ROOT CAUSE ANALYSIS FOR CYBERSECURITY

AKZHAN AZTAUKEYEVA
MOLDIR ZHANSEIITOVA
ZHARAS YERGALI
TOGZHAN ANUAR
RAKHAT TASTYBAY

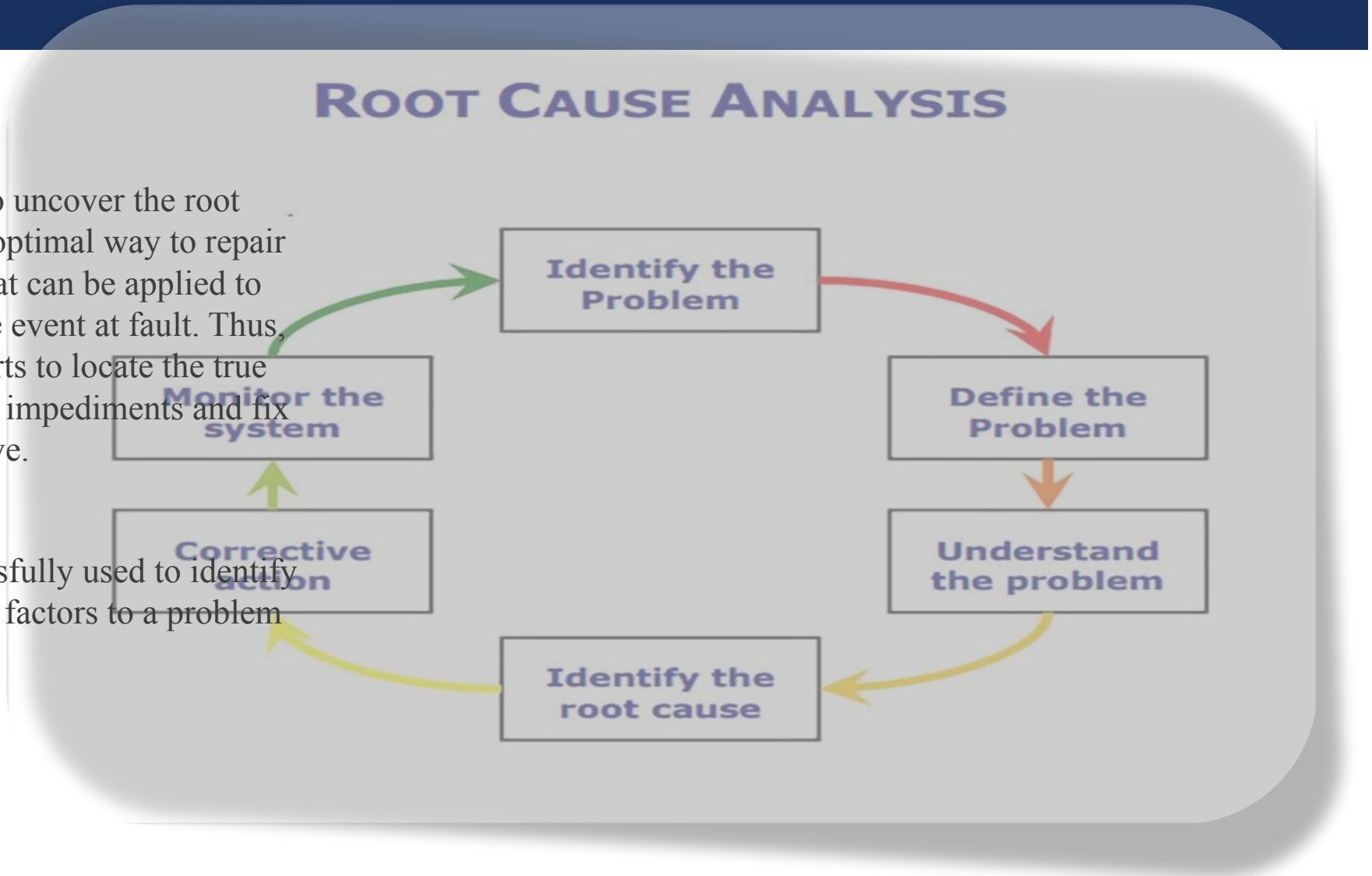
CONTENT

- Goals and objectives
- Characteristics of the state of knowledge
- Scientific methods
- Analysis of results
- Determining the scope of possible use of the results
- List of resources

