CONTENT OF THE RISK MANAGEMENT STORYBOARD

1. Risk Management Concepts & Philosophies

1.1. What is "RISK"?

An undesirable situation or circumstance that has both a likelihood of occurring and a potentially negative consequence. This is illustrated in Figure1. In the figure, *screens* refer to actions to reduce risks and *escapes* refer to nonconformities that result from risks.

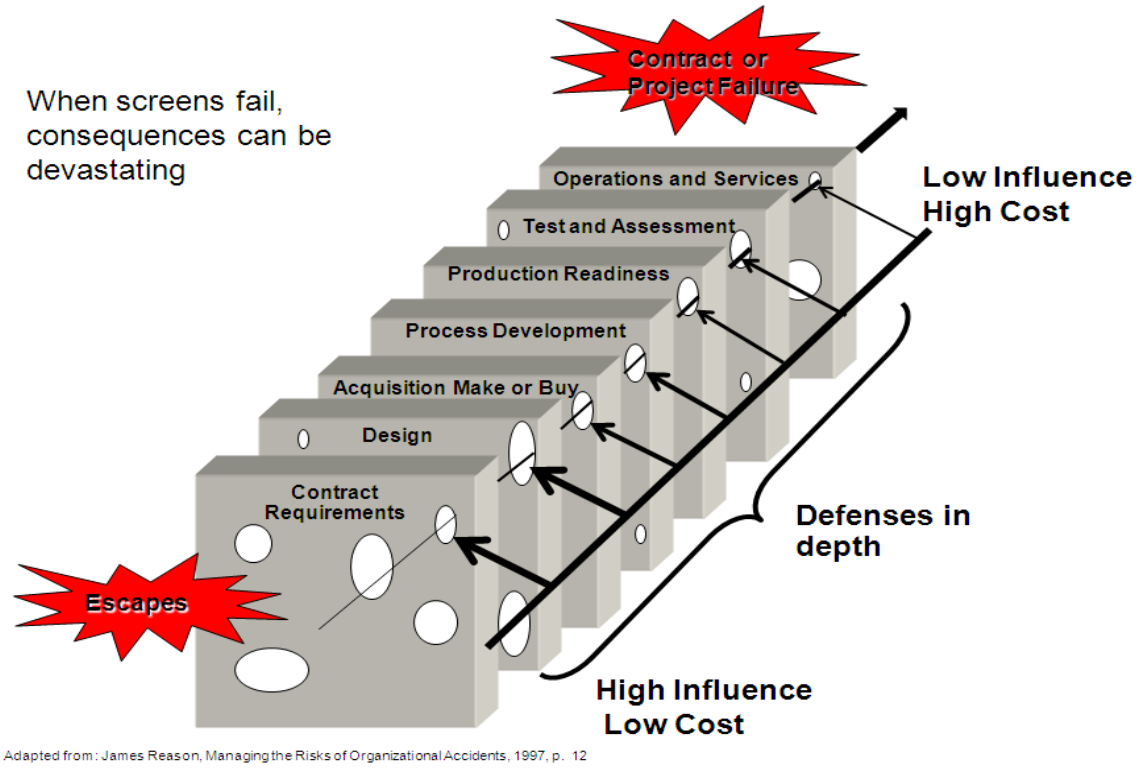


Figure 1 Risks and Their Affects on a Project / Program

Figure 1 above shows possible risks at each phase of a project / program. The holes in each slice (program step) represent a possible risk at this level. If risks are not mitigated (holes closed) there might exist a possibility for an cumulative impact on the program success (the aligned holes and a line passing through). Therefore, each organization should review each contract requirement and identify where risk of non-compliance is. A risk focal for the project should review identified risks and ensure that management is aware of each contract requirement that introduces risk in multiple areas of a project.

1.2. What is "Risk Management"?

An iterative process to identify, assess, reduce, accept, and control risks in a systematic, proactive, comprehensive and cost effective manner, taking into account the *business*, costs, technical, quality and schedule programmatic constraints. This is illustrated in Figure 2.

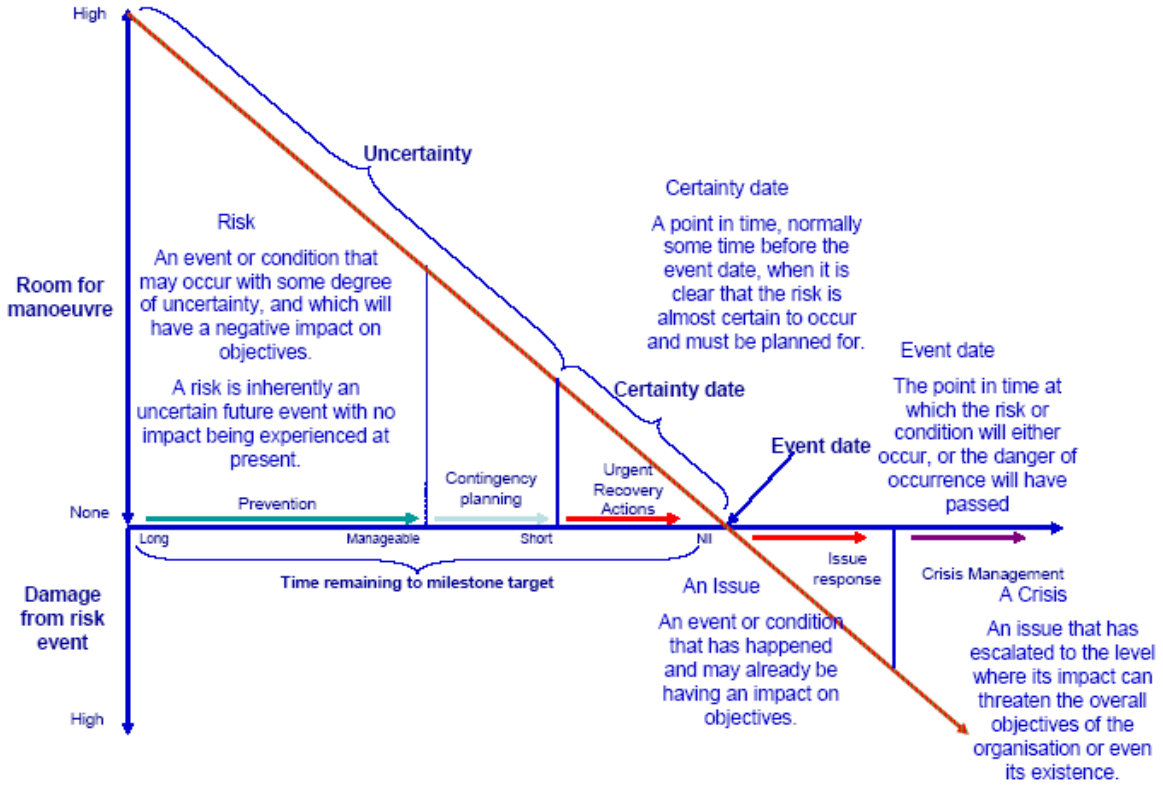


Figure 2 Risk Management Concepts

1.3. Why do we want risk management?

To reduce the chances of something harmful happening to the business. This involves a focus on the risks to meeting customer requirements, and preventing product non conformance escapes. The absence of a Risk Management program can result in known, unknown, and unknowable / unforeseen problems for the Customer and Stakeholders concerning the cost, schedule, and technical performance of programs and concerning the quality and on-delivery performance of products and services.

Risk Management & Balanced Trade Offs

Risks are present in all activities. The impact and likelihood of occurrence varies with each risk. There is a cost, schedule and technical impact to managing each risk. Therefore, risk management is a balance of application of the correct risk management approaches to a risk, dependent on the impact of that risk. This is illustrated in Figure 3.

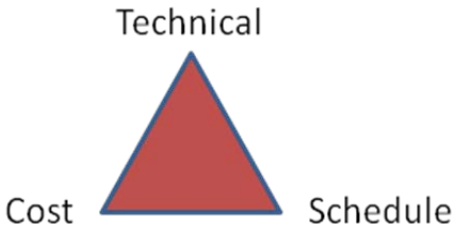


Figure 3 Cost, Schedule, and Technical Trade-offs in Risk Management

Process benefits of 'organizational management of risk':

- Increase the likelihood of achieving objectives;
- Encourage proactive management;
- Be aware of the need to identify and treat risk throughout the organization;
- Improve the identification of threats;
- Comply with relevant legal and regulatory requirements and international norms;
- Improve financial reporting and governance;
- Improve stakeholder confidence and trust;
- Establish a reliable basis for decision making and planning;
- Improve organizational controls;
- Effectively allocate and use resources for risk treatment / handling;
- Improve operational effectiveness and efficiency;
- Cost of risk management is typically less than the cost of issue management;
- Enhance health and safety performance, as well as environmental protection;
- Minimize losses and improve loss prevention and incident management; and
- Improve organizational learning and resilience.

Product, service and mission benefits of the 'organizational management of risk':

- Reduce the likelihood of delivering nonconforming product / services to customers
- Reduce the likelihood of delivering late product / services to customers
- Increase likelihood of business success
  - Increase likelihood of meeting schedules
  - Increase likelihood of meeting budgets The preserve the ability to make sound decisions based on potential conditions
- Reduce the probability & consequences of mission failure
- Reduce the probability of injury or death due to product / services failure

1.4. What does a "Risk Management Program" do?

- Describes the organization's attitude and approach towards risks, how it conducts risk management, the risks it is prepared to accept and how it plans on dealing with those it chooses not to accept and defines the main requirements for a risk management plan. A Risk Management Program:
  - Helps organization to identify risks
  - Helps organization to reduce occurrences and impacts of risks
  - Helps organization to understand significance / severity of risks

  - Promotes organizational behaviours focused on risk management
  - Increases effectiveness of product delivery to customer
  - Creates a process for who, what, when, where, how and how much
  - Helps to maintain information on historic issues
  - Helps capitalize on historic issues to prevent future issues (apply lessons learned)
  - Helps organization bring out hidden risk knowledge so it can be managed

- Risk management should encompass all the areas of business performance, and should be exerted at all levels of an organization.
- Risk management is a warranty of achieving the program's objectives, based on the investigation of all unforeseen contingencies that may affect the smooth running of a program, in compliance with the quality, cost, technical and deadline commitments.
- Risk management shall deal with possible, future events; it should not be mistaken for management a current problems / issues Risk management shall be capable, if applicable, to propose arrangements with a view to anticipation and provision of alternative solutions.
- Risk management shall be carried out methodically, in accordance with the process summarized below and detailed further on in this document:
  - Formalizing of objectives,
  - Identification and assessment of the risks,
  - Definition, valuation and acceptance of the risk mitigation plans,
  - Monitoring of the progress of execution of risk mitigation plans and analysis of their effectiveness,
  - Detection and integration of new risks into the risk management process,
  - Capitalization on the corresponding experience (lessons learned).
- The management framework providing:
  - The foundations and arrangements that will embed risk management throughout the organization at all levels.
  - Risk management policy
    - Statement of the overall intentions and direction of an organization related to risk management
  - Risk communication
  - Risk management process (implementation)
    - Systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, monitoring and reviewing risk

Risk management continuous improvement cycle

This cycle provides the framework of continuous improvement in the organization as shown in Figure 4 below.

