SGS North America - Knowledge Solutions

Risk Assessment & Root Cause Analysis

Sabrina Ippolito | April 2023

Speaker

Sabrina Ippolito
Lead Auditor
Sabrina_ippolito@me.com

Sabrina is a classically trained Biochemist and Certified Lead Auditor that ensures organizations maintain compliance in a realm of different industries, certifications and standards spanning pharmaceutical, cosmetics, and general manufacturing. She has directed, overseen, and improved several quality systems to reduce deficiencies and increase product flow across the US and Canada. She is affiliated with the professional order of Chemists of Quebec (l'OCQ) and the American Society for Quality (ASQ).

Agenda

Part 1 – Risk Management

- A brief overview of risk management
- How to analyze risk and the interested parties involved in analyzing risk
- Examples of tools that can be used

Part 2 – Root Cause Analysis (RCA)

- A brief overview of root cause analysis
- How to perform an RCA and the interested parties involved in the activity
- Examples of tools that can be used
- Q&A

Part 1: Risk Management

Introduction

What is Risk Management?

- Risk management is the ***process*** of ***identifying***, ***assessing/evaluating, prioritizing*** and ***controlling*** the probability and impact of unfortunate evets relating to financial, legal, strategic and security risks to an organization's capital and earnings.
- Through risk management, organizations can equally maximize the realization of opportunities.
- While positive deviations arising from a risk can provide an opportunity, not all positive effects of risk result in opportunities.

Poll Question #1

Is Risk management proactively embedded in your daily operations, or is it treated as a separate process periodically (e.g. once) per year?

Possible answers:

A) embedded in daily operations;

B) treated as a separate process periodically

Risk-based Thinking

- The 2015 version of ISO 9001 makes risk-based thinking more explicit and incorporates it in requirements for the establishment, implementation, maintenance and continual improvement of the QMS.
- It is up to the organization to develop a more extensive risk-based approach than is required by ISO 9001:2015. ISO 31000 provides guidelines on formal risk management which can be appropriate in specific organizational contexts.
- Not all the processes of the QMS contain the same level of risk in terms of the organization's ability to meet its objectives, and the consequences of process, product, service or system nonconformities are not the same for all organizations. For some organizations, the consequences of delivering nonconforming products and services can result in minor inconvenience to the customer. Still, for others, the consequences can be far-reaching and even fatal. "Risk-based thinking," therefore, means considering risk ***qualitatively*** (and ***quantitatively***) depending on the organization's context when defining the rigour and degree of formality needed to plan and control the QMS, as well as its component processes and activities.

Let Us Consider the Standard – ISO 9001:2015 – Clause 6: Planning

Actions to address risks and opportunities:

- One of the key purposes of a QMS is to act as a preventive tool.
- ISO 9001:2015 does not have a separate clause or sub-clause titled 'preventive action'.
- The concept of preventive action is expressed through a risk-based approach to formulating QMS requirements.
- Although risks and opportunities must be determined and addressed, there is **no requirement for formal risk management or a documented risk management process.**

Let Us Consider the Standard – ISO 9001:2015

6.1 – Actions to address risks and opportunities

- **6.1.1** – When planning for the QMS, the organization shall consider the issues referred to in **4.1** and the requirements referred to in **4.2** and determine the risks and opportunities that need to be addressed to:
  - a) give assurance that the QMS can achieve its intended result(s);
  - b) enhance desirable effects;
  - c) prevent, or reduce, undesired effects;
  - d) achieve continual improvement.

Clause 4 – Context of the Organization

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and its strategic direction and that affect its ability to achieve the intended result(s) of its QMS.

The organization shall monitor and review information about these external and internal issues.

4.2 Understanding the needs and expectations of interested parties

Due to their effect or potential effect on the organization's ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements, the organization shall determine:

a) the interested parties that are relevant to the QMS;

b) the requirements of these interested parties relevant to the QMS.

The organization shall monitor and review information about these interested parties and their relevant requirements.

Let Us Consider the Standard – ISO 9001:2015

6.1 – Actions to address risks and opportunities

- **6.1.2** The organization shall plan:

  a) actions to address these risks and opportunities;

  b) how to:

  1) integrate and implement the actions into its QMS processes (see **4.4**);

  2) evaluate the effectiveness of these actions.

Actions taken to address risks and opportunities must be proportionate to the potential impact on the conformity of products and services.

Clause 4 – Context of the Organization

4.4 Quality management system and its processes

4.4.1 The organization shall establish, implement, maintain and continually improve a QMS, including the processes needed and their interactions, per the requirements of ISO 9001:2015.

