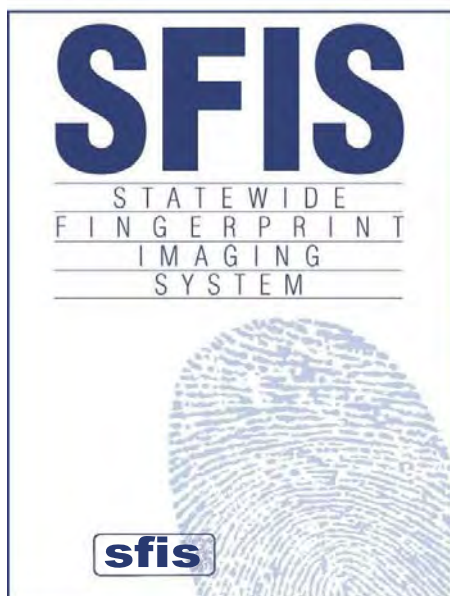


Statewide Fingerprint Imaging System (SFIS)

Risk Management Plan



VERSION 4.0

December 2009



APPROVAL

Project Name: Statewide Fingerprint Imaging System (SFIS)

Document Name: SFIS Risk Management Plan

Approval Signature:

OSI

Dave Sakauye
SFIS Project Manager

Date



TABLE OF CONTENTS

PURPOSE.....	1
REFERENCED DOCUMENTS.....	2
DEFINITIONS.....	4
SFIS RISK MANAGEMENT	10
<i>Risk Management Approach</i>	11
<i>Roles and Responsibilities</i>	13
SFIS Risk Management Responsibilities.....	13
<i>Risk Management Process</i>	16
Step 1 – Identify.....	16
Step 2 – Analyze	20
Step 3 – Plan	30
Step 4 – Implement	33
Step 5 – Track / Control.....	34
<i>SFIS Project Risk Management Process Summary</i>	36
SAMPLE REPORTS AND FORMS	41
<i>Risk Management Reports</i>	41
New / Open Risks	41
Closed / Void Risks	44
RISK MANAGEMENT DATABASE – PACS	46
<i>Risk Management Menu</i>	46
<i>Risk Management List</i>	47
<i>Risk Management Reports</i>	48
<i>Risk Management Record Maintenance</i>	49
Identification.....	49
Description.....	50
Assessment — Impact.....	51
Assessment — Recommended Response	52
Assessment — Response and Control	53
Implementation Plan	54
Closure	55
AMENDMENT HISTORY	56



PURPOSE

This document describes the Office of System Integration (OSI) (formerly Health and Human Services Data Center (HHSDC))’s Risk Management Plan (RMP) for the State of California’s Statewide Fingerprint Imaging System (SFIS) Project. The plan is used for Maintenance and Operations (M&O) activities including activities associated with In-Home Supportive Services (IHSS). The RMP defines the Risk Management process to be followed by the SFIS Project, including the roles and responsibilities of OSI’s SFIS Project Management Office / Quality Assurance (PMO / QA) support as well as the contractor, Hewlett Packard (HP) when necessary.

OSI’s SFIS PMO / QA staff will update the RMP periodically as a result of continuous process improvement efforts and changes to applicable standards.



REFERENCED DOCUMENTS

The following documents were used as reference material in the development of the SFIS Risk Management Plan.

- IEEE Standard 1012-1998: IEEE Standard for Software Verification and Validation, March 9, 1998.
- A Guide to the Project Management Body of Knowledge¹, William R. Duncan, PMI Standards Committee, Project Management Institute, 2000.
- Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, Version 1.0, Brian P. Gallagher, Christopher J. Alberts, and Richard E. Barbour, Software Engineering Institute, August 1997.
- Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, Version 1.02, Brian P. Gallagher, Software Engineering Institute, October 1999.
- Taxonomy-Based Risk Identification, Marvin J. Carr, Suresh L. Konda, Ira Monarch, F. Carol Ulrich, and Clay F. Walker, Software Engineering Institute, June 1993.
- Software Acquisition - Capability Maturity Model (SA-CMM), Jack Cooper, Matthew Fisher, and S. Wayne Sherer, Software Engineering Institute, April 1999.
- Software Risk Evaluation (SRE) Method Description, Ray C. Williams, George J. Pandelios, and Sandra G. Behrens, Software Engineering Institute, December 1999.
- Continuous Risk Management Guidebook, Audrey J. Dorofee, Julie A. Walker, Christopher J. Alberts, Ronald P. Higuera, Richard L. Murphy, and Ray C. Williams, Software Engineering Institute. 1996.
- IEEE Standard 1540-2001: IEEE Standard for Software Life Cycle Processes — Risk Management, March 17, 2001.
- ISO/IEC Standard 27005-2008: Information technology — Security techniques — Information security risk management.
- ISO/IEC Standard 27002-2005: Security techniques -- Code of practice for information security management.
- State Administrative Manual (SAM), Chapter 5305, “Risk Management”, (Revised October, 2009).
- State Administrative Manual (SAM), Chapter 5305.1, “Risk Analysis”, (Revised October, 2009).

¹ Referred to as the PMBOK throughout the RMP.



- CalSERV Risk Management Plan, Version 1.3, July 16, 2001.
- CalWin Risk Management Process, February 28, 2000.
- CalWIN Risk Management Plan, October 31, 2000.
- SAWS C-IV Risk Mitigation Strategy, July 18, 2001.
- SFIS Contract, Contract #18500, August 27, 2009.
- State of California Department of Finance (DOF) Information Technology Project Oversight Framework, Budget Letter 03-04, February 7, 2003.
- State of California Office of the Chief Information Officer, Transition of IT Project Review, Approval and Oversight Responsibilities from the Department of Finance to the Office of the State Chief Information Officer, and Information Technology Budgeting Guidelines [BL 08-06](#), issued 03-14-2008.
- State of California Office of System Integration, PMO Procedure, Project Monitoring and Control Procedure, OSI-AP-08-14, August 28, 2008.
- Risk Radar™ User's Guide, Version 2.03 for MS Access 2000 Only, Integrated Computer Engineering, Inc., June 2002.
- Risk Management Plan Tailoring Guide, Health and Human Services, Office of Systems Integration, June 23, 2004.
- Risk Management Plan Template, Health and Human Services, Office of Systems Integration, June 23, 2004.
- Risk Management Guide for Information Technology Systems, NIST Special Publication 800-30, July 2002.



DEFINITIONS

Many of the terms used in this RMP are consistent with and in many cases the exact definitions used in IEEE Standard 1540-2001. Definitions appear in Section 3 of the IEEE Standard.²

Definitions for other key terms, developed for this RMP, are presented below. The Project Management Institute (PMI), the Software Engineering Institute (SEI), and the State Administrative Manual (SAM) were also used as resources in developing the following definitions, specifically:

- *A Guide to the Project Management Body of Knowledge, 2000.*
- *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, 1997, Version 1.0, 1997.*
- *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, Version 1.02, 1999.*
- *State Administrative Manual (SAM), Chapter 5305, Risk Management”.*

Additional terms and definitions, particularly acronyms in use at the State of California can be found in the State of California Telephone Book and OSI’s organization Chart.

Accept: A mitigation approach that essentially does nothing with the risk. It is handled as a problem if it occurs. No risk management resources are expended dealing with accepted risks.

Acceptability: The exposure to loss (financial or otherwise) that an organization is willing to tolerate from a risk. NOTE — Risk acceptability may apply to an individual risk or to a collection of risks, such as the totality of risks confronting a project or enterprise. Acceptability may differ for different categories of risk and may depend on the cost of treatment or other factors.

Analyze: One of the six functions of the SEI risk management paradigm. The Analyze function is a process in which risks are examined in further detail to determine the extent of the risks, how they relate to each other, and which ones are the most important to deal with.

Assumptions: Assumptions are factors that, for planning purposes, are considered to be real, true, or certain. Assumptions affect all aspects of project planning. Assumptions generally involve some degree of risk.

CCB: Change Control Board — A formally constituted group of stakeholders responsible for approving or rejecting changes to a project’s baseline.

² IEEE Std 1540-2001, p. 3-4.



CDSS: California Department of Social Services — The program/project sponsor of SFIS.

CHHSA: California Health and Human Services Agency — The State of California agency to which both CDSS and OSI report.

Communicate: One of the six functions of the SEI risk management paradigm. The Communicate function is a process in which risk information is conveyed between all levels of a project team. Risk communication deals with the ideas of probability and negative consequences. It is present in all of the other functions of the SEI risk management paradigm and is essential for the management of risks within an organization. Communication must both fit within an organization’s culture and expose the risks that are present in an organization’s projects.

Consequence: An outcome of an event, hazard, threat or situation. NOTE — The outcome may be a loss or a gain, and may be expressed qualitatively or quantitatively.

Contingency Planning: The development of a management plan that identifies alternate strategies to be used to ensure project success if specified risk events occur.

Control: One of the six functions of the SEI risk management paradigm. Control is a process in which a decision maker analyzes the data contained in tracking reports, makes a decision, and implements the decision. The person who has accountability for a risk normally makes the control decision for that risk.

DOF: Department of Finance — Formerly the State of California’s IT control agency, replaced by the OCIO. .

DTS: Department of Technology Services — Now known as OTech. The State of California Department that provides information technology services to many State, county, federal and local government entities throughout the State of California.

HP: Hewlett Packard — The contractor responsible for SFIS maintenance and operations.

HHSDC: Health and Human Services Data Center — Formerly the State of California data center formerly responsible for monitoring and directing contractor activities on behalf of CDSS.

Identified Risk: A potential risk becomes an identified risk when it has been determined that the risk that can be described and measured. The Identified Risk is input to the SFIS Project Risk Management process and documented in the SFIS Project Risk Database with an initial risk profile.



Identify: One of the six functions of the SEI risk management paradigm. Risk identification is a process where uncertainties and issues about a project are transformed into tangible risks, which can be described and measured. Everyone on a project is responsible for identifying risks.

IHSS: In-Home Supportive Services. The IHSS Program will help pay for services provided to recipients so that they can remain safely in their own homes. To be eligible, the recipient must be over 65 years of age, or disabled, or blind. Disabled children are also eligible for IHSS. IHSS is considered an alternative to out-of-home care, such as nursing homes or board and care facilities. The types of services which can be authorized through IHSS are housecleaning, meal preparation, laundry, grocery shopping, personal care services, bathing, grooming and paramedical services), accompaniment to medical appointments, and protective supervision for the mentally impaired.

Likelihood: A quantitative or qualitative expression of the chances that an event will occur. NOTE — Quantitative expressions may include numerical scales or probabilities.

Mitigation: Risk mitigation seeks to reduce the probability and/or impact of a risk to below an acceptable threshold.

OCIO: Office of the Chief Information Officer. The State of California office with statutory authority over IT strategic vision and planning, enterprise architecture, policy, and project approval and oversight.

OSI: Office of System Integration: The State of California office responsible for monitoring and directing contractor activities on behalf of CDSS.

OTech: Office of Technology Services. Formerly known as DTS. The State of California Department that provides information technology services to many State, county, federal and local government entities throughout the State of California.

Plan: One of the six functions of the SEI risk management paradigm. Planning is a process whereby decisions are made about what should be done with a risk. The results of planning are risk action plans for individual risks or sets of related risks. Personnel who have the knowledge, expertise, background, and resources to effectively deal with risks are responsible for developing their plans.

PMO / QA: Project Management Office / Quality Assurance. Part of OSI's SFIS Project organization, reporting to the SFIS Project Manager.

Potential Risk: Issue or concern being considered by the SFIS Project's Risk Management process as a risk that can be described and measured.



Project Risk Profile: A project’s current and historical risk-related information; a compendium or aggregate of all individual risk profiles in a project. NOTE — The project risk profile information includes the risk management context, along with the chronological record of risks and their individual risk profiles, priority ordering, risk-related measures, treatment status, contingency plans, and risk action requests. A project risk profile consists of a collection of the risk profiles of all the individual risks, which in turn includes the current and historical risk states.

Qualitative Risk Analysis: Performing a qualitative analysis of risks and conditions to determine their effects on project objectives. It involves assessing the probability and impact of project risk(s) and classifying risks into categories high, medium, and low for prioritized risk response planning.

Quantitative Risk Analysis: Measuring the probability and consequences of risks and estimating their implications for project objectives. Risks are characterized by probability distributions of possible outcomes.

Risk: The likelihood of an event, hazard, threat, or situation occurring and its undesirable consequences; a potential problem.

Risk Action Request: The recommended treatment alternatives and supporting information for one or more risks determined to be above a risk threshold.

Risk Analysis: The process of identifying the vulnerabilities and threats to an organization by assessing the critical functions necessary for an organization to continue business operations, and defining the controls in place to reduce organization exposure and evaluating the cost for such controls.

Risk Category: A class or type of risk (e.g., technical, legal, organizational, safety, economic, engineering, cost, schedule). For the SFIS RMP this is based on SEI’s “Taxonomy-Based Risk Identification”.

