that were used to initiate, authorize, record, process and report transactions; this includes the correction of incorrect information and how information was transferred to the reports prepared for user entities;
 - How the system captured and addressed significant events and conditions, other than transactions;
 - The process used to prepare reports or other information for user entities;
 - Specified control objectives and controls designed to achieve those objectives;
 - Controls that we assumed, in the design of the system, would be implemented by user entities, and which, if necessary to achieve control objectives stated in the accompanying description, are identified in the description along with the specific control objectives that cannot be achieved solely by controls implemented by us; and
 - Other aspects of our control environment, risk assessment process, information and communication systems (including the related business processes), control activities and monitoring controls that were relevant to processing and reporting user entities' transactions.
 - ii. Does not omit or distort information relevant to the scope of HPES' services, while acknowledging that the description was prepared to meet the common needs of a broad range of user entities and their financial statement auditors, and may not, therefore, include every aspect of HPES' services that each individual user entity and its auditor may consider important in its own particular environment.
- b) The description includes relevant details of changes to HPES' services during the period covered by the description.
- c) HPES' controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2010 to June 30, 2011 to achieve those control objectives. The criteria we used in making this assertion, with regard to HPES' services provided to SAWS C-IV and user entities of the C-IV system, were that:
 - i. The risks that threaten the achievement of the control objectives stated in the description were identified;

- ii. The controls identified in the description would, if operating as described, provide reasonable assurance that those risks did not prevent the stated control objectives from being achieved; and
- iii. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.



Geoffrey L. Cosner
Account Delivery Manager
September 15, 2011

Managements' Description of the System

Organization Overview

California's 1995 State Budget Act facilitated the formation of up to four county consortia and delegated authority to each consortium to design an automated welfare system. The California Statewide Automated Welfare System Consortium-IV Joint Powers Authority (SAWS C-IV) was established under section 6500 of the California Government Code for this purpose and was the fourth consortium to be established. It was organized as an independent Joint Powers Authority under applicable California law and included the initial member counties of Merced, Riverside, San Bernardino, and Stanislaus. In July 2007, SAWS C-IV added 35 additional member counties from the Interim Statewide Automation Welfare System (ISAWS) for a total of 39 counties. The 35 counties migrated to the SAWS C-IV System in three waves, with the last wave going live on the system on June 1, 2010. The additional 35 member counties that have been added to SAWS C-IV are Alpine, Amador, Butte, Calaveras, Colusa, Del Norte, El Dorado, Glenn, Humboldt, Imperial, Inyo, Kern, Kings, Lake, Lassen, Madera, Marin, Mariposa, Mendocino, Mono, Monterey, Modoc, Napa, Nevada, Plumas, San Benito, San Joaquin, Shasta, Sierra, Siskiyou, Sutter, Tehama, Trinity, Tuolumne, and Yuba.

SAWS C-IV's mission is to provide an online, customer-based, fully integrated and automated system to assist in the efforts of programs including Temporary Assistance for Needy Families (TANF), Medi-Cal, CalFresh (formerly known as Food Stamps), and employment programs and assist county staff in their efforts to achieve the outcomes and performance goals required by those programs.

The C-IV System is an automated system designed to support the administration of human services and employment programs. The C-IV System is designed to provide its users (i.e., the member counties) the ability to verify public assistance eligibility, compute benefits, provide timely distribution of benefits, reduce administrative complexity, collect data and management information, and provide accurate, timely and useful management and fiscal reports. Within the C-IV System, the member counties are responsible for initiating and authorizing transactions. Recording of the data is performed by the C-IV System based upon the data entered by the member counties. The C-IV System handles the processing of that information, including processing to generate reports. Reporting from the C-IV System is provided to the member counties in the form of State-required reports and supporting detailed reports. Authorized member county users obtain reports generated by the C-IV System on demand via the reporting subsystem. Validation and submission of reports to the State for funding reimbursement are the responsibility of the member counties and follow their procedures.

The SAWS C-IV organization includes a staff of approximately 220 individuals who reside at three locations and who develop, support, and maintain the C-IV System. C-IV personnel include employees of SAWS C-IV and the member counties, the employees of two sub-service organizations (refer below to the Description of Services Provided by the Sub-Service Organizations) and other contractors. The following teams, consisting of SAWS C-IV and sub-service organization personnel, support the C-IV System and services:

- **Executive Management** – Responsible for project oversight, makes decisions on project scope and project staffing, and oversees the maintenance of the technical architecture and the production operation of the C-IV System.
- **Technical Team** – Supports and maintains the C-IV System infrastructure, including code migration for new releases, database administration, support infrastructure management, and operations. Within the Technical Team, the Maintenance and Operations Team is responsible for management of the service desk, remote support and enterprise computing groups, quality management activities, management of network and data center operations, and system administration support.
- **Application Maintenance Team** – Develops enhancements to the C-IV System, creates and maintains system reports, maintains batch processes and interfaces, and maintains C-IV business rules.
- **System Test Team** – Tracks System Change Requests (SCR) and System Information Requests (SIR) through the approval, development, and test stages until changes are incorporated into a release and moved to production. Performs system testing of SCRs and SIRs.

Description of Services Provided by Sub-Service Organizations

SAWS C-IV has contracted with a sub-service organization, Accenture (referred to as the “Primary Sub-Service Organization”) to provide computer processing products, services, and hardware to SAWS C-IV, applicable to the general computer controls over processing of transactions for users of the C-IV System. The Primary Sub-Service Organization has subcontracted certain services to a second sub-service organization, Hewlett Packard Enterprise Services (HPES) (referred to as the “Secondary Sub-Service Organization”).

The services provided by these sub-service organizations are described below. The detailed procedures for providing these services and goods are maintained in various documents at the SAWS C-IV Application Development Facility, including but not limited to, the Systems Operation and Support Plan (SOSP), the Project Control Document (PCD), and an Amended and Restated Revised System Agreement. Additional information is also located in the Information and Communication section of this report. This report addresses the relevant controls of SAWS C-IV, the Primary Sub-Service Organization, Accenture and the Secondary Sub-Service Organization, HPES.

The Primary Sub-Service Organization, Accenture

The Primary Sub-Service Organization is responsible for providing overall project management, application development, implementation, hardware, and maintenance and operations for the C-IV System. Primary Sub-Service Organization staff perform project oversight roles to support the C-IV Project Director (the Project Director) including project advisement, systems security, and project management.

The Primary Sub-Service Organization personnel lead several teams supporting the C-IV System including the Technical Team, System Test Team, Project Management Office, and the Application Development Team.

Primary Sub-Service Organization staff supporting the C-IV System are located primarily at the SAWS C-IV Application Development Facility in Gold River, California.

The Secondary Sub-Service Organization, Hewlett Packard Enterprise Services

The Secondary Sub-Service Organization was subcontracted by the Primary Sub-Service Organization to provide data center and network operations center facilities (as described below) and to provide network and infrastructure, help desk, remote maintenance, and operations support. Secondary Sub-Service organization staff participate as part of the C-IV System maintenance teams, primarily the Technical Team led by the Primary Sub-Service Organization.

Two Secondary Sub-Service Organization facilities are used to support the C-IV System:

- The **Network Operations Center (NOC) and Production Data Center (PDC)** in Monrovia, California is a single facility that houses Operations Management and Service Desk staff. This facility also houses the production C-IV System and the servers that support imaging. The production C-IV System is housed in a secured, dedicated room within the facility.
- The **Development Data Center (DDC)** in Rancho Cordova, California supports development and test environments as well as production mirroring of production data for backup and recovery purposes. The development and recovery C-IV System are housed in a room that is shared with another client of the Secondary Sub-Service Organization.

Each of these Secondary Sub-Service Organization facilities is a “shared services” facility (i.e., multiple clients are supported from each of these locations).

Relevant Aspects of the Control Environment, Risk Assessment and Monitoring

Control Environment

SAWS C-IV emphasizes the importance of internal controls in its policies, procedures, and organizational structure for SAWS C-IV and its sub-service organizations. Key components of the control environment are described below.

SAWS C-IV Governance and Management

Governance of SAWS C-IV is the responsibility of the SAWS C-IV Joint Powers Authority (JPA) Board of Directors, which consists of seven (7) county Directors representing the member counties included in C-IV. Functional oversight and support roles for SAWS C-IV are also provided by the Executive Team which consists of a JPA-appointed Project Director who maintains direct oversight of the C-IV project, Project Managers from the representative counties, a Technical Lead and Application Maintenance Manager, legal support, and a Steering Committee elected by the JPA general membership which consists of the 39 Member Counties. The JPA Board of Directors provides support for the C-IV Project and the C-IV Executive Team. The C-IV Executive Team is responsible for reviewing the resumes of all new key personnel to maintain the quality and qualifications of those working on the C-IV Project. The C-IV Project personnel direct the Primary Sub-Service Organization on functional and technical issues affecting C-IV. An Independent Verification and Validation (IV&V) vendor is utilized on a full time basis to oversee the quality of the C-IV Project work products. Each staff member working on the C-IV Project is required to sign a confidentiality agreement to protect the C-IV System production data.

