Software Risk Management And Audits

What is Risk

“Risk is the probability of suffering Loss or Gain while pursuing goals due to factors that are unpredictable or beyond control.”

A Boundary Problem

- Local issues are not regarded as Risk.
- It may be termed as **Internal Risks** that can be solved by taking *internal measures*.
- Mostly internal risks are regarded as dependency risks that are solved by better Coordination and risk communication.
- Some Internal Risks arise because of lack of Process Capability.
- When an organization is divided, more boundaries appear and employees see more internal risks.
- When the organization is integrated, internal risks are called **Process Management Issues.**

A Boundary Problem

- External conditions are beyond our control.
- There are risk factors beyond our sphere of influence.

Examples:

✓ Competitors cut down prices.

✓ Social forces may erode staff loyalty.

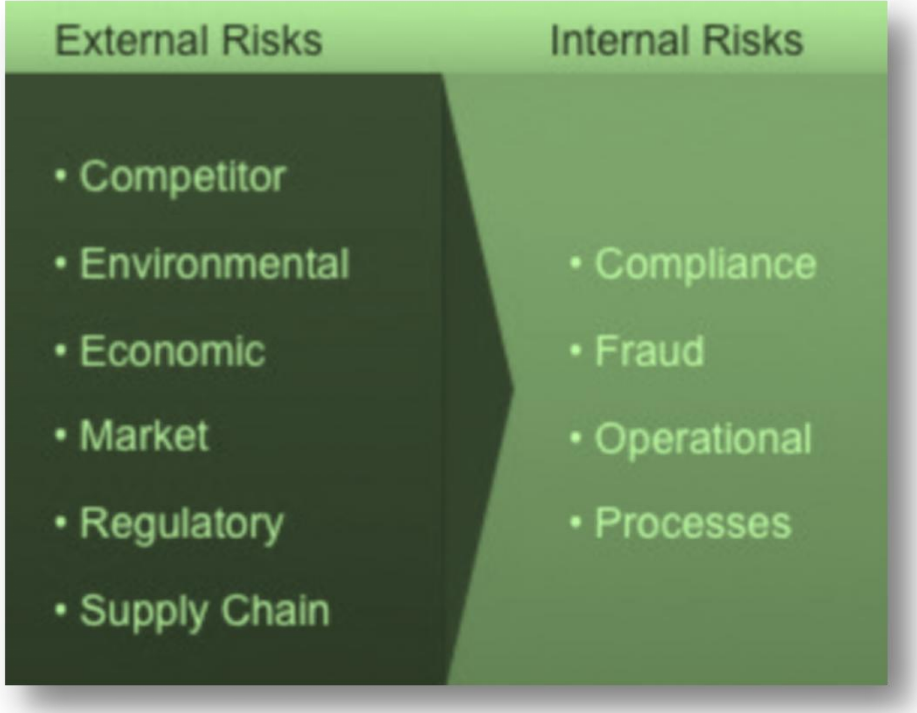
- The PM sees external risks as threats and develops strategies to deal with them

Example: The requirements keep changing; they “creep.”

A Boundary Problem

Internal Risk is the probability of suffering losses while pursuing performance and growth goals because of inadequacies in process capability and organizational structure.

External Risk is the probability of suffering loss while pursuing performance and growth goals because of uncertainties in external conditions.



External Risks

- Competitor
- Environmental
- Economic
- Market
- Regulatory
- Supply Chain

Internal Risks

- Compliance
- Fraud
- Operational
- Processes

Expressing Risk: The Basic Terms

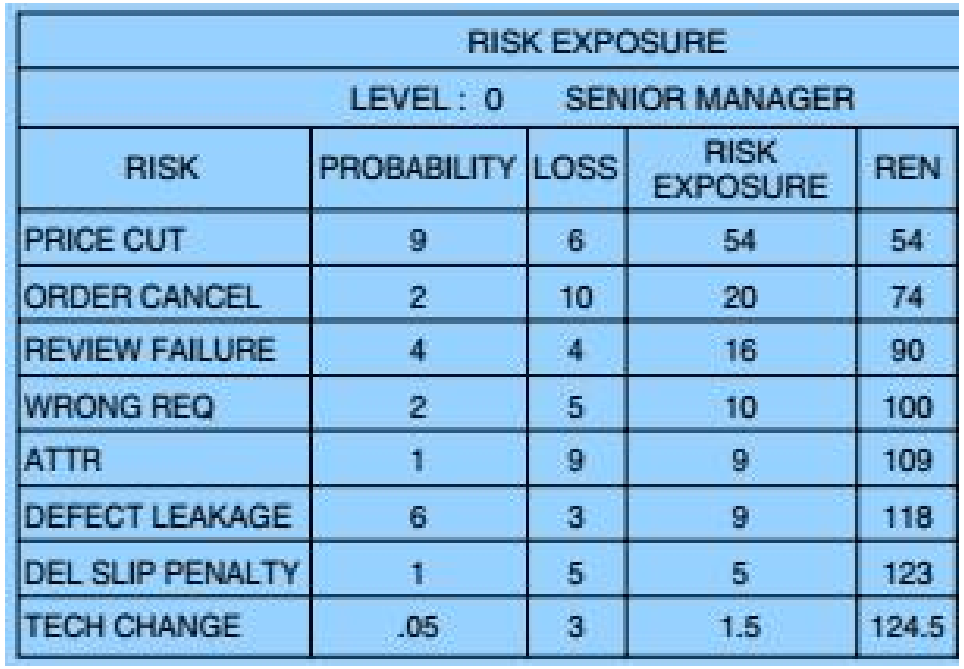
Risk culture also thrives on clear definitions of risk terms.

- ✓ **Risk ID:** A unique reference number given to each risk for traceability.
- ✓ **Risk Probability:** The probability of risk occurrence.
- ✓ **Risk Impact:** The level of damage if risk occurs.
- ✓ **Risk Exposure:** The combination of risk probability and risk impact.
- ✓ **Risk Origin:** Source of risk (internal or external).
- ✓ **Risk Category:** A group or class with a set of similar risks.
- ✓ **Risk Owner:** Process owner whose objectives are likely to be harmed by risk.

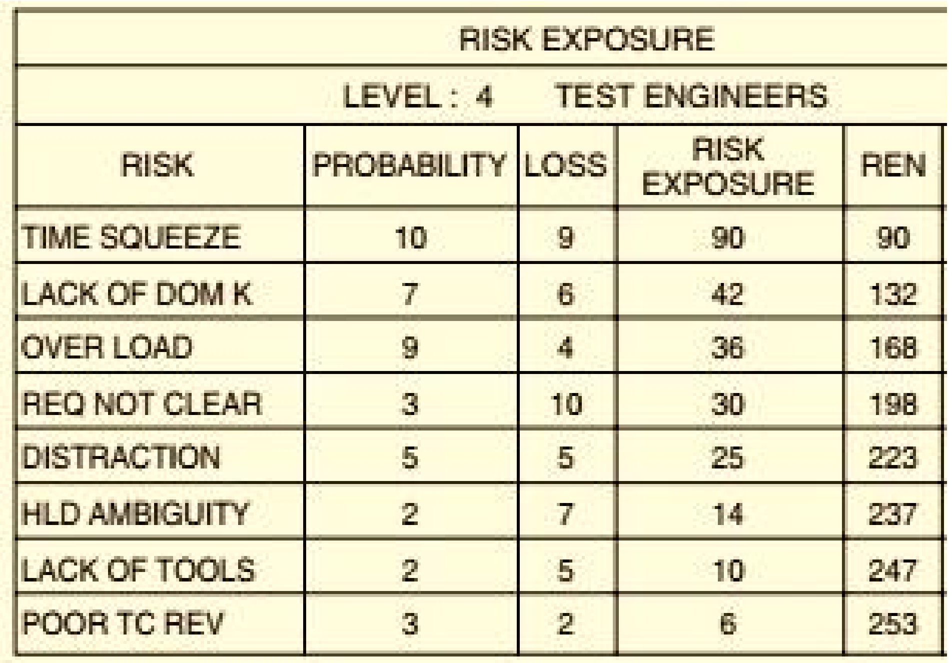
Risk Attributes

Attribute	Classes
Origin	Internal or External
Domain	Project/Process/Product or Business/Technical
Nature	Hazard/Constraint/Nominal/Trivial
Affected (key result area)	Cost/Schedule/Quality/Performance
Attack Time	Immediate/Quarterly/Yearly
Speed	Slow or Fast
Level	Process/Project/Program/SBU/Enterprise
Affected Process Area	Requirement/Design/Coding/ Testing Training management/Facilities management/Quality Management/Project Management
SEI Taxonomy	Product Engineering/Development Environment/Program Constraints
Visibility	Low/Medium/High
Affected Goals	Goal 1/ Goal 2/ Goal 3 …
Affected requirements	REQ 1 / REQ 2 /REQ 3 …