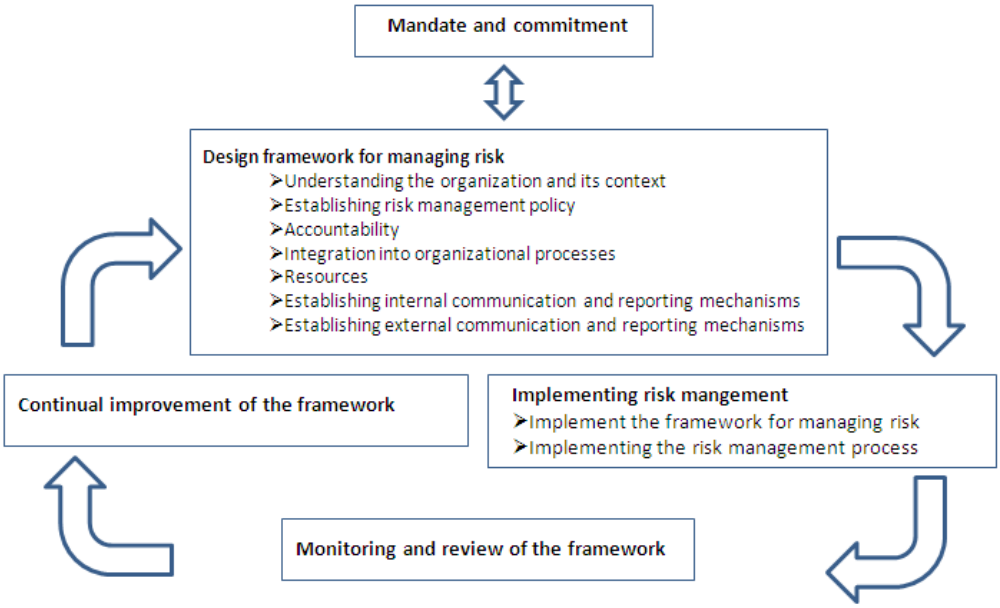


Figure 4 Continuous Risk Management Improvement Cycle

1.5. Risk Management and the 9100 Quality Standard

Risk management is a requirement of the 9100 quality standard:

General:
The standard requires a quality management system that takes into account the identification of various risks related to the circumstances of the organization in regard to its needs, particular objectives, product range, applied processes and the size of the organization.

3.2 Special Requirements (as illustrated in Figure 5)
Those requirements identified by the customer, or determined by the organization, which have high risks to being achieved, thus requiring their inclusion in the risk management process. Factors used in the determination of special requirements include product or process complexity, past experience and product or process maturity. Examples of special requirements include performance requirements imposed by the customer that are at the limit of the industry's capability, or requirements determined by the organization to be at the limit of its technical or process capabilities.

3.3 Critical Items (as illustrated in Figure 5)
A risk management has to be implemented to control of critical items such as: Safety critical items, fracture critical items, mission critical items etc. That means for all items which have a significant effect on the product realization and use of the product throughout the product life.

3.4 (& 7.2.1, 7.2.2, 7.3.3) Key characteristic: (as illustrated in Figure 5)
Is an attribute or feature which may creates a risks to product fit, form, function, performance, service life or produce ability and requires specific actions for controlling variation.

7.1.1 Risk Management while doing Project Management:
The organization shall plan and manage product realization in a structured and controlled manner to meet requirements at acceptable risk, within resource and schedule constraints.

7.1.2 Risk Management:
The organization shall establish, implement and maintain a process for managing risk to the achievement of applicable requirements, as appropriate to the organization and the product:
a) Assignment of responsibilities for risk management,
b) Definition of risk criteria (e.g., likelihood, consequences, risk acceptance),
c) Identification, assessment and communication of risks throughout product realization,
d) Identification, implementation and management of actions to mitigate risks that exceed the defined risk acceptance criteria, and
e) Acceptance of risks remaining after implementation of mitigating actions.

7.2.2 Product risk:
The organization has to ensure that risks have been identified such as:
e.g. new technology, short delivery time frame, resources, change in source of supply (Further examples see 7.1.2)

7.4.1 Supply chain risk:
The organization has to manage the risk when selecting and using suppliers.

8.5.3 Preventive actions:
The organization must establish preventive actions including risk management like: error proofing, failure mode and effect analysis and product problems by external sources.

Note: When viewing the wording of the 9100, 2009 standard, be aware of wording such as 'as appropriate', 'complexity' and other wording that provides the organization for options. Applying the concepts of Risk may have an influence as to the options that an organization implements.

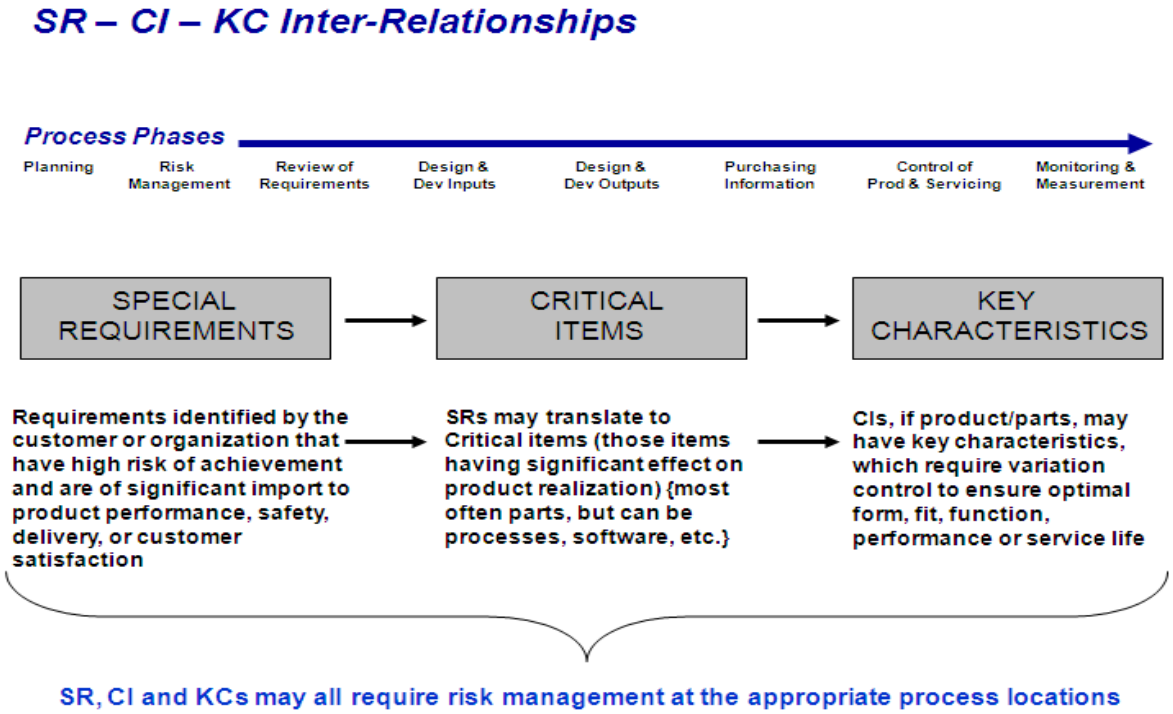


Figure 5 Relationships of Special Requirements, Critical Items and Key Characteristics

2. Processes

2.1. What are the elements of a "Risk Management Process"?

Within the risk management process, available risk information is produced and structured, facilitating risk communication and management decision-making. The results of risk assessment and reduction and the residual risks are communicated for information and follow up (Illustrated in Figure 6).

Management components typically include policies, procedures, practices, assignment of responsibilities, and sequence and timing of activities.

The risk management plan can be applied to a particular product, process, project, or program, and it may include part or all of the organization.

Risk Management Process

Figure 6 Risk Management Process

Risk Management Process

- Formalize the objectives & policies (Risk Management Plan)

Risk Identification

- Identify impacted Stakeholders
- Apply Risk Questioning in the organization's decision-making
- Verify completeness of identified risks of impacted Stakeholders
- Develop risk identification strategy (what risk areas and how to identify risks in each area – documented criteria).
- Identify (using risk ID checklists) and document risks (using standard form).

Risk Assessment

- Analyzing risks (determine likelihood, consequence, urgency, and customer priorities and preferences and determine risk handling priorities).
- Assessing risk handling options (avoid, transfer, assume, mitigate
- Tradeoffs are made among different, and often competing cost, schedule, technical, and quality goals
- Decisions on what to do, how much do, when to do, and what not to do
- Decisions on who will take mitigation actions and what actions will be applied

Risk Action Management

- Identification of owners/stakeholders of the risks
- Definition of Risk Handling Actions / Plans
- Record risk information in Risk Register
- Prioritization, Mitigation, Acceptance of the risks
- Planning and performing risk actions (what, who, when, where, how, how much)

Risk Management Tools

- Undesired events are assessed for their severity and likelihood of occurrence
- Classification of the likelihood of occurrence and severity (low, moderate, or high)
- Assessments of the alternatives for mitigating the risks are iterated

Risk Reporting & Monitoring

- Risk management reporting and communication
- Taking Additional Actions Based on Results of Initial Risk Mitigation Efforts
- Recoding Historical Issues and Lessons Learned (and using them).
- Communicating and tracking risks.
    - It is recommended that these elements be addressed in this writing but they certainly may be expressed with different words

2.2. How do the elements relate to a management system?

(Process Identification / Assess / Communicate, risk mitigation behaviour etc.)

Risk management Policy:
Multiple processes in the organization are potentially subject to risk and are to be determined.

Risk identification:
Risk identification has to be performed by a multi functional team representing all affected functions of the organization.
Risk identification should be a continuous process during the different process control points (refer to examples in section 3 figure 1). Risk identification processes are included in the organization's decision-making process. Risk managers guarantee the continuous communication flow regarding to the evolution of risks status.