Security and Acceptable Use Policies

SAWS C-IV management conveys the message that the security and acceptable use of C-IV System cannot be compromised, and it seeks to continually demonstrate, through words and actions, a commitment to strong standards, as highlighted below:

- The C-IV Information Security Policy provides a comprehensive set of security requirements to ensure protection of sensitive C-IV, client, and third party information entrusted to C-IV or to which access is otherwise available. Sections within the Information Security Policy include:
 - Roles and Responsibilities
 - Identification
 - Authentication
 - Access Control
 - Confidentiality
 - Integrity
 - Availability
 - Auditing and Accountability
 - Network Security
 - Application Development
 - Secure Operations.
- The C-IV User Security and Acceptable Use Policies are in place to outline appropriate user security and acceptable use requirements relating to the C-IV assets and information that are within the project's control and use. Sections within the User Security and Acceptable Use Policy include:
 - Scope
 - Compliance
 - General Provisions
 - Security Requirements
 - Password responsibilities
 - Sensitive information
 - Personal information

- Email responsibilities
- Instant messenger responsibilities
- Other security responsibilities
- Privacy and monitoring
- Incident handling
- Physical security
- Acceptable Use Requirements – Includes the following areas of acceptable use and prohibitions:
 - Personal rights, harassment, and workplace hostility
 - Infringement
 - Unauthorized access
 - System operations
 - Unethical behavior
 - Email or other forms of communication
 - Hardware and software acceptable use
- Every individual working on the C-IV project is expected to remain informed of and to comply with the Information Security and User Security and Acceptable Use Policies. These policies are reviewed and communicated to new C-IV and sub-service organization staff upon start on the project. Additionally, upon implementation of any updates to these Information Security and User Security and Acceptable Use Policies, it is communicated to all project staff, who are required to review the revised document.

Commitment to Competence

SAWS C-IV management specifies the level of competence needed for particular jobs and translates the desired levels of competence into requisite knowledge and skills. Relevant controls include:

- Formal job descriptions exist for project staff. Included in the written job descriptions are title, role, responsibilities, and skill requirements needed to perform the jobs adequately.
- Formal background checks are performed by the C-IV project and the sub-service organizations for all SAWS C-IV project staff. When adding new sub-service organization staff members to the C-IV project, various levels of SAWS C-IV and County personnel are involved in the interview process to ensure the desired level of competence exists.
- Confidentiality agreements are signed by each project staff. The agreement contains documentation and additional details on the following key areas: Confidential Information, Developments, Software, Assignment and Disclosure of Developments, Execution of Necessary Documents, Trade Secrets and Confidential Information, Termination, and Other General Provisions.

Management's Philosophy and Operating Style

The philosophy and operating styles of management normally have a pervasive effect on an entity. This philosophy and related styles are evident as follows:

- SAWS C-IV is structured as a consortium of 39 California counties working in cooperation under a State of California mandate for an automated welfare system. Representatives from the counties are assigned to manage the project under a Joint Powers Authority made up of executives from each member county. County project management work in close coordination with sub-service organization management to create a single, unified team environment.
- Personnel turnover in key positions is kept at a minimum.
- Policies and procedures exist to reduce the ongoing risks associated with the project staff (e.g., strict compliance with regulatory requirements, the communication of acceptable use of C-IV resources, roll on procedures that include background checks, etc.).

Organizational Structure

The organizational structure has been designed to monitor the enterprise's activities, encourage the free flow of information and ensure the appropriate segregation of incompatible duties. SAWS C-IV has the following structure in place:

- SAWS C-IV is a Joint Powers Authority Board of Directors comprised of member counties' Welfare Department Directors, who carry ultimate responsibility over the C-IV project. A separate C-IV Steering Committee made up of County Human Services management monitors the activities of the C-IV Project Director and project staff.
- SAWS C-IV contracted a third party sub-service organization, to perform project management, software development, database management, technical architecture management, and other application-related services to SAWS C-IV. The Primary Sub-Service Organization has contracted with another third party company, known as the Secondary Sub-Service Organization to provide data center facilities and operations, network security and server administration, help desk, and other operational functions.
- Limited layers of management exist between C-IV project management and sub-service organization management, who work as a single, unified team. This is an advantage relative to the flow of information, which occurs freely between the three different project entities.
- SAWS C-IV management has kept a static organizational structure. SAWS C-IV organizational roles were defined during development of the C-IV System and have changed little since that time. The major change was regionalization, including the creation of Regional Project Managers to replace County Project Managers, following the migration of the 35 counties. Changes are reviewed by the JPA Board of Directors and C-IV Steering Committee and are made when deemed necessary. One key consideration in determining the organizational structure is the objective of segregating incompatible duties.
- Incompatible duties are segregated among different job functions and are assigned to separate personnel. Segregation between the ability to make software changes on the C-IV System and implement the changes into production is systematically enforced by role-based security. Several layers of approval exist to implement C-IV System changes into production.
- SAWS C-IV has service level agreements (SLAs) in place with the Primary Sub-Service Organization to monitor and manage application and system performance. SAWS C-IV and sub-service organization management monitor application performance continuously then summarize and report to the counties monthly.

Human Resources Management Policies and Practices

SAWS C-IV has a Project Management Office that fulfills the Human Resources (HR) role for the SAWS C-IV organization. SAWS C-IV staff join the project organization as existing staff through one of the C-IV counties, or from existing staff of the Primary Sub-Service Organization or Secondary Sub-Service Organization. The following HR practices are in place at SAWS C-IV:

- Staff Management policies and procedures exist for key HR functions.
- Any departure from established policies and procedures is dealt with by the SAWS C-IV management team and the individual's respective county or sub-service organization management. SAWS C-IV management has the ability to dismiss any C-IV project personnel back to their originating county or to the sub-service organization they are employed with.
- As part of a formalized Staff Management process, communication is initiated by the SAWS C-IV teams to notify the Project Management Office of new additions, status changes and terminations. SAWS C-IV ensures that project staff access to computer systems is removed timely after termination.
- Personnel are made aware of their job responsibilities and SAWS C-IV management's expectations and are evaluated on their performance at least annually.

- Upon joining the C-IV project, county and sub-service organization project staff are informed of SAWS C-IV's strict disclosure policy and are required to sign an Employee Non-Disclosure Agreement. The Project Management Office maintains a signed Employee Non-Disclosure Agreement on file for each individual working on the C-IV project.
- SAWS C-IV has established a privacy policy to govern the actions of all project personnel as they relate to the collection, use, retention, and disclosure of client information. Each C-IV project staff member and representative must abide by SAWS C-IV's commitment to privacy in the handling of client information.

Risk Assessment

The SAWS C-IV Executive Management team, which is composed of the Project Director, Primary Sub-Service Organization Project Manager, and the Independent Verification and Valuation (IV&V) Project Manager, sets the scope and direction of Risk Management. The SAWS C-IV Executive Management team is responsible for a continuous risk appraisal process throughout the C-IV Project's life-cycle. Project Risk Management meetings are held every month to monitor and manage risk to the C-IV System.

The Risk Management database is used to track risks to the success of any portion of the C-IV project. The Project Director reviews those risks weekly.

SAWS C-IV has defined the following objectives of the Risk Management process:

- To minimize threats to achieve the C-IV Project objectives.
- To provide a systematic approach for:
 - Identifying and assessing risks;
 - Determining cost-effective risk reduction actions; and
 - Monitoring and reporting progress in reducing risk.

The overall goal of the Risk Management Strategy is to progressively reduce exposure to events that threaten the accomplishment of the C-IV Project's objectives by:

- Incorporating approaches into the C-IV Project's plans that minimize or avoid identified risks;
- Developing proactive and contingent response actions to identified risks; and
- Rapidly implementing risk responses based on timely identification of a risk occurrence.

Monitoring

Monitoring activities occur at multiple levels within the SAWS C-IV organization and monitoring is the responsibility of each C-IV maintenance team, which includes network operations, the technical team, and the operations team. Service level agreements (SLAs) have been established between SAWS C-IV and the Primary Sub-Service Organization. SAWS C-IV monitors the Primary Sub-Service Organization's adherence to the SLA requirements. System security is monitored through the intrusion detection system and bi-annual security assessments. SAWS C-IV team meetings are also held regularly to monitor relevant activities. For example, the Change Control Board (CCB) meets weekly to review and approve new System Change Requests (SCRs) and Change Orders and to monitor the status of open items, following up if necessary. The SAWS C-IV Executive Team monitors metrics on the number of SCRs entered and the number of hours spent on them. A Risk Management database is used to track risks to the success of any portion of the C-IV Project. The Project Director reviews those risks weekly.

SAWS C-IV management monitors controls to consider whether they are operating as intended and whether the controls are modified appropriately for changes in condition. SAWS C-IV has the following monitoring procedures in place:

- Service level agreements (SLAs) have been established between SAWS C-IV and the Primary and Secondary Sub-Service Organizations. Multiple levels of application and system monitoring have been implemented to monitor application performance daily and compile summary reports monthly. This allows SAWS C-IV to monitor the Primary and Secondary Sub-Service Organization's adherence to the SLA requirements;
- Monitoring activities are performed continually over the C-IV System to detect and correct errors on a timely basis;
- Necessary corrective actions are taken as required to correct deviations from policies and procedures;
- Project staff control activities and related adherence to policies and procedures are reviewed through ongoing monitoring procedures and/or separate independent evaluations;
- Entity-level (e.g., Information Security Policy, etc.) and process-level controls (e.g., periodic reviews, etc.) are reviewed for reasonableness on an on-going basis as part of managements continuous project oversight and monitoring controls (e.g., application user activity logging) are in place to detect and act when controls are circumvented; and
- C-IV management proactively responds to external auditors, independent consultants, and/or client auditors recommendations and where applicable, implements recommendations as a means to strengthen internal controls.

Information and Communication

Information Systems

The C-IV System has a three tier architecture consisting of Apache web servers, WebLogic Application servers, and an Oracle Database running on the Solaris Platform. Users access the C-IV System via web browser.

General Computer Controls

General computer controls establish the control environment in which the C-IV System is developed and operated and impact the effectiveness of controls over the C-IV System.

