

## Risk Assessment

Risk is an undesirable future situation or circumstance that has a realistic likelihood of occurring and an unfavorable consequence should it occur. Risk Management (RM) is the act or practice of controlling risk and determining how risks impact performance, schedule and cost. The purpose of risk management is to identify risks well enough in advance so that appropriate handling plans can be put into place to effectively reduce the likelihood, minimize the impact or accept the consequence of the risk occurring. The RM process provides systematic methods for identifying, analyzing, planning, tracking, controlling, communicating, and documenting risks. The OSI risk management philosophy is to create an open, honest, risk-aware culture in which risk management is considered to be a normal, healthy aspect of sound overall program management

In order to manage and assess risk, OSI utilizes a database management system that stores/retrieves program risk-related data. This *Risk Management Information System* (RMIS) provides data for creating reports and serves as the repository for all current and historical information related to program risk. This information may include risk assessment documents, contract deliverables, if appropriate, and any other risk-related reports. The OSI *Risk Management Coordinator* is responsible for the overall maintenance of the RMIS, and he or his designee are the only persons who may enter data into the database.

*Table 1* below summarizes the typical OSI risk management organizational structure to include responsibilities of program personnel performing RM.

Who	Responsibilities
Individuals / Members	<p data-bbox="524 1228 1357 1297">Engineers, Testers, Logistics Manager, Project Manager, Contractors, and Customers</p> <ul data-bbox="553 1318 1390 1549" style="list-style-type: none"><li data-bbox="553 1318 824 1350">• identify new risks</li><li data-bbox="553 1360 1166 1392">• estimate probability, impact, and time frame</li><li data-bbox="553 1402 764 1434">• classify risks</li><li data-bbox="553 1444 1040 1476">• recommend approach and actions</li><li data-bbox="553 1486 1390 1518">• track risks and mitigation plans (acquire, compile, and report)</li><li data-bbox="553 1528 902 1560">• assist in risk prioritizing</li></ul>

Who	Responsibilities
QA/Test Engineer Manager	<ul style="list-style-type: none"> <li>• integrate risk information from all individuals within the team</li> <li>• ensure accuracy of probability /impact/timeframe estimates and the classification</li> <li>• review recommendations on mitigation approach and action</li> <li>• reprioritize all risks to determine medium and high risks</li> <li>• assign or change responsibility for risks and mitigation plans</li> <li>• report their medium and high risks to the Project Manager</li> <li>• implement control decisions for risks</li> <li>• build action plans (determine approach, define scope, &amp; actions)</li> <li>• collect and report general risk measures/metrics</li> <li>• coordinate communications with Project Manager</li> </ul>
Project Manager & Test Director	<ul style="list-style-type: none"> <li>• authorize expenditures of resources for mitigation</li> <li>• integrate risk information from all team members</li> <li>• reprioritize all risks to determine the medium and high project risks</li> <li>• make control decisions (analyze, decide, execute) for medium and high project risks</li> <li>• assign or change responsibility for risks and mitigation plans within the project</li> <li>• coordinate communication with Sr. Managers and external customers</li> </ul>

**Table 1 - Responsibilities of Risk Management Personnel**

### Risk Management Elements

The OSI RM process includes these six primary activities:

- **Risk Identification:** continuous efforts to capture, acknowledge, and document risks as they are found. These can be any issue that potentially impacts program success, performance, cost, or schedule. Typical considerations include system integration or installation, system performance, technical parameters, production planning/schedule, and cost.
- **Risk Analysis:** an evaluation of all identified risks to estimate the probability of occurrence, severity of impact, timeframe of expected occurrence or when mitigation actions are needed, classification into sets of related risks, and priority ranking (i.e., low, medium, and high).
- **Risk Mitigation Planning:** establishes actions, plans, and approaches for addressing medium and high priority ranked risks and assigns responsibilities and schedules for completion. Metrics for determining the risk status are also defined during this step.