Risk assessment:
Risks are assessed via methods and tools in likelihood and severity. Based on the results of the analysis the severity will be determined and appropriate decisions and actions are taken to ensure that risks are properly managed.

Risk action management:
Incorporate risk management actions into the organization workflow to ensure that risks are properly identified, assigned and communicated to affected to personal and or organizations. Priorisation and allocation of resources are planned and executed to ensure that risks are mitigated or resolved.
Record responsible organization, department and name, planned action item completion date, and objective evidence of completion that will be observed. Planned completion dates should be based on the prioritization of risks and available resources. Maintain status of action items until the actions are complete. Verify that objective evidence of completion of the actions exist, monitor effectiveness of implemented risk actions, and if ineffective, define and execute new actions.

Risk Reporting & Monitoring:
Organizations should develop a method to communicate status of identified risk to personnel and management.
Capture information on risks and effective risk actions from the risk management processes and utilize it as part of the organization's preventive action / lessons learned processes. Information from the organization's problems / issues and opportunities, should also be included in it's lessons learned implementation process.

2.3. Risk Measurement & Monitoring

The organization should establish methods and frequencies at which the Risk Levels are evaluated / measured against the Acceptable Risk Levels identified for each process or risk area in the scope of the Risk Management Plan. As a minimum, critical processes or risk areas within the organization or Company should always be evaluated / measured. The frequency at which the Risk Level is measured should be proportional to the consequences that would be incurred if the Risk Level for the identified process goes beyond acceptable limits.

2.4. Risk Controls

The organization should incorporate, in the identified processes or risk areas; established Check points that ensure the identified levels of Acceptable Risk are not exceeded. These Check points should be strategically selected in order to allow the application of mitigation actions to bring the Risk back to the Acceptable Level. The Check points should be established as Preventative Actions not Corrective Actions.

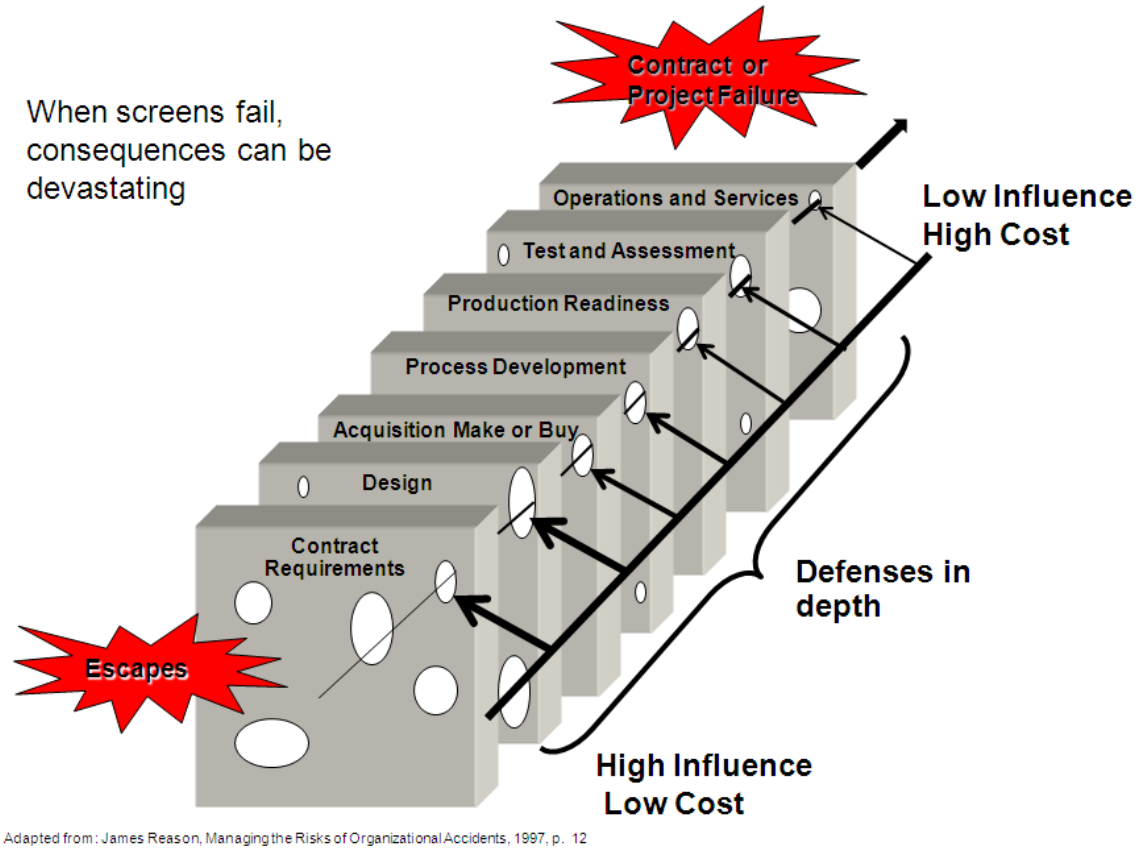
3. Examples

3.1. For Risk Types please refer to the Glossary section 5

3.2. Examples of "Risks" within Risk Types and Risk Controls:

- **Known Risks**: Commonly associated with changes to established processes where the consequences can be reasonably foreseen.
- **Unknown Risks:** Commonly associated with the start-up of new process where the consequence cannot be easily foreseen.
- **Unknowable / Unforeseen Risks:** Commonly associated with ventures in the development of new technologies, business opportunities, markets, business relationships, sectors, etc.

Referring to Figure 1 at the beginning of section 1.1, it shows holes depicting possible risks at each phase of a project / program, and that when screens fail, consequences can be devastating to a project or program. In the figure, *screens* refer to actions to reduce risks and *escapes* refer to nonconformities that result from risks. The holes in each slice (program step) represent a possible risk.



Ref .Figure 1 Risks and Their Affects on a Project / Program

The following figures define the possibilities / examples for risks (holes) at each stage/level of the program and their possible sources.

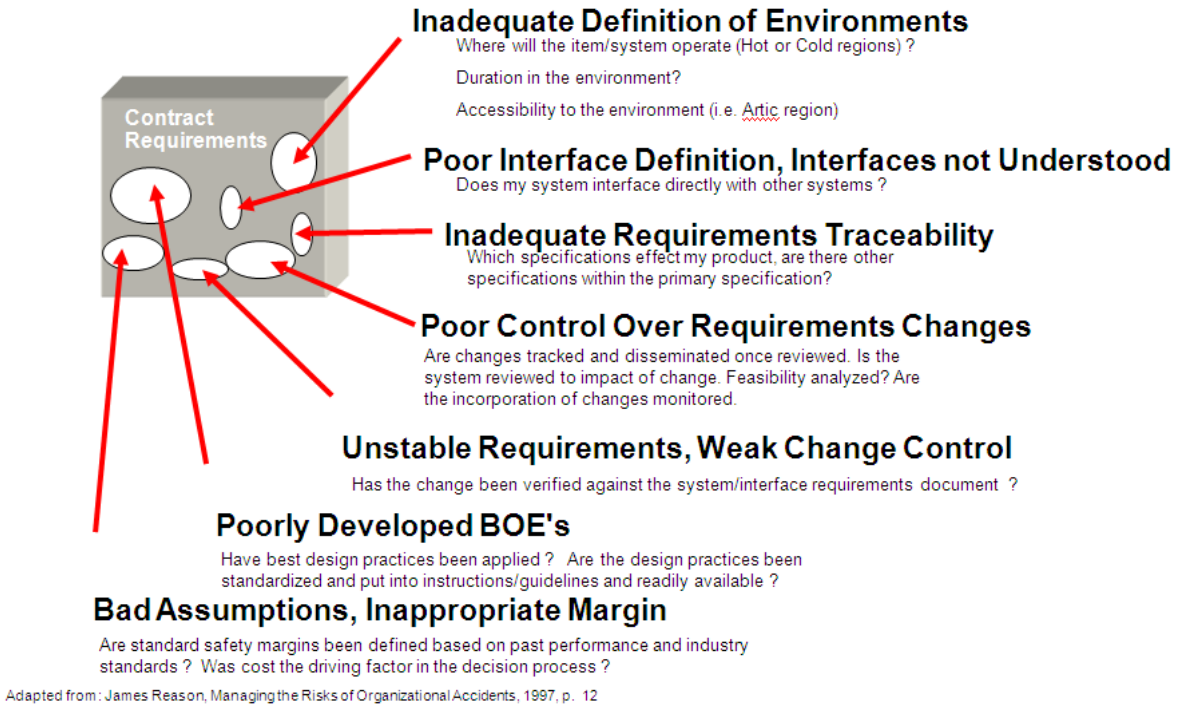
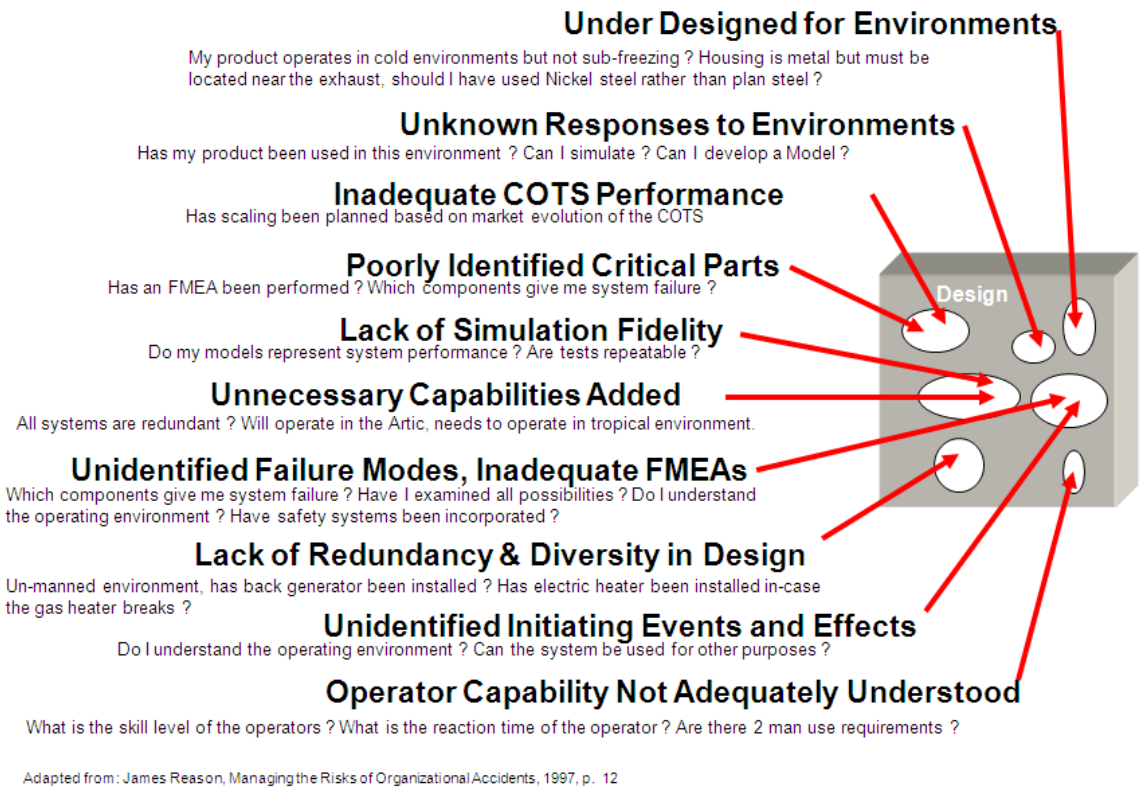
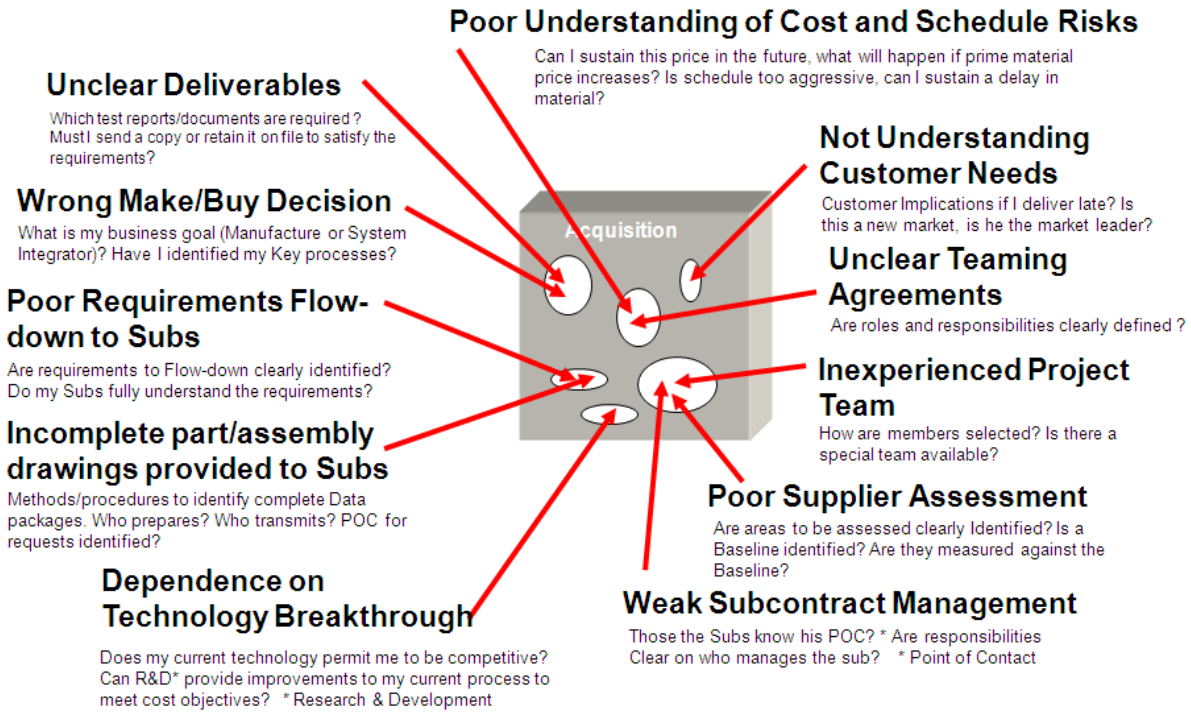