Security Management

Lead authority for the implementation of C-IV Information Security has been assigned to the Project Director, under the direction of the SAWS C-IV Joint Powers Authority Board of Directors, which has ultimate decision-making responsibility for the C-IV project. The project security organization and a Security Advisory Committee (SAC) whose members are employees or contractors of SAWS C-IV and the C-IV counties assist the Project Director. The C-IV project security organization, led by the System Security Officer (SSO), has overall technical and operational responsibility and authority for the security of the C-IV System. Day-to-day management of C-IV security matters is the responsibility of the Systems Security Officer (who is a Primary Sub-Service Organization employee). The System Maintenance and Operations Team is responsible for implementing and maintaining security controls for the production C-IV System.

Physical Security

The C-IV System is supported by three facilities including the Development Data Center in Rancho Cordova, California, the Application Development Facility in Gold River, California, and the Network Operations Center/Production Data Center in Monrovia, California. Access to the data centers is restricted based on job responsibility. The Development Data Center and Network Operations Center/Production Data Center are leased and operated by the Secondary Sub-Service Organization. Physical access to each facility is controlled using proximity badges or key-fobs that are assigned to authorized personnel only. The computer room located at the Application Development Facility can also be accessed by physical key. Physical keys to the computer room are provided to project staff who require access to the room, and who may need to access the room during power outages. Accessing the room with a physical key does not trigger logging. The computer room does not house the production C-IV System or equipment.

System Access Management

The C-IV System is configured with application security profiles that limit logical access to system functions based on the user's job responsibilities. Individual user access to the C-IV System requires a valid username and password. Access Administrators at the County level are authorized by SAWS C-IV to administer access and assign application privileges to individual County users. System Administrators (sub-services organizations' personnel) administer access privileges for SAWS C-IV and sub-service organization personnel that require access based on their job responsibilities.

The production C-IV Solaris servers are configured to enforce operating system-level security. Solaris servers are hardened with a standard hardening script to ensure consistent application of security. Administrative access is restricted to authorized administrators. All additions, modifications, and terminations of system administrator access follow a standard change management process. Application security and server administration is performed by Secondary Sub-Service personnel.

Network Security Management

The C-IV network perimeter is protected by multiple firewalls. Remote access, where required, is controlled through a virtual private network (VPN). An intrusion detection system (IDS) is in place to monitor and report attack attempts. Network security management, monitoring and administration are performed by Secondary Sub-Service Organization staff.

Network hardware and infrastructure components are configured according to established standards to help ensure consistent network security implementation. Changes to network components are controlled through the change management process.

System penetration testing and vulnerability assessments are also performed periodically to evaluate any network and system vulnerabilities.

Operations Management

C-IV has policies and procedures in place to perform daily operations over the C-IV System to ensure the availability and continuity of the application. This includes real-time backup of production data from the production Oracle database at the Network Operations Center / Production Data Center to a backup database at the Development Data Center backup location, as well as daily backups of all production servers. The application is monitored continuously using a number of different performance monitoring applications during business hours by Secondary Sub-Service Organization staff so errors can be quickly detected and corrected.

Application and Interface Processing

Access to specific functions within the C-IV System is restricted to authorized individuals based on their assigned privileges. The C-IV System performs edit/validation checks for application input fields where appropriate. Application exceptions are automatically logged and then researched by Level III support and corrected through the System Investigation Request (SIR) process.

Batch processing/interface controls exist to ensure that transactions are securely transmitted to interfacing partners and that transmitted files are received completely by SAWS C-IV. The Batch Processing/Interface team reviews lists of fatal and non-fatal job errors daily to ensure that jobs are being processed correctly. Interface development and certain error correction relating to the C-IV infrastructure are performed by the Primary Sub-Service Organization. Batch process monitoring and certain error correction relating to the C-IV infrastructure are performed by the Secondary Sub-Service Organization.

Systems Development Lifecycle and Change Management

A Systems Development Lifecycle (SDLC) has been established to make changes to the C-IV System, including both enhancements and error corrections (bug-fixes). The SCR process is used to make enhancements to the C-IV System, which includes formal documentation, approval, testing, and promotion of the change from development into production. Change approvals go through the CCB made up of C-IV management personnel, who review and approve each SCR request made. The SIR process is similar and is used to track application error fixes to completion.

Application changes are made by authorized technical personnel and are made only after proper approvals have been obtained through the CCB and a release approval meeting. Generic buildmaster accounts are utilized and only authorized technical personnel have knowledge of the password to access these accounts. The generic buildmaster accounts are utilized to perform the following tasks and do not promote application changes into the production environment: run automated jobs that do night assembly test builds, run jobs as needed production builds, run jobs for weekly system test builds and run jobs for weekly rest builds.

Communication

Communication processes are in place help ensure that key messages regarding internal control and executive tone at the top are shared with relevant internal parties across the organization. Additionally, project staff have means to communicate significant control information and report suspected improprieties to management. Relevant aspects include:

- Close teamwork and coordination between C-IV management and the Primary Sub-Service Organization and Secondary Sub-Service Organization facilitates the timely communication of information across the organization.
- Representatives of the counties, Regional Project Managers (RPMs), participate in many of the weekly C-IV management meetings and decision-making processes.

SAWS C-IV has internal communication policies and procedures to help ensure that all C-IV project team members understand their individual role and responsibilities concerning processing and controls and to ensure that significant events are communicated in a timely manner. These include formal and informal training programs, the use of e-mail messages to communicate time-sensitive information, intranet sites, routine team meetings, formal project meetings, and processes for security and availability purposes that notify key personnel via e-mail and pager in the event of problems.

Control Objectives and Related Controls

SAWS C-IV's control objectives and SAWS C-IV and sub-service organizations' related controls are included in Section III of this report, "Control Objectives, Related Controls and Tests of Operating Effectiveness." Although the control objectives and related controls are presented in Section III, they are, nevertheless, an integral part of SAWS C-IV and sub-service organizations' description of controls.

User Control Considerations

The C-IV System was designed with the assumption that internal controls would be implemented by user organizations (i.e., the member counties). These controls should be in operation at each user organization to complement C-IV control policies and procedures. The user control considerations presented below should not be regarded as a comprehensive list of all controls that should be employed by user organizations.

Responsibilities of user organizations that have joined the Joint Powers Authority to use the C-IV System include, but are not limited to, the following:

- User organizations are responsible for performing user security administration of the C-IV System, including granting, modifying, and removing access to both system users and administrators. In addition, each county or other user organization should maintain sufficient controls to ensure that usernames and passwords for their users are kept confidential;
- User organizations should maintain sufficient controls to ensure that access to C-IV System is periodically reviewed;
- User organizations are responsible for managing the strength and complexity of network and application passwords used to access the C-IV System;
- User organizations are responsible for the completeness and accuracy of data entered into the C-IV System.
- User organizations that interface to the C-IV System are responsible for the accuracy and completeness of data transferred from the originating system;
- User organizations that interface to the C-IV System are responsible for the security of the interfaced data file on their networks after transmission across the circuit;
- User organizations are responsible for reviewing reports generated by the C-IV System and reporting any significant exceptions to SAWS C-IV;
- User organizations are responsible for validating, certifying and submitting or disseminating C-IV System generated reports to the State of California and other entities.
- User organizations are responsible for monitoring the activity of their users, as appropriate;
- User organizations are responsible for troubleshooting and resolving system issues – including interface development and error correction – that are related to their network or infrastructure; and
- User organizations should track open problem tickets that are assigned to SAWS C-IV, to monitor whether open tickets are being resolved. In addition, open tickets that are assigned to the counties, should be tracked to resolution.

Section III

Control Objectives,
Related Controls
and Tests of
Operating
Effectiveness

Control Objective 1 – Security Management

SAWS C-IV maintains controls to provide reasonable assurance that management direction and support for information security is provided and security incidents are identified and resolved.

<i>SAWS C-IV's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>1.1 The SAWS C-IV information security policy has been established and covers the following topics:</p> <ul style="list-style-type: none"> - Roles and Responsibilities - Identification - Authentication - Access Control - Confidentiality - Integrity - Availability - Auditing and Accountability - Network Security - Application Development - Secure Operations. 	<ul style="list-style-type: none"> • Inspected the C-IV Information Security Policy to determine whether it exists and covers the required elements. 	<p>No exceptions noted.</p>
<p>1.2 Information security is overseen by the C-IV Project Director and the Systems Security Officer who are responsible for policy administration and monitoring.</p>	<ul style="list-style-type: none"> • Inspected the Systems Operation and Support Plan (SOSP) to determine who has responsibility for policy administration and monitoring related to information security. • Inspected job responsibilities for the Project Director and the System Security Officer to determine whether they include responsibility for information security. 	<p>No exceptions noted.</p>
<p>1.3 The SAWS C-IV Project Director, on behalf of SAWS, is responsible for approving significant modifications to the Information Security policy as necessary. Changes are then communicated to all project personnel.</p>	<ul style="list-style-type: none"> • Inspected approvals and communications for a selection of Information Security Policy updates to determine whether the Project Director approved modifications to the Information Security Policy and whether changes were communicated to all personnel. • Observed the location of the Information Security Policy to determine whether the policy is accessible to all personnel. 	<p>No exceptions noted.</p>

SAWS C-IV's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
1.4 The SAWS C-IV Project Director reviews Security Incident Reports to ensure appropriate corrective action is taken.	<ul style="list-style-type: none"> Inspected documentation for the only security incident during the period to determine whether information security incidents are handled according to established procedures and reporting guidelines and are reviewed by the Project Director. 	No exceptions noted.