Risk Scale – Case Study



RISK EXPOSURE				
LEVEL : 0 SENIOR MANAGER				
RISK	PROBABILITY	LOSS	RISK EXPOSURE	REN
PRICE CUT	9	6	54	54
ORDER CANCEL	2	10	20	74
REVIEW FAILURE	4	4	16	90
WRONG REQ	2	5	10	100
ATTR	1	9	9	109
DEFECT LEAKAGE	6	3	9	118
DEL SLIP PENALTY	1	5	5	123
TECH CHANGE	.05	3	1.5	124.5



RISK EXPOSURE				
LEVEL : 4 TEST ENGINEERS				
RISK	PROBABILITY	LOSS	RISK EXPOSURE	REN
TIME SQUEEZE	10	9	90	90
LACK OF DOM K	7	6	42	132
OVER LOAD	9	4	36	168
REQ NOT CLEAR	3	10	30	198
DISTRACTION	5	5	25	223
HLD AMBIGUITY	2	7	14	237
LACK OF TOOLS	2	5	10	247
POOR TC REV	3	2	6	253

- The total REN value in the first assessment is **124.5.**
- In the second assessment, it is **253.**
- Can we conclude that the test engineer estimate double the risk intensity compared to a senior manager? We cannot say that with confidence, these are different.

Risk Identification

We have to recognize the risks from hidden locations, name them, define them, and assign attributes from a risk classification system.

Need to search all processes, and consider all factors.

Position the risk in the correct Risk Level.

We have to review the consequence of the Risk and Rank it.

Definition : "Risk identification is the process of searching the environment, detecting risks, recognizing their attributes, and estimating their consequences"

Risk Identification Methods

Type I (generic, open-ended)

- **Intuitive Methods**
  - Mind Mapping
  - Brainstorming
  - Out-of-Box Thinking
  - Analogy
- **History Based Methods**
  - Top ten Risks
  - Risk Checklist
  - Taxonomy based Questionnaire

Type II (formal)

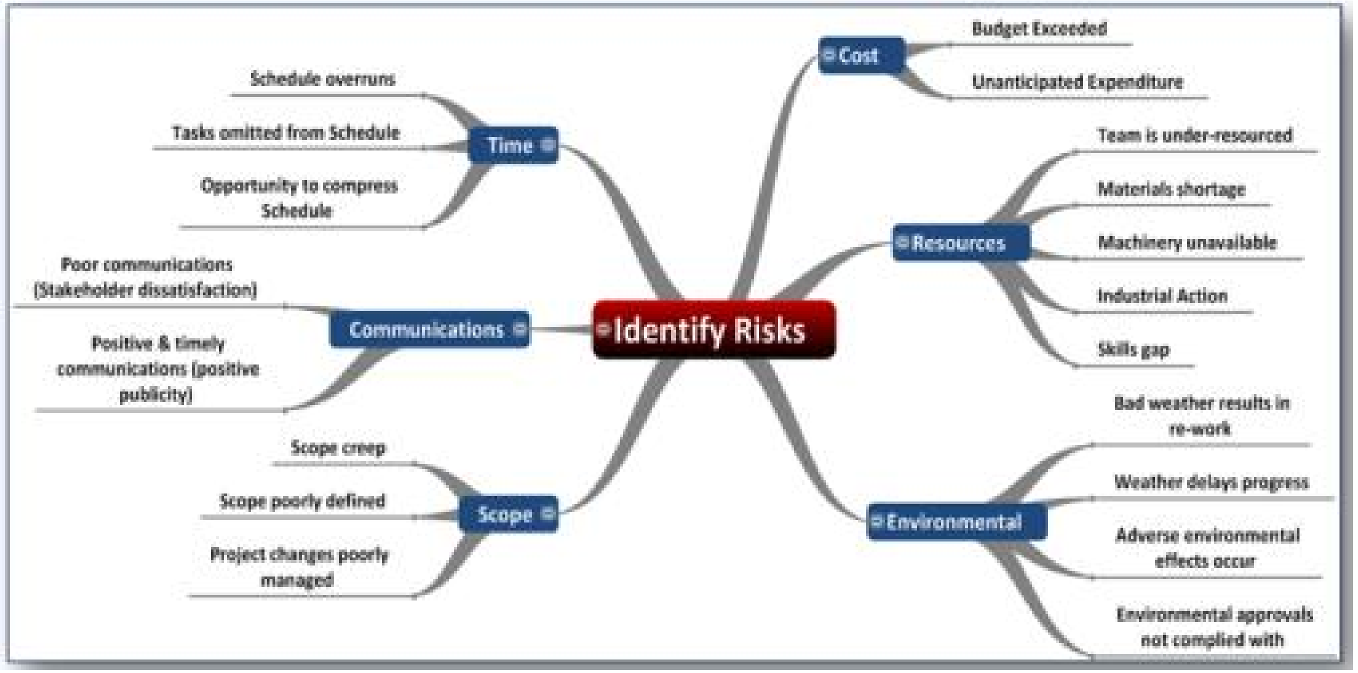
1. Context Setting
2. Data Gathering
3. Risk Discovery
4. Attribute Assignment
5. Validation
6. List

Type I: Intuitive Methods

Mind Mapping

The mind recognizes risk symptoms by mapping familiar symptoms.

Sometimes, the mapping is based on lessons learned.


Identify Risks
Time
Schedule overruns
Tasks omitted from Schedule
Opportunity to compress Schedule
Communications
Poor communications (Stakeholder dissatisfaction)
Positive & timely communications (positive publicity)
Scope
Scope creep
Scope poorly defined
Project changes poorly managed
Cost
Budget Exceeded
Unanticipated Expenditure
Resources
Team is under-resourced
Materials shortage
Machinery unavailable
Industrial Action
Skills gap
Environmental
Bad weather results in re-work
Weather delays progress
Adverse environmental effects occur
Environmental approvals not complied with

