State of California

Department of Technology

Information Technology Project Oversight Framework

SIMM Section 45

Revised April 2017

Table of Contents

Introduction

Pursuant to Government Code (GC) Sections 11545 and 11546, the California Department of Technology (CDT) is responsible for the approval and oversight of IT projects, which includes establishing and enforcing policies for information technology (IT) projects. Per State Administrative Manual (SAM) Section 4819.2, Project oversight is defined as "An independent review and analysis to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies any issues and risks affecting these project components." Independent project oversight is a process that begins immediately following project approval and continues through project closeout.

The IT Project Oversight Framework applies to all reportable projects as defined in SAM Section 4819.37 and describes the criteria that CDT will use to assess the risk, sensitivity and level of criticality and oversight for IT projects. Oversight requirements identified in this framework emphasize risk identification and reporting, along with the need for independent review of the *minimum* set of practices and products described herein. Although this framework primarily addresses Independent Project Oversight practices, Independent Verification and Validation (IV&V) requirements are also identified.

Project Classification

Project Complexity Assessment

As part of the Project Approval Lifecycle (PAL), CDT will evaluate each proposed project to determine the level of project oversight needed on a given project. When Agency/state entities submit new project proposals for approval, the Complexity Assessment tool (SIMM Sections 45C and 45D) is used to assess the complexity of the project on the two most common dimensions (business complexity and technical complexity) consisting of a series of attributes. Typical business attributes include size, geography, interaction with other departments and entities, impact to business processes, and financial risk. Typical technical attributes include level of technology integration, security needs, stability of hardware/software, and team experience. The complexity assessment is based upon CDT's extensive breadth of historical experience including lessons learned with projects and its enterprise view of the state's IT portfolio. CDT's assessment will place each individual project into one of three categories (low, medium, or high). Per SAM Section 4940, all medium and high criticality projects will receive independent oversight from CDT, oversight for low criticality projects will be provided at the discretion of CDT.

Project Management Risk Assessment

Additionally as part of PAL, CDT will evaluate the project management maturity of the Agency/state entity and its ability to carry out projects. The Project Management Risk Assessment (SIMM Sections 45A and 45B) will assess the project management capability and degree to which the IT project has established and used *minimum* project management practices, processes and deliverables documented in the California Project Management Framework (CA-PMF). As part of this assessment, CDT's Independent Project Oversight (IPO) manager may interview the appropriate Agency/state entity IT management and staff, review project documents, and continually observe the project team and project activities to determine the degree to which the requirements are being met.

The Project Management Risk Assessment will evaluate such elements as:

- Organizational commitment to a well-defined, mature project management process

- Existence of predicated management commitment, functions, and systems

- Competence of participants in any project management endeavor

- Organizational project management environment (e.g., tools, infrastructure) and how well these are integrated

- Measurement metrics in the organization and how well they are used and any applicable past performance

- Organization's continuous improvement process

Oversight Protocol

In order for CDT to effectively carry out the responsibility of providing approval and oversight of IT projects, state entities are required to:

- Take timely action to ensure that the IPO engagement begins on the project start date and continues through the duration of the project unless other direction is provided by CDT

- Provide timely access to Agency/state entity project, program, and IT management and staff

- Provide timely access to project related information, documents, repositories, tools, and reports

- Provide transparency and access to project related communications, meetings, and activities

- Provide appropriate notice and access to project related meetings

- Provide timely responses and resolution, if applicable, to IPO and IV&V observations and findings

- Provide IPO staff the opportunity to discuss and report IPO related information to project managers/directors, steering committee members, project sponsors, etc.

- Participate in periodic meetings with IPO staff to discuss IPO related information and reports

- Review draft IPO reports and provide feedback on inaccuracies to IPO staff

- Promptly submit requested and required information to CDT and/or IPO staff in accordance with Sam 4819.36

Oversight Focus Areas

Risk Management

CDT has placed a significant emphasis on risk management as a critical function of project oversight. The IPO manager must identify and quantify any issues and risks, and provide notification as appropriate. Furthermore, project managers are expected to establish suitable remediation plans for identified project risks. All projects should formally review risks at least monthly. Risks should be reviewed by a group of individuals representing all components of the project organization to ensure identification of all risks. SIMM Section 17, CA-PMF Risk Management Plan, Section 4.12 contains the *minimum* requirements for risk management, to be implemented on *all* IT projects. See Appendix A for categories and examples of risk in addition to that which is included in the CA-PMF.