Figure 7 Contract Requirements Risks



Adapted from: James Reason, Managing the Risks of Organizational Accidents, 1997, p. 12

Figure 8 Design Risks



Adapted from: James Reason, Managing the Risks of Organizational Accidents, 1997, p. 12

Figure 9 Acquisition Risks

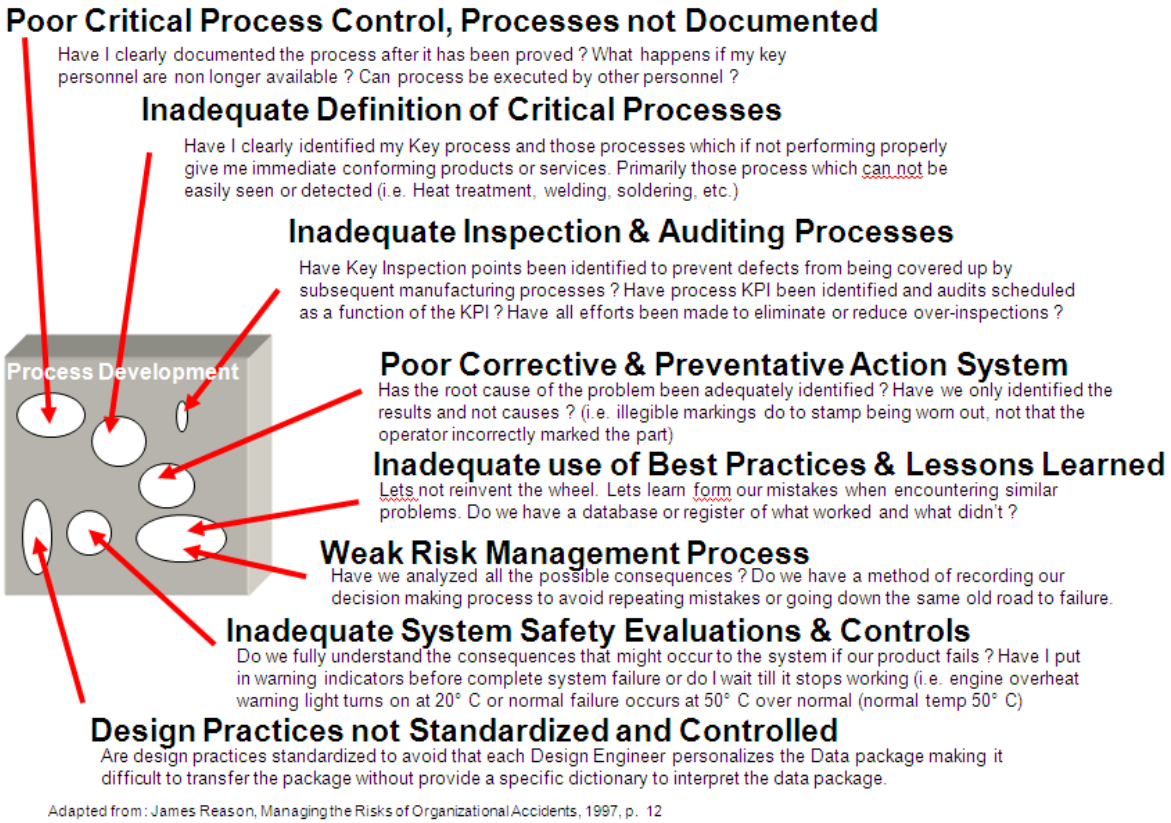


Figure 10 Process Risks

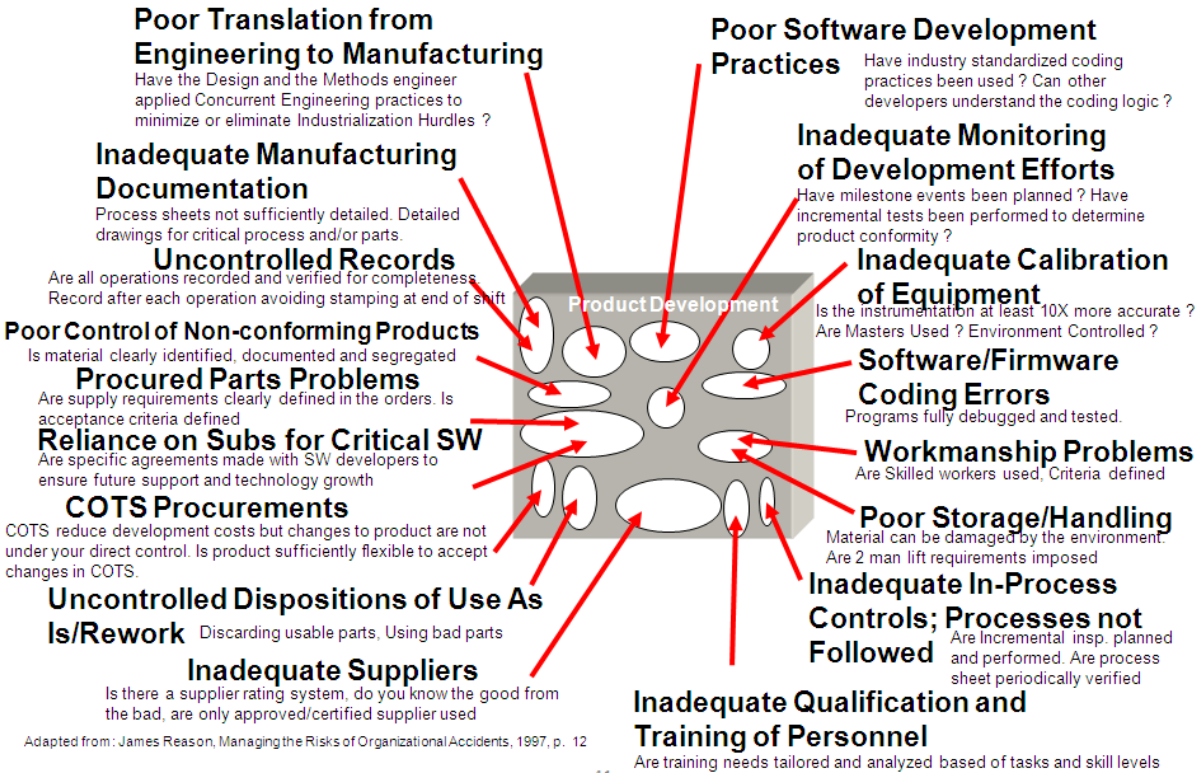


Figure 11 Product Development Risks

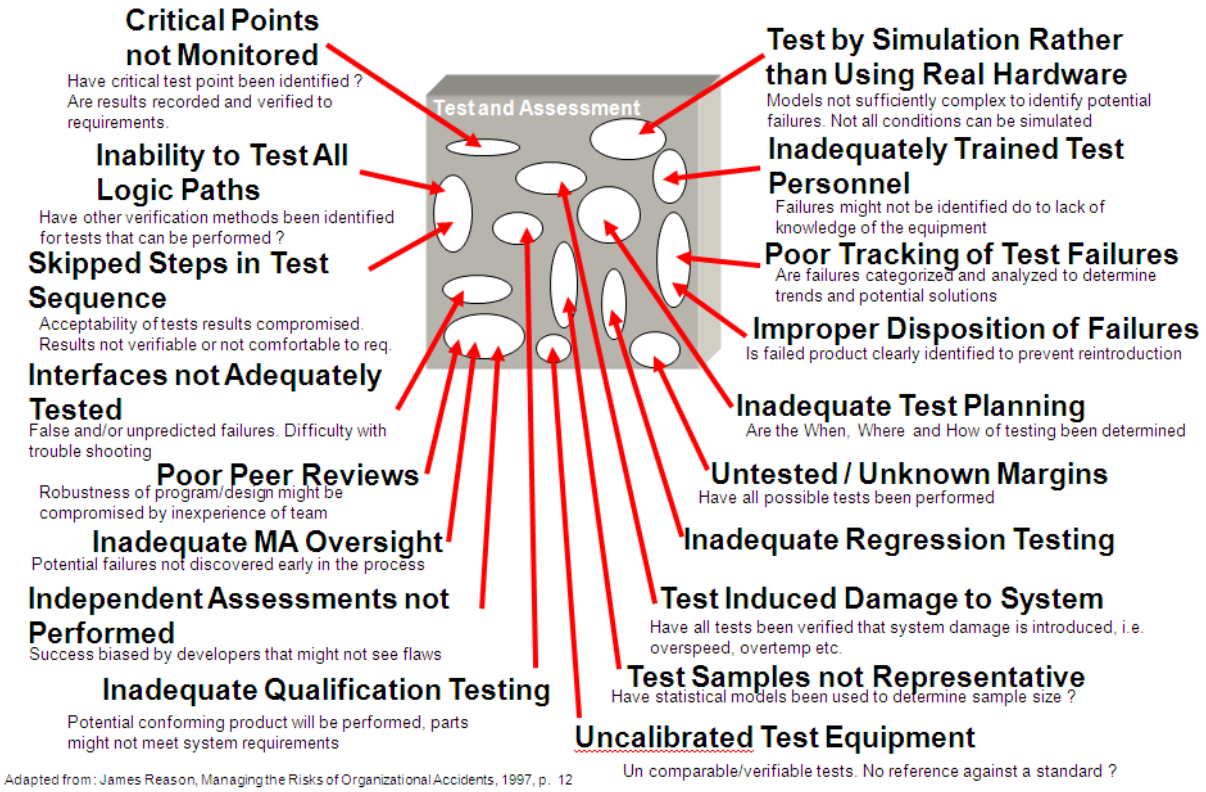


Figure 12 Example Test and Assessment Risks

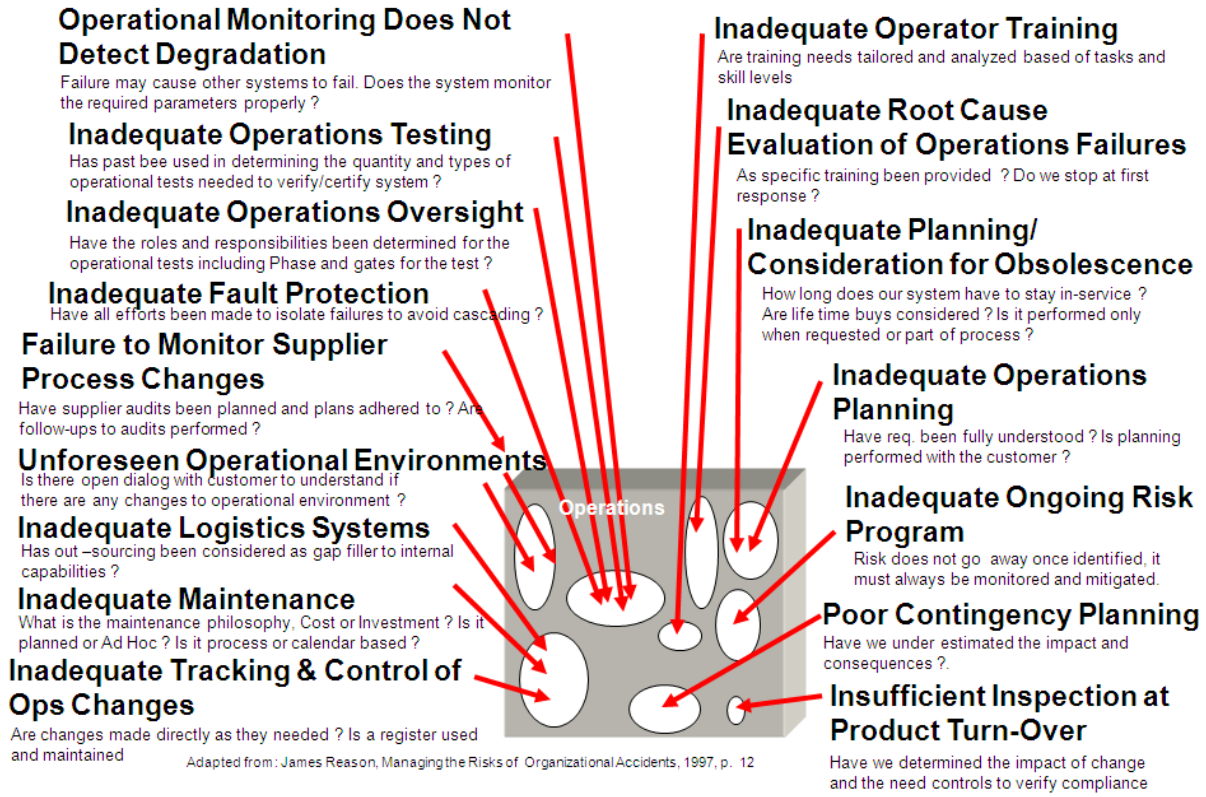


Figure 13 Operations Risks

4 Annex

4.1 Risk Management Tools

The tools in section 4 facilitate the risk management process described in sections 1 – 3.

4.1 Risk Identification

Tables 1 and 2 below are examples of documented risk identification criteria that may be used to identify risks. Risk identification criteria should always be documented in order to have a thorough, systematic, and repeatable identification of risks. See also section 3.2.

Supplier risk tables for guidance

See Table 1.

Table 1 — Supplier risk tables for guidance

Risk factors	Element for assessment	Risk identification tools	Risk reduction control tools
Quality	▪ Quality System Approvals/certification - Aerospace (EN 9100 series, regulatory authority requirements etc.) - Non Aerospace Customer ▪ Special processes approval/certification (customers, NADCAP, etc.) ▪ Previous supplier experiences on similar products to be identified ▪ Current Aerospace Customers references ▪ Contract review process ▪ Quality performance indicators (e.g. scrap, concession rate, quality system scoring result, Customers audit results, etc.)	▪ Checklists covering elements to assess risk e.g. : - Quality System assessment per EN 9101 with scoring results - Supplemental checklist for other elements	▪ Continuous Improvement plan agreed by suppliers with suppliers mandatory indicators and corrective action request ▪ Quality Assurance Plan ▪ Specific training on identified weaknesses and specific requirements ▪ Selection of relevant parts ▪ Increased products receiving inspection ▪ Identify frozen process parameters ▪ Assistance on site (including people on site for a limited time) ▪ Mandatory FAI per EN 9102 ▪ Management of process variation (SPC) ▪ Unscheduled requirements delivery versus MRP ▪ Dual source ▪ Buffer stock