Risk Classification: A category or type of risk impact (e.g. plan, process, personnel, user involvement, requirements management et al). For the SFIS RMP this is based on DOF’s “IT Project Oversight Framework, Appendix C”.

Risk Radar™: A risk management database (Microsoft Access) designed to assist project managers in identifying, prioritizing and communicating project risks.

Risk Exposure: The potential loss presented to an individual, project, or organization by a risk; a function of the likelihood that the risk will occur and the magnitude of the consequences of its occurrence. NOTE — Risk exposure is commonly defined as the product of a probability and the magnitude of a consequence, i.e., an expected value or expected exposure. The IEEE software risk management standard takes a broader view that includes qualitative expressions of risk exposure.



Risk Level of Control: A way by which a risk management process may be able to distinguish the level by which risks need to be addressed. For the SFIS RMP this is based on SID’s “Policy and Standards for Risk Management”.

Risk Management: The process of taking actions to avoid risk or reduce risk to acceptable levels.

Risk Management Plan: A description of how the elements and resources of the risk management process will be implemented within an organization or project.

Risk Management Process: A continuous process for systematically identifying, analyzing, treating, and monitoring risk throughout the life cycle of a product or service.

Risk Profile: A chronological record of a risk’s current and historical risk state information.

Risk State: The current project risk information relating to an individual risk. NOTE — The information concerning an individual risk may include the current description, causes, likelihood, consequences, estimation scales, confidence of the estimates, treatment, threshold, and an estimate of when the risk will reach its threshold.

Risk Threshold: This is sometimes referred to as Risk Trigger. The criteria (e.g., a level of risk exposure) against which stakeholders evaluate a risk. NOTE — Different risk thresholds may be defined for each risk, risk category or combination of risks. Exceeding a risk threshold is a condition that triggers some stakeholder action.

Risk Treatment: The process of selecting and implementing risk control options.

SFIS: Statewide Fingerprint Imaging System. An information technology system deployed and operated by the State of California through an outsourcing contract with HP, and used by the State and its counties to assist in detection of duplicate aid fraud.

SID: System Integration Division — Now known as OSI. The division within HHSDC formerly responsible for health and welfare applications operated on behalf of various project sponsors including CDSS.

Stakeholder: A person or group that has an interest in the management of risk.

Track: One of the six functions of the SEI risk management paradigm. Tracking is a process in which risk data are acquired, compiled, and reported by the person(s) responsible for tracking watched and mitigated risks. The information is then used to make control decisions about watched risks and mitigation plans.



Validated Risk: A risk item after analysis. The risk has been prioritized and categorized. Recommended mitigation(s) and metrics have been developed. The risk has been reviewed and accepted validated by the PMO / QA and the SFIS Project Manager.



SFIS RISK MANAGEMENT

Risk management is a key discipline for making effective decisions and communicating the results within concerned organizations. The purpose of risk management is to identify potential managerial and technical problems before they occur so that actions can be taken that reduce or eliminate the likelihood and/or impact of these problems should they occur. It is a critical tool for continuously determining the feasibility of project plans, for improving the search for and identification of potential problems that can affect information technology systems or software life cycle activities and the quality and performance of software products, and for improving the active management of projects.

SFIS risk management is based on a discipline built upon the framework of the SEI Risk Management Paradigm, displayed below. OSI SFIS staff and HP³ staff work together with respect to M&O risk management in team risk management to anticipate and avoid problems by managing project risks. Team risk management establishes a cooperative working environment throughout all levels of the project that gives everyone in the project the ability and motivation to look ahead and handle risks before they become problems. This is accomplished through a set of processes, methods, and tools described in later sections of this RMP.

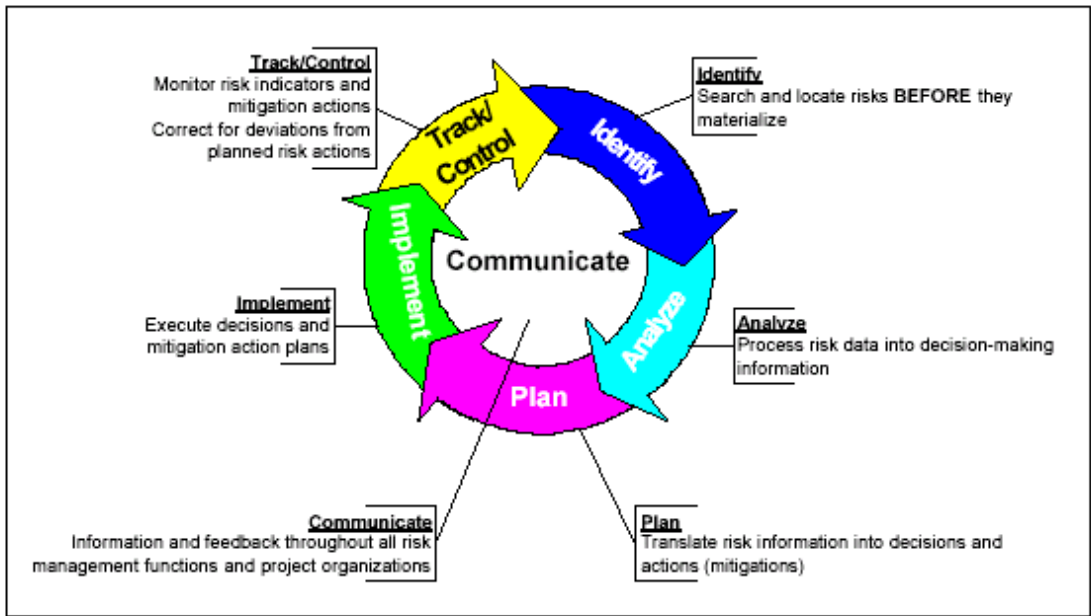
³ EDS has no role in Procurement Project risk management.



RISK MANAGEMENT APPROACH

The SFIS Project Risk Management Paradigm, depicted below, summarizes the Risk Management process for SFIS. This paradigm is adapted for SFIS from the Software Engineering Institute (SEI) Risk Management Paradigm, introduced in *Software Development Risk: Opportunity, Not Problem, 1992*, further described in *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, 1997*, and refined in *Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook, Version 1.02, 1999*. The *DOF Information Technology Project Oversight Framework* and the *Risk Management Plan Tailoring Guide*, Health and Human Services, OSI further developed the paradigm with the Risk Management Plan Template published in August 2008. The SFIS Project Risk Management Paradigm portrays the high-level process steps of the risk management process, which are:

- Identify;
- Analyze;
- Plan;
- Implement; and
- Track / Control.



Effective communication is at the heart of the risk management process and occurs at every step of the process among the OSI SFIS staff, HP, CDSS, and other SFIS Project stakeholders, vendors, and subcontractors⁴.

⁴ The M&O contractor and its subcontractors have no role in Procurement Project risk management.



Risk management roles and responsibilities are described in the section immediately following this section. Detailed risk management processes are described in the section entitled: Risk Management Process.

A vital component of SFIS' risk management is the Risk Management Databases. One logical database was specifically developed to serve as a repository for SFIS Project risk information and is closely modeled on PMBOK risk management concepts and definitions. The database is one of several logical databases developed by KPMG Consulting, Inc to support SFIS throughout development, M&O, and re-procurement of M&O services. The collection of these databases is known as: Project Administration and Control System (PACS). PACS links all logical databases together making it possible to link risks, for example with issues or change orders. The Risk Management Database portion of the PACS is more fully described in Section 6. PACS was developed using Microsoft Access and is available to both OSI and HP SFIS staffs. The SFIS PMO / QA is responsible for maintaining PACS.

A second risk management database is Risk Radar™. Risk Radar™ is commercial off-the-shelf (COTS) software. The Risk Radar™ User's Guides describes Risk Radar™ as: "A risk management database that helps project managers identify, prioritize, and communicate project risks in a flexible and easy-to-use form. Risk Radar™ provides standard database functions to add and delete risks, together with specialized functions for prioritizing and retiring project risks. Each risk can have a user-defined risk management plan and a log of historical events. A set of standard short- and long-form reports and viewgraphs can be easily generated to share project risk information with all members of the development team. The number of risks in each probability/impact category by time frame can be displayed graphically, allowing the user to visualize risk priorities and easily uncover increasing levels of detail on specific risks. Risk Radar™ provides flexibility in prioritizing risks through automatic sorting and risk-specific movement functions for priority ranking."⁵ The reason the SFIS Project employs Risk Radar™ is to maintain compatibility with other OSI projects, because all OSI projects use this software to report risks upward in the OSI organization. Since the volume of project risks is quite low, maintaining 2 risk databases is not onerous.

⁵ Risk Radar™ User's Guide, Version 2.03 for MS Access 2000 Only, Integrated Computer Engineering, Inc., June 2002.



ROLES AND RESPONSIBILITIES

OSI’s SFIS PMO / QA’s role was to develop the SFIS RMP defining the risk management processes, to implement risk management processes, to provide leadership, and facilitate communication throughout the execution of the process. The PMO / QA is also responsible for maintenance of the RMP for the duration of the project.

The role of the SFIS Project Manager is to approve the RMP, participate in risk management processes, and take ownership of risk mitigation planning and execution. The SFIS Project Manager also has the responsibility to communicate to certain project stakeholders, on an as needed basis.

The role of SFIS Project stakeholders, contractor, and subcontractors is to participate in risk management processes by providing candidate risk input. Stakeholders can participate in any, all or none of the risk management processes dependent on the nature of each individual risk.

The PMO / QA, the SFIS Project Manager, and SFIS Project staff responsibilities for detailed risk management process steps are described in the table below. None of the steps described occurs in a vacuum, the table presents the responsibility for the step not necessarily who performs that step.

SFIS Risk Management Responsibilities

Risk Management Process Step	Responsibility	Detailed Process Steps
1. Identify	PMO / QA	1-A. Identify and Assemble Potential Risks
	SFIS Staff, Stakeholders, Contractor ⁶	1-B. Provide Potential Risk Input to PMO / QA
	PMO / QA	1-C. Review Potential Risks
		1-D. Document Initial Risk Profile in Risk Management Databases

⁶ The contractor has no role with respect to risk management for the Procurement Project.



Risk Management Process Step	Responsibility	Detailed Process Steps
2. Analyze	PMO / QA	2-A. Determine Risk Category
		2-B. Determine Risk Classification
		2-C. Determine Risk Impact
		2-D. Determine Risk Probability
		2-E. Determine Risk Timeframe
		2-F. Determine Risk Severity (priority)
		2-G. Determine Risk Exposure
		2-H. Determine Risk Level of Control
	SFIS Project Manager	2-I. Develop Recommended Mitigation Strategy(s)
	PMO / QA	2-J. Develop Recommended Metrics.
SFIS Project Manager	2-K. Review Risk State, Recommended Mitigation Strategies and Metrics with OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders, as required	
PMO / QA	2-L. Update Risk Management Databases	

3. Plan	SFIS Project Manager	3-A. Assign Risk Ownership
	Risk Owner and PMO / QA	3-B. Develop Mitigation(s)
		3-C. Develop Metrics
	SFIS Project Manager	3-D. Review and Approve Mitigation(s) and Metrics
	Risk Owner and PMO / QA	3-E. Develop Risk Action Plan(s)
	SFIS Project Manager	3-F. Review and Approve Risk Action Plan(s)
		3-G. Review Mitigations, Metrics, and Action Plans with OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders, as required
	PMO / QA	3-H. Update Risk Management Databases



Risk Management Process Step	Responsibility	Detailed Process Steps
4. Implementation	SFIS Project Manager, Risk Owner, or other Assignee	4-A. Execute Risk Action Plan(s)
	PMO / QA	4-B. Update Risk Management Databases
5. Track / Control	SFIS Project Manager	5-A. Supervise Risk Action Plan(s) Execution
	PMO / QA	5-B. Track Action Plan(s)
		5-C. Re-assess Risks
	SFIS Project Manager	5-D. Review Risk Status with OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders, as required
PMO / QA	5-E. Update Risk Management and Lessons Learned Databases	



RISK MANAGEMENT PROCESS

This section describes the following SFIS Project Risk Management process steps in detail. SFIS’ approach to risk management deviates slightly from the process described in “SID Policy & Standards for Risk Management.” The SFIS Risk Management process permits use of the term To Be Determined (TBD) as a response to Risk Exposure, Risk Severity et al. This is done to permit entry of a risk into the Risk Management Databases when there may be unknowns. TBD serves as a trigger to gather additional facts when risks are reviewed. The table below describes the process flow, detailed steps, and responsibilities for each of the following process steps:

- Identify;
- Analyze;
- Plan;
- Implement; and
- Track / Control.

Step 1 – Identify

The objective of Step 1 – Identify is to discover and locate risks before they become problems using risk identification. Risk identification is a process where issues and concerns about a project are transformed into risks that can be described and measured. The responsibility for risk identification is shared between all SFIS Project participants including OSI’s SFIS staff, the PMO / QA, CDSS, HP and its subcontractors, and any other stakeholders. The PMO / QA is responsible for identifying and assembling potential risks by collecting and reviewing risk input from Project participants and stakeholders. The PMO / QA is also responsible for documenting initial risk profiles in risk management database. The PMO / QA will use input from the Project’s regularly scheduled CCB meetings to construct these initial risk profiles.