Project Management

As part of the oversight process, CDT will evaluate the demonstrated degree to which the Agency/state entity has established project management practices and processes to support successful IT projects. The CA-PMF establishes statewide standards for project management and forms the minimum requirements for IT project management for Agency/state entities required to comply with SAM Section 4800 and 4900 policies. See SAM Section 4910 for project management requirements. These practices and processes will be used to assess and evaluate Agency/state entity performance in project management and define the IT structure and environment components used to assess Agency/state entity project management maturity. The required set of practices and products is tailored to the three categories of project criticality (low, medium, or high).

All project management practices, processes and deliverables must meet the minimum level of planning required in the CA-PMF. The IPO Manager shall use the checklist located in SIMM Section 45I to conduct reviews to ensure compliance. For each item on the template, the IPO Manager will identify the document(s) or other project products that demonstrate performance of the required functions. The IPO Manager will review and assess the identified items for completeness, currency, comprehensiveness, accuracy and any other attributes pertaining to their quality and appropriateness for their intended function. There is a separate template for each level of project criticality (low, medium and high). The template should be employed as a checklist, with the team noting the result of the assessment and the principle sources of input to the assessment process. For any item found to be deficient, the deficiency must be documented separately as a finding within the IPO Manager's written report. Agencies/state entities may require additional oversight reporting, beyond that required by this framework. The documentation of additional information beyond that included in SIMM Section 45G and 45H may be added as a supplemental document to the standard reporting format.

Technical/System Development

Although overall project oversight will be provided by the IPO Manager, Independent Validation and Verification will be used to supplement IPO. The roles of Independent Project Oversight (IPO) differs from Independent Validation and Verification (IV&V). IPO focuses on project management processes and deliverables (i.e. plans, schedules, risks & issues) while IV&V focuses on the technical assessment of the system's development and deliverables to determine if the user requirements, product quality, and specifications are met. Within IV&V, the term verification refers to the process of evaluating software to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase. [IEEE-STD-610]. The term validation refers to the process of evaluating software during or at the end of the development process to determine whether it satisfies specified requirements. [IEEE-STD-610]. Agencies/state entities must comply with the requirements of SAM Section 4940.3 when utilizing IV&V services.

Reporting and Escalation

It is the intent of the CDT to appropriately and efficiently identify, report and escalate project observations, risks, and issues that are believed to present substantial risk to a project which may, if not corrected timely, lead to severe negative consequences to the project outcomes, scope, schedule, or quality. CDT will facilitate the appropriate attention, action, and/or intervention for unresolved project issues and risks that are deemed to be detrimental to a project's success. This includes the following:

1) An unresolved critical project issue or risk that may result in substantial challenge or impact to a reportable project's progress

2) A sudden or impending issue that may trigger potential failure of a reportable project, budgetary/contracting impact, potential illegal activity, and/or external requests for information or reports.

The following reports will be used to identify, report and escalate project observations, risks and issues. Table 2 details the escalation path that CDT staff will use to facilitate the resolution of the aforementioned items. Although this table represents the standard escalation process, the circumstances of a situation may result in levels being appropriately bypassed as determined by the judgement of CDT.

Project Status Report

The Project Status Report (PSR) is designed to report the minimum IT project status information from Team Members, the Project Manager, and/or Project Sponsors to other project participants and interested parties. In addition, the PSR is designed to report the status of reportable IT projects to the Department of Technology based upon the reporting schedule as described in the SIMM Section 05A. The Agency/state entity shall provide reports to the Department of Technology regularly at a frequency depending upon project criticality, see Table 1 for reporting requirements. The Agency/state entity will compile and report results in writing, following the format of the PSR template located in SIMM Sections 45E and 45F.