Environment safety	▪ ISO 14001 certification ▪ Hazardous products involved ▪ Safety plant classification (if any) ▪ Accident rating in the past years with trend ▪ Safety policy (e.g. equipment availability, fire escape) ▪ Training for health & safety	▪ Specific checklist depending of nature of supply ▪ Analysis of safety rules/controls implemented by supplier ▪ Supplier action plan overview	▪ Mitigation plan ▪ Dual source ▪ Buffer Stock
Work environment	▪ EN 9100 requirements (subclause 6.4)	▪ Specific checklist depending on nature of supply ▪ Quality system assessment per EN 9101	▪ Preventive and/or corrective action plan ▪ Part/process specific work environment plan

continued

Table 2 — Product risk tables for guidance

Risk factors	Element for assessment	Risk identification tools	Risk reduction control tools
Safety Classification	▪ Safety classification ProcessClassified part manufacturingControl of classified parts to Customers requirements ▪ Customer approval status (e.g. agreement to manufacture certain parts classification)	▪ Checklist for Process assessment	▪ Improvement of safety classification process ▪ Recovery planLife Limited ▪ Overhaul inspection ▪ Retrofit ▪ Classification planLimitation for procurement
Special Process Involvement	▪ Each special process ▪ Employee skills, experience and certification ▪ Documentation for special processes, including qualification file ▪ Evidence of control parameters ▪ Equipment ▪ Special Process approval documentation issued by other customers (e.g. certificate, report)	▪ Checklist covering all elements to be assessed including review of approval files ▪ Key process indicators	▪ Training ▪ On site assistance ▪ Limitation for procurement ▪ Recovery plan ▪ Quality inspection plan ▪ Statistical Process Control ▪ Frozen process parameters
Design Complexity	▪ Design & Development Plan ▪ Technologies involved ▪ Material selection/resources ▪ Design maturity level ▪ Previous experience ▪ Number of Sub-components ▪ Similarity of existing designed product ▪ Feasibility to manufacture the design	▪ Design process audit ▪ FMEA (Failure Modes and Effect Analysis) ▪ Lesson learned ▪ Design of Experiments ▪ Review of current development plan ▪ Tolerance analysis	▪ Updated Design and Development plan including tests ▪ Concurrent engineering ▪ Requirements review with Customer ▪ Technology to be adopted ▪ Performances required including cost & timeframeDesign for six sigma

4.2 Risk Register

A risk register should be used to record known information about each risk. Figure 14 provides an example format and content. This information should be stored electronically with multiple backup copies.