Step 1-A — Identify and Assemble Potential Risks

Discover and identify issues and concerns, which could negatively affect the success of the project, through the use of risk identification methods and the application of industry standards (e.g., IEEE, PMI, SEI). Methods to identify risks may include: monitoring project activities, examining artifacts and documentation, field trips to county sites, observing, interviewing, surveying, participating in discussions and meetings. Particularly good sources for issues and concerns are the regularly scheduled SFIS CCB meetings. These issues and concerns result in potential risks.



Risk identification methods practiced by the PMO / QA will assemble potential risk inputs from both SFIS Project participants and activities. SFIS Project participants include the OSI SFIS Project team, CDSS, HP and its subcontractors, and other stakeholders. SFIS Project activities include SFIS M&O, development and implementation of IHSS functionality, and observation by SFIS project participants of all aspects of M&O.

Responsibility: PMO / QA.

Step 1-B — Provide Potential Risk Input to PMO / QA

SFIS Project participants, including the OSI SFIS project team, CDSS, HP and their subcontractors, and other stakeholders are the primary sources for identifying issues and concerns and submitting these as potential risk input to the Risk Management process. Typically the Project participants submit candidate risks to the PMO / QA as input to Step 1-C.

The methods used by the SFIS Project participants to submit potential risks to the PMO / QA include, but are not limited to:

- Oral;
- E-mail; or
- Written communication, etc.

Responsibility: OSI SFIS staff, CDSS, HP and their subcontractors, and other stakeholders.

Step 1-C — Review Potential Risks

This step consists of getting potential risk input from the PMO / QA (step 1-A), and the other SFIS Project participants (step 1-B) and reviewing these potential risks. Risks that can be described and measured will become identified risks. The PMO / QA will discuss the potential risk and seek consensus with other SFIS Project participants, especially members of the CCB, on determining if a potential risk becomes an identified risk. A determination will be made with respect to confidentiality: Can the risk be exposed to any project participants?

Reviewing potential risks includes defining each risk and capturing appropriate information about the risk to perform risk analysis in Step 2 – Analyze. Defining the risk requires an understanding of the definition of a risk (see Section 3 - Definitions). Using this definition, whether or not a negative impact to SFIS will occur if the risk is realized needs to be determined.



Next, an informal determination of the risk’s negative impact will be performed. The fundamental question to answer is: Is this risk’s negative impact such that it should be included in SFIS’ Risk Management process? A more formal determination of negative impact occurs to Step 2 — Analyze.

Finally, the likelihood of the potential risk occurring needs to be assessed. This is an informal assessment that seeks to determine the probability of the potential risk. A more formal assessment of risk probability occurs in Step 2 — Analyze. If the probability of the risk occurring is low, the risk probably will be excluded from SFIS’ risk management process.

Reviewing potential risks also requires that the PMO / QA collect the data necessary to perform Step 1-D.

Responsibility: PMO / QA.

Step 1-D — Document Initial Risk Profile in Risk Management Databases

Documenting the risk’s initial profile consists of entering the data elements described below in the Risk Management Databases. For the PACS risk management database a few data elements, notably certain dates are system-generated. All data elements may change over time. Data elements required to create a risk’s initial profile in the PACS Risk Management Database include:

- Title: A very brief description of the potential risk;
- Initiated By: Name of the person that submitted the potential risk to the PMO / QA;
- Date Initiated: Date the potential risk was submitted to the PMO / QA;
- Description: A detailed description of the potential risk that includes possible consequences if the risk should actually occur. Risk threshold is usually included in the risk description;
- Risk Category: Those categories into which a risk falls. Categories are described in SEI’s “Taxonomy-Based Risk Identification”;
- Risk Classification: The class into which a risk falls. Classes are described in DOF’s “IT Project Oversight Framework, Appendix C”;
- Risk Probability: A value of High, Medium, Low, or To Be Determined (TBD);
- Risk Impact: A value of High, Medium, Low, or TBD;
- Risk Level of Control: a value of No Control, Minimal, Moderate, High, or TBD;
- Assigned To: The name of the project participant that is the risk owner. Ownership of a risk can change during the period a risk is open;
- Assigned Date: The date at which the potential risk was assigned to the risk owner; and
- Risk Confidential: A value of Yes or No.



For the Risk Radar™ Database the following data elements required to create a risk's initial profile:

- Title: A very brief description of the potential risk;
- Description: A detailed description of the potential risk that includes possible consequences if the risk should actually occur. Risk threshold is usually included in the risk description;
- Status: This shows the current status of this risk in the risk management process. For instance, it may indicate whether it is actively being mitigated, being watched, on hold, etc.;
- Probability: This contains the current estimate for the probability (in percent) that the risk will occur over the impact time frame (see below). Values from 1% (extremely unlikely) to 99% (almost certain) are valid;
- Impact: This represents the current estimate for the impact the risk will have on the project if it materializes. Like probability above, this will likely be an educated guess. An impact is an undesirable consequence, which would negatively influence the project. The values of 1 to 5 represent a subjective ranking of the impact: 1=very low, 2=low, 3=moderate, 4=high, 5=very high.
- Impact Time Frame Fields: The first field is the earliest date the risk impact could materialize and the second field is the latest date it could materialize. Note that the keyword “BOP,” meaning beginning of project, can be placed in the first field and the keyword “EOP,” meaning end of project, can be placed in the second field.
- Responsible Person: This is the person responsible for tracking or managing the risk.
- Program Areas: Describes project areas or components that are affected by the risk here. This might include specific products or configuration items that would be impacted if the risk were to materialize.
- Affected Phases: Describe development phases (such as requirements or design), work packages, or work activity network components that identify which phase would be impacted if the risk were to materialize.
- Risk Area: This is used to assign the risk to a risk category.
- Control: This is used to indicate whether the source of the risk is internal or external to the organization.
- Contingency Plan: The contingency plan is the set of actions to take should the risk materialize. If the plan is extensive, this will likely point to another document.
- Risk Mitigation Description: This is used to describe the approach or other background information regarding the mitigation efforts that will be taken on the risk.
- Historical Events Log: This table allows recording status of the risk.

Responsibility: PMO / QA.



Step 2 – Analyze

The objective of Step 2 – Analyze is to take the data contained in the initial risk profile collected in Step 1 – Identify and create information that can be used in decision-making. Impacts, probabilities, and timeframes for risks are categorized and prioritized as part of this step. The SFIS Project Manager will review risks with the OSI Deputy Director – SAWS, the OSI Director, CDSS, HP⁷, and other stakeholders as required. When all the above activities are completed, the identified risks have become validated risks.

Step 2-A — Determine Risk Category

Perform analysis to determine risk category. Individual risk items can belong to one or more categories. Risk categories are based on the SEI Risk Taxonomy from *Taxonomy-Based Risk Identification, 1993*. Risk categories include:

- Requirements — Includes:
 - Stability;
 - Completeness;
 - Clarity;
 - Validity;
 - Feasibility;
 - Precedent; and
 - Scale.
- Design — Includes:
 - Functionality;
 - Difficulty;
 - Interfaces;
 - Performance;
 - Testability;
 - Hardware constraints; and
 - Non-developmental software.
- Code and Unit Test — Includes:
 - Feasibility;
 - Unit test; and
 - Coding / implementation.
- Integration and Test — Includes:
 - Environment;
 - Product; and
 - System.
- Engineering Specialties — Includes:
 - Maintainability;

⁷ The contractor has no role with respect to risk management for the Procurement Project.



- Reliability;
 - Safety;
 - Security;
 - Human factors; and
 - Specifications.
- Development Process — Includes:
 - Formality;
 - Suitability;
 - Process;
 - Control;
 - Familiarity; and
 - Product control.
- Development System — Includes:
 - Capacity;
 - Suitability;
 - Usability;
 - Familiarity;
 - Reliability;
 - System support; and
 - Deliverability.
- Management Process — Includes:
 - Planning;
 - Project organization;
 - Management experience; and
 - Program interfaces.
- Management Methods — Includes:
 - Monitoring;
 - Personnel management;
 - Quality assurance; and
 - Configuration management.
- Work Environment — Includes:
 - Quality attitude;
 - Cooperation;
 - Communication; and
 - Morale.
- Resources — Includes:
 - Schedule;
 - Staff;
 - Budget; and
 - Facilities.
- Contract — Includes:
 - Type of contract;
 - Restrictions; and
 - Dependencies.
- Program Interfaces — Includes:



- End users;
- Subcontractors;
- Prime contractor;
- State management (CDSS, OCIO, DGS, OSI);
- Vendors; and
- Politics.

Responsibility: PMO / QA.

Step 2-B — Determine Risk Classification

Perform analysis to determine risk classification. Individual risk items can belong to one or more class. Risk classes are taken from taken from the DOF IT Project Oversight Framework, Appendix C (*Categories and Examples of Risk*) and Appendix D (*Project Risk List*). Risk classes include:

- Plan/Schedule.
- Organization and Management.
- Development Environment.
- User Involvement.
- Contractor Performance.
- Requirements Management.
- Product Characteristics.
- External Environment.
- Personnel.
- Design and Implementation.
- Process.

Responsibility: PMO / QA.

Step 2-C — Determine Risk Impact

Determining the risk impact considers the anticipated consequences that the risk would have on the project, if the risk occurs. The table, Criteria for Risk Impact below provides a guide for assessing the consequences and determining the risk impact, expressed as “High,” “Medium,” “Low,” or “TBD”. Determination of risk impact is a subjective process that considers the criticality of internal and external project factors within the unique context of SFIS. The PMO / QA will use the criteria identified in the table below as a guide for assigning risk impact, but will confirm the risk impact with the SFIS Project Manager, the Project Sponsor, and Stakeholders as required (Step 2-K).



Criteria for Risk Impact

Impact	Criteria
High	<p>The risk represents a significant negative impact on project budget, schedule, or quality. Risk consequences include one or more of the following:</p> <ul style="list-style-type: none"> • Significant schedule delay; • Significant cost increase; • Significant technical change; • Significant resource change; • Significant political repercussions; • Significant end user dissatisfaction; and • Significant stakeholder dissatisfaction.
Medium	<p>The risk’s material impacts would significantly affect users, clients, or other key stakeholders. Risk consequences include one or more of the following, but do not include consequences already identified as “High”:</p> <ul style="list-style-type: none"> • Moderate schedule delay; • Moderate cost increase; • Moderate technical change; • Moderate resource change; • Moderate political repercussions; • Moderate end user dissatisfaction; and • Moderate stakeholder dissatisfaction.
Low	<p>The risk does not represent a significant or material impact on project budget, schedule or quality. Risk consequences include one or more of the following, but do not include consequences already identified as “High” or “Medium”:</p> <ul style="list-style-type: none"> • Minor schedule delay; • Minor cost increase; • Minor technical change; • Minor resource change; • Minor political repercussions; • Minor end user dissatisfaction; and • Minor stakeholder dissatisfaction.
TBD	Risk impact has not yet been assessed.

Responsibility: PMO / QA.



Step 2-D — Determine Risk Probability

Determining risk probability considers the likelihood of the risk occurring. The table, Criteria for Risk Probability, below provides a guide for assessing the likelihood and determining the risk probability, expressed as “high,” “medium,” “low,” or “TBD”. Determination of risk probability is a subjective process that considers the criticality of internal and external project factors within the unique context of SFIS. The PMO / QA will use the criteria identified in the table below as a guide for assigning risk probability, but will confirm the risk impact with the SFIS Project Manager, the Project Sponsor, and Stakeholders as required (Step 2-K).

Criteria for Risk Probability

Probability	Criteria
High	The risks are almost certain or very likely to occur.. There is a greater than 60% confidence that the risks will occur.
Medium	The risks may occur or have a 50/50 chance of occurring. There is a 30-60% confidence that the risks will occur.
Low	The risks are unlikely to occur or will probably not occur. There is less than 30% confidence that the risks will occur.
TBD	Risk probability has not yet been assessed.

Responsibility: PMO / QA.

Step 2-E — Determine Risk Timeframe

The risk timeframe is the period of time within which the risk is expected to occur. The table, Criteria for Risk Timeframe, below is a guide for evaluating the period of time a risk is expected to occur and determining the risk timeframe, expressed in terms of “Short-Term”, Medium-Term, “Long-Term”, or TBD. Determination of risk timeframe is a subjective process that considers the criticality of internal and external project factors within the unique context of SFIS. The PMO / QA will use the criteria identified in the table below as a guide for assigning risk timeframe, but will confirm the risk timeframe with the SFIS Project Manager, the Project Sponsor, and Stakeholders as required (Step 2-K).

Criteria for Risk Timeframe

Timeframe	Criteria
Short-Term	The risk is most likely to occur in less than 6 months.
Medium-Term	The risk is most likely to materialize between 6 months to 1 year from now.
Long-Term	The risk is most likely to materialize in a period of greater than 1 year.
TBD	Risk timeframe has not yet been assessed.