Type I: Intuitive Methods

Brainstorming

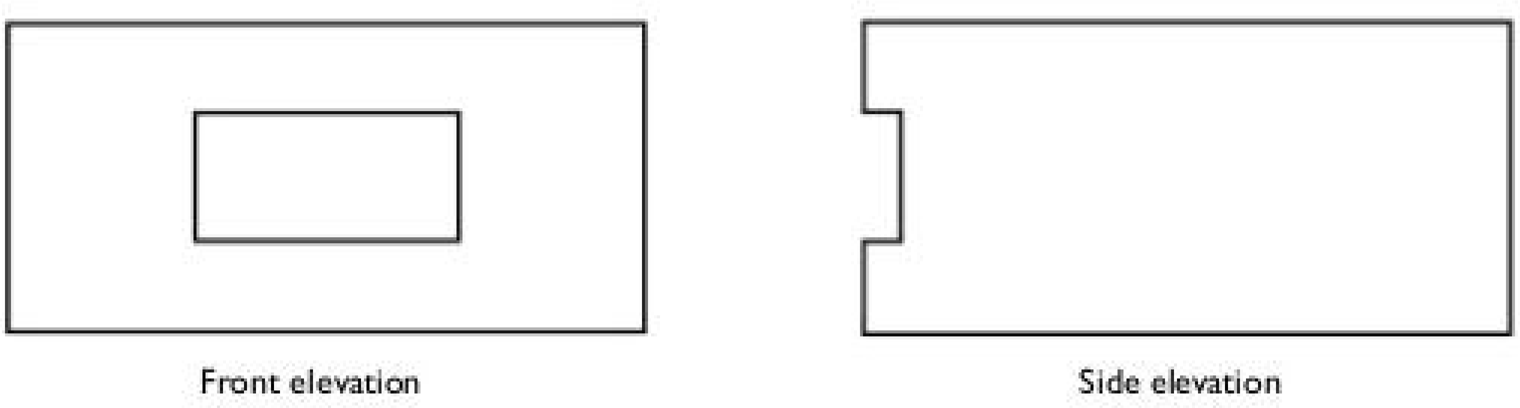
- ✓ Invite Team
- ✓ Explain the objective
- ✓ Set a Time Limit
- ✓ Encourage Ideas for identification
- ✓ Prepare basic Risks list
- ✓ Filtering, Classifying and Clarifying
- ✓ Finalized Risk List.

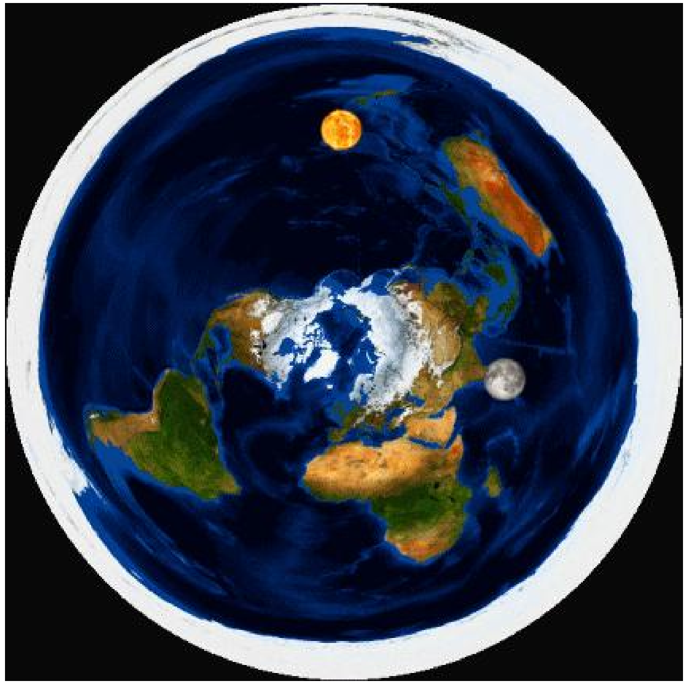
Type I: Intuitive Methods

Out-of-the-Box Thinking

We can see risks better if we stand out of the box and take an external and holistic perspective of the situation.

How can these two drawings both be correct?
What does this object look like? Describe or draw it.





Type I: History-Based Methods

- Caper Jones approaches risk management like managing diseases
- That "risk lists" demonstrated by Rex Black's "Critical Testing Processes."

CAPER JONES

1. Artificial maturity levels
2. Canceled projects
3. Corporate politics
4. Cost overruns
5. Creeping user requirements
6. Crowded office conditions
7. Error-prone modules
8. Excessive paperwork
9. Excessive schedule pressure
10. Excessive time to market

REX BLACK's

1. Functionality
2. Load, capacity, and volume
3. Reliability/stability
4. Stress, error handling, and recovery
5. Date and time handling
6. Operations and maintenance
7. Data quality
8. Performance
9. Localization
10. Compatibility
11. Security/privacy
12. Installation/migration
13. Documentation
14. Interfaces

Risk Analysis

Definition : "The purpose of risk analysis is to understand risks better, and to verify and correct risk attributes."

Definition : "The purpose of risk analysis is to select risks for mitigation."

Screening the Risks

Hazard Risks (catastrophic risks, or killer risks): are those with highest impact on the project. They have the potential to cause maximum damage.

- ***Solution:*** **Murphy's law** (Go by the wise advice: if something can wrong, it will). If we take hazard risks, we must have a good reason for doing so. There must be great returns with continuous risk monitoring and special early-warning systems to detect signals much before the catastrophe occurs.

Constraints: 100% percent probability of occurrence.

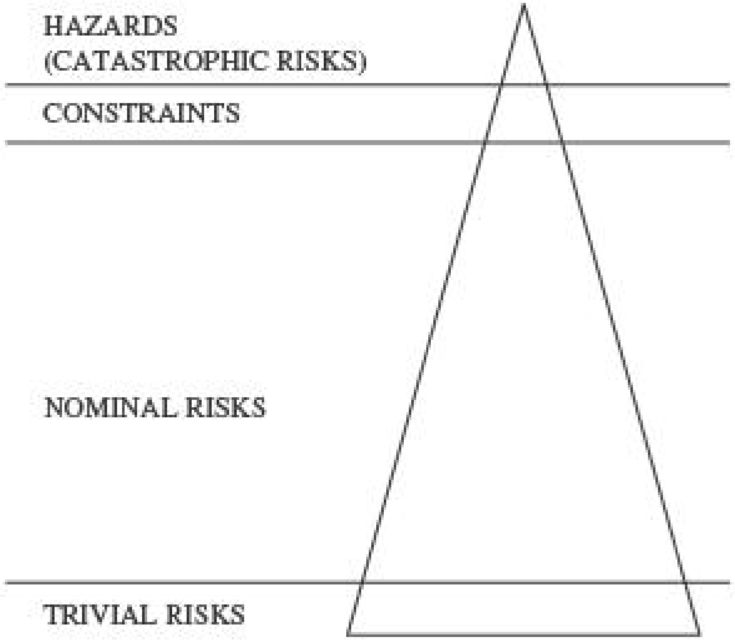
- ***Solution:*** The project runs within these constraints. **System Management or Project Management approaches** will be used to handle such constraints.

Normal Risk: Having normal impact on project.

- ***Solution:*** **Calculate Risk and Prioritized using the Pareto law:** 20 percent of risks account for 80 percent of exposure.

- **Trivial Risk:** Very low impact (negligible) on project.

- ***Solution:*** The trivial risks are kept aside.

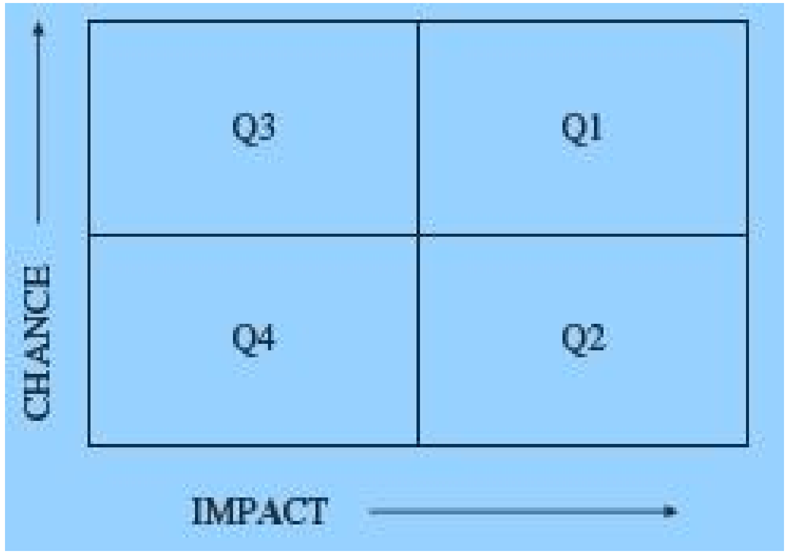


First-Order Analysis: Quadrant Map

Quadrant Mapping helps in getting a bird's eye view of risks and responding to critical risks first.