RISK REGISTER

A				B		C			D			
Supplier _____ Site _____				Recovery Indicator _____		Product/Service-Supplier Criticality RAG			Supply Manager _____			
E	F	G		H	I	J	K	L	M	N	O	P
Risk Item No.	Risk Title	Risk Description		Risk Impact	Risk Prob'ty	Risk Criticality	Risk RAG	Date Raised	Risk Owner	Action Plan	Plan Status	Status RAG
		Cause	Impact									

Figure 14 Risk Register

Risk Register Field Descriptions

Field A - Supplier/Site

Record here the company name of the supplier and the site at which the risk applies (important where the supplier operates at more than one location).

Field B - Supply Recovery Indicator

This field captures an indicator indicating the time that it would take to reinstate that supply-product / service if the supplier failed to maintain production. The indicator given in the table below shows the total impact in terms of time that it would take to recover a supply (with a new supplier), that a total supply failure would cause.

Factors to be considered in determining the Recovery indicator for a supply are:

- Is the current supplier the sole source used for such equipment / materials?
- Is the current supplier the only possible source of such equipment / materials?
- Does the current supplier own the design and/or patent for this equipment / material (would design / development be necessary for an alternative source)?
- Is the current supplier the owner of the technology (would redesign / development be necessary for an alternative technology)?
- Does the current supplier own the tooling (would there be a tool-manufacturing programme necessary for an alternative supplier)?
- Are there other potential suppliers available with:
    - Design capabilities.
    - Quality approval.
    - Adequate manufacturing capacity?
- Is there a worldwide shortage of the raw materials?

Field C - Product/Supplier Criticality RAG (Red Amber Green)

Record here the colour and level of the Product/Supplier Criticality. For example: green may indicate low risk, amber, moderate risk, red, high risk, and purple, very high risk.

Field D - Supply Manager

Record here the name of the person (the Buyer or Vendor Controller) that is responsible, on a day to day basis, for placing orders on and managing the supply through this supplier. This person will be responsible for updating and status reporting.

Field E - Risk Number

This is a unique series of characters that will identify each particular risk.

Field F - Risk Title

The title should indicate the type or area of the risk in a few words.

Field G - Risk Description

For the purposes of full understanding it is important that in describing a risk both cause and impact statements are made. For that reason the field is in two parts. As an example:
{For an observation that a supplier manufacturing facility lacks adequate maintenance:
Risk Title:
- *Lack of Maintenance.*

Risk description:
- *Cause: A lack of planned maintenance in manufacturing facility.*
- *Impact: Production machinery failure resulting in a disrupted product supply where repairs to key machinery could take up to three weeks}*

Field H - Risk Impact

A subjective factor for impact is to be used as a basis of comparing the effects on supply a risk will have compared with others. A figure 1, 2, 3 or 4, representing low, medium, high or very high levels of impact, are to be entered in this field. Where necessary these factors can be quantified for an exact ranging of impact for either costing or comparative purposes.

Field I - Risk Probability

As for Impact this is a subjective view of the probability of occurrence of the risk. Again a figure 1, 2, 3 or 4 (low, medium, high or very high) is to be placed in this field.

Field J - Risk Criticality

Risk Criticality is a figure derived from the multiplication of the Impact and Probability factors described above. It serves as a means of gauging risks for comparative prioritisation and as an indicator of urgency.

Field K - Risk RAG

The RAG indicator of the risk gives an indication for risk prioritisation where e.g. Red indicates those risks of a very high criticality requiring immediate attention and Violet, Amber, Green of relatively low criticality requiring correspondingly a lower level of priority.

Field L - Date Raised

Record here the date on which the risk was first identified and entered into the risk register.

Field M - Risk Owner

The Risk Owner is the person nominated to develop and manage the action plan for this risk. Although responsibility for risk handling, e.g. mitigation or

contingency planning and execution may be invested with the supplier the Risk Owner here is the manager who will oversee and agree with the supplier's activities.

Field N - Action Plan

This is a summary of the programme and activities that will eliminate the risk or reduce it to an acceptable level. According to the size of the task (costs, number of staff, duration etc.) the action plan may be declared a project.

Field O - Plan Status
Record here a brief statement on the achievements, reasons for any delay to the Action Plan and recovery activities.

Field P - Status RAG
Red, Amber, Green indication of the status of the Action Plan

4.3 Risk Assessment / Scoring

This section provides tools for scoring or assessing risk levels. The first method allows for assessing risk level as one variable, the second allows for assessing risk level as two independent variables risk likelihood and risk consequence or impact.

4.3.1 Assess Risk Level

EXAMPLE

PRODUCT: Stringer Sec.14/15		Risk level							No.001		
Product Risk Assessment (PRA)		1	2	3	4	weighting	Result	Max. possible Result	Risk register Yes		No
N° A	Safety Classification										
N° A.1	Safety classification process responsibility			3		2	6	8	Yes		
N° A.2	Classified part manufacturing	1				0,5	0,5	2			
N° A.3	Control of classified parts to customer requirements				4	1	4	4	Yes		
N° A.4	Customer Approval status	1				1	1	4			
	Total Risk			3		4,5	11,5	18			
					R	⇨ 5	12,7	20	⇦	M	

$$\text{Product Risk Assessment Scoring (PRAS)} = \frac{R \times 20}{M} = \frac{11{,}5 \times 20}{18} = 12{,}7$$

	15		
D VERY HIGH 15 < R < 20	C HIGH 11 < R < 15	B MEDIUM 11 < R < 7	A LOW 5 < R < 7

The risk leader agrees on the risk scoring		
Representative : Smith	Signature :	Date :

Figure 15 Risk Level Assessment Table

The following instructions are for using Figure 15 to assess risk level.

1. Give the form a unique number for purpose traceability,
2. For each assessed element or section define the risk level from 1(low) to 4 (very high),
3. Define appropriate weight for each element or section (not both at the same time),
4. Multiply the risk level by the weight for each assessed element or section to determine the "result",
5. Multiply the max. risk level by the weighting to obtain the maximum possible result for each assessed element or section,
6. Indicate "yes" or "no" wether it is necessary to fill in the risk register form for risk management,
7. Add assessed element or section risk for total risk and compare with maximum possible risk (e.g. per 20, 100, 1 000),
8. Perform rating after defining limits for each level (e.g. low, medium, high, very high).

4.3.2 Determine Likelihood and Consequence Levels

Assessing risk levels based on the independent variables of risk likelihood and risk consequence or impact provides more information about a risk than assessing only a risk level.

This process step is performed on each identified risk. If risk levels are compared for prioritizing, levels of likelihood, and consequence (impact) should be determined using the same method and criteria (such as the same assessment tables or templates). Otherwise, the levels of risks have inconsistent bases.

Initial assessment of levels is based on information from the risk owner.

To determine likelihood level, select a level from an "assessment table," such as the one shown in Table 2. The table provides subjective values that should not be used for quantitative methods (calculations).

Table 2 Risk Likelihood Assessment Table

1	Low	Proven or completely mitigated by an approved plan
2	Minor	Demonstrated or well mitigated by approved plan
3	Moderate	Partially demonstrated or mitigated by approved plan
4	Significant	Analytically demonstrated possible mitigate plan
5	High	Speculative with no mitigation plan

To determine consequence (impact) level, appropriate levels are selected from templates or assessment tables for the selected consequence categories including technical, schedule, cost, or other templates/assessment tables, such as the one shown in Table 3. In the figure, the technical and schedule consequences have subjective scales that do not involve calculations and the cost consequence has a objective scale that may be used in calculations.

Table 3 Risk Assessment Table for Technical, Schedule, and Cost Consequences

Team Consequences / Impacts	Given the risk event occurs, what is the magnitude of the impact to your project / program?					
	Impact Level / Type:	**1**	**2**	**3**	**4**	**5**
	Technical (everything not related to schedule or cost)	Minimal or no impact	Moderate impact. Same approach retained	Moderate impact but alternatives available	Major impact but alternatives available	Major impact and no alternatives available
	Schedule	Minimal or no impact	Additional activities required. Able to Meet Need Dates	Key project / program milestones slip ≤ 1 month	Key project / program milestones slip > 1 month, or Project / program Critical Path impacted	Cannot achieve Key project / program or Major Program Milestone(s)
	Cost	Minimal or no impact	Project / program budget increase < 5%	Project / program budget increases > 5%, or another project/program is impacted	Project / program budget increases > 10%, or other project/programs impacted	Project / program budget increases > 20%

If nominal scales are used, specific thresholds for technical, cost, and schedule consequence criteria need to be included in the Risk Management Plan. The values of cost impact are for illustration only. Individual projects may consider a high (level 5) cost increase to be either 5% or 50%, for example. Depending on the analysis method documented in the Risk Management Plan, the consequence level used to determine the risk level may be the highest of the levels assessed, or may be a combination of the levels assessed. The technical, schedule, and cost consequences are assessed for each risk, although one or more of these may be judged as low. It is recommended that all levels assessed be retained for risk review board activities. Where multiple consequence levels are assesses the project or organization may use the highest consequence level to represent the risk level or combine the consequence levels. If combining the consequences levels is the approach selected by the program, a linear combination of numeric consequence levels from each template is a suitable method for combining the results from multiple consequence assessments: This may be applied only if the consequence scales are objective, having absolute, not relative, subjective values.

4.4 Risk Status Reports

4.4.1 Risk Statistics

Statistics may be reported to give an overall view of risk management status, which may include:

- Quantity of open, closed, and total risks by high, medium, and low risk levels
- Quantity of open, closed, and total risks by initiating department within the organization.
- Open risks aging (from initiation date to today) by total, risk level and by responsible department within the organization.

4.4.2 List of Prioritized Risks

Prioritization of risks in an organization should be based on

- Largest risk level or largest risk likelihood and risk impact,
- Greatest urgency (the time between now and when a risk may occur),
- Largest quantity of risks related to a special requirement or critical item, and
- Customer priorities and preferences concerning risk management.

A matrix of these factors should be developed for all organization risks and used by the Risk Review Board to prioritize risks for risk handling actions

4.4.3 Individual High and Moderate Risks

Individual risk registers for high and moderate risks may also be a topic of discussion at the risk review board.

4.5 Risk Reviews

There is generally one risk review meeting for an organization. However, larger organizations may elect to have one review for Product Design Risks and another review for Operations (Manufacturing and Supply Chain) Risks and have one program-level review where high risks from the lower reviews would be elevated. A risk reviews may be conducted in existing management meetings of the organization.