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
1.5 The SAWS C-IV Systems Security Officer, on behalf of the Primary Sub-Service Organization, is responsible for approving significant modifications to the Information Security policy as necessary, in coordination with the C-IV Security Advisory Committee (SAC). Changes are then communicated to appropriate project personnel.	<ul style="list-style-type: none"> Inspected approvals and communications for a selection of Information Security Policy updates to determine whether the System Security Officer approved modifications to the Information Security Policy and whether changes were communicated to appropriate project personnel. 	No exceptions noted.
1.6 The Primary Sub-Service Organization maintains confidentiality agreements for each individual working on the SAWS C-IV project.	<ul style="list-style-type: none"> Inspected confidentiality agreements for a selection of Primary Sub-Service Organization employees to determine whether confidentiality agreements are maintained for Primary Sub-Service Organization employees working on the SAWS C-IV project. 	No exceptions noted.
1.7 The Primary Sub-Service Organization has incident handling policies and procedures for the C-IV system. These policies and procedures include coverage of all phases of the Incident Handling Lifecycle: Identification, Containment, Eradication, Recovery and Follow-Up.	<ul style="list-style-type: none"> Inspected the SAWS C-IV SOSP Volumes to determine whether they address handling of Security Incidents. Inspected the SAWS C-IV SOSP Volumes to determine whether procedures are in place for each phase of the security incident handling lifecycle. 	No exceptions noted.

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
1.8 The Secondary Sub-Service Organization maintains confidentiality agreements for each individual working on the SAWS C-IV project.	<ul style="list-style-type: none"> Inspected confidentiality agreements for a selection of Secondary Sub-Service Organization employees to determine whether confidentiality agreements are maintained for Secondary Sub-Service Organization employees working on the SAWS C-IV project. 	No exceptions noted.
1.9 The Secondary Sub-Service Organization has information security incident handling policies and procedures for the C-IV system. These policies and procedures include coverage of all phases of the Incident Handling Lifecycle: Identification, Containment, Eradication, Recovery and Follow-Up.	<ul style="list-style-type: none"> Inspected the SAWS C-IV SOSP Volumes to determine whether they address handling of Security Incidents. Inspected the SAWS C-IV SOSP Volumes to determine whether procedures are in place for each phase of the security incident handling lifecycle. 	No exceptions noted.

Control Objective 2 – Physical and Environmental Security

SAWS C-IV maintains controls to provide reasonable assurance that physical access to facilities housing the SAWS C-IV application and supporting systems are restricted to properly authorized individuals and such facilities are protected from environmental hazards.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
Physical Access Administration		
2.1 The granting of access to the Application Development Facility is approved by the individual's Team Lead in accordance with the C-IV Project Roll-On procedures.	<ul style="list-style-type: none"> Inspected completed roll-on forms for a selection of new SAWS C-IV, Primary Sub-Service Organization and Secondary Sub-Service Organization project staff to determine whether their physical access was approved 	No exceptions noted.
2.2 Physical access to the Application Development Facility is removed within 5 days of project staff termination date.	<ul style="list-style-type: none"> Inspected a system generated list of employees with physical access to the ADF and compared it to a system generated list of terminated employees to determine whether any terminated employees had physical access to the ADF. Inspected evidence of physical access deactivation for a selection of project staff who rolled off the project to determine whether their physical access was revoked within 5 days of their termination date. 	<p>KPMG noted that for 17 of 22 terminated project staff selected, physical access had been removed but there was no documentation of the timing of the removal.</p> <p><i>Refer to Section IV for managements' response.</i></p>

Application Development Facility

2.3 The Application Development Facility is protected by physical site security.

- Access to the Application Development Facility building requires a valid proximity key-fob (after normal business hours).
- Access to the computer room within the Application Development Facility is restricted to authorized personnel through proximity key-fob authentication or physical key access.

- Observed the proximity key-fob readers in operation at the Application Development Facility to determine whether key-fob authentication is required for building access after normal business hours.
- Inspected the Application Development Facility physical access list for all users with key-fob and physical key access to the computer room and reviewed their job responsibilities with management to determine whether access was reasonable based on the users' roles and responsibilities.
- Re-performed an attempt to obtain access to the Application Development Facility computer room with an invalid key-fob from a C-IV project staff person without access to the computer room to determine whether access to the Application Development Facility computer room is restricted.

No exceptions noted.

2.4 Access to the Application Development Facility and computer room is automatically logged.

- Re-performed an entry to the Application Development Facility and computer room using the key-fob access readers and inspected the access log to determine whether entry was logged.

No exceptions noted.

2.5 All entrances to the Application Development Facility are video monitored and recorded.

- Observed the video monitoring and recording operations in place at the Application Development Facility to determine whether all entrances to the Application Development Facility are video monitored and recorded.

No exceptions noted.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
2.6 Support systems housed at the Application Development Facility are protected from power failures and other electrical anomalies using UPS systems.	<ul style="list-style-type: none"> Observed the UPS systems in operation at the Application Development Facility protecting support systems to determine whether the support systems are protected from power failures and other electrical anomalies. Inspected UPS software configurations for monitoring and routine testing of the UPS units to determine whether support systems are protected from power failures and other electrical anomalies. 	No exceptions noted.
2.7 Systems housed in the Application Development Facility computer room are protected by a fire suppression system.	<ul style="list-style-type: none"> Observed the fire suppression system in place in the Application Development Facility computer room to determine whether systems housed in the Application Development Facility computer room are protected. Inspected the most recent fire suppression inspection documentation and the results of inspection to determine whether the fire suppression system at the Application Development Facility is maintained. 	No exceptions noted.

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
Physical Access Administration		
2.8 The granting of access to the Secondary Sub-Service Organization's facilities requires approval from Secondary Sub-Service Organization's C-IV Operations Management personnel.	<ul style="list-style-type: none"> Inspected completed Roll-On forms and the associated emails for a selection of Secondary Sub-Service Organization's new hires granted physical access to the Network Operation Center / Production Data Center to determine whether proper approvals were obtained. 	No exceptions noted.

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>2.9 Physical access to the Secondary Sub-Service Organization's facilities is removed in a timely manner when C-IV project staff members are terminated. A separation checklist is completed for terminated Secondary Sub-Service Organization's staff members.</p>	<ul style="list-style-type: none"> Inspected the system generated list of personnel with access to the Network Operations Center / Production Data Center and Development Data Center and compared it to the system generated list of terminated employees to determine whether any terminated employees had physical access. Inspected Secondary Sub-Service Organization's separation checklists for a selection of terminated project staff to determine whether a checklist was completed and access to the Secondary Sub-Service Organizations facilities was removed timely upon project staff termination. 	<p>No exceptions noted.</p>
<p>2.10 The Secondary Sub-Service Organization's Operations Manager reviews physical access to the Network Operations Center / Production Data Center C-IV areas on a quarterly basis to ensure that access is appropriate.</p>	<ul style="list-style-type: none"> Inspected documentation for a selection of quarters to determine whether the Secondary Sub-Service Operations Manager reviews access to the Network Operations Center / Production Data Center for appropriateness and takes appropriate corrective action. 	<p>No exceptions noted.</p>

Network Operations Center / Production Data Center and Development Data Center

<p>2.11 Production C-IV systems (housed at the Network Operations Center / Production Data Center) and supporting and development systems (housed at the Development Data Center) are protected by multiple levels of physical site security.</p> <ul style="list-style-type: none"> - Access to the Network Operations Center / Production Data Center and Development Data Center buildings is restricted to authorized operations and facilities personnel through proximity badge authentication. - Access to the rooms within the Network Operations Center / Production Data Center and Development Data Center that house C-IV systems is restricted to authorized operations and facilities personnel through proximity badge authentication. 	<ul style="list-style-type: none"> • Observed the proximity badge access readers in operation at the Network Operations Center / Production Data Center and Development Data Center to determine whether access is restricted to authorized operations and facilities personnel through proximity badge authentication. • Inspected the physical access user access lists for the Network Operations Center / Production Data Center and Development Data Center and reviewed job responsibilities with management to determine whether C-IV staff with access to the Network Operations Center / Production Data Center and Development Data Center is appropriate based on job roles and responsibilities. 	<p>No exceptions noted.</p>
<p>2.12 Badge access to the Network Operations Center / Production Data Center and Development Data Center is automatically logged.</p>	<ul style="list-style-type: none"> • Observed an entry using the badge access pads to the Network Operations Center / Production Data Center and Development Data Center and inspected the badge access log to determine whether entry was automatically logged. 	<p>No exceptions noted.</p>
<p>2.13 All entrances to the Network Operations Center / Production Data Center and Development Data Center are video recorded.</p>	<ul style="list-style-type: none"> • Observed the video monitoring and recording operations in place at the Network Operation Center / Production Data Center and Development Data Center to determine whether entrances are video recorded. 	<p>No exceptions noted.</p>
<p>2.14 Visitors to the Network Operations Center / Production Data Center and Development Data Center facilities are escorted and their date and time of entry and departure are recorded.</p>	<ul style="list-style-type: none"> • Observed the front desk reception visitor handling process to determine whether visitors are checked in/out and are escorted. • Inspected visitor logs for a selection of days to determine whether visitors' entry and departure are recorded while on-site at the Network Operations Center / Production Data Center and Development Data Center. 	<p>No exceptions noted.</p>

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
2.15 Production C-IV systems (housed at the Network Operations Center / Production Data Center) and supporting systems (housed at the Development Data Center) are protected from power failures and other electrical anomalies using UPS systems and backup generators.	<ul style="list-style-type: none"> Observed the UPS systems and backup generators in operation at the Network Operations Center / Production Data Center and Development Data Center to determine whether the production and support systems are protected from power failures and other electrical anomalies. Inspected entries in the Network Operations Center / Production Data Center and Development Data Center Generator Log for a selection of weeks to determine whether backup generators are tested weekly. 	No exceptions noted.
2.16 Systems housed at the Production Data Center and Development Data Center are protected by fire suppression systems.	<ul style="list-style-type: none"> Observed the fire suppression systems in place in the Network Operations Center / Production Data Center and Development Data Center C-IV areas to determine whether systems housed in the Network Operations Center / Production Data Center and Development Data Center are protected by fire suppression systems. Inspected the most recent fire suppression system testing documentation and the results of testing to determine whether the fire suppression system at the Network Operations Center / Production Data Center and Development Data Center are tested. 	No exceptions noted.
2.17 Emergency exits at the Network Operations Center / Production Data Center and Development Data Center are alarmed.	<ul style="list-style-type: none"> Observed emergency exits at the Network Operations Center / Production Data Center and the Development Data Center to determine whether emergency exits exist and are alarmed. 	No exceptions noted.