The organization shall determine the processes needed for the QMS and their application throughout the organization and shall:

a) determine the inputs required and the outputs expected from these processes;

b) determine the sequence and interaction of these processes;

c) determine and apply the criteria and methods (including monitoring, measurements and related performance indicators) needed to ensure the effective operation and control of these processes;

d) determine the resources needed for these processes and ensure their availability;

e) assign the responsibilities and authorities for these processes;

f) **address the risks and opportunities as determined in accordance with the requirements of 6.1**;

g) evaluate these processes and implement any changes needed to ensure that these processes achieve their intended results;

h) improve the processes and the quality management system.

Poll Question #2

Within your organization, is risk management a process conducted solely by mid/senior level leadership?

Possible answers:

A) **Yes;**

B) **No;**

C) **I’m unsure**

Putting it all Together

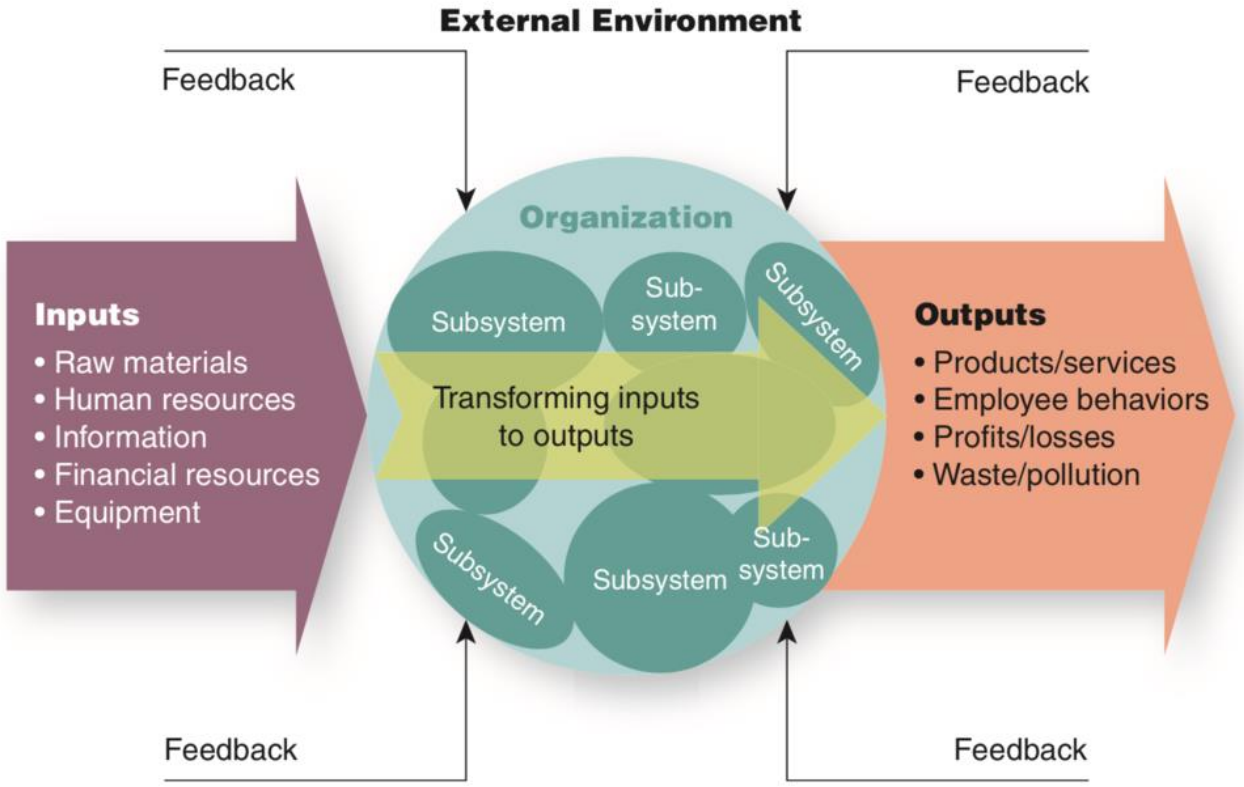
When ***identifying*** and ***evaluating*** risk, involve pertinent individuals to partake in the exercise. Their expertise is invaluable and paints a better picture of the situation, in comparison to generic information!

Consider identify and evaluate risk relating to:

1. **the organization;**
2. **interested parties (internal/ external);**
3. **based on processes.**

NB: did you consider any legal, regulatory, environmental or any other requirements?