Risks are represented in four quadrants in a two-dimensional chart showing Impact in the X-axis and Probability in the Y-axis.

Quadrant I: High-Impact High-Probability Risks
Quadrant II: High-Impact Low-Probability Risks
Quadrant III: Low-Impact High-Probability Risks
Quadrant IV: Low-Impact Low-Probability Risks



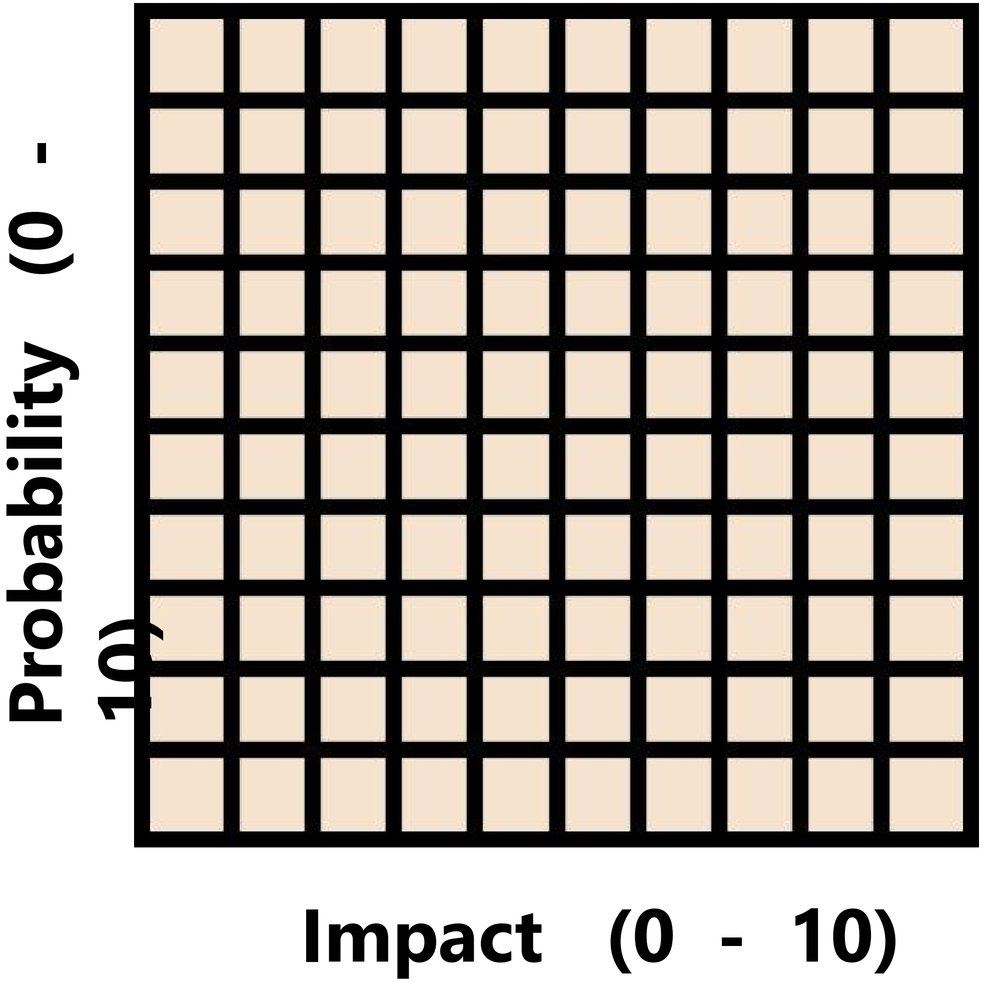
First-Order Analysis: Quadrant Map

Some people use a 10 by 10 grid analysis, which is a refinement over quadrant analysis.

The X-axis represents Impact on a scale 0 to 10.

The Y axis represents probability of risk in a scale 0 to 10.

Each grid location has a specific risk value: location 1 by 1 is the lowest, 5 by 5 medium, and 10 by 10 the most critical problem.

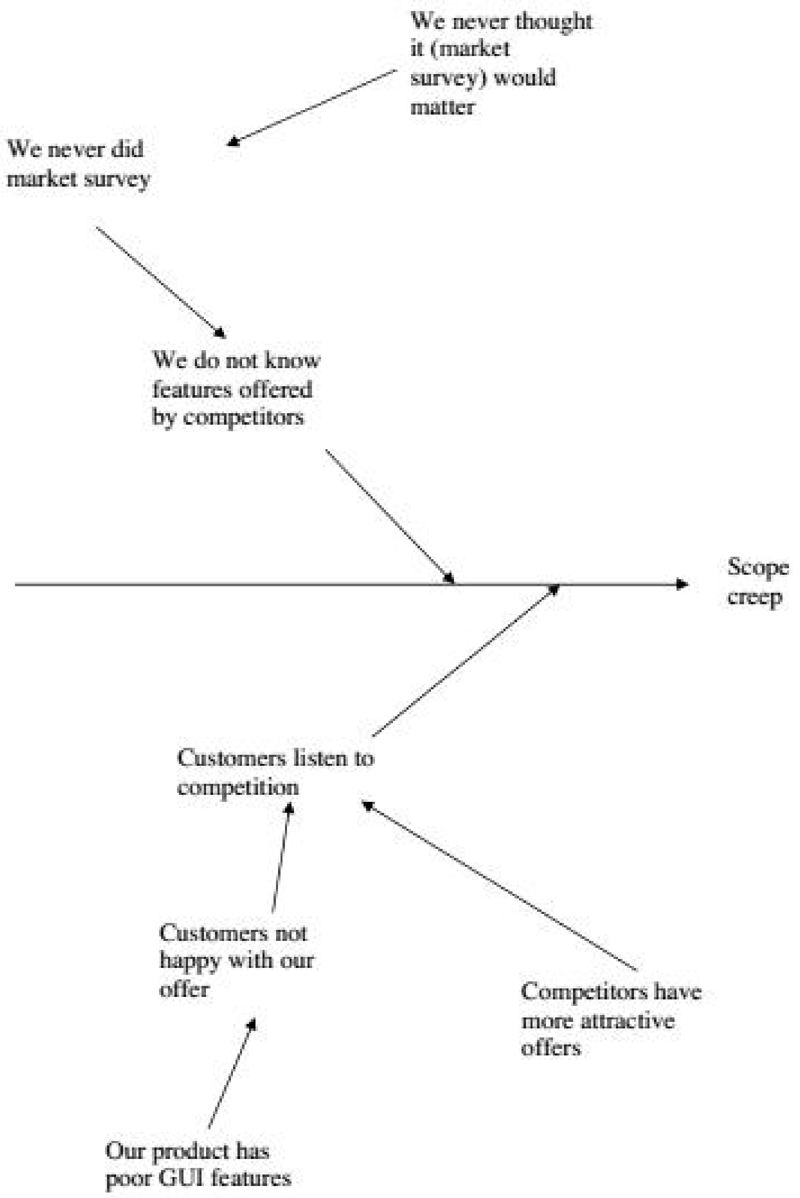


Second-Order Analysis: *Causal Analysis*

Risk: Scope Creep

1. **Cause:** Customer listens to competitors
    1.1 **Sub Cause:** Customers are not happy with our offer.
        1.1.1 **Root Cause:** Our product has poor GUI features
    1.2 **Sub Cause**: Competitors have more attractive offers.
        1.2.1 **Root Cause:** No idea

2. **Cause:** We do not know features offered by competitors
    2.1 **Sub Cause:** We never did market survey.
        2.1.1 **Root Cause:** We never thought it would matter


We never thought it (market survey) would matter
We never did market survey
We do not know features offered by competitors
Scope creep
Customers listen to competition
Customers not happy with our offer
Competitors have more attractive offers
Our product has poor GUI features

Ownerless Risks

- It is possible that the risk log does not contain the risk owner’s name.
- That is because nobody owned the risk, or was willing to own it.
- Absence of risk owners is equivalent, in effect, to absence of process owners.
- This issue must be “escalated” to higher management.
- Analysis of ownerless risks is not a profitable endeavor.