Control Objective 3 – System Access Management

SAWS C-IV maintains controls to provide reasonable assurance that access to the production C-IV system is restricted to properly authorized individuals.

SAWS C-IV's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
User Access Management		
3.1 The granting of access to production C-IV Systems for consortium staff joining the C-IV project team requires approval from C-IV management.	<ul style="list-style-type: none"> Inspected the C-IV Production Environment Access Request form for a selection of new consortium staff granted access to the Production C-IV System during the audit period to determine whether access was approved. 	No exceptions noted.
3.2 C-IV System access for consortium employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.	<ul style="list-style-type: none"> Inspected a system generated list of active C-IV application users and compared it to a list of terminated project staff to determine whether any terminated consortium project staff had C-IV System access. Inspected documentation for a selection of terminated consortium project staff to determine whether access was removed within 5 days of termination or job function change. 	KPMG noted that for 2 of 5 terminated project staff selected, logical access to the C-IV System was removed after 5 days. <i>Refer to Section IV for managements' response.</i>
3.3 SAWS C-IV has defined the following password requirements for access to the production C-IV application and supporting systems. SAWS C-IV directs by policy that personnel should follow these regardless of the system's ability to enforce them: <ul style="list-style-type: none"> - Passwords must be 8 characters in length. - Passwords are required to contain at least one uppercase letter, one lowercase letter, and one special character. - Null passwords are prohibited. - Passwords are set to expire at the following intervals: 30 days for Administrator passwords, 60 days for user passwords, and 180 days for Application passwords used by systems. - Minimum password age is 7 days. - Passwords cannot be reused for one year. - Accounts lock out after 5 invalid password entry 	<ul style="list-style-type: none"> Inspected the SAWS C-IV Information Security Policy's Authentication Policy to determine whether the C-IV password management process exists and covers the required elements. 	No exceptions noted.

SAWS C-IV's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>attempts.</p> <p>Management permits certain system exceptions in the UNIX and Windows environments based on system or business rule limitations:</p> <ul style="list-style-type: none"> - UNIX cannot enforce complex passwords. Complex passwords in Windows are not enforced for 2 Counties per County technical requirements. - Password expiration is not set in UNIX due to technical application requirements. Windows password expiration is set to 60 days. - Minimum password age is not set in UNIX due to technical application requirements. - Account lockout after a number of invalid attempts cannot be enforced in UNIX. <p><i>Also, please refer to controls 3.7, 3.12 and 3.13 for additional test work on passwords.</i></p>		

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
User Access Management		
<p>3.4 The granting of access to production C-IV Systems for Primary Sub-Service Organization staff joining the C-IV project team requires approval from a Primary Sub-Service Organization C-IV team manager or team lead.</p>	<ul style="list-style-type: none"> • Inspected the C-IV Production Environment Access Request form for a selection of new Primary Sub-Service Organization staff granted access to the Production C-IV System during the audit period to determine whether access is approved. 	<p>No exceptions noted.</p>
<p>3.5 C-IV application access for Primary Sub-Service Organization employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.</p>	<ul style="list-style-type: none"> • Inspected a system generated list of active C-IV application users and compared it to a list of terminated project staff to determine whether any terminated Primary Sub-Service Organization project staff had C-IV application access. • Inspected documentation for a selection of terminated Primary Sub-Service Organization project staff to determine whether access is removed within 5 days of roll-off. 	<p>KPMG noted that for 1 of 15 terminated project staff selected, logical access to the C-IV application was removed after 5 days.</p> <p><i>Refer to Section IV for managements' response.</i></p>

Application Access Management

<p>3.6 A unique user ID and password are required for user authentication to the C-IV application.</p>	<ul style="list-style-type: none"> • Inspected a system generated list of C-IV users to determine whether there are any duplicate user IDs for the C-IV application. • Re-performed an attempt to add an existing user ID in the C-IV application to determine whether a unique ID is required for user authentication to the C-IV application. • Re-performed the logon process to the C-IV application and attempted to bypass authentication into the application by typing the Web page names/addresses directly into the Web browser to determine whether the application forces use of user ID and password for user authentication. 	<p>No exceptions noted.</p>
--	---	-----------------------------

<p>3.7 Application password parameters have been configured in accordance with SAWS C-IV password requirements:</p> <ul style="list-style-type: none"> - Passwords must be 8 characters in length. - Passwords are required to contain at least one uppercase letter, one lowercase letter, and one special character. - Null passwords are prohibited. - Passwords are set to expire at the following intervals: 30 days for Administrator passwords, 60 days for user passwords, and 180 days for Application passwords used by systems. - Passwords cannot be reused for one year. - Accounts lock out after 5 invalid password entry attempts. 	<ul style="list-style-type: none"> • Inspected the password settings configuration in the C-IV application to determine whether the C-IV application is configured to enforce the SAWS C-IV password policy requirements. • Observed a password change to an invalid password attempt to determine whether the C-IV application enforces the SAWS C-IV password requirements. 	<p>No exceptions noted.</p>
--	---	-----------------------------

Also, please refer to control 3.3 for additional test work on password policy requirements and controls 3.12 and 3.13 for test work on supporting systems passwords.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
3.8 Access to specific functions within the C-IV application is restricted to appropriate individuals based on their job function.	<ul style="list-style-type: none"> Inspected a system generated list of personnel with "Security" or "System Administrator" privileges within the C-IV application and reviewed their job responsibilities with management to determine whether access to specific functions within the C-IV application is restricted to appropriate individuals based on their job function. Re-performed an attempt within the C-IV application to access an administrator-level function from a lesser level of system access to determine whether the roles/groups are restricting access based on assigned privileges. 	No exceptions noted.

Database Access Management

3.9 Only authorized Primary Sub-Service Organization Database Administrators have administrative access to the production C-IV database.	<ul style="list-style-type: none"> Inspected a system generated list of users with the 'DBA' or 'SYSDBA' roles on the production C-IV database server and compared them to the current employee list and to the organization chart to determine whether access is limited to authorized Oracle Database Administrators. 	No exceptions noted.
--	--	----------------------

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
---	--	---

User Access Management

3.10 The granting of access to production C-IV systems for Secondary Sub-Service Organization staff joining the C-IV project team requires approval from a Secondary Sub-Service Organization C-IV team manager.	<ul style="list-style-type: none"> Inspected the C-IV Production Environment Access Request form for a selection of Secondary Sub-Service Organization Staff who were granted access to the Production C-IV System during the audit period to determine whether access was approved. 	No exceptions noted.
--	---	----------------------

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
3.11 C-IV application access for Secondary Sub-Service Organization employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.	<ul style="list-style-type: none"> Inspected a system generated list of active C-IV application users and compared it to a list of terminated project staff to determine whether any terminated Secondary Sub-Service Organization project staff had C-IV application access. Inspected documentation for a selection of terminated Secondary Sub-Service Organization project staff to determine whether access is removed within 5 days of roll-off. 	<p>KPMG noted that for 1 of 2 terminated project staff selected, logical access to the C-IV application was removed after 5 days.</p> <p><i>Refer to Section IV for managements' response.</i></p>

Operating System Access Management

3.12 Production Windows servers supporting the SAWS C-IV system have been configured in accordance with the SAWS C-IV password requirements.	<ul style="list-style-type: none"> Inspected the Windows group password policy for a selection of servers on the production C-IV network (c-iv.net) to determine whether Production Windows servers supporting the SAWS C-IV system have been configured in accordance with the SAWS C-IV password requirements. 	No exceptions noted.
3.13 Production UNIX servers supporting the SAWS C-IV system have password length configured in accordance with the SAWS C-IV password requirements. Password complexity, expiration and reuse requirements are required by policy but cannot be systematically enforced.	<ul style="list-style-type: none"> Inspected the password settings configuration for a selection of Sun Solaris UNIX servers in the production C-IV application environment to determine whether the SAWS C-IV requirement of password length is enforced. 	Noted UNIX systems are not configured to enforce password complexity, expiration, and reuse requirements as stated in the policy.
3.14 Unix Root and other privileged UNIX access to the C-IV system is restricted to authorized system administration personnel.	<ul style="list-style-type: none"> Inspected SU logs and user access lists for a selection of production Sun Solaris UNIX servers to determine whether only authorized users have production UNIX system administration capabilities. Compared a system generated list of users for a selection of production Sun Solaris Unix servers to the system generated list of terminated employees to determine whether any terminated employees have access to the UNIX servers. 	No exceptions noted.