1. The Organization



2. Interested Parties

INTERESTED PARTIES

Interested Parties	Interest / Concerns / Needs / Expectations	Strengths, Weaknesses, Opportunities, Threats	Control / Verification	Potential Impact / Risk
Internal				
Management	Knowledgeable; Industry experience; Grow sales, Gross Profit & maintain profitability. Offering new products and services (i.e. Doepker).	**Strength:** Knowledge, flexibility of adaptation to changes **Weakness:** All functions other than Production monitored by 1 person. **Opportunity:** Enhance employee responsibilities (i.e. Cross Training) **Threat:** Business slow down – USD, impacted, aggressive pricing wars.	Internal audits, management review.	Lack of direction and fluidity of the qulity management system.
Employees		**Strength:** **Weakness:** **Opportunity:** **Threat:**		
External				
Clients		**Strength:** **Weakness:** **Opportunity:** **Threat:**		
Suppliers / Sub-contractors		**Strength:** **Weakness:** **Opportunity:** **Threat:**		
Regulatory Bodies		**Strength:** **Weakness:** **Opportunity:** **Threat:**		
Financial Institution		**Strength:** **Weakness:** **Opportunity:** **Threat:**		

3. Processes

IDENTIFICATION OF RISK RELATED TO INTERNAL PROCESS ACTIVITIES

Process	*Input/Output*	*Risk/Opportunity*	*Performance Monitoring*	*Responsibility*
Sales / Marketing	**Input:** Leads, market intelligence, customer information.	**Risks:** - Loss of clients, - Low profit margins, - Loss of large/potential opportunities.	Gross Margin on Sales, Sales performance of clients, Various Win Rates in Performance Indicators, Sales objectives.	Sales (VP Sales)
	Output: Customer Relationship, Business Development, Opportunities, Orders.	**Opportunities:** - Contribution to good reputation, - Contribute to clients, - Increase number of orders.		
Quote	**Input:**	**Risks:**		Sales (VPs)
	Output:	**Opportunities:**		
Order Processing / Scheduling / Planning	**Input:**	**Risks:**		Sales / Operations (VP Sales, VP Ops.)
	Output:	**Opportunities:**		
Servicing	**Input:**	**Risks:**		Production / QC (Service Manager)
	Output:	**Opportunities:**		
Purchasing	**Input:**	**Risks:**		Purchasing (Purchasing Manager)
	Output:	**Opportunities:**		
Receiving	**Input:**	**Risks:**		Receiving (Receiving Manager)
	Output:	**Opportunities:**		
Shipping	**Input:**	**Risks:**		Shipping (Receiving Manager | Sales Person | Service Manager)
	Output:	**Opportunities:**		
Invoicing	**Input:**	**Risks:**		Financial accounting (VP)
	Output:	**Opportunities:**		
Leadership / Management	**Input:**	**Risks:**		Management (VP)
	Output:	**Opportunities:**		

Different Ways of Assessing Risk

Qualitatively

Simple Risk Matrix

	Consequences		
Likelihood	Minor	Moderate	Major
Likely			
Possible			
Unlikely			

Risk Treatment Key

Intolerable Risk Level. Immediate action required
Tolerable Risk Level. Risks must be reduced so far as is practicable.
Broadly Acceptable Risk Level. Monitor and further reduce where practicable.

Different Ways of Assessing Risk

Quantitative

RISK ANALYSIS - MATRIX & LEGENDS

	PROBABILITY OF OCCURRENCE				
IMPACT	**Remote (1)** Very unlikely to occur (<5% of happening)	**Unlikely to occur (2)** 1) Event has never occurred to date. 2) Reoccurence <= 1 event / 10 years 3) Has not been observed in past but still a possibility (5 - 9% chance of happening)	**Moderate (3)** May occur 1) Event has occurred in past 2) Reoccurence <= 1 event / 5 years (10 - 50% chance of happening)	**Likely to occur (4)** 1) Infrequent event 2) Reoccurence <= 1 event / 1 year 3) Has been observed under similar circumstances (50 - 90% chance of happening)	**Highly likely to occur (5)** 1) Repetitive event 2) Reoccurence >= 1 event / 1 year 3) Frequent event during project 4) Frequent events under similar circumstances (>90% chance of happening)
Insignificant (1) Minor problem easily handled by normal day-to-day processes	1	2	3	4	5
Not Critical (2) Some disruption to operations i.e. damage equal up to **$5K**	2	4	6	8	10
Moderately Critical (3) Significant time / resources required i.e. damages may equal up to **$50K**	3	6	9	12	15
Critical (4) Operations severely damaged i.e. damages may equal up to **$100K**	4	8	12	16	20
Catastrophic (5) Business survival is at risk i.e. damage may equal to **$1M**	5	10	15	20	25