Risk Response Plans

Risk response is the process of controlling identified risks. Risk response is a planning and decision making process whereby stakeholders decide how to deal with each risk.

Negative:

- **Avoid:** Change your strategy or plans to avoid the risk or removing route cause.
- **Mitigate**: Take action to reduce the risk by reducing chance or impact.
- **Transfer**: Change the owner of risk.

Positive:

- **Share:** Distributing the risk across multiple partners, teams or projects.
- **Enhance:** Enhancement is an action that is taken to increase the chance of the risk occurring.
- **Exploit**: Exploiting a risk is to make use of resources that become available if the risk occurs. For example, if a task finishes early, you plan to reassign the resource to more work.

- **Accept**: Decide to take the risk. (Active, Passive)
- **Contingency:** Making plans to handle the risk if it occurs (Plan B).

Positive Risk Response Example

Customer offered *20,000$ bonus* if the program coding is completed two months earlier than planned.

Exploit: Allocate a Senior Programmer

Enhance: Train your Programmer

Share: Contract the program coding

Accept: Do Nothing

Negative Risk Response Example

Adventurous trip to go swim with sharks and take exotic photos, deadly *shark attack* has been identified as main threat for this trip.

Avoid: Rent a metal cage

Mitigate: User shark baits

Transfer: Hire a professional

Accept: Take a spear gun or doing nothing

	Risk Identification	Risk Analysis	Risk Response Plan	Risk Monitoring and Control
Inputs	✓ Project Charter ✓ Project Scope Statement ✓ Project Plan ✓ Historical Information ✓ Lessons Learned	✓ Identified Risks ✓ Work Performance information	✓ Prioritized Risks ✓ Project Plan	✓ Work Performance ✓ Change Requests ✓ Project Plan ✓ Ongoing Risk Analysis
Tools & Technologies	✓ TYPE I ✓ Intuitive ✓ Mind Mapping ✓ Brainstorming ✓ Analogy ✓ Out of Box ✓ History Based ✓ Top Ten Risks ✓ Checklist ✓ Questionnaires ✓ TYPE II (Formal)	✓ First Order Analysis ✓ Risk Screening ✓ Quadrant Map ✓ Top Ten Risk List ✓ Risk Distribution ✓ Internal-External ✓ Project – Product – Process ✓ Second Order Analysis ✓ Time and Causal Analysis ✓ Process and Performance Area Map	✓ Negative ✓ Avoid ✓ Transfer ✓ Mitigate ✓ Positive ✓ Share ✓ Enhance ✓ Exploit ✓ Accept (Active, Passive) ✓ Contingency Plan	✓ Risk Reassessment ✓ Risk/Project audits ✓ Variance and Trend analysis ✓ Performance measurement ✓ Reserve management
Output	✓ Identified Risks ✓ Project Plan Updates	✓ Prioritized Risks	✓ Risk Response Plan ✓ Contingency Reserve ✓ Project Plan Updates	✓ Corrective actions ✓ Workaround plans ✓ Project plan updates ✓ Update Risk Response Plan ✓ Lessons learned

#	Date	Risk	Probability of Occurrence (H/M/L)	Impact (H/M/L)	Expected Value (H/M/L)	Response Actions Action By – Target Date	Status
1	04/15/18	**Vendor may not deliver application software on time**					
2	04/15/18	**Subject matter experts may not be available on dates planned**					
3	04/15/18	**Snowstorm may prevent cutover team from working on site**					
4	04/15/18	**Server capacity may not support the planned number of users**					
5	04/15/18	**Client may change requirements causing delay in cutover**					

#	Date	Risk	Probability of Occurrence (H/M/L)	Impact (H/M/L)	Expected Value (H/M/L)	Response Actions Action By – Target Date	Status
1	04/15/18	**Vendor may not deliver application software on time**	**H**	**H**	**H**		
2	04/15/18	**Subject matter experts may not be available on dates planned**	**L**	**L**	**L**		
3	04/15/18	**Snowstorm may prevent cutover team from working on site**	**L**	**H**	**M**		
4	04/15/18	**Server capacity may not support the planned number of users**	**M**	**M**	**M**		
5	04/15/18	**Client may change requirements causing delay in cutover**	**M**	**H**	**H**		

#	Date	Risk	Probability of Occurrence (H/M/L)	Impact (H/M/L)	Expected Value (H/M/L)	Response Actions Action By – Target Date	Status
1	04/15/18	Vendor may not deliver application software on time	H	H	H	Establish a penalty clause in the contract with the vendor . JR – 4/18/18	
2	04/15/18	Subject matter experts may not be available on dates planned	L	L	L	(No need to address since Expected Value is "Low")	
3	04/15/18	Snowstorm may prevent cutover team from working on site	L	H	M	Arrange for key team members to stay in a nearby hotel. BD – 4/20/18	
4	04/15/18	Server capacity may not support the planned number of users	M	M	M	Arrange for extra server capacity to be installed JR – 4/21/18	
5	04/15/18	Client may change requirements causing delay in cutover	M	H	H	Establish a "freeze" date, with any changes applied to a future release LK – 4/22/18	

Quality Audits

"A systematic and independent examination to determine whether quality activities and related results comply with planned arrangements, and whether these arrangements are implemented effectively and are suitable to achieve objectives"

GOAL: To collect objective evidence to permit an informed judgment about the status of the systems or product being audited

Basic Types of Quality Audits

- **Internal (First Party, Self):** This type includes audits by company employees, consultants and contractors to its own company.

- **External (Second Party, Third Party):**

i. **Supplier Audit (Second Party):**

   a. Customer employee(s) audit your company or
   b. Your employee(s) audit a company which supplies your company with a product or service

ii. **Independent Organization(Third Party Audit)**

   a. A customer wants an audit of your company

Audit Sub-Types

- Compliance (do we comply with the standard)

Example: Desk audit of high level systems

- System (the theory)