Responsibility: PMO / QA.

Step 2-F — Determine Risk Exposure

Risk exposure is potential loss presented to a project or organization by a risk; a function of the likelihood that the risk will occur and the magnitude of the consequences of its occurrence. Risk exposure is determined from the risk attributes impact and probability, and is used, in conjunction with timeframe, to prioritize risks for mitigation and escalation. Risk exposure for each risk will be derived from the intersection of that risk’s impact and probability in the table below.

Criteria for Risk Exposure

Impact	Probability			
		High	Medium	Low
High		High	High	Medium
Medium		High	Medium	Low
Low		Medium	Low	Low

Reference: Department Of Finance, Information Technology Project Oversight Framework, Section 5 - Risk Mgmt and Escalation Procedures.

Responsibility: PMO / QA.

Step 2-G — Determine Risk Severity (Priority)

The priority of the risk is a determination of the importance of the risk to SFIS based upon:

- The possible impact of the risk;
- The probability of the risk occurring; and
- The risk’s timeframe.

The table below is used for determining risk priority using the risk impact, probability, and timeframe, described as “High”, “Medium”, “Low”. The PMO / QA will use the criteria described in the table below as an initial guide for assigning risk severity, but will confirm the risk severity with the SFIS Project Manager in Step 2-K.



Determination of Risk Severity

Time Frame	Exposure			
		High	Medium	Low
	Short-Term	High	High	Medium
	Medium-Term	High	Medium	Low
Long-Term	Medium	Low	Low	

Responsibility: PMO / QA.

Step 2-H — Determine Risk Level of Control

Determining a risk’s level of control distinguishes the level necessary to effectively address the risk. The level of risk control is an important factor in risk escalation. The level of control determination indicates who has the capability and authority to influence a risk. The table below describes each level of control.

Level of Control

Level of Control	Definition
No Control	No resource within OSI can control the outcome of this risk
Minimal	The OSI Director or his/her designee has the authority to control the outcome of this risk
Moderate	The OSI Deputy Director - SAWS or his/her designee has the authority to control the outcome of this risk
High	The SFIS Project Manager or a Project Team Leader has the authority to control the outcome of this risk

Responsibility: PMO / QA.



Step 2-I — Develop Recommended Mitigation Strategy(s)

Develop recommended actions to mitigate the risk. In order to develop the most effective actions, it is necessary to determine if the risk is to be shared with another stakeholder, such as the contractor or SFIS' Project sponsor. Sharing the risk does not mean that ownership of a risk is jointly held; rather it means that the other stakeholders are active partners in formulating risk response actions. The mitigation strategy can now be determined. The possible risk mitigation strategies include:

- **Avoidance:** Risk Avoidance is changing the project plan to eliminate the risk or condition or to protect the project's objectives from its impact. Some examples of risk avoidance are adding resources or time, or reducing project scope.
- **Transference:** Risk transference is seeking to shift the consequences of a risk to a third party along with ownership of the risk response. Transferring the risk gives a third party responsibility for a risk's management; it does not eliminate the risk. Some examples of risk transference are performance bonds or warranties.
- **Mitigation:** Mitigation seeks to reduce the probability and/or consequences of a risk to an acceptable risk threshold. Some examples of mitigation are adding resources, or designing redundancy into an important subsystem.
- **Acceptance:** Acceptance is deciding not to change a project plan to address a risk, or not being able to devise an effective risk response. Passive acceptance requires no action. Active acceptance includes development of a contingency plan should the risk occur. A common acceptance response is setting aside additional funding whose purpose is to successfully manage risks.

In most risks, the SFIS Project Manager will define actions that are designed to eliminate or reduce the risk, in lieu of recommending acceptance of a risk, notable for critical, high, and medium priority risks. If acceptance is recommended, the SFIS Project Manager will prepare a contingency plan. Recommended mitigation(s) are developed by the SFIS Project Manager, and will be defined in additional detail in Step 3 – Plan after the review described by Step 2-K. There may be multiple recommended mitigations identified for a risk item. Risk threshold is considered in recommended mitigation(s).

Responsibility: SFIS Project Manager, or as assigned by the SFIS Project Manager.

Step 2-J — Develop Recommended Metrics

Develop the recommended methods to track the recommended risk mitigation(s) and to measure the effectiveness and success of the mitigation(s). The actual metrics are developed by the PMO / QA and the SFIS Project Manager in the course of risk planning in Step 3 – Plan. There may be multiple recommended metrics identified for a risk mitigation action. These metrics are typically coupled to a risk threshold.

Responsibility: PMO / QA.



Step 2-K — Review Risk with OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders

The SFIS Project Manager assisted by the PMO / QA as required reviews the risk with the Director of OSI, CDSS, CHHSA, OCIO, DGS⁸, and other stakeholders, as required. The OSI Director, CDSS, CHHSA, OCIO, DGS, and other stakeholders, as required will validate the risk state including:

- Risk Category;
- Risk Classification;
- Risk Impact;
- Risk Probability;
- Risk Timeframe;
- Risk Exposure;
- Risk Severity;
- Risk Level of Control;
- Recommended Risk Owner;
- Recommended Mitigation(s) and risk thresholds; and
- Recommended Metrics.

If necessary, the above elements of the risk state will be revised based on input from the reviewers. The result of the review is to either declare the risk as a “validated risk” or discard the risk. The initial forum for reviewing risks will be the weekly CCB Meetings. The SFIS Project Manager, assisted by the PMO / QA as required will review risks with the OSI Director, CDSS, CHHSA, OCIO, DGS⁹, and other SFIS stakeholders on a monthly basis, or as required. Additional meetings may be scheduled as needed.

The determination of to which level of responsibility risks are escalated is described in the following table. The project criticality of SFIS is considered by OCIO / DGS to be high. Therefore, all SFIS risks with risk severity of high will be escalated to OCIO / DGS.

Determination of Risk Escalation

Project Criticality	Risk Severity			
		High	Medium	Low
High		OCIO / DGS	CHHSA	CDSS / OSI
Medium		CHHSA	CHHSA	CDSS / OSI
Low		CHHSA	CDSS / OSI	

⁸ For Procurement Project risks.

⁹ For Procurement Project risks.



The sequence in which a risk is escalated is depicted in the charts below. The SFIS Project Manager initiates all risk escalations, assisted by the PMO / QA. Either the SFIS Project Manager or the OSI Deputy Director – SAWS escalates directly to CDSS. The OSI Director will be made aware of escalations but will not normally manage escalations except within the CHHSA.

Sequence of Risk Escalation for M&O Risks





Step 2-L — Update Risk Management Databases

The PMO / QA updates the Risk Management Databases' risk information based on risk planning, including initial Risk Owner, Recommended Risk Mitigation(s), Recommended Risk Metrics, and recommended Mitigation Action Plans. The data housed in the Risk Management Database at this point is preliminary and may or may not be changed by subsequent events occurring in later steps of the risk management process.

Responsibility: PMO / QA.

Step 3 – Plan

The objective of Step 3 – Plan is to plan for risk mitigation. Risk planning involves assignment of risk ownership (if different from initial risk owner, development of risk mitigation(s), development of risk metrics, reviewing and approving risk mitigation(s) and metrics, evolving mitigation(s) into action plan(s), and recording risk state changes in the Risk Management Databases.

Step 3-A — Assign Risk Ownership

Identify the person to be assigned responsibility for developing risk mitigation(s), metrics, and action plan(s), and implementing and monitoring mitigation action plan(s). Assignment of ownership may be required at this time if the initial risk owner, assigned in Step 2-K is changed, or no risk ownership was assigned.

When someone external to OSI's SFIS Project Team can control risk events or mitigation(s), a Risk Owner will be assigned from OSI's SFIS Project Team, even though plans and actions to address a validated risk may be controlled external to OSI. In this case where the risk actions or mitigation(s) are controlled externally, the Risk Owner will assume responsibility for coordination and reporting on risk actions and plans of the external party.

Responsibility: SFIS Project Manager.

Step 3-B — Develop Mitigation(s)

Develop response(s) to the risk, designed to eliminate, reduce or accept the risk. The Risk Owner is responsible for developing mitigation(s) for the risk. Mitigation(s) developed by the Risk Owner may be based on recommended mitigations, as identified in Step 2-I, or may be developed independently. The Risk Management Databases will



separately identify, through status updates, recommended mitigation(s) identified in Step 2-I and mitigation(s) developed by the Risk Owner. In certain cases, risks may be outside of project control and as a result, cannot be mitigated but must be accepted. In these instances, the Risk Owner will develop contingency plan(s). These contingency plans will be executed, if the risk occurs.

Responsibility: SFIS Project Manager or as assigned by the SFIS Project Manager.

Step 3-C — Develop Metrics

Develop the methods to track risk mitigation(s) and to measure the success and effectiveness of mitigation(s). Metrics may also be used to set risk thresholds that stimulate some action, for example execution of a contingency plan or mitigation plan. The Risk Owner is responsible for developing metrics for each risk mitigation. Metrics developed by the Risk Owner may be based on recommended metrics, as identified in Step 2-J, or may be developed independently. The Risk Management Databases will separately identify, through status updates, recommended metrics identified in Step 2-J and metrics developed by the Risk Owner. In those instances where contingency plans are required in lieu of mitigation(s), metrics will measure the success and effectiveness of the contingency plans in managing the impacts of the risk.

Responsibility: SFIS Project Manager or as assigned by the SFIS Project Manager.

Step 3-D — Review and Approve Mitigation(s) and Metrics

The SFIS Project Manager and the PMO / QA reviews the risk mitigation(s), risk thresholds, and metrics developed by the Risk Owner. If necessary, mitigation(s), risk thresholds, and metrics are revised based on this review. A significant facet of the review is assessment of whether the risk response is the most suitable given the priority of the risk. The PMO / QA assures that all critical and high risks are managed to either eliminate the risk entirely or reduce risk below its threshold. If the SFIS Project Manager directs acceptance of a risk, the PMO / QA will request a contingency plan from the risk owner.

The SFIS Project Manager approves risk mitigation(s), risk thresholds, and metrics. In some cases, this entails escalations to obtain additional approvals from OSI, CDSS, or other stakeholders. The output of Step 2-H — Determine Risk Level of Control may be useful if approvals outside the scope of the SFIS Project Manager's scope of authority are required.

Responsibility: SFIS Project Manager and PMO / QA for review, SFIS Project Manager and/or the OSI Deputy Director – SAWS for approvals.



Step 3-E — Develop Risk Action Plan(s)

Risk action plans to implement risk mitigations, or contingency plans and determination of risk thresholds are developed by the Risk Owner to whom the mitigation(s) have been assigned. Action plan development may be delegated by the Risk Owner, however the Risk Owner has overall responsibility for mitigation of the risk and is the designated point of contact for the PMO / QA for purposes of risk tracking. The PMO / QA is available to the Risk Owner to assist in the development of action and contingency plans. Responsibility: Risk Owner and PMO / QA.

Step 3-F — Review and Approve Risk Action Plan(s)

The SFIS Project Manager and the PMO / QA reviews the action and contingency plans developed by the Risk Owner. If necessary, these plans are revised based on this review.

The SFIS Project Manager approves action and contingency plans. In some cases, this entails escalations to obtain additional approvals from OSI, CDSS, or other stakeholders.

Responsibility: SFIS Project Manager and PMO / QA for review, SFIS Project Manager for approvals.

Step 3-G — Review Mitigations, Metrics, and Action Plans with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders

The SFIS Project Manager, assisted by the PMO / QA reviews the risk with the OSI Deputy Director – SAWS, Director of OSI, CDSS, OCIO, DGS, and other stakeholders, as required. The OSI Director, CDSS, CHHSA, OCIO, DGS, and other stakeholders, as required will validate the risk state including:

- Risk Category;
- Risk Classification;
- Risk Impact;
- Risk Probability;
- Risk Timeframe;
- Risk Exposure;
- Risk Severity;
- Risk Level of Control;
- Risk Ownership assignment;
- Mitigation(s);
- Metrics and
- Action Plans.



If necessary, the above elements of the risk state will be revised based on input from the reviewers. The result of the review is to gain acceptance of action or contingency plans. The initial forum for reviewing mitigation(s), metrics, and action plans will be the weekly CCB Meetings. The SFIS Project Manager, assisted by the PMO / QA as required will review mitigation(s), metrics, and action plans with the OSI Director, CDSS, CHHSA, OCIO, DGS and other SFIS stakeholders on a regular basis, or as required. Additional meetings may be scheduled as needed.

Responsibility: SFIS Project Manager and PMO / QA.

Step 3-H — Update Risk Management Databases

The PMO / QA will update the Risk Management Databases' risk state information based on risk planning, including risk ownership assignment, mitigation(s), metrics, actions plans, and contingency plans developed by the risk owner.

Responsibility: PMO / QA.

Step 4 – Implement

The objective of Step 4 – Implement is to mitigate risks. Risk implementation focuses on implementation of risk mitigation action plans, and recording risk state changes in the Risk Management Database.