Legend	Probability	Impact
1	(<5%) Remote - Very unlikely to occur	Insignificant
2	[5 - 9%] Unlikely to occur	Not critical
3	[10 - 50%] Moderate - May occur	Moderately critical
4	[50 - 90%] Likely to occur	Critical
5	(>90%) Highly likely to occur	Catastrophic

Total RPN - (P x I	Priority	Corrective Action (CA) Required?
[15 - 25]	1	Yes - risk must be eliminated, otherwise reduced.
[08 - 12]	2	Yes - if judged necessary. A justification is required if CAR is not initiated.
[01 - 06]	3	No - No corrective Action required.

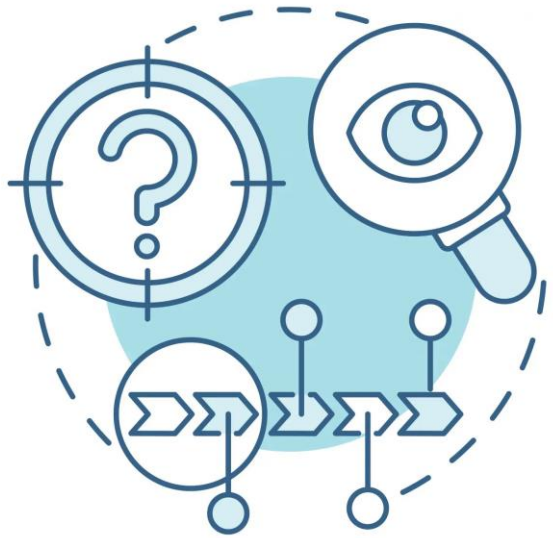
Analyzing Risk

RISK ANALYSIS

No.	Risk	Probability (P) [1 - 5]	Impact (I) [1 - 5]	TOTAL - RPN (PxI)	Corrective Action Required (Yes | No)	Corrective Action # *(or Justification why Corrective Action is not required)*	Due Date | Assigned to (Chaperone)	Status - Open | Closed
1	Strategic - Competitor coming on to the market	5	5	25	Yes	23-001 Maintain customer relationship, re-assess pricing strategy, be better prepared for next opportunity	On-going | I. MIURA	Open
2	Compliance - responding to new health and safety legislation	2	4	8	Yes	23-002 Review Policies and implement procedures.	On-going | I. MIURA	Open
3	Financial - non-payment by a customer	1	3	3	No	N/A	N/A	N/A
4	Financial - increased interest charges on a business loan							
5	Operational - the breakdown of key equipment							
6	Operational - the theft of key equipment/documents etc.							
7	Environmental - natural disasters							
8	Employee risk management - maintaining sufficient staff numbers and cover							
9	Employee risk management - employee safety							
10	Employee risk management - employee up-to-date skills							
11	Political and economic instability in any foreign market where goods are exported							
12	Commercial risks - failure of key suppliers							
13	Commercial risks - failure of key customers							
15	Insufficient customer support							