The membership of a risk review team should include management from affected departments within an organization and executives. The members should represent not only affected departments but also all significant projects in the organization.

The responsibilities and authority of a risk review team may include:
1. Overseeing the performance of the risk management process.
2. Ensuring correction or improvement of the risk management process.
3. Prioritizing risks for risk handling actions
4. Reviewing proposed risk handling actions (avoid, transfer, assume, or mitigate).
5. Reviewing performance to plan for execution of risk handling actions.
6. Reviewing affect of risk handling on project or organization performance.

The accountability of a risk review team may include:
1. Documenting decisions made.
2. Reviewing performance of the risk management process with the organization’s executives.
3. Reviewing affect of risk handling on project or organization performance with the organization’s executives.
4. Addressing feedback from organization’s executives on risk management performance.

4.6 Process Metrics

One or more of the following metrics are recommended to monitor the performance of an organization's risk management process. It is recommend to select the vital few metrics that are most important to the customer and stakeholders and manage and improve the RM process using the metrics. Metrics 1 – 5 may be more appropriate when the RM process is immature and metrics 6 – 13 when the RM process is well established and relatively mature.

Metric targets should be defined by management and documented for each metric, and whenever a metric exceeds or falls below a target, action must be taken to improve the control or capability of the RM process.

4.6.1 Percent of Risk Practitioners Trained Using the Organization's Documented Risk Management Plan as Syllabus

This metric measures the level of preparation within an organization to apply the RM process efficiently. It should be tracked monthly until all practitioners in the organization are trained, and then quarterly thereafter to ensure changes in personnel are addressed. The metric should be calculated as the number of practitioners trained divided by the total number of practitioners in the organization, the quantity times 100%. The organization should define, by role or responsibility, risk practitioners. It is important that project management and all design-build team leaders receive training in the organization's RM plan.

This effectiveness metric may be calculated as number of risk practitioners trained divided by the number of risk practitioners, and then multiplying the quantity by 100%. Actual performance should be tracked against a target percentage of at least 95%. If actual performance falls below the target, a project, or the entire organization, should take corrective action.

4.6.2 Customer Involvement and Perception

- The RM process is consistent with customer expectations.
- Customer is involved with the established RM process.
- Customer comments on the RM process are encouraged and recorded, and reviewed and addressed by the risk review board.

4.6.3 Organization RM Requirements

- A recognized and documented RM process/plan is in place.
- Mitigation/handling plans exist for moderate and high risks.
- Risks are communicated from the lowest team level and consolidated with appropriate assessment at the organizational level.
- RM data are available to all team members.
- A management focal point or lead for the process and each project are identified.
- All risks are assigned to a responsible owner (typically a team leader or manager).
- If management is not represented in the risk review board, periodic management reviews of risk status and results are conducted.

4.6.4 RM Process Maturity Development

- The current state of the organization's RM process maturity is assessed using the RM Maturity Model.
- Management defines the next stage of RM process maturity to be achieved using the model and defines an estimated completion date.

- Management ensures that a plan is developed and executed to achieve the next stage of RM process maturity by the estimated completion date." Sources for this material are listed in the References section.

4.6.5 Effectiveness of Determining Root Cause

Root-cause analysis is a systematic approach for determining all the contributors to a problem before attempting to implement a corrective action or risk mitigation plan. Usually, what is observed as the problem is not the problem itself or the cause of a problem, but an indication or symptom of a problem. If a solution is applied to the symptom, the actual problem will not be resolved permanently or completely or may even be unaffected by the solution. Elimination of root causes leads to complete and permanent resolution of a problem.

This analysis step focuses on implementation problems within the RM process.

An approach to determine root cause is identifying systematically many potential causes and eliminating potential causes with known facts and data to determine actual causes.

Metric: percentage of risks that achieved planned risk likelihood and risk impact.

4.6.6 RM Process Improvement Recommendations

To facilitate this, a standard feedback form or website may be offered to all stakeholders and users of the RM process.

Metric: quantity of RM process improvement recommendations per quarter.

4.6.7 Risk Mitigation Performance-To-Plan

Urgency is a key factor in effective RM—i.e., the time period before an unfavourable event can occur. Hence, when mitigation actions are planned and accomplished is of utmost importance. Mitigation action completions can be tracked using a "burn-down" plan to show actual event completions for the period versus the planned event completions. This metric provides an indication of the level of support of a department within the organization to the RM process.

To make the metric meaningful, actual performance should be tracked against a target of approved commitments. If the percentage of on-time completions falls below the target completion rate, the project or the organization may choose to implement corrective action.

Risk mitigation performance to plan may be calculated as the number of mitigation events actually accomplished divided by the number of mitigation events planned to be completed, and then multiplying the quantity by 100%. This effectiveness metric should be tracked periodically (e.g., monthly) against a minimum target value (e.g., 95%). If the metric falls below the target, a project or the organization should take corrective action.

4.6.8 Percent of Moderate and High Risks With Mitigation Plans

This effectiveness metric measures the effectiveness of the RM process in defining mitigation plans where needed. It may be tracked at each major milestone through completion of the project. In general, the smaller the percentage, the more effective the RM process. The metric may be applied based on current risks with or without consideration of urgency.

The metric may be calculated as the number of moderate and high risks with handling plans divided by the number of moderate and high risks, and then multiplying the quantity by 100%. This effectiveness metric should be tracked periodically against a minimum target value (e.g., 95%). If the metric falls below the target, a project or the organization should take corrective action.

4.6.9 Time from Risk Identification to Risk Handling Strategy in Place

This efficiency metric measures the cycle time of the RM process. It may be based on each risk item, each category of risks, or moderate and high risks combined. To obtain the most information about the RM process, it is recommended to measure the cycle time for each risk item. This metric may be calculated as the date the risk handling strategy is in place minus the date the risk was identified.

Actual performance should be tracked against a target cycle time for the RM process (e.g., 90% of risks within 10 days).

4.6.10 Percent of Risks Identified by Lowest Affected Team

This metric measures the level of support of organizations within a project or the organization to an implementation of the RM process that identified risks mainly at the team level. This metric is not an effective measure for implementations that identify risks from the top level down. It indicates compliance with the bottom-up approach.

It may be tracked at each major milestone through completion of the project. In general, the larger the percentage, the more effective the RM process, because risks identified by the lowest affected team are usually identified early, before likelihood or consequences have had a chance to increase.

The metric may be calculated as the number of risks identified by the lowest affected team divided by the total number of risks identified on a project or in the organization, and then multiplying the quantity by 100%.

Actual performance should be tracked against a target percentage. It is recognized that some system-level risks, and some risks associated with organizations or activities external to the project or the organization, may be “visible” only from the higher levels within the organization A suggested target is about 67% of the risks on a project or in the organization should be identified at the lowest possible level. If actual performance falls below the target, a project or the organization should take corrective action.

4.6.11 Percent of Mitigation Plan Tasks Included In Project/Team/Organization Schedules

This metric measures the thoroughness and completeness, and therefore the effectiveness, of risk mitigation plans, as well as project or organization commitment to accomplishing them. Mitigation plans need to be monitored regularly to ensure that they are being executed and are achieving the planned reduction. The easiest way to monitor these plans is to use the system established on the project for monitoring all schedules. Tracking risk mitigation activities within team schedules ensures resources are identified to conduct the mitigation effort, and that early visibility is available of any erosion to the plan.

This metric may be calculated as the number of mitigation plan tasks included in project or organization schedules divided by the total number of mitigation plan tasks identified, and then multiplying the quantity by 100%.

Actual performance should be tracked against a target percentage. A reasonable target is to have at least 95% of risk mitigation tasks included in team schedules. If actual performance falls below the target, a project or the organization should take corrective action.

4.6.12 Ratio of Cost Savings Attributed to Risk Management over the Cost of Conducting Risk Management

This effectiveness metric measures the simple return on investment attributed to the RM process. This metric is measurable only for those risks where the consequences are stated as cost consequences and costs of performing mitigation actions are collected. To minimize costs of the metric, it may be applied to project risks only. It may be tracked at each major milestone through completion of the project. In general, the larger the percentage, the more effective the RM process. It may be calculated as the cost savings attributed to the RM process divided by cost of conducting the RM process. The cost savings should be determined.

Determining Cost Savings

- Outcome Cost Savings (less cost of risk mitigation)
- Risk did not occur because of RM process. Expected risk exposure L*Ce where L is the likelihood of the consequence and Ce is the expected cost consequence
- The consequence of the risk is less than the expected consequence because of the RM process Expected consequence of the risk (Ce) minus actual consequence of the risk (Ca)

- The consequence of the risk is greater than or equal to the expected consequence.. No credit to the RM process
- Alternate: Subtract actual consequence of the risk (Ca). This is a charge against an ineffective RM process
- Risk did not occur because of factors other than the RM process.
  None. No credit to the RM process

The costs of the RM process include labour hours and other resources involved in identifying risks, analyzing risks, defining risk handling options, developing and implementing risk mitigation plans, and tracking and reporting risks. Nonrecurring activities such as development and implementation of a PRMP and process or improving the plan or process may be excluded or amortized over several years. Actual performance should be tracked against a target ratio of at least 1.5:1. If actual performance falls below the target, a project or the organization should take corrective action.

4.6.13 Percent of Project or Organization Targets Met

This effectiveness metric should be measured for technical, cost, and schedule targets. Targets should be formally defined and documented by project or organization management. It may be calculated by the number of project or organization targets met divided by the number of project or organization targets, multiplied by 100%
This is a meaningful RM process metric only when the following conditions are met:

1. RM process was in place in accordance with this document.

2. RM process was adequately supported by the project or organization as reflected by the foregoing metrics.

3. The project or organization targets were defined either at the beginning of the project or in adequate time to manage risks.

The target for the metric should be at least 80%. If actual performance falls below the target, a project or organization should take corrective action.