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>3.15 System administrators are required to use SU when remotely executing commands requiring Unix Root privileges. Root access is only permitted at the console.</p>	<ul style="list-style-type: none"> Inspected Sun Solaris UNIX system configuration parameters for a selection of production C-IV application servers to determine whether they are configured to require SU when remotely executing commands requiring root privileges as well as prevent remote direct login to root and restrict direct root login to the system console. 	<p>No exceptions noted.</p>

Control Objective 4 – Network Security Management

SAWS C-IV maintains controls to provide reasonable assurance that access to the C-IV production network is restricted to authorized individuals and changes to networking equipment are authorized, tested, approved, properly implemented and documented.

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>4.1 SAWS C-IV network firewalls and routers are configured in accordance with C-IV's Network Management Operations policies.</p>	<ul style="list-style-type: none"> Inspected firewall rule sets for a selection of firewalls to determine whether they are configured in accordance with C-IV requirements. Inspected routing tables and access control lists (ACL) for a selection of routers to determine whether they are configured in accordance with C-IV requirements. 	<p>No exceptions noted</p>
<p>4.2 Changes to the production infrastructure environment follow the SAWS C-IV Change Order process which includes the following steps:</p> <ul style="list-style-type: none"> - Change Order initiation by Network Operations Team, System Operations Team, and Technical Team - Change Order review by the Technical Team - Review and approval by the C-IV Technical Manager and C-IV Technical Lead - Change Order scheduling/ implementation. - Change Order close-out. 	<ul style="list-style-type: none"> Inspected supporting documentation for a selection of network infrastructure changes obtained from the change order tracking system to determine whether the Change Order process requirements were followed and required approvals were obtained and documented. 	<p>No exceptions noted</p>
<p>4.3 A Virtual Private Network (VPN) is used to remotely access C-IV's production (c-iv.net domain) and non-production network (c-iv.org domain).</p>	<ul style="list-style-type: none"> Inspected the VPN configuration to determine whether a VPN is used to remotely access C-IV's network and whether data transmission through VPN is encrypted. Inspected the VPN user access list and reviewed their business role with management to determine whether VPN user and administrator access to the non-production and production networks is restricted to personnel with a business need for VPN access. Compared the VPN user access list to the terminated employee list to determine whether any terminated employees had VPN access. 	<p>No exceptions noted</p>

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>4.4 SAWS C-IV has implemented an intrusion detection system (IDS), to detect and report suspicious network traffic on selected network segments, which is monitored by the Secondary Sub-Service Organization's C-IV staff at the Network Operations Center.</p>	<ul style="list-style-type: none"> • Observed IDS monitoring activities for the IDS sensors on the C-IV network to determine whether IDS is operating and IDS activity is monitored by the C IV Network Team at the Network Operations Center. • Inspected the configuration screen of the IDS management console system to determine whether the sensors are placed on the devices identified by C-IV Network Management. • Inspected the IDS log in the IDS management console for each IDS sensor to determine whether the sensors are in operation and are detecting and reporting suspicious network traffic. 	<p>No exceptions noted</p>

Control Objective 5 – Operations Management

SAWS C-IV maintains controls to provide reasonable assurance that production systems and data are backed up to an alternate location; production systems are protected against viruses; and production systems are monitored with appropriate corrective action taken when required.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
5.1 Procedures exist to ensure that corrective action is taken when operational problems or errors are reported.	<ul style="list-style-type: none"> Inspect daily Batch Processing / Interface error reports for a selection of days and the corresponding completed SIRs or other incident handling documentation for the Fatal Batch Processing / Interface errors noted therein to determine whether procedures exist and were followed for reporting and taking corrective action on operational problems or errors. 	No exceptions noted.

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
5.2 Policies and procedures exist to provide guidelines and controls for Network Operations Management and Data Center Operations including the following control areas: <ul style="list-style-type: none"> - Data Center Operations - Network Operations Management - Network Disaster Recovery 	<ul style="list-style-type: none"> Inspected SAWS C-IV policies and procedures to determine whether they exist and provide guidelines and controls for Network Operations Management and Data Center Operations including the following control areas: <ul style="list-style-type: none"> - Data Center Operations - Network Operations Management - Network Disaster Recovery. Observed the location of SAWS C-IV policies and procedures related to Network Operations Management and Data Center Operations to determine whether they are available to employees. 	No exceptions noted

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
5.3 Production C-IV data is replicated offsite daily to the Development Data Center.	<ul style="list-style-type: none"> Inspected the Oracle DataGuard configuration to determine whether the production database is configured to replicate data offsite from the Production Data Center to the Development Data Center multiple times daily. Inspected the production database files for a selection of days to determine whether production C-IV data is replicated offsite at least daily from the PDC to the DDC. 	No exceptions noted.
5.4 The production C-IV application, supporting systems and data are backed up to tape daily according to an established backup schedule.	<ul style="list-style-type: none"> Inspected the backup schedule configuration from the backup software for the Windows and UNIX environments to determine whether production C-IV data is backed up daily according to an established backup schedule. 	No exceptions noted.
5.5 Access to backup media containing production data is restricted to authorized C-IV personnel.	<ul style="list-style-type: none"> Observed the proximity badge access readers and access restrictions in operation at the Network Operations Center / Production Data Center and Development Data Center to determine whether access to backup media containing production data is restricted to authorized personnel. Inspected the physical user access lists from the Network Operations Center / Production Data Center and Development Data Center and reviewed their job responsibilities with management to determine whether access to backup media is restricted to authorized personnel. 	No exceptions noted.

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>5.6 Inventories of SAWS C-IV information technology assets are maintained by the Secondary Sub-Service Organization's C-IV project staff and are updated during the implementation of new hardware and software.</p>	<ul style="list-style-type: none"> • Inspected inventory records for a selection of recently procured equipment to determine whether information technology asset management information is entered into the C-IV tracking system. • Inspected the physical location of a selection of production C-IV system hardware assets identified from the C-IV tracking system to determine whether information technology asset records maintained in the tracking system are accurate. • Inspected C-IV tracking system records for a selection of production C-IV system hardware assets identified from a physical walkthrough to determine whether information technology asset records maintained in the tracking system are complete. 	<p>No exceptions noted.</p>
<p>5.7 Anti-virus software on the enterprise anti-virus server is configured to obtain updated virus definitions daily and the virus definition updates are pulled by client workstations and Windows servers.</p> <p>The C-IV Secondary Sub-Service Organization's team at the Network Operations Center installs and maintains anti-virus software on all Windows servers and desktop machines, including C-IV project staff workstations.</p>	<ul style="list-style-type: none"> • Inspected the enterprise anti-virus server software configuration to determine whether it is configured to obtain updated virus definitions daily. • Inspected anti-virus definition file update configurations for a selection of client workstations and Windows servers to determine whether they are configured to pull virus definitions updates. 	<p>KPMG noted 2 of 15 servers selected did not have the latest anti-virus software definitions installed.</p> <p><i>Refer to Section IV for managements' response.</i></p>

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>5.8 The Secondary Sub-Service Organization project staff monitors C-IV system availability, capacity and performance and follow an Event and Alarm Monitoring, Handling, and Escalation procedure which include event / alarm handling processes to provide a standard means for acting on/correcting events or alarms that take place while monitoring the C-IV network. Faults detected and negative conditions identified are acted upon and escalated as appropriate for resolution / notification.</p>	<ul style="list-style-type: none"> ● Inspected the availability, capacity, and performance monitoring systems configurations to determine whether they are configured to notify the Secondary Sub-Service Organization's C-IV project staff of faults and negative conditions. ● Observed the Secondary Sub-Service Organization's C-IV project staff process to determine whether they are monitoring C-IV's Network system availability, capacity, and performance monitoring systems. ● Inspected evidence for a selection of alerts to determine whether the faults detected and negative conditions identified are acted upon and escalated, as needed, for resolution/ notification. 	<p>No exceptions noted.</p>

Control Objective 6 – Systems Development and Change Management

SAWS C-IV maintains controls to provide reasonable assurance that changes to existing applications and systems are authorized, tested, approved, properly implemented and documented.

<i>SAWS C-IV's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>6.1 SAWS C-IV has established a System Change Request (SCR) process that defines requirements for making changes to the production C-IV application. The process includes the following requirements:</p> <ul style="list-style-type: none"> - Initiate/Request SCR. - SCR is reviewed by the System Change Request Board (SCRB). - SCR is reviewed by the Change Control Board (CCB). - After development, the code is passed to the system test environment. - Once system testing is completed, the code is passed to the staging environment. - SCR is reviewed by the Release Management Team and Project Director for implementation approval. 	<ul style="list-style-type: none"> • Inspected SAWS C-IV Policies and Procedures to determine whether they address the requirements for making changes to the production C-IV application. 	No exceptions noted.
<p>6.2 System change requests are documented in the form of an SCR and tracked using the Serena Tracker tool.</p>	<ul style="list-style-type: none"> • Inspected records in the Serena Tracker system for a selection of system changes to determine whether each was documented and tracked in Serena Tracker through the initiation, approval, testing, and implementation phases. 	No exceptions noted.
<p>6.3 SCRs are reviewed and approved by Change Control Board (CCB).</p>	<ul style="list-style-type: none"> • Inspected System Change Request tickets and Change Control Board (CCB) meeting minutes for a selection of system changes to determine whether each was reviewed and approved by the Change Control Board (CCB). 	No exceptions noted.
<p>6.4 The SAWS C-IV Project Director documents the approval of SCRs to be included in a scheduled release.</p>	<ul style="list-style-type: none"> • Inspected approval documentation for a selection of System Change Requests (SCRs) released during the audit period to determine whether the SAWS C-IV Project Director approved the SCR. 	No exceptions noted.