Table 1: Destination and Frequency of Project Status Report

Project Status Report (PSR)			
Project Criticality	**Low**	**Medium**	**High**
Report to	Department/Agency / CDT	Department/Agency/ CDT	Department/Agency/ CDT
Reporting Frequency	Quarterly	Monthly	Monthly

Independent Project Oversight Report

A project in the traditional sense is considered successful if it is on time, within budget, and within scope (conforms to approved requirements). The deficiencies, issues, findings and recommendations identified throughout the oversight process must be incorporated into the appropriate project management processes (e.g. planning and tracking, risk management, etc.). The Independent Project Oversight Report (IPOR) is used to detail a project's progress against the project objectives,

scope, schedule, and cost defined in the approved Project Approval Lifecycle documents. This report must be completed by the IPO Manager who shall identify and quantify any issues and risks affecting project objectives. The IPO Manager must focus the IPOR on the most critical issues by prioritizing observations, risk, and issues to point out the most significant concerns and present them in plain language. As the project progresses, the IPOR will also track the disposition of the IPO Manager's prior findings, recommendations and identified deficiencies through oversight reporting. In addition to reporting on compliance with the appropriate project management practices, the IPO Manager will report on any other material findings, conclusions and recommendations made as a result of the review and assessment.

The IPO Manager shall provide reports to management regularly at a frequency depending upon project criticality, see Table 2 for reporting requirements. The IPO manager will compile and report results in writing, following the format of the IPOR template located in SIMM Sections 45G and 45H.

Table 2: Destination and Frequency of Independent Project Oversight Reports

Independent Project Oversight Report (IPOR)			
Project Criticality	**Low**	**Medium**	**High**
Report to	Department/Agency / CDT	Department/Agency/ CDT	Department/Agency/ CDT
Reporting Frequency	At Discretion of CDT	Monthly	Monthly

Corrective Action Plan (CAP)

Corrective action can be implemented at any point within the project when the project as a whole, or a specific task or tasks, have taken the project in a direction in conflict with project requirements, objectives and/or deliverables. Early intervention is traditionally more effective as it can involve a more minor and timely correction than later intervention. The Corrective Action Plan (CAP) is an activity initiated for the purpose of altering the course of a task or project that may have lost focus or somehow deviated from the pre-specified direction it was intended to take. This new direction should be well-documented and should, upon execution, turn the task or project in a way such that it better aligns with the goals, expectations, and ultimate results laid out in the Project Approval Lifecycle and/or project management plan.

CDT will leverage the CAP to evaluate the project's planned remediation actions to determine their likelihood of successfully resolving the specified risk or issue. If approved, the CAP provides definitive metrics to allow CDT to monitor the progress of the planned actions. CDT's assessment of the progress against the CAP will be documented in the IPOR. If CDT determines that the project team is not effectively implementing the actions outlined in the CAP, CDT may take action to further escalate the lack of progress and adherence to the CAP. If those escalation efforts fail to correct the specified issues or risks, CDT will then continue escalation activities up to and including suspending or terminating an IT project.

CAP should be considered for (not limited to) the following:

- When other escalation actions or communications have failed to bring about sufficient resolution to an issue or risk.

- When deficiencies are identified with respect to the last approved project approval documents (PAL, SPR), the requirements specified in SAM, SIMM, Project Management Plans, Processes and Procedures, and/or vendor contract.

- When project performance significantly deviates from the last approved project approval documents (PAL, SPR), and the project is trending towards the need for an SPR.

- When established performance measures are not met.

- Identified deviations or deficiencies are serious in nature and show a clear danger to the project's success.

CAP should not be considered for (not limited to) the following:

- As a substitute for normal project management and oversight activities.
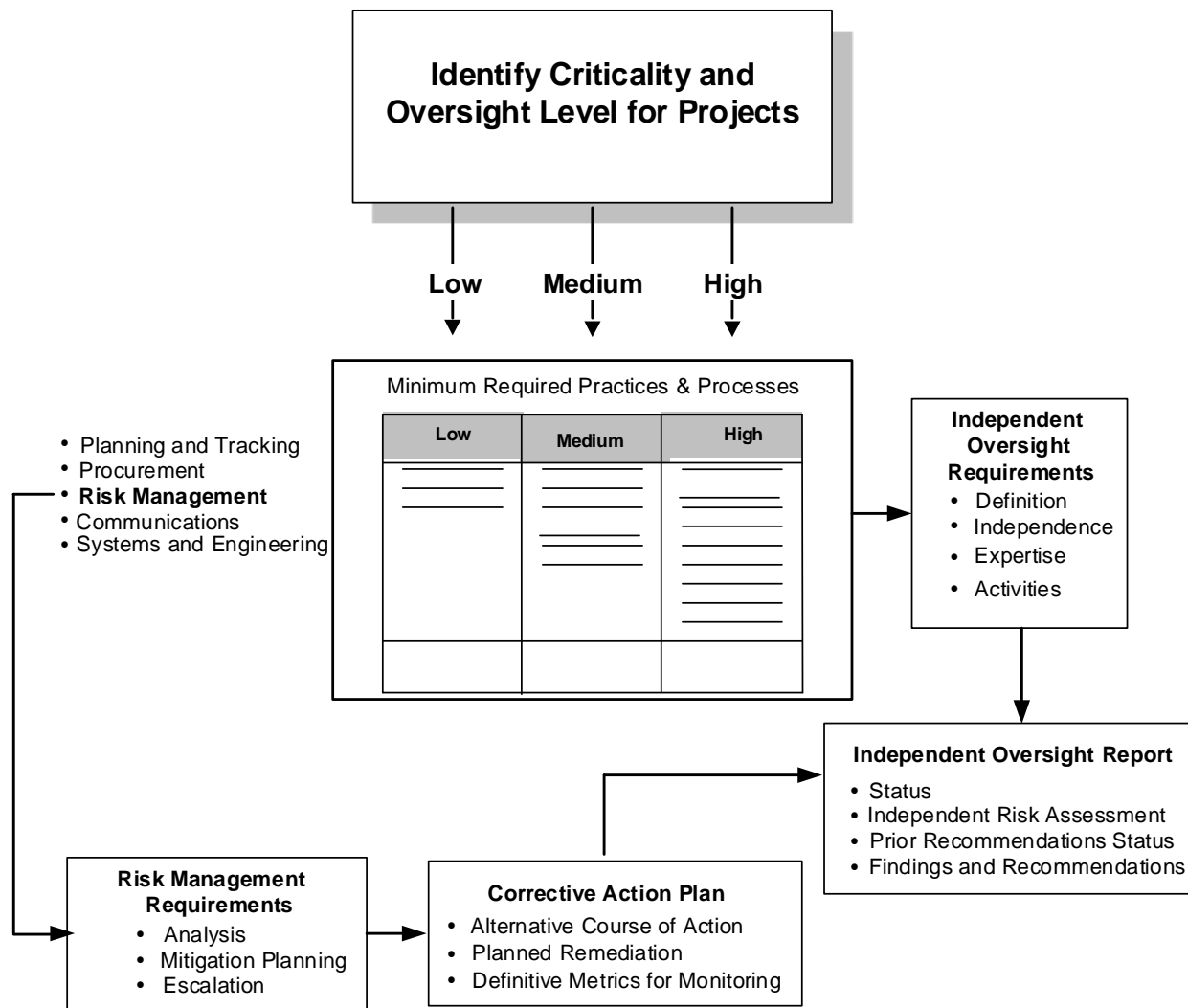
Table 3: Escalation Path

Level	Escalation From:	Escalation To:	Communication Channels	Artifacts or Remediation	Escalation Criteria	Escalation Activities
1	IPO Manager	• Project Manager/ • Director	• Project meetings • Oversight meetings • Independent Project Oversight Report (IPOR) – Statewide Information Management Manual (SIMM) Section 45 Appendix G IPOR Template	• IPOR findings	• Routine project risks/issues	Discuss the project status and critical concerns with Project Manager and/or Director. Document key information in the IPOR.
2	IPO Manager	• Steering Committee • Project Sponsor • CDT Section Manager • CDT Branch Chief • CDT Statewide Technology Procurement (STP) • CDT Office of Information Security (OIS)	• IPOR • Steering Committee reports • CDT project issue escalation (if applicable) • Special Project Report (SPR) – SIMM Section 30 • Escalation Process – Issue Document Template	• IPOR findings • Issue Document • SPR	• Stagnant yellow IPOR focus areas • Yellow IPOR focus areas trending red • Red focus areas • Significant SPR analysis concerns	Discuss any issues or risks requiring escalation with the CDT Section Manager or the Branch Chief. If the Section Manager or Branch Chief concur with the concerns, complete the CDT Escalation Process - Issue Document.
3	CDT Branch Chief	• Project Sponsor • Steering Committee • Agency Chief Information Officer (AIO) • CDT OSPD Chief	• Meetings • Steering Committee reports • CDT Escalation Process – Issue Document Template • Corrective Action Plan	• Delay or deny approval of project documents – Project Approval Lifecycle (PAL) Stage/Gate or SPR • Issue Document	• Stagnant red focus areas • Stagnant SPR approval condition remediation	Escalate the issues or risks with the appropriate parties. Verify the factual basis for the concerns and assess the impact of the issue. Provide written feedback to the IPO Manager if additional information is needed to validate the concern or if a different approach is warranted. Take action to escalate and/or resolve the issue with the project including communicating a firm resolution date to the project, if applicable. Document the action and results in the Issue Document. Determine if