Example: Audit of Document Control

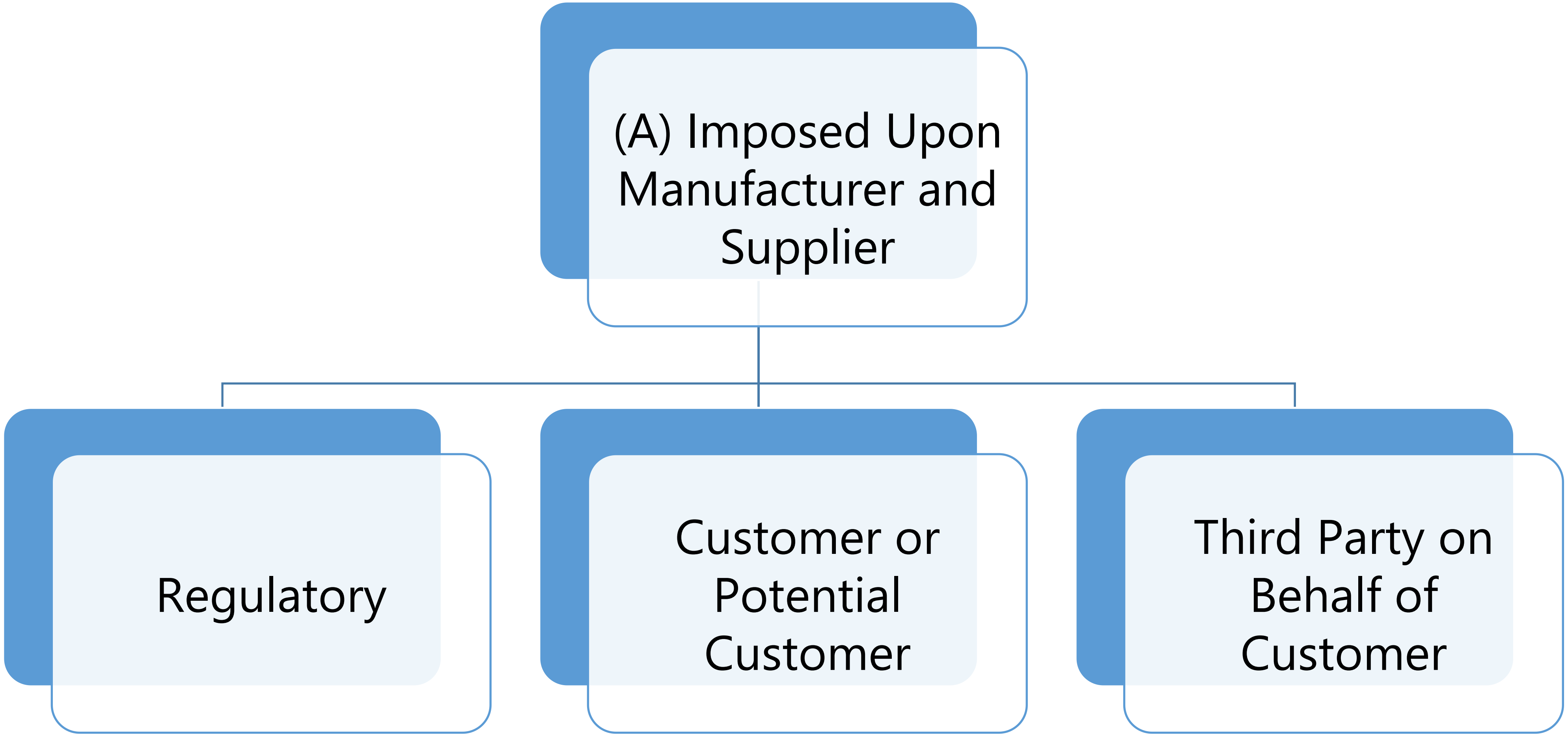
- Process (the practice)

Example: Audit of any process (manufacturing)

- Product (the result)

Example: Audit of finished products to fulfill technical specifications

Who Perform an Audit



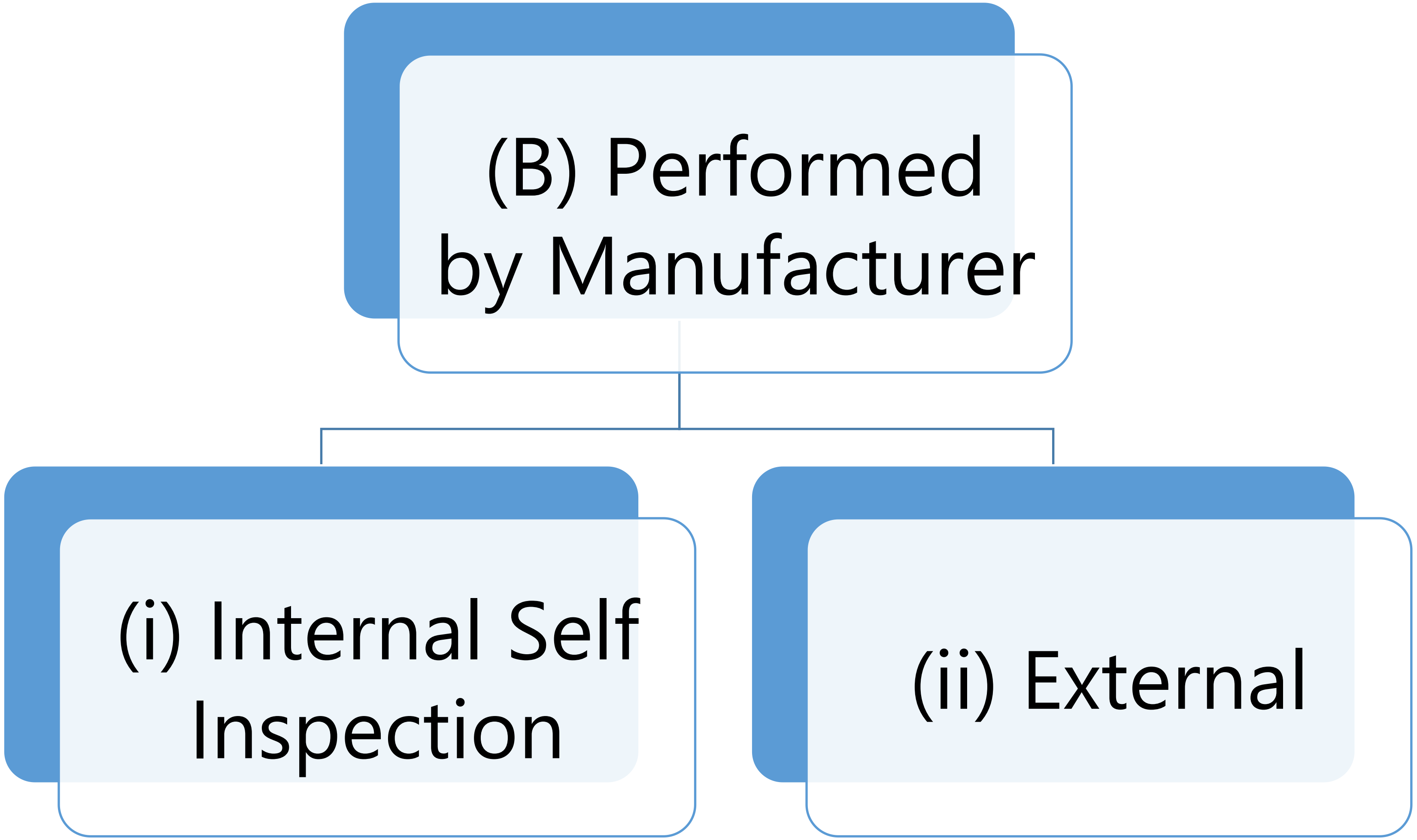
(A) Imposed Upon Manufacturer and Supplier

Regulatory

Customer or Potential Customer

Third Party on Behalf of Customer

Who Perform an Audit



(B) Performed by Manufacturer

(i) Internal Self Inspection

(ii) External

Reason of Quality Audit

INTERNAL:

in order to

- ✓ Determine the level of compliance
- ✓ Build confidence (hopefully) in the QA system
- ✓ Build interdepartmental trust, understanding, and communication
- ✓ Determine measures necessary to improve, e.g.,:
  - ▪ Premises, equipment, environment
  - ▪ Operations, actions, procedures
  - ▪ Personnel/training
  - ▪ Provide a stimulus for improvement
  - ▪ Recommend corrective action **(CAPA)**
  - ▪ Monitor improvement