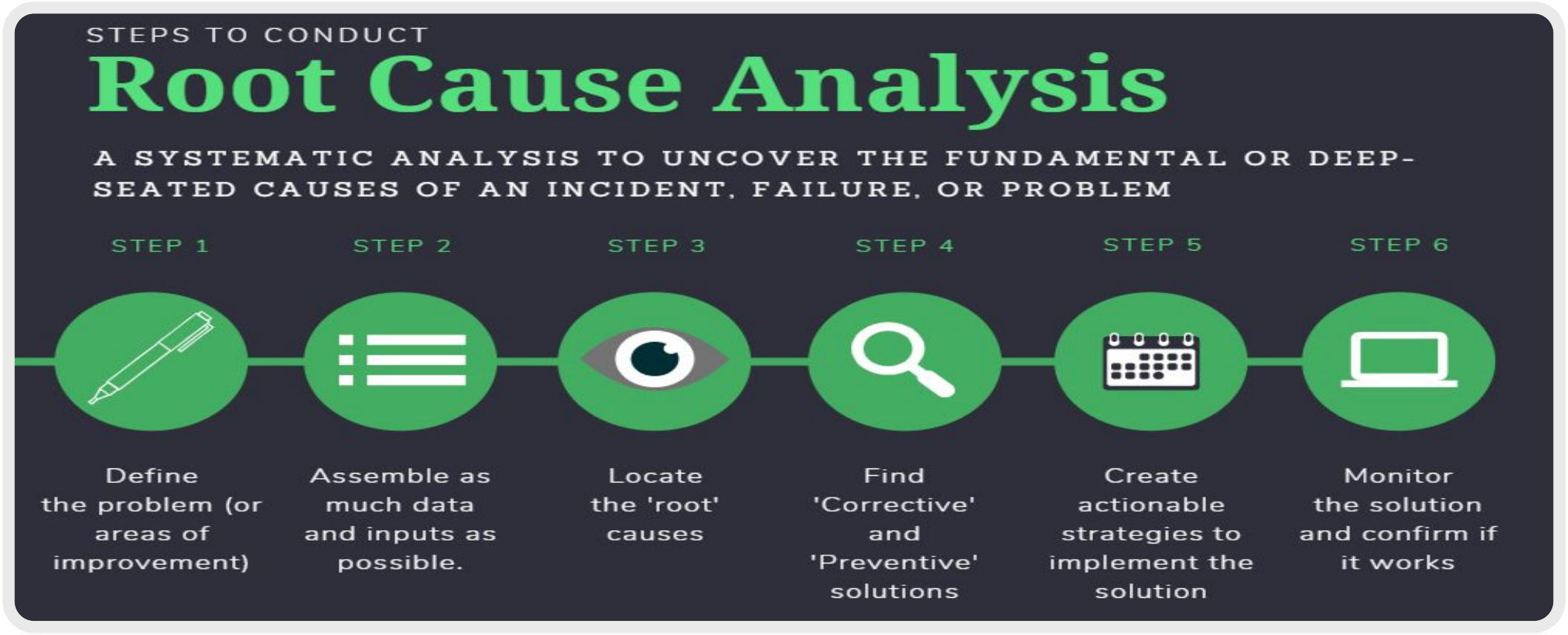
GOALS AND OBJECTIVES

- **Root cause analysis aims** to uncover the root cause of problems, find the optimal way to repair faults, and find a solution that can be applied to prevent the recurrence of the event at fault. Thus, the method supports all efforts to locate the true causes of processes faults or impediments and fix them to continuously improve.

- **The RCA method** is successfully used to identify root causes and contributing factors to a problem and create a prevention plan