Level	Escalation From:	Escalation To:	Communication Channels	Artifacts or Remediation	Escalation Criteria	Escalation Activities
						remediation action should be implemented by CDT. If the issue remains unresolved, provide the OSPD Deputy Director with the Issue Document and other pertinent information, and schedule a meeting to discuss next steps.
4	CDT OSPD Deputy Director	• Department Director or Chief Deputy Director • Project Sponsor • AIO • California Department of Finance (DOF) • Director, CDT	• Meetings • AIO Portfolio Meeting discussions • CDT Escalation Process – Issue Document • Corrective Action Plan (CAP)	• Delay or suspend procurement activities and/or contract award • Escalation to DOF: o Delay or suspend project funding o Denial of future year project funding • Issue Document	• Continued stagnation • Stagnant CAP resolution	Escalate the issues or risks with the appropriate parties. If applicable, send a letter requiring a CAP. If applicable, identify and implement remediation action(s). Document the escalation actions and results in the Issue Document. If the matter cannot be resolved, escalate to the Directorate.
5	CDT Directorate	• Department Director or Chief Deputy Director • Agency Secretary or Undersecretary • Governor's Office	• Meetings • CDT Escalation Process - Issue Document • CAP	• Suspend or terminate Project	• Continued Stagnation	Escalate the issues or risks with the appropriate parties. If applicable, identify and implement remedial action(s).

Project Oversight Framework Components

The flow diagram illustrates the major components and flows of information involved in implementing the oversight framework described in this document. This diagram identifies the flow of oversight reporting and risk escalation and highlights the role of CDT in administering the oversight framework, assessing Agency/state entity capabilities and individual project criticality, and providing additional oversight to the State's most critical IT projects.

Figure 1: Project Oversight Framework Components

Identify Criticality and Oversight Level for Projects

Low   Medium   High

Minimum Required Practices & Processes

Low	Medium	High

- Planning and Tracking
- Procurement
- **Risk Management**
- Communications
- Systems and Engineering

Independent Oversight Requirements
- Definition
- Independence
- Expertise
- Activities

Independent Oversight Report
- Status
- Independent Risk Assessment
- Prior Recommendations Status
- Findings and Recommendations

Risk Management Requirements
- Analysis
- Mitigation Planning
- Escalation

Corrective Action Plan
- Alternative Course of Action
- Planned Remediation
- Definitive Metrics for Monitoring

Summary of Templates and Instructions

The subsections of SIMM 45 contain the templates briefly described below.

- SIMM 45A & 45B – Project Management Risk Assessment. A tool for independent project oversight to evaluate the maturity of an Agency/state entity's project management capability and its ability to carry out projects.

- SIMM 45C & 45D – Complexity Assessment. Used to determine the level of project oversight needed on a given project, as well as providing guidelines to the qualifications for the Project Manager.

- SIMM 45E & 45F – Project Status Report. Identifies the minimum IT project status reporting information from the Team Member, Project Manager, and/or Project Sponsor to other project participants and interested parties.

- SIMM 45G & 45H – Independent Project Oversight Report. Provides a template and instructions for the written project oversight report format to be submitted by independent oversight providers to departments, Agencies and the Department of Technology.

- SIMM 45I – Project Oversight Checklists. Transforms the practices and processes described in the California Project Management Framework (CA-PMF) into a questionnaire/checklist format for use in independent oversight reviews of project management practices.

Appendix A: Categories and Examples of Risk

Plan/Schedule

Schedule is optimistic, "best case," rather than realistic, "expected case"

Plan omits necessary tasks

Schedule was based on the use of specific team members, but those team members were not available

Cannot build a product of the size specified in the time allocated

Product is larger than estimated (in lines of code, function points, or percentage of previous project's size)

Effort is greater than estimated (per line of code, function point, module, etc.)

