

Systems Integration Division (SID)

SID Policy on Risk Management

⌘ ⌘ ⌘ ⌘ ⌘ ⌘ ⌘ ⌘

April 26, 2004

California Health and Human Services Agency Data Center

Revision History

REVISION	DATE OF RELEASE	PURPOSE
Initial Draft	April 26, 2004	Initial Release

Approval



CHRISTINE DUNHAM, SID ASSISTANT DIRECTOR

1 INTRODUCTION

1.1 Adoption of SID Policy

As part of its ongoing commitment to process improvement and quality within the division, the Systems Integration Division (SID) is adopting this SID Policy and Standard for Risk Management. This policy will help to clarify and enhance its current practices, continue to align the organization with the Software Engineering Institute's Capability Maturity Model (SEI's CMM), and ensure compliance with the Department of Finance (DOF) Information Technology Oversight Framework (Budget Letter 03-04, dated 7 February 2003).

1.2 Applicability

[1.2.1]¹ This policy shall apply to all SID projects² effective the date of this policy. Projects that are in the middle of an SID life cycle process³ (at the effective date of this policy) are required to demonstrate due diligence in complying with this policy within 30 days, to the degree that it does not jeopardize their ability to satisfy prior project commitments.

[1.2.2] The SID Assistant Director shall consider special situations for non-compliance on a case-by-case basis.

[1.2.3] Projects requesting a waiver from the requirements in this policy shall comply with the Deviation/Waiver Process (iManage SIDdocs #2484).

[1.2.4] Projects that are in the Maintenance and Operations (M&O) life cycle phase shall, at a minimum, assess and report compliance with this policy on an annual basis.

[1.2.5] All other projects shall, at a minimum, assess and report compliance with this policy at the start of a new life cycle phase.

1.3 References

The following documents were used in the creation of this policy:

¹ Brackets [] are used as a reference designator for explicitly stated policy requirements ("shall's"). The numbers in the brackets are included in the SID Compliance Toolbox (iManage SIDdocs #2093) using a policy reference designator (e.g. PM Policy-1.2.1) for ease of verification and traceability to applicable CMM and TOSU requirements.

² In this document, SID Projects refer only to projects of a statewide nature (e.g. CWS/CMS, CMIPS, EBT, ISAWS, SFIS, etc.) and not to software release projects that are part of a routine Maintenance & Operations life cycle, or internally created projects and initiatives.

³ The SID Best Practices web site defines the typical life cycle for software acquisition projects in the organization. Definitions for each life cycle phase are available at www.bestpractices.cahwnet.gov/processes.htm.

- ?? Information Technology Oversight Framework, Budget Letter 03-04, dated 7 February 2003, Department of Finance – Technology Oversight and Security Unit.
- ?? Software Acquisition Capability Maturity Model (SA-CMM), Version 1.02, Key Process Area 3.4 – Acquisition Risk Management, April 1999, Software Engineering Institute.
- ?? Taxonomy-Based Risk Identification, June 1993, SEI.
- ?? Software Risk Evaluation Method Description, December 1999, SEI.
- ?? Project Management Body of Knowledge (PMBOK), 2000, Project Management Institute.
- ?? SID Policy on Project Management, iManage SIDdocs #2453, 23 February 2004, Systems Integration Division (SID).
- ?? Best Practices Web Site (BPweb), Systems Integration Division (SID), <http://www.bestpractices.cahwnet.gov>.
- ?? Glossary and Acronyms, BPweb, SID.

1.4 Compliance Verification

[1.4.1] The SID Best Practices Support Group (BPSG) shall assess compliance to this policy at least annually using the applicable categories of the SID Compliance Assessment Toolbox (iManage SIDdocs #2093). For more information on compliance assessments, refer to the BPSG Project Plan.

1.5 Relationship to Other Policies

This policy is subordinate to the SID Policy on Project Management.

2 POLICY STATEMENT

It is the policy of SID to follow, adhere to, and implement proven project management best practices in compliance with the SEI CMM methodology, the DOF IT Project Oversight Framework, and the PMI PMBOK.

[2.0.1] Project Managers shall comply with the requirements, procedures and processes referenced in this policy document.

2.1 Required Documentation

[2.1.1] Projects shall document their specific approach to risk management in accordance with the SID Risk Management Template and associated tailoring guidance on the BP website.

[2.1.2] Projects shall update and maintain the Risk Management Plan until the system is retired or terminated.

[2.1.3] Projects shall produce and manage a minimum set of risk management supporting documentation with a defined hierarchical relationship in accordance with the SID MPP Template (iManage SIDdocs #2513).

[2.1.4] Documentation related to risk management shall be tailored and revised (as appropriate) to accommodate the differences between SID acquisition life cycle phases as defined on the BP website.