- **Risk Tracking:** an activity to capture, compile, and report risk attributes and metrics which determine whether or not risks are being mitigated effectively and risk mitigation plans are being performed correctly.
- **Risk Controlling:** an activity that utilizes the status and tracking information to make a decision about a risk or risk mitigation effort. A risk may be closed or watched, a mitigation action may be re-planned, or a contingency plan may be invoked. Decisions on the appropriate resources needed are also determined during this activity.
- **Risk Communicating and Documenting:** an overt action to communicate and document the risk at all steps of the RM process. This can be in the form of an action item log, risk information sheet, risk database, mitigation plan, program status reports, tracking log, and/or meeting decision such as Program Management Reviews (PMRs).

### **Risk Management Information System (RMIS)**

The OSI Risk Management Information System (RMIS) provides the means to enter and access data, control access, and create reports. The following are examples of basic reports that may be used to manage its risk program:

- Risk Information Form
- Risk Action Report
- Risk Tracking Documentation
- Risk Monitoring Documentation

If functional managers need additional reports, they work with the Risk Management Coordinator to create them. Access to the reporting system is controlled.

Key to the RMIS is data elements that reside in the database. Listed below (*Table 2 - RMIS DBMS Elements*) are the types of risk information that are typically included in the database. "Element" is the title of the database field; "Description" is a summary of the field contents. The Risk Management Coordinator will create the standard reports such as, the RIF, Risk Monitoring, etc. The RMIS also has the ability to create "ad hoc" reports, which can be designed by users and the Risk Management Coordinator.

Element	Description
Risk Identification (ID) Number	Identifies the risk and is a critical element of information, assuming that a relational database will be used by the PMO. (Construct the ID number to identify the organization responsible for oversight.)
Risk Event	States the risk event and identifies it with a descriptive name. The statement and risk identification number will always be associated in any report.
Priority	Reflects the importance of this risk priority assigned by the PMO compared to all other risks, e.g., a one indicates the highest priority.
Date Submitted	Gives the date that the RIF was submitted.
Major System/Component	Identifies the major system/component based on the Work Breakdown Structure (WBS).
Subsystem/Functional Area	Identifies the pertinent subsystem or component based on the WBS.
Category	Identifies the risk as technical/performance cost or schedule or combination of these.
Statement of Risk	Gives a concise statement (one or two sentences) of the risk.
Description of Risk	Briefly describes the risk; lists the key processes that are involved in the design, development, and production of the particular system or subsystem. If technical/performance, include how it is manifested (e.g., design and engineering, manufacturing, etc).
Key Parameters	Identifies the key parameter, minimum acceptable value, and goal value, if appropriate. Identifies associated subsystem values required to meet the minimum acceptable value and describes the principal events planned to demonstrate that the minimum value has been met.
Assessment	States if an assessment has been done. Cites the Risk Assessment Report (see next paragraph), if appropriate.
Analysis	Briefly describes the analysis done to assess the risk; includes rationale and basis for results
Process Variance	States the variance of critical technical processes from known standards or best practices, based on definitions in the program's RM plan.

Element	Description
Probability of Occurrence	States the likelihood of the event occurring, based on definitions in the program's risk-management plan.
Consequence	States the consequence of the event, if it occurs, based on definitions in the program's risk-management plan.
Time Sensitivity	Estimates the relative urgency for implement the risk-handling option.
Other Affected Areas	If appropriate, identifies any other subsystem or process that this risk affects.
Risk Handling Plans	Briefly describes plans to mitigate the risk. Refers to any detailed plans that may exist, if appropriate.
Risk Monitoring Activity	Measurement and metrics for tracking progress in implementing risk-handling plans and achieving planned results for risk reduction.
Status	Briefly reports the status of the risk-handling activities and outcomes relevant to any risk-handling milestones.
Status Date	Lists date of the status report.
Assignment	Lists individual assigned responsibility for mitigation activities.
Reported By	Records name and phone number of individual who reported the risk.

**Table 2 - RMIS DBMS Elements**