Re-estimation in response to schedule slips does not occur, or is overly optimistic or ignores project history

Excessive schedule pressure

A delay in one task causes cascading delays in dependent tasks

Unfamiliar or complex areas of the product take more time than expected to design and implement

Organization and Management

Project lacks an effective top-management sponsor

Layoffs and cutbacks reduce team's capacity

Inefficient team structure reduces productivity

Lack of specific technical expertise

Management review/decision cycle is slower than expected

Budget cuts

Non-technical third-party tasks take longer than expected (control agency approvals, procurement, equipment purchase, legal reviews, etc.)

Project plans are abandoned under pressure

Inaccurate status reporting

Development Environment

Facilities are not available on time

Facilities are available but inadequate (e.g., no phones, network wiring, furniture, office supplies, etc.)

Facilities are crowded, noisy, or disruptive

Development tools are not in place by the desired time

Development tools do not work as expected; developers need time to create workarounds or to switch to new tools

Developers unfamiliar with development tools

Development tools do not provide the planned productivity

Development environment structure, policies, procedures are not clearly defined

User Involvement

User introduces new requirements after agreed upon requirements specification is complete

User finds product to be unsatisfactory

User does not buy into the project and consequently does not provide needed support

User input is not successfully solicited

User review/decision cycles for plans, prototypes, and specifications are slower than expected

User will not participate in review cycles for plans, prototypes, and specifications or is incapable of doing so

User communication time (e.g., time to answer requirements-clarification questions) is slower than expected

User-mandated support tools and environments are incompatible, have poor performance, or have inadequate functionality

User has expectations for development speed that developers cannot meet

Contractor Performance

Contractor does not deliver components when promised

Contractor delivers components of unacceptably low quality, and time must be added to improve quality

Contractor does not provide the level of domain expertise needed

Contractor does not provide the level of technical expertise needed

Requirements Management

Requirements have been base lined but continue to change

Requirements are poorly defined, and further definition expands the scope of the project

Additional requirements are added

Vaguely specified areas of the product are more time-consuming than expected

Product Characteristics

Error-prone modules require more testing, design, and implementation work than expected

Unacceptably low quality requires more testing, design, and implementation work to correct than expected

Development of flawed software functions requires redesign and implementation

Development of flawed user interface results in redesign and implementation

Development of extra software functions that are not required extends the schedule

Meeting product's size or speed constraints requires more time than expected, including time for redesign and re-implementation

Requirements for interfacing with other systems, other complex systems, or other systems that are not under the team's control result in unforeseen design, implementation, and testing

Requirement to operate under multiple operating systems takes longer to satisfy than expected

Development in an unfamiliar or unproved software environment

Development in an unfamiliar or unproved hardware environment

Dependency on a technology that is new or still under development

External Environment

Product depends on law, policy or regulations that change frequently

Multiple stakeholders outside the normal department chain of command

Key software or hardware components become unavailable, unsupported or are unexpectedly scheduled for de-support

Personnel

Acquisition of required project staff takes longer than expected

Task prerequisites (e.g., training, completion of other projects) cannot be completed on time

Poor relationships between project team and users or other stakeholders slow decision making and follow through

Lack of needed specialization (includes technical and domain knowledge) increases defects and rework

Personnel need extra time to learn unfamiliar software tools or environment

Personnel need extra time to learn unfamiliar hardware environment

Personnel need extra time to learn unfamiliar software language

Unplanned turnover of contractor key personnel

Unplanned turnover of State key personnel

New development personnel are added late in the project, and additional training and communications overhead reduces existing team members' effectiveness

Conflicts between team members

Problem team members are not removed from the team

The personnel most qualified to work on the project are not available or are not used

Personnel with critical skills needed for the project cannot be found

Key personnel are available only part time

Not enough personnel are available for the project

People's assignments do not match their strengths

Design and Implementation

Design fails to address major issues

Design requires unnecessary and unproductive implementation overhead

Flawed design

Use of unfamiliar methodology

Necessary functionality cannot be implemented using the selected methods and tools

Schedule savings from productivity enhancing tools are overestimated

Components developed separately cannot be integrated easily

Data conversion activities are underestimated or are ignored

Process

Inaccurate progress tracking

Upstream quality-assurance activities are limited or cut short

Poor quality assurance

Too little formality (lack of adherence to software policies and standards)

Too much formality (bureaucratic adherence to software policies and standards)

Weak risk management fails to detect major project risks

Project management and tracking consumes more resources than expected