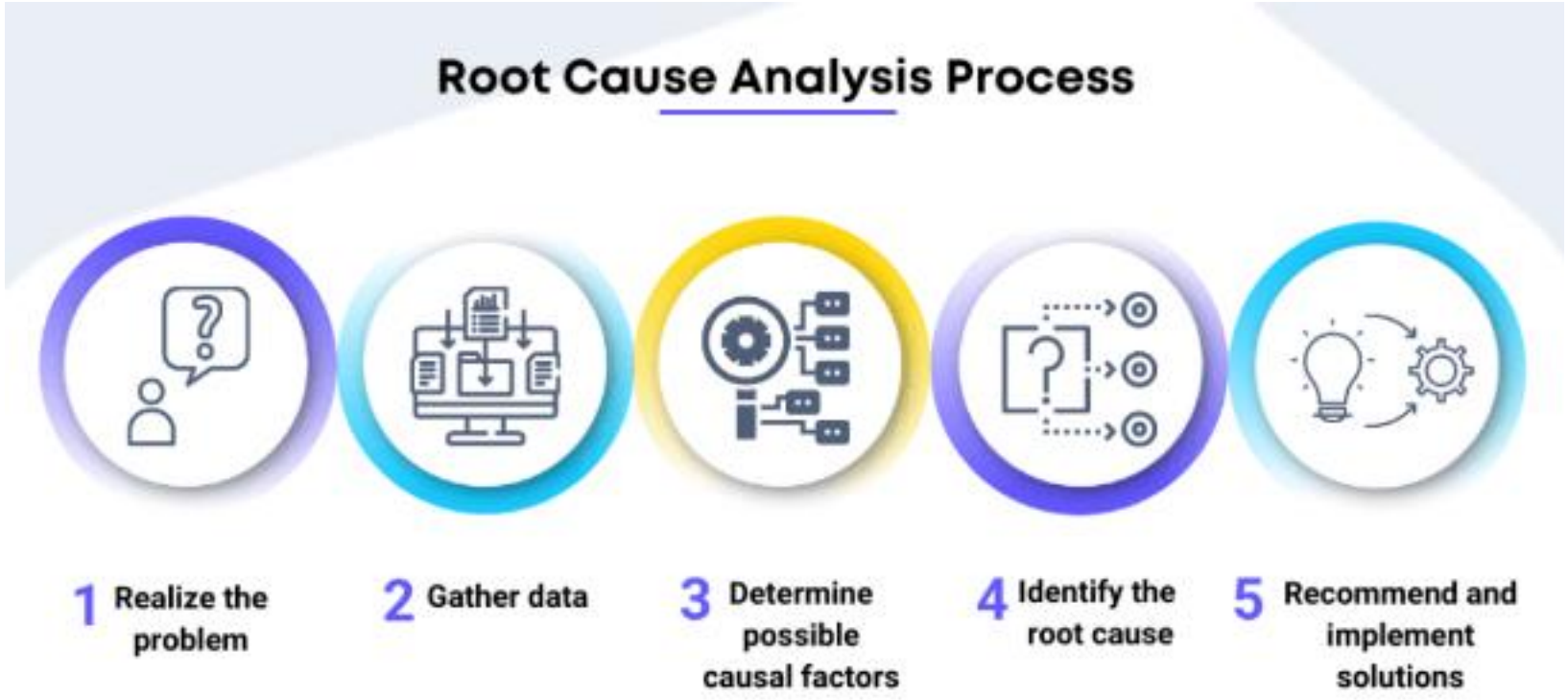
Part 2 – Root Cause Analysis (RCA)

Root Cause Analysis

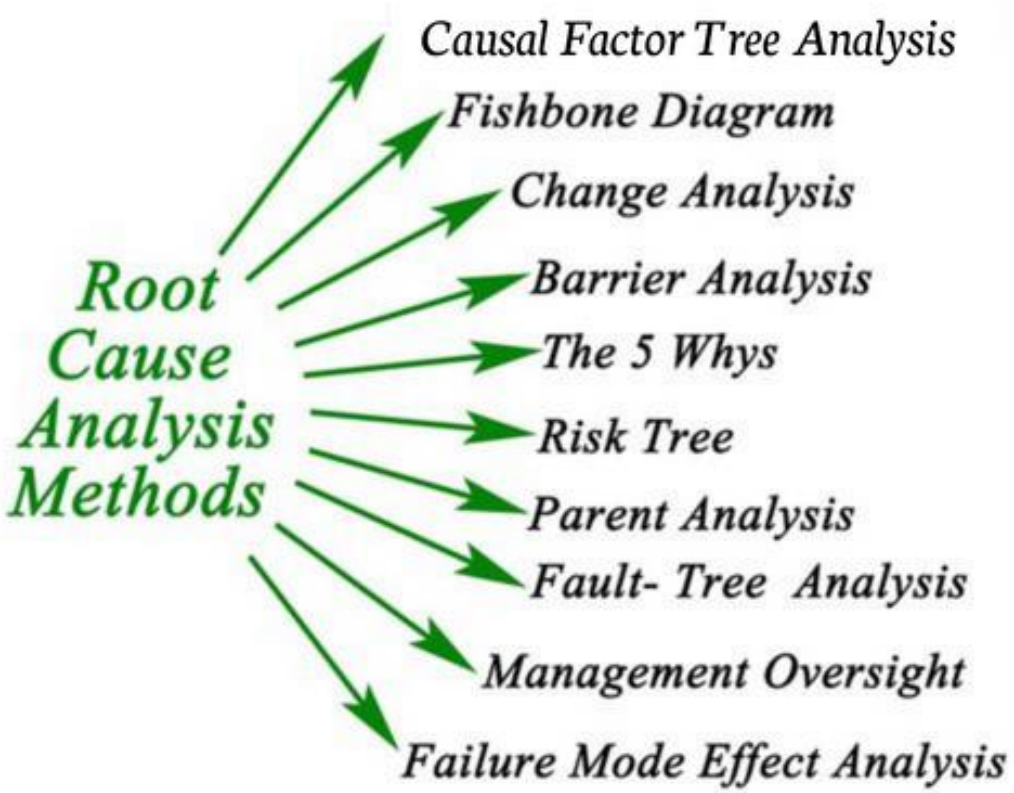


- A root cause analysis is used to determine why a nonconformity or an incident occurred.
- Most root cause analyses conducted by organizations are flawed—only looking at superficial reasons (e.g. apathy, human error, another section was responsible, head office made me do it…).
- Approximately 90% are management system deficiencies.