Step 4-A — Execute risk action plan(s)

The SFIS Project Manager is responsible for the execution of the risk mitigation action plans and contingency plans. The SFIS Project Manager will coordinate, delegate, and authorize risk owners, as required, to enable execution of action or contingency plans.

Responsibility: SFIS Project Manager, risk owners, or other assigned stakeholders.

Step 4-B — Update Risk Management Databases

The PMO / QA will update the Risk Management Databases risk state information based on the implementation status of the action or contingency plans, as provided by the risk owners.

Responsibility: PMO / QA.



Step 5 – Track / Control

The objective of Step 5 – Track / Control is to insure that all steps of SFIS’ risk management process are being adhered to and, as a result, project risks are being effectively mitigated. Risk tracking / control provides supervision and tracking of risk mitigation action plan or contingency plan execution, re-assessment of risks, reporting risk status, and recording risk state changes in the Risk Management Databases.

Step 5-A — Supervise Risk Action Plan(s) Execution

The SFIS Project Manager is responsible for supervision of the execution of mitigation action and contingency plans for all risks identified in the Risk Management Databases.

Responsibility: SFIS Project Manager.

Step 5-B — Track Action Plan(s)

The risk owner is responsible for tracking the execution of mitigation action and contingency plans and providing feedback to the PMO / QA with respect to changes in risk status.

Responsibility: Risk owners and PMO / QA.

Step 5-C — Re-Assess Risks

The PMO / QA will re-assess the risk state information in the Risk Management Databases to determine if any changes are needed, e.g., risk priority, risk timeframe, based upon project events, risk analysis, or other information. Re-assessment of risk state information in the Risk Management Databases will be performed a monthly basis, however may be performed more frequently, if required. Changes in risk state will be reviewed monthly in the CCB meeting normally occurring in the third week of every month or as required.

Responsibility: PMO / QA.

Step 5-D — Review Risk Status with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, DGS, and Other Stakeholders

Using risk state information from the Risk Management Databases, the SFIS Project Manager, assisted by the PMO / QA, as required will review mitigation(s), metrics, and action and contingency plans with the OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, DGS, and other SFIS stakeholders on a monthly basis, or as



required. Additional meetings may be scheduled as needed. Risk status reporting will focus on critical and high priority risks. Information presented will include the status of risk mitigation action and contingency plans, changes in priority for validated risks, and new risks.

Responsibility: SFIS Project Manager.

Step 5-E — Update Risk Management and Lessons Learned Databases

The PMO / QA will update the Risk Management Databases risk state information based on tracking and control of the action or contingency plans using input from all available sources. The PMO / QA and the SFIS Project Manager will determine if the information concerning a risk is appropriate for entry into the SFIS Lessons Learned Database. If deemed appropriate, the information will be entered by the PMO / QA.

Responsibility: PMO / QA and SFIS Project Manager.



SFIS PROJECT RISK MANAGEMENT PROCESS SUMMARY

The table below depicts the SFIS Project’s risk management process in tabular form and summarizes the process.

Risk Management Process Step	Responsibility	Detailed Process Steps	Inputs	Outputs
1-Identify	PMO / QA	1-A. Identify Potential Risks	QA Risk Analysis Project Incidents and Events Project Documentation Risk Identification Methods Industry Standards (IEEE, PMI, SEI) State of California Policy and Standards (OSI, OCIO)	Potential risks
	SFIS Project staff, stakeholders, and contractors ¹⁰	1-B. Provide Candidate Risk Input to PMO / QA	Project Incidents and Events Project Documentation	Potential risks
	PMO / QA	1-C. Review Potential Risks	Potential risks	Identified risks
		1-D. Record Identified Risks in the Risk Management Databases	Identified risks	Initial risk profiles Updated Risk Management Databases
2-Analyze	PMO / QA	2-A. Determine Risk Category	Risk Management Databases Project Incidents and Events Project Documentation Industry Standards (IEEE, PMI, SEI) State of California Policy	Updated Risk Management Databases Risk Reports
		2-B. Determine Risk Classification		
		2-C. Determine Risk Impact		
		2-D. Determine Risk Probability		
		2-E. Determine Risk Timeframe		

¹⁰ The contractor has no role with respect to risk management for the Procurement Project.



Risk Management Process Step	Responsibility	Detailed Process Steps	Inputs	Outputs
		2-F. Determine Risk Exposure	and Standards (OSI, OCIO)	
		2-G. Determine Initial Risk Severity		
		2-H. Determine Risk Level of Control		
		2-I. Develop Recommended Mitigation Strategy(s)		
		2-J. Develop Recommended Metrics.		
SFIS Project Manager	2-K. Review Risk State, Recommended Mitigation Strategies and Recommended metrics with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, and Other Stakeholders	Risk Reports	Validated risks	
PMO / QA	2-L. Update Risk Management Databases	Risk Management Databases Validated risks	Updated Risk Management Databases	
3. Plan	SFIS Project Manager	3-A. Assign Risk Ownership	Risk Reports Project Incidents and Events Risk Management Databases Project Documentation	Risk ownership Mitigation(s) Metrics Risk thresholds
		3-B. Develop Mitigation(s)		
		3-C. Develop Metrics		



Risk Management Process Step	Responsibility	Detailed Process Steps	Inputs	Outputs
	PMO / QA and SFIS Project Manager	3-D. Review and Approve Mitigation(s) and Metrics	Risk Reports Project Incidents and Events Risk Management Databases Project Documentation Mitigation(s) Metrics	Approved Mitigation(s) Approved Metrics
	Risk Owner and PMO / QA	3-E. Develop Risk Action Plan(s)	Risk Reports Project Incidents and Events Risk Management Databases Project Documentation Approved Mitigation(s) Approved Metrics	Risk action plan(s) Contingency Plans
	PMO / QA and SFIS Project Manager	3-F. Review and Approve Risk Action Plan(s)	Risk Action Plan(s) Contingency Plans	Approved Risk Action Plan(s) Approved Contingency Plans
	SFIS Project Manager	3-G. Review Mitigations, Metrics, and Action Plans with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, and Other Stakeholders	Risk ownership Approved Mitigation(s) Approved Metrics Approved Risk action plan(s) Approved Contingency Plans	Updated Risk Management Databases
	PMO / QA	3-H. Update Risk Management Databases	Risk Management Databases	Updated Risk Management Databases



Risk Management Process Step	Responsibility	Detailed Process Steps	Inputs	Outputs
4. Implementation	SFIS Project Manager, risk owners, or other assigned stakeholders	4-A. Execute Risk Action Plan(s)	Risk Reports Approved Risk Action Plan(s) Approved Contingency Plans	Risk state changes
	PMO / QA, SFIS Project Manager	4-B. Update Risk Management Databases	Risk state changes Risk Management Databases	Updated Risk Management Databases
5. Track / Control	SFIS Project Manager	5-A. Supervise Risk Action Plan(s) Execution	Risk Management Databases Risk Reports Risk state changes	Updated Risk Management Databases
	PMO / QA	5-B. Track Action Plan(s)	Risk Reports Approved Risk Action Plan(s) Approved Contingency Plans	Risk state changes
	PMO / QA	5-C. Re-assess Risks	Risk Management Databases Risk state changes Risk reports Project Incidents and Events Project Documentation Risk Analysis Industry Standards (IEEE, PMI, SEI) State of California Policy and Standards (OSI, OCIO)	Updated Risk Management Databases



Risk Management Process Step	Responsibility	Detailed Process Steps	Inputs	Outputs
	SFIS Project Manager	5-D. Review Risk Status with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, OCIO, and Other Stakeholders	Risk Management Databases Risk Reports Risk state changes	Updated Risk Management Databases
	PMO / QA, SFIS Project Manager	5-E. Update Risk Management and Lessons Learned Databases	Risk Management Databases Lessons Learned Database	Updated Risk Management and Lessons Learned Databases



SAMPLE REPORTS AND FORMS

RISK MANAGEMENT REPORTS

The following sample reports, extracted from the PACS have been edited to demonstrate report content, and fit the portrait oriented format. Actual Microsoft Access reports may have somewhat different appearances from the following samples.

New / Open Risks

New/ Open Risks for SFIS

<i>Control #/</i>	<i>Initiated By/ Date Initiated</i>	<i>Assigned To/ Date Assigned</i>	<i>Impact/ Probability/Type</i>	<i>Risk Categories</i>	<i>Budget/One Time Cost/On-Going Cost</i>	<i>Timeframe/ Response/PM Action</i>
SF-RI-0025 Low	Fahr, Sam 07/23/02	Fahr, Sam 07/23/02	Low High (> 60%) Controllable	Contract Design Integration and Testing Management Process Product Engineering Requirements Resources	TBD	Long-term (> 12 months) Mitigation Mitigate

Title: Operation of Multiple Fingerprint Scanner Types in SFIS Production

Description:

The Identix Touchview II fingerprint Scanner is no longer being manufactured by Identix. Currently, the SFIS Project has a number of spares and given the failure and replacement rates of these scanners we probably have enough to support the project for a year or more. Currently, Identix is refurbishing broken scanners and returning repaired scanners to the Project. It is unclear how long Identix will continue to provide this service, particularly because Identix recently merged with Visionics. Therefore, the project will require a different scanner at some point in the future. The Project Team believes it will be possible to have multiple types of scanners present in production but does not at this time understand the technical implications of multiple scanner types.

Reason or Type Transference:

Suggested Strategies && Measures:

Develop a contingency plan that permits installation of a different scanner type without substantially compromising fingerprint match accuracy, or other SFIS operations, and is



cost effective. Ideally, the new scanner will not require any other workstation hardware modifications, nor require changing the remote workstation operating system.

Implementation Plan:

CR SF-C-0369 has been completed and closed, and work on CO SF-O-0200 has begun. Using the data and information presented in the study commissioned by the Change Order, develop a contingency plan to be executed, if needed.

Costs, fingerprint accuracy, and other business and technical considerations need to be elements of this plan. Acceptance of the Fingerprint Scanner Contingency plan by the SFIS Project Manager.

Status Desc.: 03/04/04 Per CCB, Henry Loret de Mola reported that HP is awaiting additional answers from Printrak.
 02/10/04 Per Henry Loret de Mola's e-mail dated 2/10/04 - Forwarded electronic version of "Draft" Missing BINS Matching Statistics to PMO. Reference iManage document #13,285.
 02/05/04 Per CCB and Sam Fahr's e-mail dated 2/5/04 - A list of questions that the State wanted answered in HP' assessment was supplied by Sam Fahr on 1/29/04 to the remainder of HHSDC SFIS staff for comment and revision.
 02/04/04 Per Henry Loret de Mola's e-mail dated 2/4/04 - No time estimate for the response to the Printrak question is available. The request has been escalated. Anticipate a response on a date request by 2/6/04.
 01/08/04 Per CCB, HP received the draft report from Printrak. Wes Crews has some questions he wants answered. Henry Loret de Mola stated that fingerprint image quality would probably deteriorate during the conversion from one scanner type to another. Henry offered to make available the draft report to the State, but the State decided to wait until the HP questions were resolved.
 08/07/03 Per CCB and Sam Fahr's e-mail dated 8/7/03 - This risk is no longer on hold because SFIS funding has been restored. HP reported that the mitigation plan is approximately 50% complete, and that there was no problem acquiring parts for the Identix scanners.
 06/05/03 Per CCB, Mitigation on-hold until the fate of SFIS has been decided.

Control #/	Initiated By/ Date Initiated	Assigned To/ Date Assigned	Impact/ Probability/Type	Risk Categories	Budget/One Time Cost/On-Going Cost	Timeframe/ Response/PM Action
reviewed by the CCB and	03/12/03	Per Sam Fahr e-mail dated 3/7/03 - Changed "Timeframe", was short-term. Changed "Implementation Plan". The risk categories for this risk were				
		changed, if necessary.				
	03/06/03	Per CCB, Sam Fahr to revise.				
	02/06/03	Per Sam Fahr e-mail dated 2/6/03 - Established "Risk Categories".				
	02/05/03	Per Sam Fahr e-mail dated 2/5/03 - Established "Risk Type", "Timeframe", and "PM Action".				
	12/12/02	Updated, per Sam Fahr e-mail dated 12/9/02.				
	12/05/02	Per CCB, Sam Fahr to develop Mitigation Plan.				
	07/23/02	Added and opened per Sam Fahr e-mail dated 7/22/02.				
SF-RI-0037	Fahr, Sam	Calate, Jennifer	High	Contract		Immediate (< 1 month)
TBD	03/04/04	03/04/04	TBD			Acceptance
			Uncontrollable			Wait

Title: Assembly Bill 2013 terminates SFIS
Description:



Statewide Fingerprint Imaging System (SFIS)

AB2013 terminates SFIS. As long as the bill is alive the future of SFIS is at risk. This risk was opened for tracking purposes since we cannot control activity on this bill. AB1057 providing for a Los Angeles County finger imaging system is currently inactive.

Reason or Type Transference:

Suggested Strategies && Measures:

Implementation Plan:

Closure Conditions:

Status Desc.: 03/04/04 Added per CCB and Sam Fahr's e-mail dated 3/4/04.