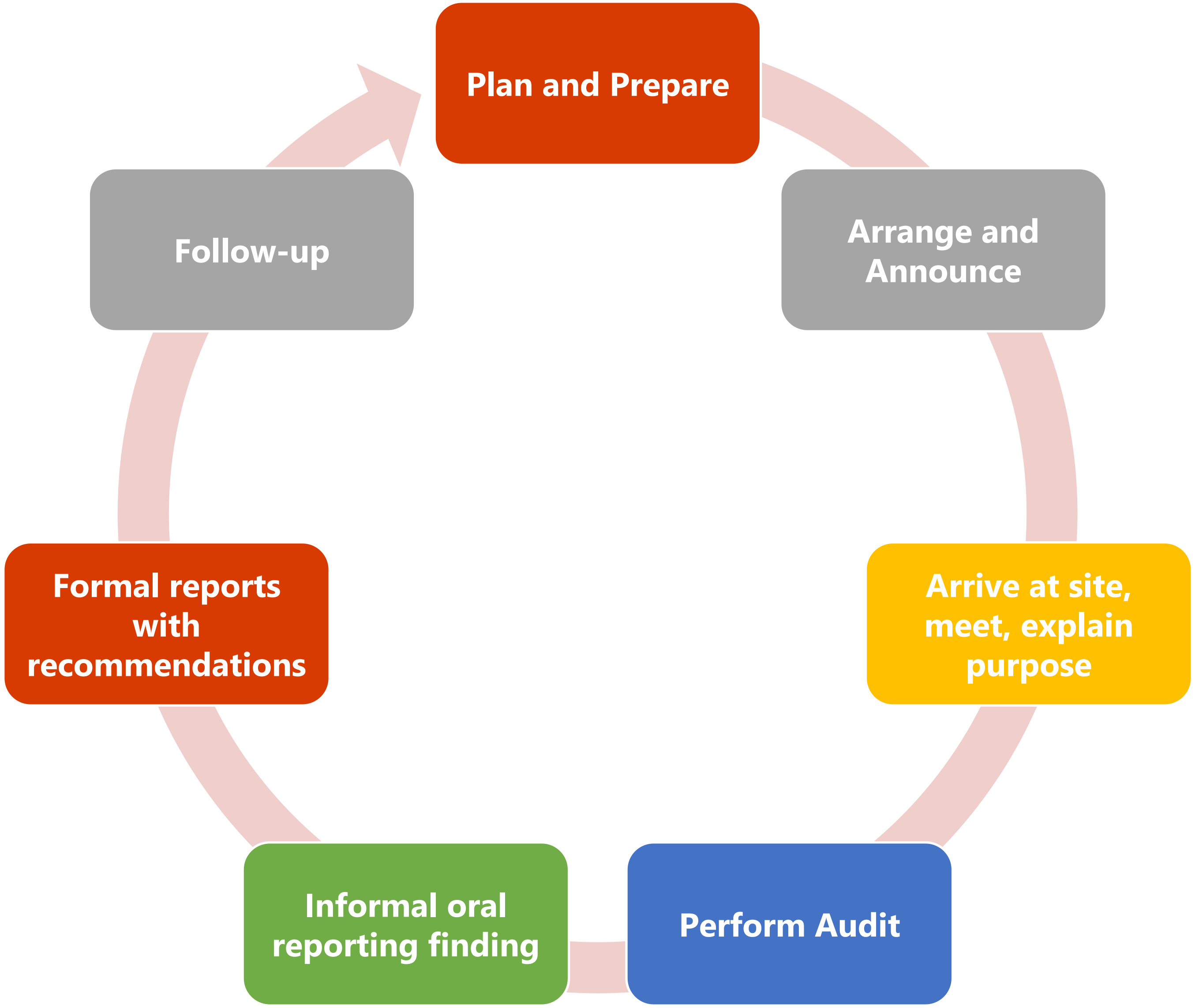
Reason of Quality Audit

EXTERNAL:

in order to

- Establish and monitor capability of supplier or contractor to deliver Goods and services that are fit for purpose (and on time, and in the quantity required)
- Build mutual confidence.
- Promote understanding and communication between the parties involved
- And in general, as listed for “internal”