Let us Consider the Process



Possible Tools



Poll Question #3

What tool does your organization utilize to analyze the root cause of an undesirable event?

Possible answers:

A) **Fishbone Diagram;**

B) **The 5 Whys;**

C) **Risk Tree;**

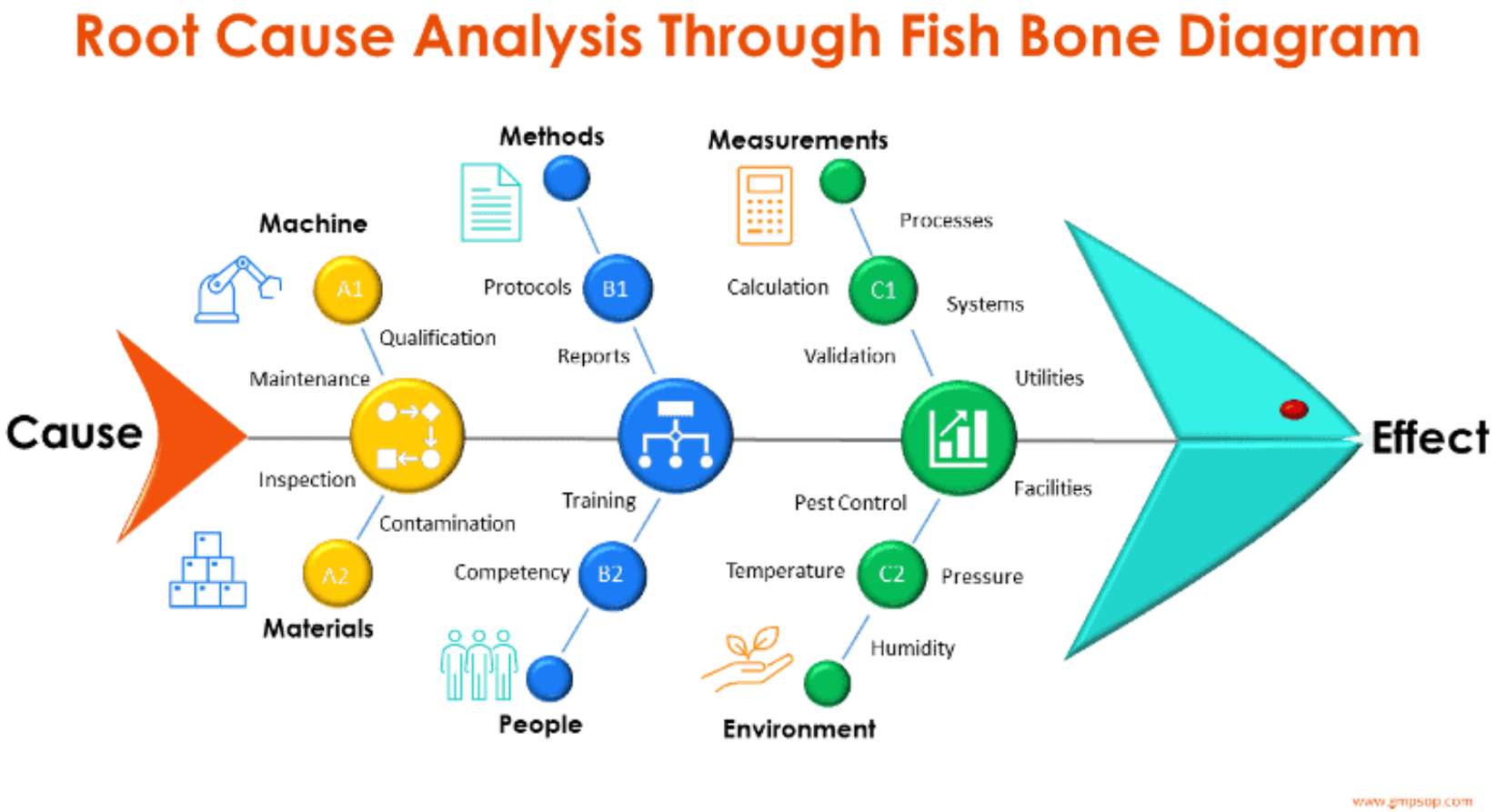
D) **FMEA;**

E) **The organization leaves it up to the employees to determine the method they are most comfortable using;**