Closed / Void Risks

Closed / Voided Risks for SFIS

<i>Control #/</i>	<i>Initiated By/ Date Initiated</i>	<i>Assigned To/ Date Assigned</i>	<i>Impact/ Probability/Type</i>	<i>Risk Categories</i>	<i>Budget/One Time Cost/On-Going Cost</i>	<i>Timeframe/ Response/PM Action</i>
Closed						
SF-RI-0006 Low	Albani, Ric 02/04/00	Fahr, Sam 02/07/02	Low Low (< 30%) Controllable	Management Methods	No Impact	Long-term (> 12 months) Transference Wait

Title: Technical Document Configuration Management

Description:

Document configuration management does not currently exist, because there is no real programmer documentation (flow charts, HIPO diagrams, etc.). Each developer is busy coding and the plan is to create the documentation following

Control

completion of the development effort and following acceptance by HHSDC of the System Design Document (SDD) towards the end of Phase I. This approach is not unusual when time is critical but creates a risk for both HP and HHSDC.

The Risk Initiator has left the SFIS Project. The risk has been assigned to Sam Fahr.

Reason or Type Transference:

Suggested Strategies && Measures:

The contractor should develop a configuration management plan and adhere to that plan. Where appropriate the State should develop processes and procedures that interface with and support the contractor's plan. The Plan and the State's processes should be applicable not simply to documentation but to all configurable items.

The State should initially and then periodically perform an in-depth review of the contractor's CM processes and procedures to ensure adherence to the Plan.

Implementation Plan:

The contractor developed a configuration management plan; this plan maybe found at "\\SAWSADM1\MISC\SFIS\EDS DELIVERABLES\CM Plan 102201.doc". The State reviewed and approved this plan. See SF-I-0168.

The State developed an acceptance and validation procedure. This procedure may be found at "\\SAWSADM1\MISC\SFIS\IV&V Deliverables\CHANGE VALIDATION PROCESS.doc". See SF-A-0065.

The State plans to review HP internal configuration management processes. See SF-A-0064.



Control #/	Initiated By/ Date Initiated	Assigned To/ Date Assigned	Impact/ Probability/Type	Risk Categories	Budget/One Time Cost/On-Going Cost	Timeframe/ Response/PM Action
-------------------	---	---------------------------------------	-------------------------------------	----------------------------	---	--

Closure Conditions:

Acceptance by all parties of the Validation and Acceptance Procedures and successful review of HP' internal configuration management procedures.

Status Desc.:	02/06/03	Per Sam Fahr e-mail dated 2/6/03 - Established "Risk Categories".
	02/05/03	Per Sam Fahr e-mail dated 2/5/03 - Established "Timeframe".



RISK MANAGEMENT DATABASE – PACS

The following screen prints were taken from the PACS and illustrate the capabilities of the Risk Management Database.

RISK MANAGEMENT MENU





RISK MANAGEMENT LIST

Microsoft Access - [Risk Management List]

File Edit View Insert Format Records Tools Window Help

Confidential Double click on Risk record to review

ID	Date	Status	Initiated By	Title	Assi
-0029	11/15/02	Open	Fahr, Sam	Security Exposure on EDS' LAN	Fahr,
-0028	10/29/02	Open	Fahr, Sam	Questionable Throughput Performance	Fahr,
-0026	10/03/02	Open	Fahr, Sam	No Effective Way to Measure Fingerprint Matching Accuracy	Fahr,
-0025	07/23/02	Open	Fahr, Sam	Operation of Multiple Fingerprint Scanner Types in SFIS Production	Fahr,
-0011	07/06/00	Open	Fahr, Sam	Stored Transaction Security Exposure	Saka

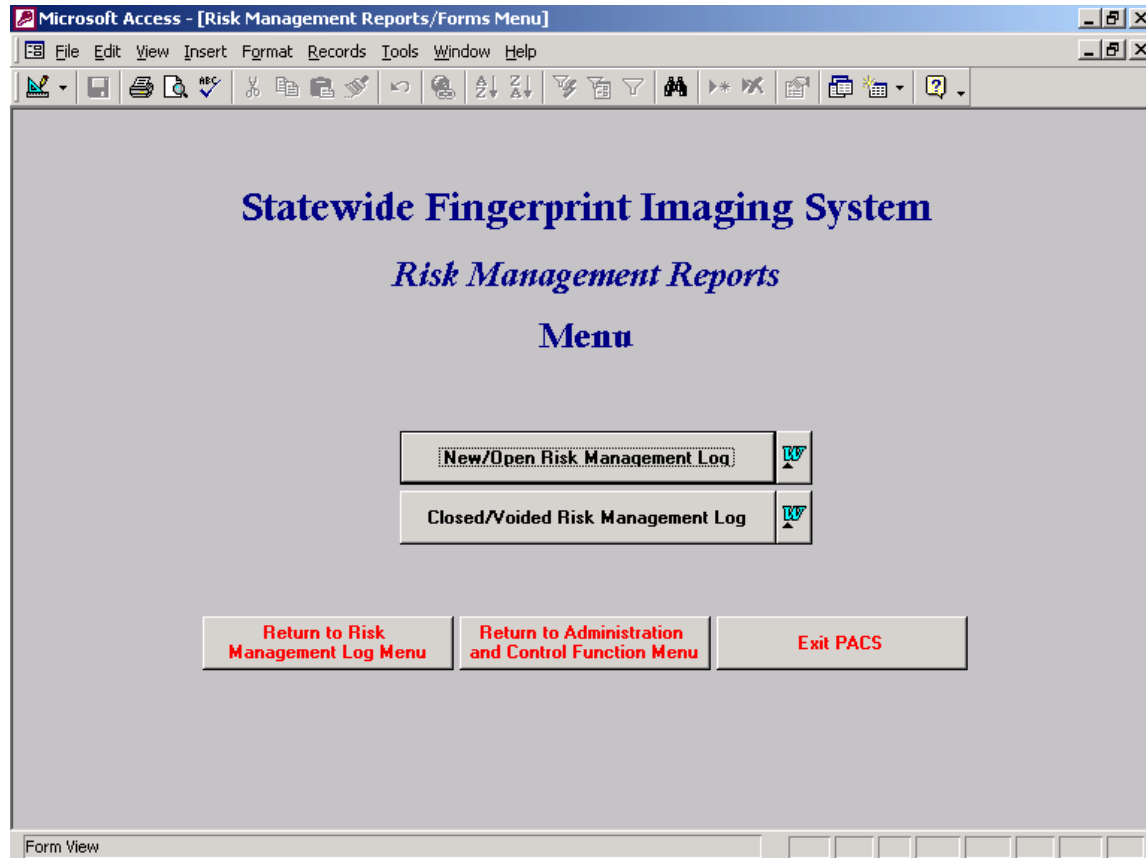
Forms

Exit Summary Identification Assessment Response Closure

Form View



RISK MANAGEMENT REPORTS





RISK MANAGEMENT RECORD MAINTENANCE

There are numerous screens that comprise the PACS' record maintenance functionality. These screens are displayed below

Identification

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 02/08/00

Control Number: SF-RI-0001 Status: Closed
 Risk Confidential: Date Closed: 03/01/00
 Title: SAWS-TA/COTS to SCI/Full Development

Assessment - Response & Control	Implementation Plan	Closure	File Attachments
Identification	Description	Assessment - Impact	Assessment - Recommended Response

Initiated By: Sorrels, Jorg Date Initiated: 10/01/99
 Project Mgr.: Christie, George PM Validation: Yes No TBD Validation Date: 10/01/99
 PM Comments:

Status Description:
 Status Date: _____ Status Description: _____

Record: 14 |<|>|>>|*

Forms

New Find Undo Save < > Exit Summary
 Identification Assessment
 Response Closure

Choose name from drop down menu or defaults to unknown



Description

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed
 Priority: High
 Risk Confidential: Date Closed: 10/15/03
 Title: Sheyko vs. Saenz
 Assigned To: Christie, George Assigned Date: 03/06/03

Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan	Closure
Identification	Description	Assessment - Impact	
<p>Description:</p> <p>CDSS has a policy in CalWORKS of fingerprinting all adults in the assistance unit, even if not all adults have applied for benefits in their own right. The issue in the case is whether we can/should do that. If it were decided that other adults who haven't applied for assistance couldn't be fingerprinted, it might have some affect on the SFIS workload. There are 3 potential detrimental effects if the courts rule in favor of the advocacy</p> <p>Risk Event iManage Doc #: _____</p> <p>RAM Date: 08/05/98 Risk Impact: High Risk Probability: Low (< 30%) Risk Type: Uncontrollable</p> <p>Risk Category(s):</p> <ul style="list-style-type: none"> RiskCategory Requirements Resources <p>Record: 1 of 4</p> <p>Undo Save Print Exit</p>			

Enter description of Risk Event. FLTR NUM



Assessment — Impact

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed
 Priority: High
 Risk Confidential: Date Closed: 10/15/03
 Title: Sheyko vs. Saenz
 Assigned To: Christie, George Assigned Date: 03/06/03

Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan	Closure				
Identification	Description	Assessment - Impact					
Budget: TBD	Budget File iManage Doc #:						
One-Time Cost:	On-Going Cost:						
Timeframe: Long-term (> 12 months)	Timeframe File iManage Doc #:						
Task(s) Affected:	<table border="1"> <thead> <tr> <th>WBS #</th> <th>WBS Name</th> </tr> </thead> <tbody> <tr> <td> </td> <td> </td> </tr> </tbody> </table>			WBS #	WBS Name		
WBS #	WBS Name						
Other Projects Affected:	<table border="1"> <tr> <td> </td> </tr> </table>						

Record: [Navigation icons]

Undo Save Print Exit

Choose Budget from drop down menu. FLTR NUM



Assessment — Recommended Response

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed

Risk Confidential: Priority: High

Title: Sheyko vs. Saenz Date Closed: 10/15/03

Assigned To: Christie, George Assigned Date: 03/06/03

Identification	Description	Assessment - Impact
Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan
		Closure

Response: Acceptance

Reason or Type Transference:

Suggested Strategies & Measures:

Suggested Strategies & Measures iManage Doc #: _____

Assessment Completed By: _____ Assessment Completion Date: _____

Undo Save Print Exit

Choose Response from drop down menu. FLTR NUM



Assessment — Response and Control

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed
 Priority: High
 Risk Confidential: Date Closed: 10/15/03
 Title: Sheyko vs. Saenz
 Assigned To: Christie, George Assigned Date: 03/06/03

Identification	Description	Assessment - Impact	
Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan	Closure
PM Action: Wait	For Mitigation Actions		
Change Order Required: <input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> TBD	Change Request Number: [] []	Date Initiated: []	
Title: []			
<input type="button" value="Undo"/> <input type="button" value="Save"/> <input type="button" value="Print"/> <input type="button" value="Exit"/>			

Choose PM Action from drop down menu. FLTR [] [] [] NUM [] []



Implementation Plan

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed
 Priority: High
 Risk Confidential: Date Closed: 10/15/03
 Title: Sheyko vs. Saenz
 Assigned To: Christie, George Assigned Date: 03/06/03

Identification	Description	Assessment - Impact
Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan
		Closure
Implementation Plan:		
IP File iManage Doc #:		
Cost Not To Exceed:	One-time Costs:	or On-going Costs:
Schedule:	If Change:	
Not To Exceed:	Workdays	
Coordination with Other Projects:		
Conditions for Closure:		
Mitigations Authorization:		Mitigation Date:

Undo Save Print Exit

Enter Implementation Plan description FLTR NUM



Closure

Microsoft Access - [Risk Management Log]

File Edit View Insert Format Records Tools Window Help

Confidential *Risk Management Log* Date Logged: 03/06/03

Control Number: SF-RI-0034 Status: Closed
Priority: High
Risk Confidential: Date Closed: 10/15/03
Title: Sheyko vs. Saenz
Assigned To: Christie, George Assigned Date: 03/06/03

Identification	Description	Assessment - Impact
Assessment - Recommended Response	Assessment - Response & Control	Implementation Plan

Risk Realized: Yes No TBD Response Successful: Yes No TBD

Lesson(s) Learned:

Undo Save Print Exit

Form View FLTR NUM



AMENDMENT HISTORY

Version	Date	Section, Page(s)and Text Revised
Version 4	12/31/2009	Reflects addition of IHSS and completion of the Procurement Project
Version 4	12/31/2009	Entire RMP: Changed footers From “Version 3.2” To “Version 4.0.”
Version 4	12/31/2009	Entire RMP: Deleted references to the Procurement Project as it has been completed.
Version 4	12/31/2009	Entire RMP: Changed references From “EDS” To “HP.”
Version 4	12/31/2009	Entire RMP: Deleted references to DGS as the Procurement Project has been completed.
Version 4	12/31/2009	Referenced Documents, p. 2, Revised From “SFIS Contract, Contract #98136, September 7, 1999.” To “SFIS Contract, Contract #18500, August 27, 2009.” ,
Version 4	12/31/2009	Referenced Documents, p. 2, Added ISO/IEC Standard 27005-2008: “Information technology — Security techniques — Information security risk management”, ISO/IEC Standard 27002-2005: “Security techniques -- Code of practice for information security management”, State Administrative Manual (SAM), Chapter 5305, “Risk Management”, (Revised October, 2009), and State Administrative Manual (SAM), Chapter 5305.1, “Risk Analysis”, (Revised



Version	Date	Section, Page(s)and Text Revised
		October, 2009).
Version 4	12/31/2009	Referenced Documents, p. 3, Added “State of California Office of System Integration, PMO Procedure, Project Monitoring and Control Procedure, OSI-AP-08-14, August 28, 2008.”
Version 4	12/31/2009	Referenced Documents, p. 3, Added “Risk Management Guide for Information Technology Systems”, NIST Special Publication 800-30, July 2002.
Version 4	12/31/2009	Definitions, p. 6, Added “IHSS: In-Home Supportive Services. The IHSS Program will help pay for services provided to recipients so that they can remain safely in their own homes. To be eligible, the recipient must be over 65 years of age, or disabled, or blind. Disabled children are also eligible for IHSS. IHSS is considered an alternative to out-of-home care, such as nursing homes or board and care facilities. The types of services which can be authorized through IHSS are housecleaning, meal preparation, laundry, grocery shopping, personal care services, bathing, grooming and paramedical services), accompaniment to medical appointments, and protective supervision for the mentally impaired.”