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
6.5 Logical access to Serena Version Manager is limited to authorized personnel including the following teams: Development, DBA, System Test (Administrators of Tracker and Version Manager), Independent Test, and Team Lead Groups.	<ul style="list-style-type: none"> Inspected access rights for a selection of users from the Serena Version Manager user access list and compare to the organization chart and active employee list and review them with management to determine whether access is restricted to authorized personnel. 	No exceptions noted.
6.6 The development team performs independent peer code reviews on SCRs meeting 40-hour completion minimum criteria.	<ul style="list-style-type: none"> Inspected supporting documentation for a selection of SCRs to determine whether an independent code review was performed on SCRs meeting the 40-hour criteria. 	No exceptions noted.
6.7 System defects, identified in either the production or testing environments, are documented using a System Investigation Request (SIR) and tracked using the Serena Tracker tool in accordance with the SIR process.	<ul style="list-style-type: none"> Inspected System Investigation Requests (SIRs) for a selection of system defects to determine whether system defects were documented in System Investigation Requests (SIRs) and tracked to completion using the Serena Tracker application. 	No exceptions noted.
6.8 System Change Requests (SCRs) undergo testing before implementation into C-IV Production Release.	<ul style="list-style-type: none"> Inspected System Change Request (SCR) testing documentation for a selection of changes to determine whether testing was performed prior to inclusion into a C-IV Production Release. 	No exceptions noted.
6.9 A Release Management Team has been established to recommend release approval. The team holds a "Green Light" meeting before each major release to determine the content of the release based on acceptance criteria.	<ul style="list-style-type: none"> Inspected the Release Management Team's Release notes for a selection of implemented System Change Requests (SCRs), to determine whether the SCRs were discussed in a "Greenlight" meeting and were included in the release based on acceptance criteria. 	No exceptions noted.

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>6.10 Development, testing, and staging environments are physically and logically separated from the production C-IV environment. Developers and System Testers do not have access to promote code changes from the development and testing environments into production.</p>	<ul style="list-style-type: none"> • Inspected the Serena Version Manager user access configuration to determine whether access to promote changes is restricted to authorized users. • Inspected the user access list for the Serena Version Manager system and compared it to the organization chart to determine whether only authorized users have administrative access, based on their job roles and responsibilities, and whether developers & system testers have access to promote code changes to the staging (pre-production) environment for release into C-IV production. • Inspected the data centers and the network addresses for the supporting servers to determine whether the Development/Test environment is physically and logically separated from the Production C-IV Environment. 	<p>No exceptions noted.</p>
<p>6.11 Priority-fix SCRs that are implemented between regularly scheduled releases are subject to the standard SCR process after implementation.</p>	<ul style="list-style-type: none"> • Inspected supporting documentation for a selection of priority changes to determine whether the System Change Request (SCR) process requirements were followed and required approvals were obtained and documented after implementation. 	<p>No exceptions noted.</p>
<p>6.12 Changes to the production environment follow the SAWS C-IV Change Order process which includes the following steps:</p> <ul style="list-style-type: none"> - Change Order initiation by Service Desk/ Network. Operations Center/ Primary Sub-Service Organization personnel. - Change Order review by the Technical Team. - Configuration Control Board review. - Change Order scheduling/ implementation. - Change Order close-out. 	<ul style="list-style-type: none"> • Inspected supporting documentation for a selection of network infrastructure changes to determine whether the Change Order process requirements were followed and required approvals were obtained and documented. 	<p>No exceptions noted.</p>

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
6.13 The ability to implement database changes is restricted to the database administrators (DBAs).	<ul style="list-style-type: none"> Inspected a user access list for a selection of users with the 'DBA' or 'SYSDBA' roles on the production C-IV database server to determine whether access is limited to authorized Oracle Database Administrators. 	No exceptions noted.
6.14 Database changes are implemented in accordance with the SCR process.	<ul style="list-style-type: none"> Inspected change control documentation for a selection of database changes to determine whether they are implemented in accordance with the System Change Request (SCR) process. 	No exceptions noted.
6.15 The Project for C-IV County Migration follows a SDLC that includes initiation, planning, development, testing and implementation phases.	<ul style="list-style-type: none"> Inspected the County Migration and Implementation documentation to determine whether the project is following the SDLC and contains the required deliverables for each phase. 	No exceptions noted.

Control Objective 7 – Application and Interface Processing

SAWS C-IV maintains controls to provide reasonable assurance that application and interface processing are monitored and exceptions are identified and resolved.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
7.1 Job design documents exist for each C-IV application batch process/interface to ensure field types, lengths, and formats are properly defined and translated.	<ul style="list-style-type: none"> Inspected design documents for a selection of C-IV jobs to determine whether job design documents exist for each C-IV application batch process/interface selected and include the required elements. 	No exceptions noted.
7.2 The application performs automated checks to help ensure that files are fully downloaded and properly formatted before processing by the application.	<ul style="list-style-type: none"> Inspected the application code to determine whether the application is configured to check if the file is fully downloaded. Inspected the most current execution log file for a selection of batch jobs/interfaces to determine whether the application checked the data structure of downloaded files. 	No exceptions noted.
7.3 Error notifications for rejected interface files, transmission errors and record drops are reviewed by the batch processing team and tracked to resolution.	<ul style="list-style-type: none"> Inspect Batch Processing/interface error reports from a selection of days and inspected completed SIRs or other documented procedures performed for Fatal Batch Processing/Interface errors to determine whether the Batch team receives and reviews Batch Processing/interface error reports daily and follows the System Investigation Request (SIR) process to correct major interface errors. 	No exceptions noted.

Control Objective 8 – Communications Security

SAWS C-IV maintains controls to provide reasonable assurance that data transmissions between SAWS C-IV and its users are secured through encryption or private circuits.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
8.1 All connections between the C-IV system border routers and interfacing entities are private, dedicated circuits.	<ul style="list-style-type: none"> • Inspected invoices for private circuits for WAN connections on the C-IV network to determine whether the WAN connections on the C-IV network are private and dedicated circuits. • Inspected the configuration of the border router to determine whether all connections between the C-IV system border routers and interfacing entities are private, dedicated circuits. 	No exceptions noted.
8.2 Secure FTP is used to transfer sensitive files between C-IV and interfacing entities over the private circuits.	<ul style="list-style-type: none"> • Inspected the firewall configuration to determine whether SFTP is enabled on the Internet-facing firewalls. Also noted that FTP is allowed for other specific purposes and is limited to specific IP addresses. 	No exceptions noted.
8.3 In-transit communications via the C-IV System's Web-based user interfaces are protected.	<ul style="list-style-type: none"> • Observed that an SSL is in operation on the C-IV production application when a user logs-into the webpage. • Inspected the SSL server configuration to determine whether it is configured to protect the C-IV System's Web-based user interfaces through the use of SSL. 	No exceptions noted.

Control Objective 9 – Reporting

SAWS C-IV maintains controls to provide reasonable assurance that output reports are produced timely and delivered to the correct recipient.

SAWS C-IV's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>9.1 From July 2010 through March 2011, the Reports Sub-Committee (County Report Leads, C-IV Business Analysts, Reports Team) meet every other month to review necessary report changes and bug fixes. Starting in March 2011, the Reports Sub-Committee meets on a quarterly basis to review necessary report changes and bug fixes. These changes and bug fixes follow the System Change Request (SCR) and System Investigation Request (SIR) processes, respectively.</p>	<ul style="list-style-type: none"> • Inspected Reports Sub-Committee meeting minutes for a selection of months/quarters to determine whether the Reports Sub-Committee meets to review report changes and bug fixes. • Inspected SCRs and SIRs discussed in a selection of Reports Sub-Committee meeting minutes to determine whether report creation and modification followed the established SCR and SIR processes. 	<p>No exceptions noted.</p>

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>9.2 The Primary Sub-Service Organization's C-IV Reporting Team follows the System Change Requests (SCR) and System Investigation Requests (SIR) processes for the creation of new reports, the modification of existing reports, and report bug fixes.</p>	<ul style="list-style-type: none"> • Inspected documentation for a selection of SCRs associated with report creations/ modifications to determine whether they follow the SCR process for creation of new reports and modification of existing reports. • Inspected documentation for a selection of SIRs associated with defect fixes for existing reports to determine whether they follow the SIR process for defect fixes. 	<p>No exceptions noted.</p>
<p>9.3 The System Test team develops, documents, and maintains sets of test scenarios to test report-related System Change Requests (SCRs), ensuring the scenarios are representative of production cases.</p>	<ul style="list-style-type: none"> • Inspected test scenario documentation for a selection SCRs associated with report creations / modifications to determine whether the test team develops, documents, and maintains sets of test scenarios to test report-related SCRs. 	<p>No exceptions noted.</p>

Primary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>9.4 The C-IV Batch Team / Operations Team reviews batch jobs when errors occur. If a report-related error occurs, an automated email is sent to the batch and report teams and the report team will take action. If necessary, a SIR is created to identify and correct the report-creation error.</p>	<ul style="list-style-type: none"> • Inspected the automated batch job error code configuration to determine whether it is configured to produce an automated email if there is a report related error. • Inspected the automated email that is sent to the Batch Team and Report Team to determine whether it indicates whether a report was skipped. • Inspected the documentation for a selection of report related errors to determine whether an email is sent to the Reports Team notifying them of the errors and if necessary the Reports Team performed corrective action. 	<p>No exceptions noted.</p>
<p>9.5 Reports are made available to authorized County users through the SAWS C-IV Web-based system.</p>	<ul style="list-style-type: none"> • Inspected the SAWS C-IV Web-based system configuration to determine whether it restricts access to reports to authorized County users. • Observed the log in process to the SAWS C-IV web-based system using a specific County ID and inspected the reports available to that user to determine whether reports are made available to only authorized County users. 	<p>No exceptions noted.</p>

Control Objective 10 – Customer Support

SAWS C-IV maintains controls to provide reasonable assurance that problems impacting C-IV system users are appropriately addressed in a timely manner.