4.7 Lessons Learned

The organization’s lessons learned database should contain information such as:

1. Lesson summary (2-3 lines).

2. Lesson details

   a. Product, service, or process involved (include name and number)

   b. Description of risk, issue, or success

   c. Causes of risk, issue, or success

   d. Lessons learned, recommended future preventive actions, or wisdom gained that could be replicated.

e. Lessons validated (Yes., No)

3. Index categories (tags to locate lessons learned) such as:

a. Beneficiary (customer name, department of organization),

b. Program or Project Phase (request for quote, contract negotiation, contract award, contract compliance, requirements development, technology development, design development, design verification, design validation, initial production readiness, production rate readiness, product build, product integration (next higher assembly), product installation (in customer end product), product test, product returns, warranty, service delivery),

c. Classification (may select multiple items - missing requirements, incomplete requirements, misunderstanding of requirements, incorrect requirements applied, missing inputs / materials, incomplete inputs / materials, incorrect inputs / materials applied, incorrect operational environment, missing tools, incorrect tools, nonconforming tools, no training, inadequate training, missing certification / qualification, missing equipment / machines, incorrect equipment / machines, nonconforming equipment / machines, undocumented methods, incomplete methods, incorrect methods)

d. Lessons Learned Contributor (name, department, submittal date, phone number, email)

e. Lessons Learned Validator (manager name, department, submittal date, phone number, email)

It is important to have a contributor and validator as views concerning lessons learned may vary. Unvalidated lessons learned should remain in the database as historical information. In the end, time tells the truth.

f. Rationale for Lessons Learned Not Implemented and Validating Manager

This is an important data element to mitigate liability risks. For example, if a safety lesson learned was identified for a certain product and was not used on a similar product and an injury or death occurred because of the similar product, there should be rationale explaining why the safety lesson learned was not implemented on the similar product.

The validating manager should be one responsible for the product or knowledge domain.

4. There should be an organizational lessons learned process that requires:

a. lessons learned to be recorded in each phase of program or project.

b. lessons learned database to be researched prior to planning of all future programs and projects

c. Evidence of application of lessons learned on all future programs and projects (e.g., policy and procedure changes) or rationale for not applying applicable lessons learned is recorded.

4.8 Organizational Risk Maturity Model

This risk management maturity model should be used periodically to assess the maturity of the organization's risk management process and to define goals to achieve certain maturity levels (1-5) by certain dates.

Levels / Key Attributes	**1 No Process**	**2 Process Defined / Not Effective**	**3 Process Defined & Effective**	**4 Systems Approach**	**5 System Optimized**
Process					
• Process - Developing a risk identification strategy, - Identifying and documenting risks - Analyzing risk - Assessing risk handling options - Planning & performing risk handling - - Communicating & tracking risks	• No Risk Management Processes established by policies and procedures **(Ad-hoc)**	• All Risk Management Processes are established by policies and procedures • Process metrics not implemented or metrics demonstrate that process is not effective **(Repeatable / not effective)**	• Risk Management Processes are established by policies and procedures • Process metrics demonstrate consistent process effectiveness **(Repeatable / effective)**	• Same as 3 plus: • Risk Management Processes are integrated (outputs from one become inputs to another) • Metrics are used to make decisions on process improvements • Process metrics demonstrate continual Improvments • Lessons Learned Collected • Benchmarks Processes **(Managed)**	• Same as 4 plus: • Lessons Learned are implemented on new projects and programs. • Metrics demonstrate that Risk Management process is effective and efficient (**Optimized)**
• Behavior/Actions	• Identification, Communication and & Mitigation of Risk Begins After Issues Occur (Reactive)	• Identification, Communication and & Mitigation of Risk Associated with Product Requirements	• Identification, Communication. & Mitigation of Risk Associated with Management System Requirements	• Identification, Communication. & Mitigation of Risk Integrated with Business Processes (Policy & procedure changes)	• Identification, Communication & Mitigation of Risk Drives Business Decisions; Interaction of risks understood and managed

• Closed-loop Risk Management Process	• Trial & Error Solutions To Issues; in Fire Fighting Mode	• Issue management Driven by Experience	• Preventive Action Drives Risk Management	• Organizational Lessons Learned Feedback into Proposal & Planning, and Other Processes	• Aggregates Effects pf Individual Risks to Assess Program Impacts • Risk Management Processes have Forecasting / Predictive Capability
• Scope of Application	• Product Design department for special design requirements	• Product Design, Product Quality, & Contracts departments for special design and build requirements, critical items, and key characteristics (AS9100C)	• Product Design, Product Quality, Contracts, Manufacturing, & Supply Chain departments for special design, build, and support requirements, critical items, and key characteristics	• Product Design, Product Quality, Contracts, Manufacturing, & Supply Chain departments, and Key Customers for special design, build, and support requirements, critical items, and key characteristics	• All departments in organization, key customers, and key suppliers for all special requirements, critical items, and key characteristics
Organization/People					
• Culture	• No Organizational Understanding of Risk Management Concepts	• Organizational Risk Culture is Based on Individual Knowledge	• Risk Methods in use at Organizational, Product & Process Activities	• Risk Management Understanding Active in All Phases of Product Lifecycle	• Risk Management Understanding Promoted & Drives Decisions in All Phases of Product Lifecycle
• Awareness & Training	• No Training Planned	• Only Selective Training; No Evidence Of Application	• Training & Awareness of Risk across the Organization	• Risk Management Ownership Defined	• Integral Part Of The Organization, Risk Management Is Inherent
• Responsibility	• No Responsibility Defined	• Responsibility Defined But Not Acting	• Responsibility Defined But No Definition Of Workload	• Responsibility Defined But No Operational Resource Network In Place	• Responsibility Defined Dedicated Resource Network Available And Acting

Tools & Data	• No Tools And Data Defined	• Tools And Data Defined But Not Practiced	• FMEA/PFMEA Tools Applied	• Risk Based Acquisition With Suppliers • Design Lifecycle Risk Tools Driving Project Risk Decisions • Tools Being Systematically Applied	• Cross Organizational Based Risk Tools Driving Risk Decisions o Cross Lifecycle o Cross Project / Program o Cross Product
Process Metrics	• No Process Metrics Implemented or • No Corrective Actions Implemented	• No Corrective Actions Implemented based on Process Metrics	• Corrective Actions Not Preventive But Reactive	• Effectiveness of Corrective and Preventive Actions Assessed; Lessons Learned Documented	• Risk Prediction / Forecasting/ Indication Metrics • Effectiveness and Efficiency Metrics Used to Improve Risk Management Processes

4.9 Benchmark Process

Benchmarking involves comparing the organization's risk management process to other risk management processes used in our outside of its industry. The organization should identify strengths and weaknesses of each process relative to its own application and make decisions on changes to the organization's process.

a. Review national and international standards.

ISO 9001 Quality Management Standard

ISO 13485 Medical Devices

SAE ARP 9113 Supply Chain Risk Management Guideline

BSI BIP 2024 Project Risk Management. Processes, techniques and insights

BSI BIP 2028 The project manager's guide to handling risk

FAA 8040.4 Safety Risk Management

ISO 31000 Risk management - Principles and guidelines

ISO 31010 Risk management – Risk assessment techniques

b. Review customer and supplier risk management processes.

4.10 Getting Started

This section provides guidance on how to start a risk management process in an organization. It is an integration of the information in this document.

1. Identify a risk management process owner. This is generally a number of management.

2. Identify a focal to implement the risk management process.

3. Focal understand the processes in section 2 and select tools to facilitate the process from section 4.

4. Focal explain process and tools to each department in the organization. Training materials may be made from this guidelines document.

5. Focal obtain commitment from one or more departments to use the process and tools.

6. Focal prepare risk status reports and communicate them to affected management (section 4.4)

7. Process owner establish a risk review team of affected managers and executives to make decisions on risks and the risk management process (section 4.5).

8. Focal select and implement effectiveness and efficiency metrics for the risk management process (section 4.6)

9. Focal communicate risk management process metrics with risk status reports to affected management (section 4.5).

10. Process owner establish process to implement lessons learned from past programs on future programs (section 4.7).

11. Focal assess maturity of organization's risk management process (section 4.8) and plan process improvement opportunities.

12. Focal benchmark risk management processes to identify approaches to improve the organization's risk management process (section 4.9).

5 GLOSARY

5.1 Examples of "Risk" Types:

- **Financial:** Those risks discovered/analyzed during company financial reviews. Covered here are the risks associated to continued business brought about by the lack of financial stability which includes funding position, bank credit, debit collection possibilities and trading performance as well as ability to maintain competitive product prices.
- **Strategic:** Those risks associated with maintaining Customer commitments and market domination through the supply chain, supply sourcing policies, openness with programs and their problems, responsiveness to customer changing needs, total manufacturing capacity and technologies (plus potential for development), type/number of customers, joint-ventures, revenue sharing, etc. Willingness and ability to implement and maintain security and confidentiality polices shall also be considered.
- **Compliance/Effectiveness:** Those risks associated with the ability to deliver on time, to quality and cost as will as the ability to develop market share, improve lead times, prices, quality, etc. and improve/maintain customer support. Ability to respond to program changes and customer needs (modifications, build schedules, delivery etc.).
- **Operational/Planning:** Including Physical/Environmental Risks to the Supply Chain as a consequence of potential disaster based on geographic location such as potential flood, earthquake, extreme changes to climatic conditions, production techniques/materials or the effects of production bottlenecks, logistics, facilities, resources, prima material availability, fire/explosion, insurrection etc. are all to be considered in terms of protection and

contingency planning for the Supply Chain. Risk issues associated with production/logistic planning of the material to be furnished, including sub-tier supplier planning activities shall also be considered.

- **Human Factors:** Those risks associated with Staff turnover, available skills and training, employment levels, staff relationships and management expertise fall within this category as does employer to employee relationships and willingness and ability to communicate effectively with suppliers and customers. They include human needs, expectations, attitude, motivation as well as anthropometric factors (physical dimensions of the human being).
- **Political:** Risks resulting from National /International trading (import and export controls and duties Etc.) that could be affected by differing Government polices and effects of Government ownership and subsidization, cultural, language and employment legislation etc.
- **Environment, Health and Safety:** Those risks associated with product development, manufacturing, materials and support that can adversely have an impact on the environment and people. It should be noted that EHS will be subjected to increasing controls from national and international authorities as protection of the local and world environment for the well being of the world and mankind has become a focalized topic by the major industrial nations and the United Nations as a whole.
- **Ethical, legal and image:** Those risks associated with the non application of fair/appropriate business practices, fraud, non compliance to Equal Employment Opportunity (EEO) requirements and Child Labor Acts, responsibilities to customers/stakeholders/users, suppliers/sub-tires and employees. This includes risks on how the company is perceived by the customer, employees and general public.

- **COTS** – Commercial Off the Shelf
- **FMEA** – Failure Mode Effect Analysis
- **POC** – Point of Contact
- **R&D** – Research and Development
- **RED Team** – Group specifically organized and assigned to address Urgent and High Risk issues
- **KPI** – Key Process Indicators
- **SW** - Software