Version	Date	Section, Page(s)and Text Revised
Version 4	12/31/2009	Definitions, p. 6, Added “OTech: Office of Technology Services. Formerly DTS. The State of California Department that provides information technology services to many State, county, federal and local government entities throughout the State of California.”
Version 4	12/31/2009	Risk Management Process, Step 1-a, p. 16, Revised From “SFIS Project activities include SFIS M&O and observation by SFIS project participants of all aspects of M&O.” To “SFIS Project activities include SFIS M&O, development and implementation of IHSS functionality, and observation by SFIS project participants of all aspects of M&O.”
Version 4	12/31/2009	Risk Management Process, Step 5-c, p. 33, Revised From “Changes in risk state will be reviewed monthly in the first CCB meeting of every month.” To “Changes in risk state will be reviewed monthly, normally occurring in the third week of every month or as required..”
Version 3.2	12/31/2008	
Version 3.2	12/31/2008	Entire RMP: Changed footers From “Version 3.1” To “Version 3.2.”
Version 3.2	12/31/2008	Entire RMP, Changed From “DOF” To “OCIO” where appropriate.



Version	Date	Section, Page(s)and Text Revised
Version 3.2	12/31/2008	Referenced Documents, p. 3, Added “State of California Office of the Chief Information Officer, Transition of IT Project Review, Approval and Oversight Responsibilities from the Department of Finance to the Office of the State Chief Information Officer, and Information Technology Budgeting Guidelines BL 08-06 , issued 03-14-2008.”
Version 3.2	12/31/2008	Definitions, p. 6, Added “ OCIO: Office of the Chief Information Officer (OCIO). The State of California office with statutory authority over IT strategic vision and planning, enterprise architecture, policy, and project approval and oversight.”
Version 3.2	12/31/2008	Definitions, p. 6 Revised From “ HHSDC: Health and Human Services Data Center — The State of California data center formerly responsible for monitoring and directing contractor activities on behalf of CDSS.” To “ HHSDC: Health and Human Services Data Center — Formerly the State of California data center formerly responsible for monitoring and directing contractor activities on behalf of CDSS.”
Version 3.2	12/31/2008	Definitions, p. 6 Revised From “ DOF: Department of Finance — The State of California’s IT control agency.” To “ DOF: Department of Finance — Formerly the State of



Version	Date	Section, Page(s)and Text Revised
		California’s IT control agency.”
Version 3.1	08/31/2007	
Version 3.1	08/31/2007	Entire RMP: Changed footers From “Version 3.0” To “Version 3.1.”
Version 3.1	08/31/2007	Entire document: Replaced “Project Director” with “Project Manager.”
Version 3.1	08/29/2008	Referenced Documents: Added: “ISO/IEC 27005-2008: Information technology — Security techniques — Information security risk management.”
Version 3.1	08/29/2008	Deleted Section: Risk Management Database – Risk Radar™.
Draft Version 3.0	03/02//2007	
Draft Version 3.0	03/02//2007	Entire RMP: Changed footers From “Version 2.2” To “Version 3.0”.
Draft Version 3.0	03/02//2007	Entire document: Replaced “Project Manager” with “Project Director.”
Draft Version 3.0	03/02//2007	Entire RMP: Added footnote “The contractor has no role with respect to risk management for the Procurement Project.”
Draft Version 3.0	03/02//2007	Entire RMP: Added: “EDS and is subcontractors do not participate in risk management for the Procurement Project.”
Draft Version 3.0	03/02//2007	Referenced Documents, p. 3 Added bulleted items: Risk Management Plan Tailoring Guide,



Version	Date	Section, Page(s) and Text Revised
		Health and Human Services, Office of Systems Integration, June 23, 2004, and Risk Management Plan Template, Health and Human Services, Office of Systems Integration, June 23, 2004.
Draft Version 3.0	03/02//2007	Definitions, p. 5, Added: “ DTS: Department of Technology Services — The State of California Department that provides information technology services to many state, county, federal and local government entities throughout the State of California.”
Draft Version 3.0	03/02//2007	SFIS Risk Management, p. 9, Revised From “OSI SFIS staff and EDS ¹¹ staff work together where appropriate in team risk management to anticipate and avoid problems by managing project risks.” To “OSI SFIS staff and EDS ¹² staff work together with respect to M&O risk management in team risk management to anticipate and avoid problems by managing project risks.” Added: “OSI SFIS staff performs Procurement Project risk management; EDS has no role in Procurement Project risk management.”

¹¹ EDS has no role in Procurement Project risk management.

¹² EDS has no role in Procurement Project risk management.



Version	Date	Section, Page(s)and Text Revised
Draft Version 3.0	03/02//2007	<p>Risk Management Approach, p. 11, Revised From “The database is one of several logical databases developed by KPMG Consulting, Inc to support SFIS throughout development and M&O.” To “The database is one of several logical databases developed by KPMG Consulting, Inc to support SFIS throughout development, M&O, and re-procurement of M&O services.</p> <p>Added: “A separate instance of the PACS was created to support the Procurement Project.”</p> <p>Added: “The Procurement Project instance of the PACS is not available to EDS.”</p>
Draft Version 3.0	03/02//2007	<p>Roles and Responsibilities, p. 12 Added: “The contractor and their subcontractors do not participate in risk management for the Procurement Project.</p>
Draft Version 3.0	03/02//2007	<p>SFIS Risk Management Responsibilities, p. 13, Revised From “2-K. Review Risk State, Recommended Mitigation Strategies and Metrics with OSI Director, CDSS, CHHSA, DOF, and Other Stakeholders” To “2-K. Review Risk State, Recommended Mitigation Strategies and Metrics with OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”</p> <p>Revised From “3-G. Review Mitigations, Metrics, and Action Plans with OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders” To “2-K. 3-G. Review</p>



Version	Date	Section, Page(s)and Text Revised
		Mitigations, Metrics, and Action Plans with OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”
Draft Version 3.0	03/02//2007	SFIS Risk Management Responsibilities, p. 14, Revised From “5-D. Review Risk Status with OSI Director, CDSS, CHHSA, DOF, and Other Stakeholders” To “5-D. Review Risk Status with OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 15, Revised From “The PMO / QA will use input from the Project’s regularly scheduled CCB meetings to construct these initial risk profiles.” To “The PMO / QA will use input from the Project’s regularly scheduled CCB and Procurement Project meetings to construct these initial risk profiles.” Revised From “Particularly good sources for issues and concerns are the regularly scheduled SFIS CCB meetings.” To “Particularly good sources for issues and concerns are the regularly scheduled SFIS CCB and Procurement Project meetings.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 16, Revised From “The PMO / QA will discuss the potential risk and seek consensus with other SFIS Project participants, especially members of the CCB on determining if a potential risk becomes an identified risk.” To “The PMO / QA will discuss the potential risk and seek consensus with other



Version	Date	Section, Page(s) and Text Revised
		SFIS Project participants, especially members of the CCB and members of the Procurement Project team, on determining if a potential risk becomes an identified risk.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 19, Revised From “The SFIS Project Director will review risks with the OSI Director, CDSS, EDS and other stakeholders as required.” To “The SFIS Project Director will review risks with the OSI Deputy Director – SAWS, the OSI Director, CDSS, EDS ¹³ , and other stakeholders as required.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 25, Revised From “The OSI Director has the authority to control the outcome of this risk.” To “The OSI Director or his/her designee has the authority to control the outcome of this risk.” Revised From “The Project Manager has the authority to control the outcome of this risk.” To “The OSI Deputy Director - SAWS or his/her designee has the authority to control the outcome of this risk.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 27, Revised From “The SFIS Project Director assisted by the PMO / QA as required reviews the risk with the Director of OSI, CDSS, CHHSA, DOF, and other stakeholders, as required.” To “The SFIS Project Director, assisted by the PMO / QA as required

¹³ The contractor has no role with respect to risk management for the Procurement Project.



Version	Date	Section, Page(s)and Text Revised
		<p>reviews the risk with the Director of OSI, CDSS, CHHSA, DOF, DGS¹⁴, and other stakeholders, as required.”</p> <p>Revised From “The project criticality of SFIS is considered by DOF to be high. Therefore, all SFIS risks with risk severity of high will be escalated to DOF.” To “The project criticality of SFIS is considered by DOF / DGS to be high. Therefore, all SFIS risks with risk severity of high will be escalated to DOF / DGS.”</p>
Draft Version 3.0	03/02//2007	<p>Risk Management Process, p. 28, Revised From “The Project Manager escalates directly to CDSS.” To “Either the SFIS Project Director or the OSI Deputy Director – SAWS escalates directly to CDSS.”</p> <p>Risk Management Process, p. 28, Added: “OSI Deputy Director – SAWS” to Sequence of Risk Escalation for M&O Risks drawing and re-sequenced escalation path.</p>
Draft Version 3.0	03/02//2007	<p>Risk Management Process, p. 28, Added: Sequence of Risk Escalation for Procurement Project Risks drawing.</p>
Draft Version 3.0	03/02//2007	<p>Risk Management Process, p. 31, Revised From “Responsibility: SFIS Project Manager and PMO / QA for review, SFIS Project Manager for approvals.” To “Responsibility: SFIS Project Director and PMO / QA for review, SFIS Project</p>

¹⁴ For Procurement Project risks.



Version	Date	Section, Page(s) and Text Revised
		Director and/or the OSI Deputy Director – SAWS for approvals.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 32, Revised From “The SFIS Project Manager, assisted by the PMO / QA reviews the risk with the Director of OSI, CDSS, and other stakeholders, as required.” To “The SFIS Project Director, assisted by the PMO / QA reviews the risk with the OSI Deputy Director – SAWS, Director of OSI, CDSS, DOF, DGS, and other stakeholders, as required.”
Draft Version 3.0	03/02//2007	Risk Management Process, p. 34, Added: “Changes in risk state for the Procurement Project will be reviewed weekly at the Procurement Project Meetings.” Revised From “Using risk state information from the Risk Management Databases, the SFIS Project Manager, assisted by the PMO / QA, as required will review mitigation(s), metrics, and action and contingency plans with the OSI Director, CDSS, CHHSA, DOF, and other SFIS stakeholders on a monthly basis, or as required.” To “Using risk state information from the Risk Management Databases, the SFIS Project Director, assisted by the PMO / QA, as required will review mitigation(s), metrics, and action and contingency plans with the OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, DOF, DGS, and other SFIS stakeholders on a monthly basis, or as required.”



Version	Date	Section, Page(s)and Text Revised
Draft Version 3.0	03/02//2007	SFIS Project Risk Management Process Summary, p. 37, Revised From “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended metrics with OSI Director, CDSS, CHHSA, DOF, and Other Stakeholders” To “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended metrics with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”
Draft Version 3.0	03/02//2007	SFIS Project Risk Management Process Summary, p. 37, Revised From “3-G. Review Mitigations, Metrics, and Action Plans with OSI Director, CDSS, CHHSA, DOF, and Other Stakeholders” To “3-G. Review Mitigations, Metrics, and Action Plans with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”
Draft Version 3.0	03/02//2007	SFIS Project Risk Management Process Summary, p. 40, Revised From “5-D. Review Risk Status with, OSI Director, CDSS, CHHSA, DOF, and Other Stakeholders” To “5-D. Review Risk Status with OSI Deputy Director – SAWS, OSI Director, CDSS, CHHSA, DOF, DGS, and Other Stakeholders”
Draft Version 2.2	10/24/2005	
Draft Version 2.2	10/24/2005	Entire RMP: Changed footers From “Version 2.0” To “Version 2.2”.