<i>SAWS C-IV's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>10.1 SAWS C-IV Project Management has a Service Level Agreement (SLA) with the Primary Sub-Service Organization that defines maintenance and operation performance standards covering performance, service desk, system availability, and system planning.</p>	<ul style="list-style-type: none"> Inspected the Service Level Agreement between SAWS C-IV and the Primary Sub-Service Organization to determine whether it addresses maintenance and operation performance standards covering performance, service desk, system availability, and system planning. Inspected Service Level Agreement Performance Reports for a selection of months to determine whether they are sent to SAWS C-IV project staff and include performance, service desk, system availability and system planning metrics. 	No exceptions noted.

<i>Primary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>10.2 The Primary Sub-Service Organization's C-IV Project staff report on adherence to SLAs to SAWS C-IV Project Management monthly.</p>	<ul style="list-style-type: none"> Inspected Service Level Agreement Performance Reports for a selection of months to determine whether they are sent to SAWS C-IV project staff and include performance, service desk, system availability and system planning metrics. 	No exceptions noted.
<p>10.3 A three-tier, multi-branch support structure is in place to support the tracking and resolution of problems reported by County Users. The Primary Sub-Service Organization performs the following level of support:</p> <ul style="list-style-type: none"> Level III Support – Primary Sub-Service Organization staff (including Developers, Technical Architecture Team members, and DBAs) handle technical issues that cannot be addressed by the Secondary Sub-Service Organization's Level I and II support. Certain problems may be routed back to the Counties if necessary. 	<ul style="list-style-type: none"> Inspected closed service desk tickets for a selection of reported problems to determine whether there is evidence of handling by Level I, II and III support, indicating a three-tier, multi-branch support structure is in place to support the tracking and resolution of problems reported by County Users. 	No exceptions noted.

<i>Secondary Sub-Service Organization's Description of Controls</i>	<i>KPMG's Tests of Operating Effectiveness</i>	<i>Results of KPMG's Tests of Operating Effectiveness</i>
<p>10.4 The Secondary Sub-Service Organization's C-IV Service Desk serves as the point of contact for C-IV system users to report incidents and problems and to request other C-IV system maintenance and operations services. Problem tickets are created, updated and tracked to completion by C-IV Service Desk Staff using CA-Unicenter's Service Desk application.</p>	<ul style="list-style-type: none"> ● Observed the Service Desk Operations at the Secondary Sub-Service Organization Network Operations Center to determine whether the Service Desk serves as the point of contact for C-IV system users to report incidents and problems and to request other C-IV system maintenance and operations services. ● Inspected closed service desk tickets for a selection of reported problems to determine whether tickets are created, updated, and tracked to completion in a timely manner. ● Inspected open service desk tickets for a selection of reported problems that are still open to determine whether timely action is being taken to resolve the issue. ● Inspected meeting minutes for a selection of weekly Maintenance and Operations meetings to determine whether the a "new, open and closed service requests by week" report is provided. 	<p>No exceptions noted.</p>

Secondary Sub-Service Organization's Description of Controls	KPMG's Tests of Operating Effectiveness	Results of KPMG's Tests of Operating Effectiveness
<p>10.5 A three-tier, multi-branch support structure is in place to support the tracking and resolution of problems reported by County Users. The Secondary Sub-Service Organization performs the following level of support:</p> <ul style="list-style-type: none"> - Level I Support – Secondary Sub-Service organization support staff handle the initial user contact, problem ticket creation and tracking, and troubleshooting. - Level II Support – Secondary Sub-Service organization support staff classifies the problem as technical, functional, or database-related and attempt to resolve the problem. Database-related problems and other problems that cannot be resolved by Level II Support are routed to the Primary Sub-Service Organization's - Certain problems may be routed back to the Counties if necessary. 	<ul style="list-style-type: none"> • Inspected closed service desk tickets for a selection of reported problems to determine whether there is evidence of handling by Level I, II and III support, indicating a three-tier, multi-branch support structure is in place to support the tracking and resolution of problems reported by County Users. 	<p>No exceptions noted.</p>

Section IV

Additional
Information
Provided by
Management

Managements' Response to Exceptions Noted in the Results of KPMG's Testing

The following are management's responses to the exceptions noted in the results of KPMG's testing as described in Section III.

Control Objective and Control Activity Description	Exception Noted by KPMG	Managements' Response
<p><i>Objective 2—Physical and Environmental Security</i></p> <p>2.2—Physical access to the Application Development Facility is removed within 5 days of project staff termination date.</p>	<p>KPMG noted that for 17 of 22 terminated project staff selected, physical access had been removed but there was no documentation of the timing of the removal.</p>	<p>As a result of last year's SAS No. 70 examination, we modified our process. The change led to tracking when the request to remove physical access was made and not when the key fob was returned or access was deactivated. Notwithstanding, access for all 22 individuals was removed prior to the end of the period.</p>
<p><i>Objective 3—System Access Management</i></p> <p>3.2—C-IV System access for consortium employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.</p>	<p>KPMG noted that for 2 of 5 terminated project staff selected, logical access to the C-IV System was removed after 5 days.</p>	<p>These two incidents occurred prior to a process change that was implemented as a result of the feedback provided in last year's SAS No. 70 examination. Management feels sufficient processes are now in place to provide reasonable assurance that similar occurrences will not happen again. Additionally, the logical access logs indicate none of the terminated project staff accessed the C-IV application after their roll-off date.</p>
<p><i>Objective 3—System Access Management</i></p> <p>3.5—C-IV application access for Primary Sub-Service Organization employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.</p>	<p>KPMG noted that for 1 of 15 terminated project staff selected, logical access to the C-IV application was removed after 5 days.</p>	<p>This incident occurred prior to a process change that was implemented as a result of the feedback provided in last year's SAS No. 70 examination. Management feels sufficient processes are now in place to provide reasonable assurance that similar occurrences will not happen again. Additionally, the logical access logs indicate this terminated project staff did not access the C-IV application after their roll-off date.</p>
<p><i>Objective 3—System Access Management</i></p> <p>3.11—C-IV application access for Secondary Sub-Service Organization employees is removed within 5 days of termination or when the employee no longer requires such access due to a change in job function.</p>	<p>KPMG noted that for 1 of 2 terminated project staff selected, logical access to the C-IV application was removed after 5 days.</p>	<p>This individual's access was found during an internal PMO review on 4/20/2011 and their access was deactivated that day. We have verified that this individual did not access the C-IV application after their roll-off date.</p>

Control Objective and Control Activity Description	Exception Noted by KPMG	Managements' Response
<p><i>Objective 5—Operations Management</i></p> <p>5.7— Anti-virus software on the enterprise anti-virus server is configured to obtain updated virus definitions daily and the virus definition updates are pulled by client workstations and Windows servers.</p> <p>The C-IV Secondary Sub-Service Organization's team at the Network Operations Center installs and maintains anti-virus software on all Windows servers and desktop machines, including C-IV project staff workstations.</p>	<p>KPMG noted 2 of 15 servers selected did not have the latest anti-virus software definitions installed.</p>	<p>One of the servers is a secure server that does not have access to the internet. The Server was missing the latest CA Unicenter patch that allows the server to receive virus definition updates (which were approximately 1 month old). The patch has been installed and the definitions are up to date.</p> <p>The other server is a NAIT (integration testing) server. The server successfully downloaded updates until June. No reason has been found as to why it stopped downloading updates. The server was checked for viruses and found to be clean. A change was implemented to add a conditional forwarder to every domain (previously not an option since we were using Windows 2000, but now we have upgraded to Windows 2008 where this option is available). Additionally, a DNS entry has been added in the event that a short name or .com name is used.</p>

Disaster Recovery

The C-IV disaster recovery approach relies upon the C-IV system's high-availability, modular, and fault tolerant design and uses the development data center as a hot site. The Development Data Center provides a fully equipped backup site capable of supporting the level of service required for emergency processing during the disaster recovery period.

SAWS C-IV has established disaster recovery procedures as described below. The Maintenance and Operations Management Team is responsible for assignment and implementation of these disaster recovery procedures.

SAWS C-IV overall disaster recovery procedures focus on four core areas:

- Emergency Response – This procedure is used for Emergency Response activities in the event of a disaster affecting the Network Operations Center / Production Data Center and includes contacting the appropriate emergency service agencies and notifying the Emergency Management Team. SAWS C-IV is responsible for the official Emergency Declaration.
- Disaster Recovery Migration – This procedure is used for migration of C-IV production operations to the Development Data Center within 24 hours of declaring a disaster.
- Resume Production Operations – This procedure is used for the return of C-IV production operations to the Network Operations Center / Production Data Center once the capacity to host the C-IV System has been restored.
- Recovery Testing – This procedure is used for the testing and maintenance of the C-IV Disaster Recovery procedures for restoration of business critical production operations in the event of a disaster affecting the Network Operations Center / Production Data Center.

SAWS C-IV network disaster recovery procedures focus on two core areas:

- Network Disaster Recovery – This process provides the procedures used to relocate and enable production operations using the Development Data Center.
- Network Return to Production Site – This process provides the procedures used to move production operations back to the Network Operations Center / Production Data Center.