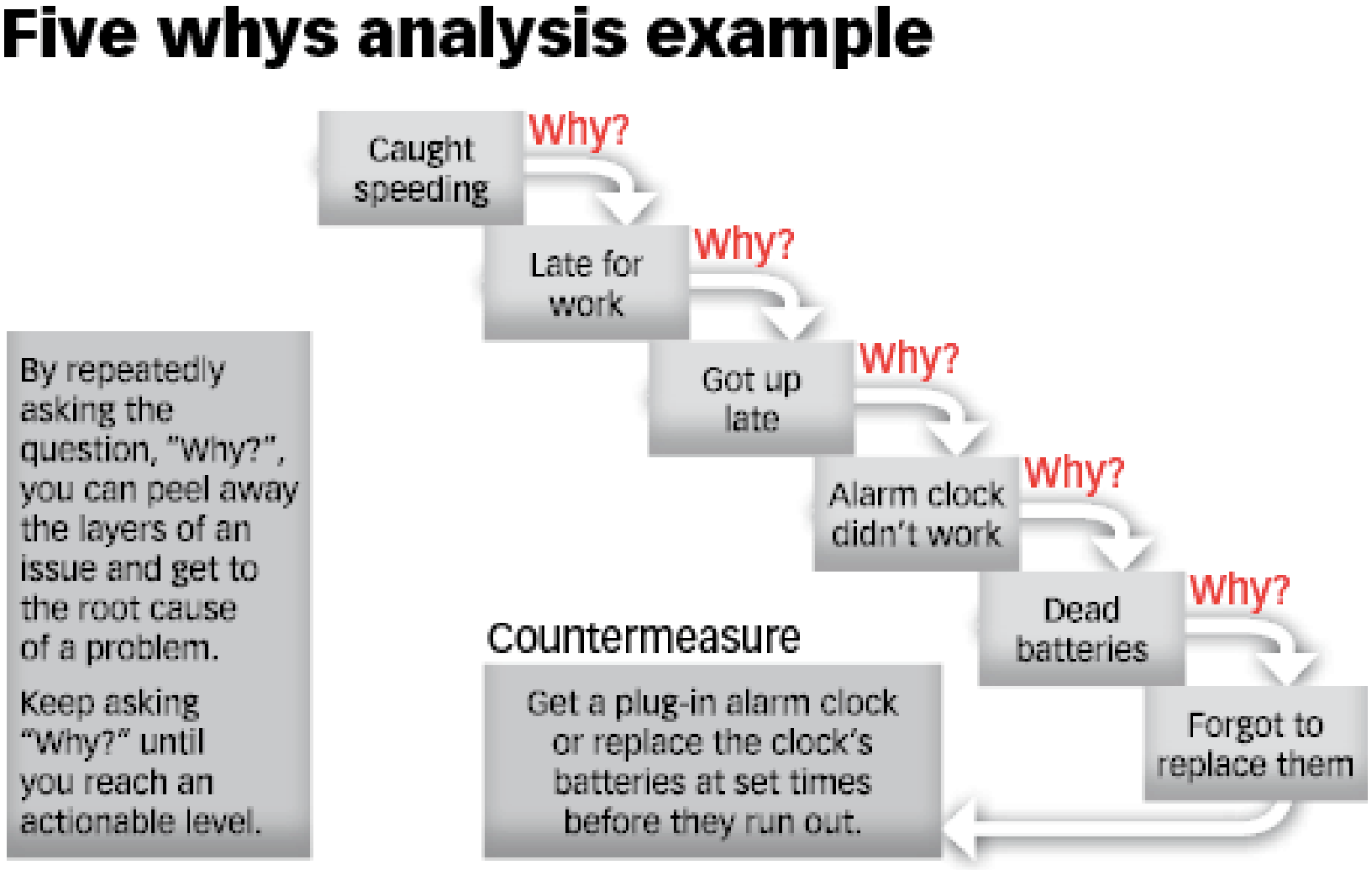
F) **We currently do not carry out the root cause analysis process;**

G) **I am unaware**

Tools – Fish Bone Diagram



Tools – 5 Whys


Five whys analysis example
Caught speeding
Why?
Late for work
Why?
Got up late
Why?
Alarm clock didn't work
Why?
Dead batteries
Why?
Forgot to replace them
By repeatedly asking the question, "Why?", you can peel away the layers of an issue and get to the root cause of a problem.
Keep asking "Why?" until you reach an actionable level.
Countermeasure
Get a plug-in alarm clock or replace the clock's batteries at set times before they run out.