Quality Audits Steps



Plan and Prepare

Arrange and Announce

Arrive at site, meet, explain purpose

Perform Audit

Informal oral reporting finding

Formal reports with recommendations

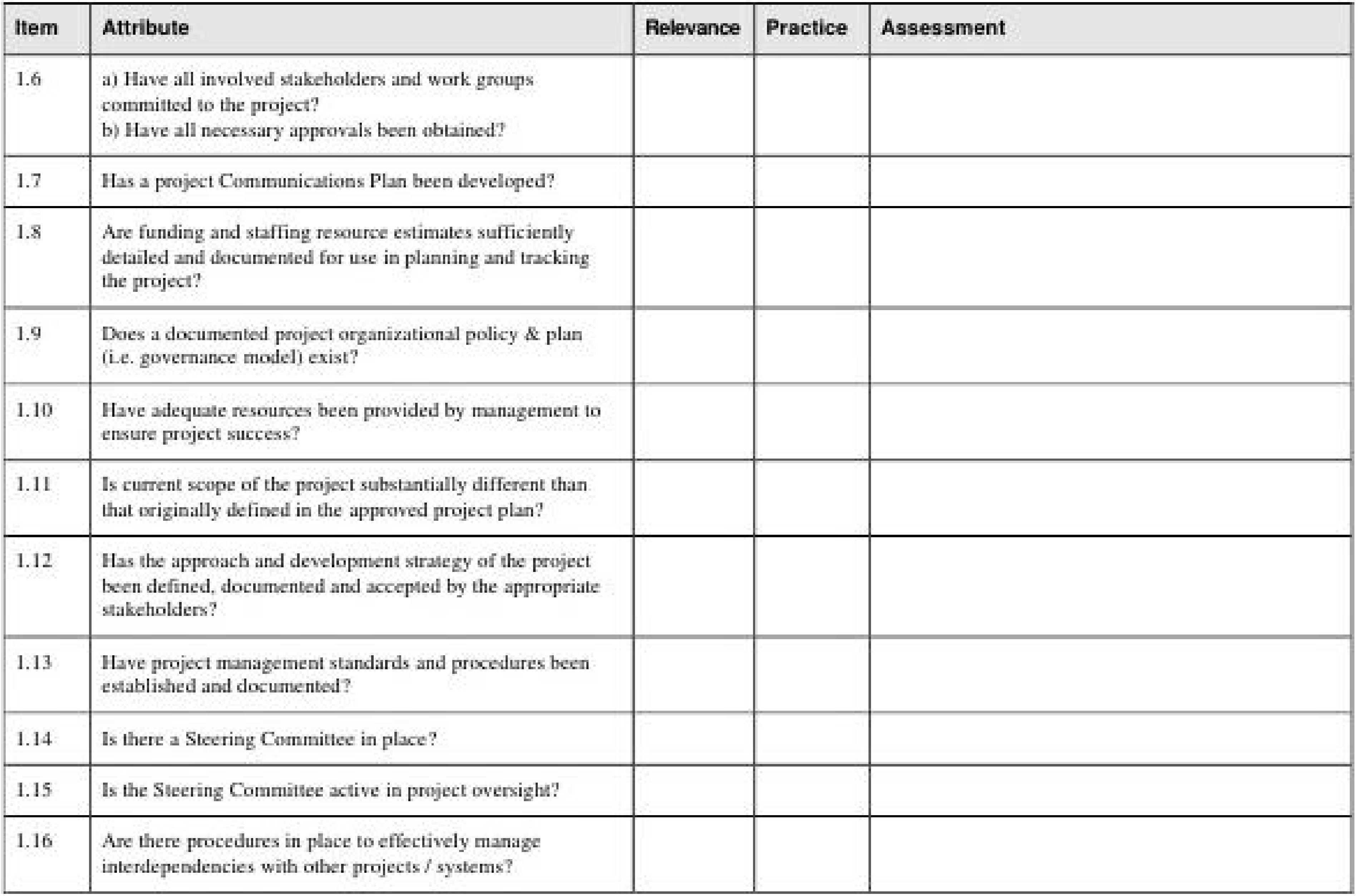
Follow-up

Process Audits

examination of

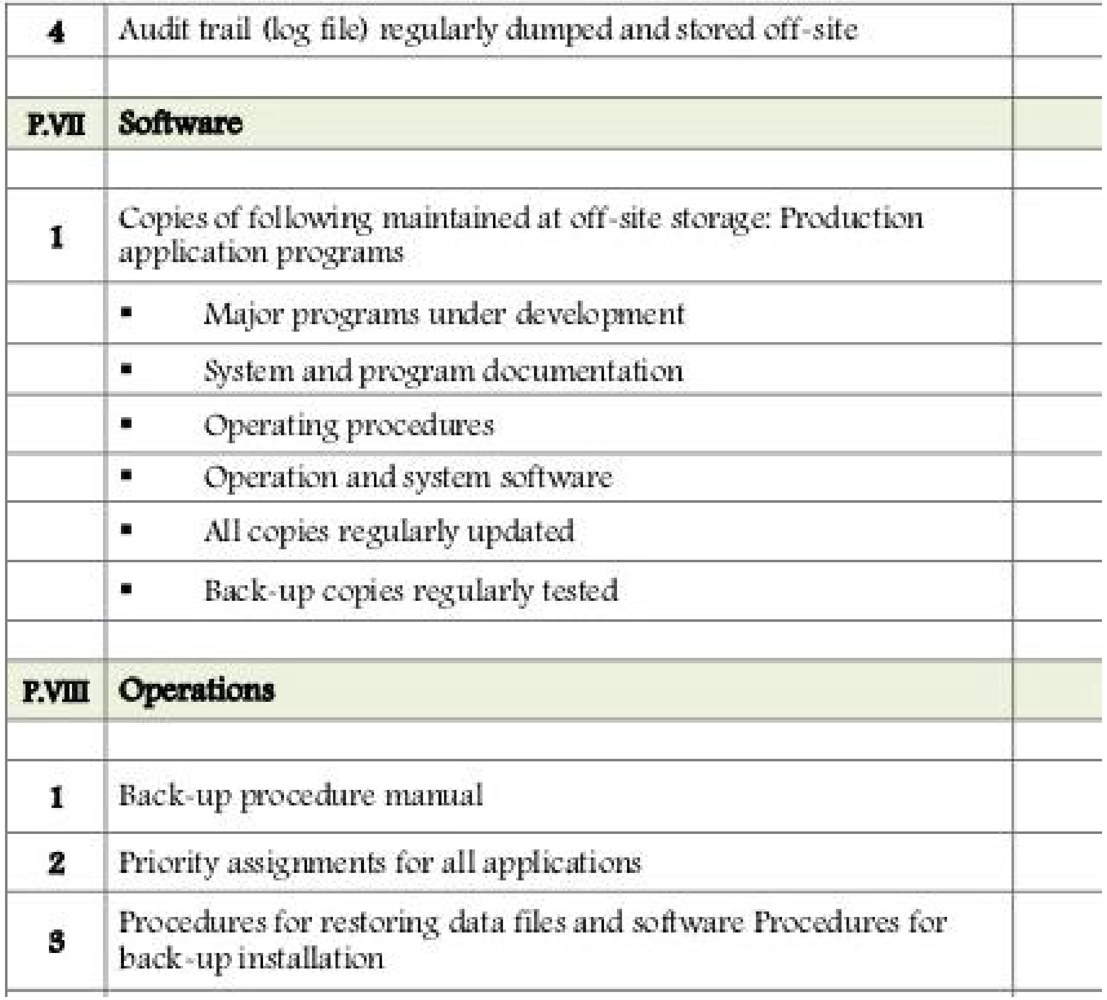
1. established methods
2. instructions
3. work flow for processes
4. maintenance programs for production equipment
5. material handling
6. housekeeping around the work area

Typical Checklist for Quality Audits

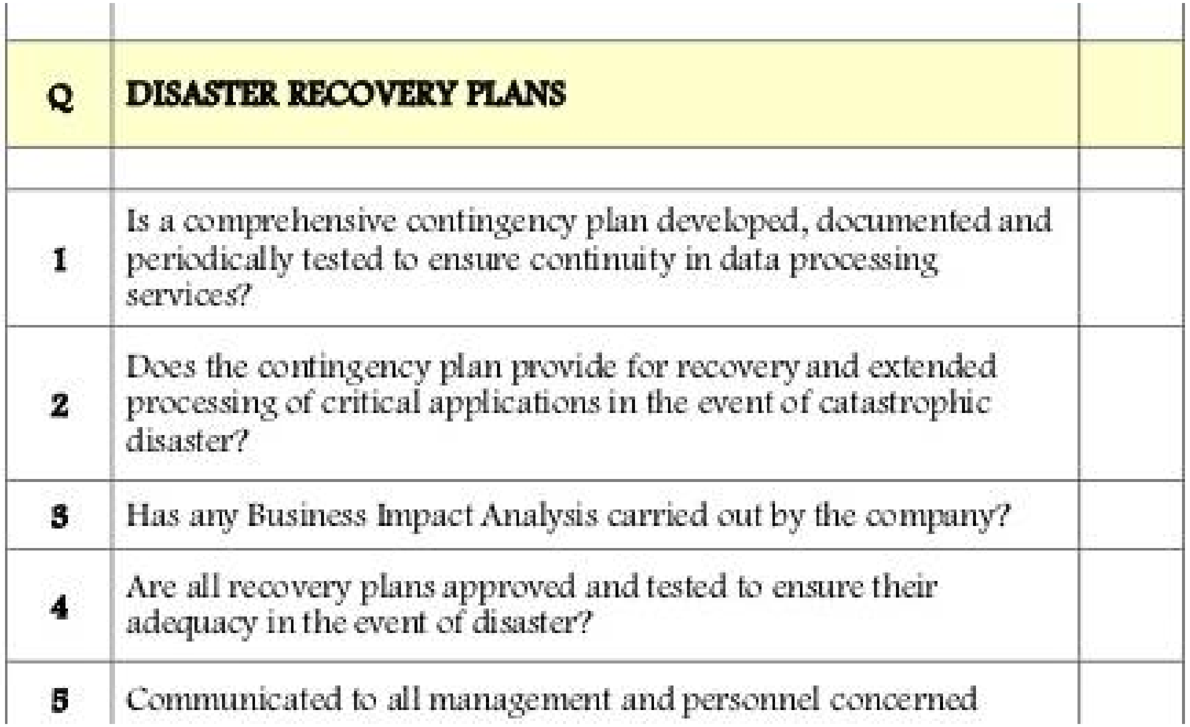


Item	Attribute	Relevance	Practice	Assessment
1.6	a) Have all involved stakeholders and work groups committed to the project? b) Have all necessary approvals been obtained?			
1.7	Has a project Communications Plan been developed?			
1.8	Are funding and staffing resource estimates sufficiently detailed and documented for use in planning and tracking the project?			
1.9	Does a documented project organizational policy & plan (i.e. governance model) exist?			
1.10	Have adequate resources been provided by management to ensure project success?			
1.11	Is current scope of the project substantially different than that originally defined in the approved project plan?			
1.12	Has the approach and development strategy of the project been defined, documented and accepted by the appropriate stakeholders?			
1.13	Have project management standards and procedures been established and documented?			
1.14	Is there a Steering Committee in place?			
1.15	Is the Steering Committee active in project oversight?			
1.16	Are there procedures in place to effectively manage interdependencies with other projects / systems?			

Typical Checklist for Quality Audits



4	Audit trail (log file) regularly dumped and stored off-site	
P.VII	**Software**	
1	Copies of following maintained at off-site storage: Production application programs	
	▪ Major programs under development	
	▪ System and program documentation	
	▪ Operating procedures	
	▪ Operation and system software	
	▪ All copies regularly updated	
	▪ Back-up copies regularly tested	
P.VIII	**Operations**	
1	Back-up procedure manual	
2	Priority assignments for all applications	
3	Procedures for restoring data files and software Procedures for back-up installation	



Q	**DISASTER RECOVERY PLANS**	
1	Is a comprehensive contingency plan developed, documented and periodically tested to ensure continuity in data processing services?	
2	Does the contingency plan provide for recovery and extended processing of critical applications in the event of catastrophic disaster?	
3	Has any Business Impact Analysis carried out by the company?	
4	Are all recovery plans approved and tested to ensure their adequacy in the event of disaster?	
5	Communicated to all management and personnel concerned	

Any Question?

End!