Version	Date	Section, Page(s)and Text Revised
Draft Version 2.2	10/24/2005	Entire RMP: Changed From “HSDC” or “SID” To “OSI”, where required.
Draft Version 2.2	10/24/2005	Referenced Documents, p. 3. Deleted <ul style="list-style-type: none"> • “SID CMM policies, Best Practices web site (http://bpweb and http://www.bestpractices.cahwnet.gov), SID. • “SID Standards for Risk Management, Best Practices web site (http://bpweb and http://www.bestpractices.cahwnet.gov), SID. • “SID Policy & Standards for Risk Management, http://bpweb/SID%20Policies/SID%20Policy%20for%20Risk%20Mgmt%20(1806_10)%20Signed.PDF, July 16, 2003.”
Draft Version 2.1	04/30/2004	Initial Draft Version 2.1. Change to reflect separate risk management plan for the SFIS Procurement Project.
Draft Version 2.1	04/06/2004	Changed document title From “SFIS Risk Management Plan” To “SFIS Maintenance and Operations Risk Management Plan”.
Draft Version 2.1	04/06/2004	Entire RMP: Changed footers From “Risk Management Plan” To “M & O Risk Management Plan”.
Draft Version 2.0	03/31/2004	Initial Draft Version 2.0. Changed to conform to SID Policy & Standards for Risk Management through inclusion of Risk Radar™
Draft Version 2.0	03/12/2004	Entire RMP: Added Risk Radar™ content.



Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	Entire RMP: Changed Version # From 1.0 To 2.0 — all footers.
Draft Version 2.0	09/30/2003	Entire RMP: Changed From “V&V” To “QA.”
Draft Version 2.0	09/30/2003	Purpose. p. 1, and Definitions. p. 5 — Changed From “Verification and Validation” To “Quality Assurance”.
Draft Version 2.0	09/30/2003	Referenced Documents. p. 2 — Added “Software Acquisition - Capability Maturity Model”, “Software Risk Evaluation (SRE) Method Description”, “Continuous Risk Management Guidebook”, and “Information Technology Project Oversight Framework”.
Draft Version 2.0	09/30/2003	Referenced Documents. p. 3 — Added “SID CMM policies”, “SID Standards for Risk Management”, and SID Policy & Standards for Risk Management, July 16, 2003”.
Draft Version 2.0	09/30/2003	Definitions. p. 5 — Added “DOF” and “CHHSA”.
Draft Version 2.0	09/30/2003	Definitions. p. 6 — Added “For the SFIS RMP this is based on SEI’s “Taxonomy-Based Risk Identification”.” Added “Risk Classification”.
Draft Version 2.0	09/30/2003	Definitions. p. 7 — Added “Risk Level of Control”, and “SID”.
Draft Version 2.0	09/30/2003	Risk Management Approach. P. 9. — Added “The <i>DOF Information Technology Project Oversight Framework</i> and the <i>SID Policy & Standards for Risk Management</i> further



Version	Date	Section, Page(s) and Text Revised
Draft Version 2.0	09/30/2003	<p>developed the paradigm.”</p> <p>Risk Management Process. SFIS Risk Management Responsibilities Table. p. 13 — Added new table entry: “2-B. Determine Risk Classification.” Added new table entry: “2-G. Determine Risk Exposure.” Added new table entry: “2-H. Determine Risk Level of Control.” These additions caused subsequent entries in this portion of the table to be renumbered. The additions also caused the steps described on p. 18-24 to be renumbered. Changed From “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended Metrics with SID Director, CDSS, and Other Stakeholders” To “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended Metrics with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”. Changed From “3-G. Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, and Other Stakeholders” To “3-G. Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”.</p>
Draft Version 2.0	09/30/2003	<p>Risk Management Process. SFIS Risk Management Responsibilities Table. p. 14 — Changed From “5-D. Review Risk Status with SID Director, CDSS, and Other Stakeholders” To</p>



Version	Date	Section, Page(s)and Text Revised
		“5-D. Review Risk Status with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”. Changed From “5-E. Update risk management database” To “5-E. Update risk management and Lessons Learned Databases”
Draft Version 2.0	09/30/2003	Risk Management Process. p. 17 — Added “Risk Classification” and Risk Level of Control” to bulleted list.
Draft Version 2.0	11/21/2003	Risk Management Process. Step 2-A — Determine Risk Category. P.18 – 20. Revised bulleted items to more closely correspond to “SEI Risk Taxonomy from Taxonomy-Based Risk Identification, 1993”.
Draft Version 2.0	09/30/2003	Risk Management Process. p. 20 — Added new step: “2-B. Determine Risk Classification.” This addition caused subsequent steps (p. 18-24) in this process to be renumbered.
Draft Version 2.0	09/30/2003	Risk Management Process. Criteria for Risk Impact Table. p. 21 — Added “The risk represents a significant negative impact on project budget, schedule, or quality.”, “The risk’s material impacts would significantly affect users, clients, or other key stakeholders.”, and “The risk does not represent a significant or material impact on project budget, schedule or quality.”
Draft Version 2.0	09/30/2003	Risk Management Process. Criteria for Risk Probability Table. p. 22. — Changed From “It is very likely that the risk will occur.” To “The risks



Version	Date	Section, Page(s)and Text Revised
		<p>are almost certain or very likely to occur.” Changed From “It is somewhat likely the risk will occur.” To “The risks may occur or have a 50/50 chance of occurring. Changed From “It is unlikely the risk will occur” To “The risks are unlikely to occur or will probably not occur.” Step 2-E — Determine Risk Timeframe. Deleted “immediate”. Added “Medium-Term”.</p>



Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	<p>Risk Management Process. Criteria for Risk Timeframe Table. p. 22. — Deleted “No impact”.</p> <p>Deleted “The timeframe for the risk does not have an affect on risk impact.”</p> <p>Deleted “Immediate”.</p> <p>Deleted “The risk is expected to occur within a very short period of time, less than 1 month.”</p> <p>Changed From “The risk is expected to occur within the near-term, between 1 and 12 months.”</p> <p>To “The risk is most likely to occur in less than 6 months.”</p> <p>Added “Medium-Term”.</p> <p>Added “The risk is most likely to materialize between 6 months to 1 year from now.”</p> <p>Changed From “The risk is expected to occur in the far-term, more than 12 months in the future.”</p> <p>To “The risk is most likely to materialize in a period of greater than 1 year.”</p>
Draft Version 2.0	09/30/2003	<p>Risk Management Process. p. 23. — Added new Step: 2-F — Determine Risk Exposure.</p> <p>Added new table: Criteria for Risk Exposure</p> <p>Changed From “Step 2-G — Determine Initial Risk Priority” To “Step 2-G — Determine Risk Severity (Priority)”</p> <p>Changed From “The table below is used for determining risk priority using the risk impact, probability, and timeframe, described as “Critical”, “High”, “Medium”, “Low”, or “TBD”. To “The table below is used</p>



Version	Date	Section, Page(s) and Text Revised
		for determining risk priority using the risk impact, probability, and timeframe, described as “High”, “Medium”, “Low”, or TBD”. Deleted “Determination of risk timeframe is a subjective process that considers the criticality of internal and external project factors within the unique context of SFIS.”
Draft Version 2.0	09/30/2003	Risk Management Process. p. 24. — Deleted Determination of Risk Priority Table. Added Determination of Risk Severity Table. Added “Step 2-H — Determine Risk Level of Control”.
Draft Version 2.0	09/30/2003	Risk Management Process. p. 25. — Added “The sequence in which a risk is escalated is depicted below. The SFIS Project Manager initiates all risk escalations, assisted by the PMO / QA. The HHSDC SID Director escalates directly to CDSS. The HHSDC Director to whom the SID Director reports will be made aware of escalations but will not normally manage escalations.” Added Sequence of Risk Escalation Diagram.





Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	<p>Risk Management Process. p. 26. — Changed From “Step 2-K — Review Risk with SID Director, CDSS, and Other Stakeholders” To “Step 2-K — Review Risk with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”.</p> <p>Changed From “The SFIS Project Manager, assisted by the PMO / QA as required reviews the risk with the Director of SID, CDSS, and other stakeholders, as required. The SID Director, CDSS, and other stakeholders, as required will validate the risk state including:” To “The SFIS Project Manager, assisted by the PMO / QA as required reviews the risk with the Director of SID, CDSS, CHHSA, DOF, and other stakeholders, as required. The SID Director, CDSS, CHHSA, DOF, and other stakeholders, as required will validate the risk state including:”</p> <p>Added “Risk Classification”, Risk Level of Control, and “Risk Exposure” to bulleted list.</p> <p>Changed From “The SFIS Project Manager, assisted by the PMO / QA as required will review risks with the SID Director, CDSS, and other SFIS stakeholders on a monthly basis, or as required.” To “The SFIS Project Manager, assisted by the PMO / QA as required will review risks with the SID Director, CDSS, CHHSA, DOF, and other SFIS stakeholders on a monthly basis, or as required.”</p> <p>Added “The determination of to which level of</p>



Version	Date	Section, Page(s)and Text Revised
		responsibility risks are escalated is described in the following table. The project criticality of SFIS is considered by DOF to be high. Therefore, all SFIS risks with risk severity of high will be escalated to DOF.” Added Determination of Risk Escalation Table.
Draft Version 2.0	09/30/2003	Risk Management Process. p. 29. — Added “The output of Step 2-H — Determine Risk Level of Control may be useful if approvals out side the scope of the SFIS Project Manager’s scope of authority are required.”



Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	<p>Risk Management Process. p. 30. — Changed From “Step 3-G — Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, and Other Stakeholders” To “Step 3-G — Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”.</p> <p>Changed From “The SFIS Project Manager, assisted by the PMO / QA reviews the risk with the Director of SID, CDSS, and other stakeholders, as required. The SID Director, CDSS, and other stakeholders, as required will validate the risk state including:” To “The SFIS Project Manager, assisted by the PMO / QA reviews the risk with the Director of SID, CDSS, CHHSA, DOF, and other stakeholders, as required. The SID Director, CDSS, CHHSA, DOF, and other stakeholders, as required will validate the risk state including:”</p> <p>Added “Risk Classification”, Risk Level of Control, and “Risk Exposure” to bulleted list.</p>





Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	<p>Risk Management Process. p. 32. — Changed From “Step 5-D — Review Risk Status with SID Director, CDSS, and Other Stakeholders” To “Step 5-D — Review Risk Status with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”.</p> <p>Changed From “Using risk state information from the Risk Management Database, the SFIS Project Manager, assisted by the PMO / QA, as required will review mitigation(s), metrics, and action and contingency plans with the SID Director, CDSS, and other SFIS stakeholders on a monthly basis, or as required.” To “Using risk state information from the Risk Management Database, the SFIS Project Manager, assisted by the PMO / QA, as required will review mitigation(s), metrics, and action and contingency plans with the SID Director, CDSS, CHHSA, DOF, and other SFIS stakeholders on a monthly basis, or as required.”</p> <p>Changed From “Step 5-E — Update Risk Management Database” To “Step 5-E — Update Risk Management and Lessons Learned Databases”</p> <p>Added “The PMO / QA and the SFIS Project Manager will determine if the information concerning a risk is appropriate for entry into the SFIS Lessons Learned Database. If deemed appropriate, the information will be entered by the PMO / QA.”</p>



Version	Date	Section, Page(s) and Text Revised
		<p>Changed From “Responsibility: PMO / QA” To “Responsibility: PMO / QA and SFIS Project Manager.”</p>
Draft Version 2.0	09/30/2003	<p>SFIS Project Risk Management Process Summary. p. 34. — Added new table entry: “2-B. Determine Risk Classification.” Added new table entry: “2-F. Determine Risk Exposure.” These additions caused subsequent entries in this portion of the table to be renumbered. Added “State of California Policy and Standards (SID, DOF)”</p>
Draft Version 2.0	09/30/2003	<p>SFIS Project Risk Management Process Summary. p. 35. — Added new table entry: “2-H. Determine Risk Level of Control.” Changed From “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended Metrics with SID Director, CDSS, and Other Stakeholders” To “2-K. Review Risk State, Recommended Mitigation Strategies and Recommended Metrics with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”</p>
Draft Version 2.0	09/30/2003	<p>SFIS Project Risk Management Process Summary. p. 36. — Changed From “3-G. Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, and Other Stakeholders” To “3-G. Review Mitigations, Metrics, and Action Plans with SID Director, CDSS, CHHSA, DOF, and Other Stakeholders”</p>



Version	Date	Section, Page(s)and Text Revised
Draft Version 2.0	09/30/2003	<p>SFIS Project Risk Management Process Summary. p. 37. — Changed From “5-D. Review Risk Status with SID Director, CDSS, and Other Stakeholders” To “5-D. Review Risk Status with SID Director, CDSS, and Other Stakeholders”.</p> <p>Changed From “PMO / QA” To “PMO / QA, SFIS Project Manager”.</p> <p>Changed From “5-E. Update Risk Management database” To “5-E. Update Risk Management and Lessons Learned Databases”</p> <p>Changed From “Updated Risk Management Database” To Updated Risk Management and Lessons Learned Databases”</p>
Version 1.0	02/07/2003	Final Version 1.0
Draft Version 1.0	12/06/2002	Initial Draft Version 1.0