[2.1.5] The status of risk management activities shall be documented and reviewed periodically (such as at key milestones and prior to a contract end) with the project management team, quality management team, and Project Manager.

[2.1.6] The status of all high criticality risks shall be documented and reviewed at least monthly by the project management team, quality management team, Project Manager and SID Assistant Director.

[2.1.7] Measurements showing the status of risks and risk management activities shall be documented, tracked, and analyzed for trends.

Refer to the SID Policy on Quality Management for the specific metrics.

2.2 Risk Management Roles & Responsibilities

[2.2.1] The Project Manager shall designate a specific individual to fulfill the role of the Risk Manager.

[2.2.2] The Risk Manager shall be responsible for implementation of this policy and for all risk management activities, either directly or by overseeing the work of others, including the development and maintenance of the Risk Management Plan (based on the SID Risk Management Plan Template).

[2.2.3] Projects shall tailor their risk management program to accommodate the project's position in the SID Acquisition Life Cycle in accordance with the SID Risk Management Plan Template and associated tailoring guidance.

[2.2.4] The risk management functions identified in the model functional organizational chart shall be addressed in the Risk Management Plan.

For more information, see the model organizational chart and specific roles and responsibilities on the BP website. Depending on the size and life cycle phase of the project, multiple individuals may perform a role or a single individual may perform multiple roles.

2.3 Risk Management Training

[2.3.1] Risk Managers shall participate in initial and refresher SID Training for Risk Managers.

[2.3.2] Risk Managers shall facilitate a project orientation to risk management as part of the project-specific Training Plan.

2.4 Risk Management Tools

[2.4.1] Risk items shall be identified, controlled, and periodically updated using Risk Radar, the SID division standard Project Risk Database (PRD).

3 RISK MANAGEMENT METHODOLOGY

The SID has adopted the SEI Risk Paradigm as its risk management methodology. The requirements for implementing SID's risk management methodology are defined in the subsequent sections. The major elements of the risk management methodology are as follows.

- ?? Risk Identification
- ?? Risk Analysis
- ?? Risk Planning
- ?? Risk Implementation
- ?? Risk Tracking and Control
- ?? Risk Communication

[3.0.1] The Risk Management Plan shall describe or reference the specific processes and procedures that will be used to identify and manage the project's risks.



3.1 Risk Identification

[3.1.1] Projects shall identify and document potential project risks before they become problems.

[3.1.2] Risk statements shall clearly describe the concern, likelihood of the risk occurring, and specific consequences and impacts should the risk occur.

[3.1.3] Projects shall use the SEI's Taxonomy-Based Risk Identification schema (with associated questions) as a tool for identifying potential project risks.

[3.1.4] The primary use of the SEI Taxonomy shall be to aid projects in the identification of potential risks, NOT in mandating categories for managing risks.

Projects are strongly encouraged to use other tools or methods (e.g., brainstorming, List of SID-Specific Risks, etc.) as a way to identify risk areas not specifically addressed by the Risk Taxonomy. Risk areas unique to SID include such things as:

- ?? Business Process Re-engineering (BPR),
- ?? Statewide Implementation,
- ?? Project-specific functional areas, and
- ?? Communications with Advocacy groups, unions and other public stakeholders.

3.2 Risk Analysis

[3.2.1] Projects shall analyze and transform risk items into information that can be used to aid decision-making and to validate the risk information.

[3.2.2] Projects shall incorporate the guidance provided below into their project Risk Management Plan.

[3.2.3] Recommendations for mitigating and measuring risk items and reviewing risk item information shall be included in the description and analysis of the risks.

[3.2.4] Projects shall classify risks using the following categories taken from the DOF IT Project Oversight Framework, Appendix C (*Categories and Examples of Risk*) and Appendix D (*Project Risk List*).

- ?? Plan/Schedule
- ?? Organization and Management
- ?? Development Environment
- ?? User Involvement
- ?? Contractor Performance
- ?? Requirements Management
- ?? Product Characteristics

- ?? External Environment
- ?? Personnel
- ?? Design and Implementation
- ?? Process

Note: Projects may add additional classifications to meet the unique needs of the project.

[3.2.5] Projects shall consult their oversight representative(s) before finalizing risk categories.

[3.2.6] Projects shall adopt a High, Medium, Low rating when assigning impacts to identified risks.

- ?? **High-** The risk represents a significant negative impact on project budget, schedule, or quality.
- ?? **Medium-** The risk's material impacts would significantly affect users, clients, or other key stakeholders.
- ?? **Low-** The risk does not represent a significant or material impact on project budget, schedule or quality.

[3.2.7] Projects shall adopt the following rating when assigning probability to identified risks.

- ?? **High-** The risks are almost certain or very likely to occur.
- ?? **Medium-** The risks may occur or have a 50/50 chance of occurring.
- ?? **Low-** The risks are unlikely to occur or will probably not occur.