Tools – FMEA
(Failure, Mode & Effects Analysis)

Process Step	Potential Failure Mode	Potential Failure Effect	SEV[1]	Potential Causes	OCC[2]	Current Process Controls	DET[3]	RPN[4]	Action Recommended
What is the step?	In what ways can the step go wrong?	What is the impact on the customer if the failure mode is not prevented or corrected?	How severe is the effect on the customer?	What causes the step to go wrong (i.e., how could the failure mode occur)?	How frequently is the cause likely to occur?	What are the existing controls that either prevent the failure mode from occurring or detect it should it occur?	How probable is detection of the failure mode or its cause?	Risk priority number calculated as SEV x OCC x DET	What are the actions for reducing the occurrence of the cause or for improving its detection? Provide actions on all high RPNs and on severity ratings of 9 or 10.
ATM Pin Authentication	Unauthorized access	• Unauthorized cash withdrawal • Very dissatisfied customer	8	Lost or stolen ATM card	3	Block ATM card after three failed authentication attempts	3	72	
	Authentication failure	Annoyed customer	3	Network failure	5	Install load balancer to distribute workload across network links	5	75	
Dispense Cash	Cash not disbursed	Dissatisfied customer	7	ATM out of cash	7	Internal alert of low cash in ATM	4	196	Increase minimum cash threshold limit of heavily used ATMs to prevent out-of-cash instances
	Account debited but no cash disbursed	Very dissatisfied customer	8	• Transaction failure • Network issue	3	Install load balancer to distribute workload across network links	4	96	
	Extra cash dispensed	Bank loses money	8	• Bills stuck to each other • Bills stacked incorrectly	2	Verification while loading cash in ATM	3	48	

1. **Severity**: Severity of impact of failure event. It is scored on a scale of 1 to 10. A high score is assigned to high-impact events while a low score is assigned to low-impact events.
2. **Occurrence**: Frequency of occurrence of failure event. It is scored on a scale of 1 to 10. A high score is assigned to frequently occurring events while events with low occurrence are assigned a low score.
3. **Detection**: Ability of process control to detect the occurrence of failure events. It is scored on a scale of 1 to 10. A failure event that can be easily detected by the process control is assigned a low score while a high score is assigned to an inconspicuous event.
4. **Risk priority number**: The overall risk score of an event. It is calculated by multiplying the scores for severity, occurrence and detection. An event with a high RPN demands immediate attention while events with lower RPNs are less risky.

Table 1: Managing Operational Risk in Financial Services

Poll Question #4

Is RCA managed by one individual or one department, or is it a collaborative effort between departments within your organization?

Possible answers:

A) one individual or one department;

B) it is a collaborative effort between pertinent interested parties;

C) I'm unsure

Root Cause Analysis

Date:	CORRECTIVE ☐	COMPLAINT ☐	Request # (YY-###):
Department Affected:		Requested By:	
Customer/Supplier Complaint: →		Customer/Supplier Name:	
NC #'(s): →		Sub-contractor Name:	

SECTION 1: Description of the nonconformity/ risk:	Immediate Action:
Responsibility:	

SECTION 2: Risk Analysis:

Probability (P) =
Impact (I) =

Risk Priority Number (RPN = P x I) =

SECTION 3: Root Cause Analysis (i.e. 5 Why's, Fishbone Diagram etc.):

Completed By:

SECTION 4: Action Plan:	Assigned to:	Due Date:	Effective / Closure Date:
1.	1.	1.	1.
2.	2.	2.	2.
3.	3.	3.	3.
4.	4.	4.	4.

Projected Completion:

SECTION 5: Follow-Up:

Completed By:

SECTION 6: Risk Analysis:

Probability (P) =
Impact (I) =

Risk Priority Number (RPN = P x I) =

Authorised Closure: _____ Date: _____

How to Evaluate Effectiveness

- Review the Nonconformity description
- Review the Root cause
- Ensure that the corrective action proposed addresses the problem and the root cause
- Verify that the corrective action is implemented
- Verify that the corrective action has prevented the nonconformity – this may require a waiting period

Thank you!

Do you have any questions?

Email

- Sabrina_Ippolito@me.com

Web

- https://www.sgs.com/certification

Social

facebook.com/SGS/
twitter.com/sgsnorthamerica
linkedin.com/company/sgs