[3.2.8] Projects shall define the timeframes when risks could materialize and a mitigation/contingency plan must be implemented using a Short-Term, Medium-Term, or Long-Term rating.

- ?? **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.

[3.2.9] Projects shall assign the following risk exposure (impact versus probability) ratings as shown in the matrix below.

		Probability		
		High	Medium	Low
Impact	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.

[3.2.10] Projects shall define risk severity (priority) as a function of Risk Exposure and Timeframe for determining the relative PRIORITY of the identified risks.

[3.2.11] Projects shall assign risk severity ratings (timeframe versus exposure) as shown in the matrix below.

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

3.3 Risk Management Planning for Mitigations/Contingencies

[3.3.1] Projects shall document their risk mitigation/contingency strategy for each risk in the Project Risk Database.

[3.3.2] Projects shall assign a specific individual (the risk owner) to be responsible for the mitigation and ownership of a specific risk.

[3.3.3] The development of risk mitigation/contingency strategies shall include specific checkpoints/triggers for actions and measurements.

Acceptable actions include: taking action to avoid the risk altogether, accepting the risk without action, watching for a period of time before deciding what to do, if anything, or actively mitigating the impacts of a risk.

[3.3.4] The Risk Manager and project management team shall review and approve risk mitigation/contingency plans and measurements prior to their implementation.

[3.3.5] Changes to risk profile information shall be documented in the Project Risk Database and reviewed with the project management team, Risk Manager, and Risk Owner.

3.4 Risk Management Implementation

[3.4.1] Projects shall execute their risk mitigation/contingency action plans and record risk profile information changes in a Project Risk Database (PRD).

[3.4.2] Measurements showing the progress and status of risk action plans shall be made and used to determine if the action plans need to be modified or continued.

3.5 Risk Tracking and Controlling

[3.5.0.1] Projects shall track and control the risk management process to insure that all steps are being followed and, as a result, risks are being mitigated.

[3.5.0.2] Projects shall oversee and track action plan execution, re-assessment of risks, reporting of risk status, and recording of risk information changes in a Project Risk Database (PRD).

3.5.1 Division-Level Risk Reporting

[3.5.1.1] The Management Steering Council (MSC) shall track risks that impact multiple projects in the SID organization.

[3.5.1.2] Risk affecting multiple SID projects shall be periodically discussed and tracked as formal agenda items at the monthly MSC meetings.

3.5.2 Project Risk Reporting and Escalation

[3.5.2.1] Projects shall report risks to SD on a monthly basis (or as needed).

[3.5.2.2] Projects shall report risks to their oversight representative(s) using Appendix E: Risk Management Form of the DOF IT Project Oversight Framework reporting guidelines, and any other reporting guidelines of the oversight entity.

[3.5.2.3] Projects shall define risk escalation as a function of Project Criticality (see DOF's IT Project Oversight Framework, Section 2) and Risk Severity (see above) as a means for determining which risks will be escalated based on the matrix below. Not all risks require escalation, and escalation of project risks will not necessarily result in a change in project criticality.

		Risk Severity		
		High	Medium	Low
Project Criticality	High	DOF	CHHS	CDSS / DHS / HHSDC / SID
	Medium	CHHS	CHHS	CDSS / DHS / HHSDC / SID
	Low	CHHS	CDSS / DHS / HHSDC / SID	

3.5.3 Level of Risk Control

Projects may include a Level of Control category with the four choices as shown below. This category can be used to aid in risk escalation (e.g., SID-Level, HHSDC Director-Level, PM-Level, etc.).

Level of Control	Definition
No Control	No resource within SID or HHSDC can control the outcome of this risk
Minimal	The SID Assistant Director or HHSDC Director has the authority to control the outcome of this risk
Moderate	The Project Manager has the authority to control the outcome of this risk
High	A Project Team Leader has the authority to control the outcome of this risk

3.6 Risk Communication

[3.6.1] Projects shall perform ongoing communication that enables the sharing and effective management of risks throughout the project life cycle.

[3.6.2] Projects shall include communication of project risks as an ongoing activity that is documented in the project Risk Management Plan and Communication Plan.

Some projects have “confidential” risks that could have legal ramifications if inadvertently released. The notion of “public” risks needs to be considered when deciding to offer risks for the purpose of lessons learned.

[3.6.3] Projects shall coordinate the release of potentially sensitive information with their legal advisors before submitting items to the public or across projects.

[3.6.4] At the completion of the project or retirement of the system, the project office shall review all remaining risks and document the final status of all risks.

[3.6.5] Lessons learned shall be captured and forwarded to the Best Practices Support Group for incorporation into the division’s repository of lessons learned.

[3.6.6] The PRD shall be archived and stored in accordance with the appropriate retention policy.