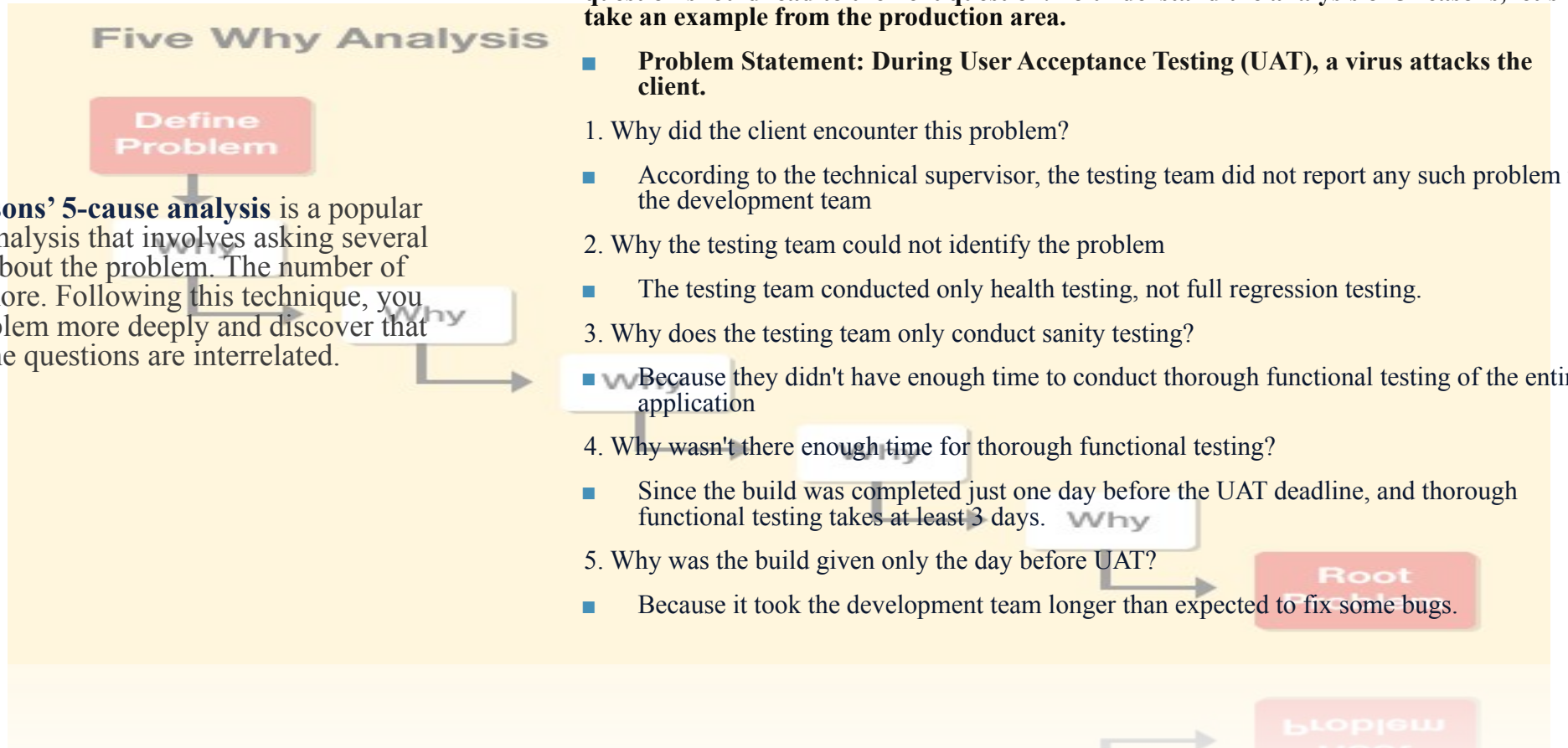


CHARACTERISTICS OF THE STATE OF KNOWLEDGE



SCIENTIFIC METHODS

Analysis of the '5 reasons' 5-cause analysis is a popular method of. root cause analysis that involves asking several additional questions about the problem. The number of "why" can be five or more. Following this technique, you can understand the problem more deeply and discover that the answers to the questions are interrelated.



It is important to note that we are not just asking 5 random questions - the answer to each question should lead to the next question. To understand the analysis of 5 reasons, let's take an example from the production area.

- **Problem Statement: During User Acceptance Testing (UAT), a virus attacks the client.**

1. Why did the client encounter this problem?

- According to the technical supervisor, the testing team did not report any such problem to the development team

2. Why the testing team could not identify the problem

- The testing team conducted only health testing, not full regression testing.

3. Why does the testing team only conduct sanity testing?

- Because they didn't have enough time to conduct thorough functional testing of the entire application

4. Why wasn't there enough time for thorough functional testing?

- Since the build was completed just one day before the UAT deadline, and thorough functional testing takes at least 3 days.

5. Why was the build given only the day before UAT?

- Because it took the development team longer than expected to fix some bugs.

SCIENTIFIC METHODS

Failure Mode and Consequence Analysis (FMEA) helps to prioritize failure modes and recommends corrective measures to prevent catastrophic failures and improve quality.

If you notice, there are two specific aspects of FMEA, namely:

Failure mode: it includes the definition of various ways, types (or modes) in which something can fail.

Consequence analysis: It consists in analyzing the consequences and consequences of each of the failure modes.

- **Example: In the Acme division for the production of aluminum coils, there was a problem with vibration inherent in one of the mixers. Now the FMEA analysis has been carried out to identify various types of failures, their consequences and possible causes.**

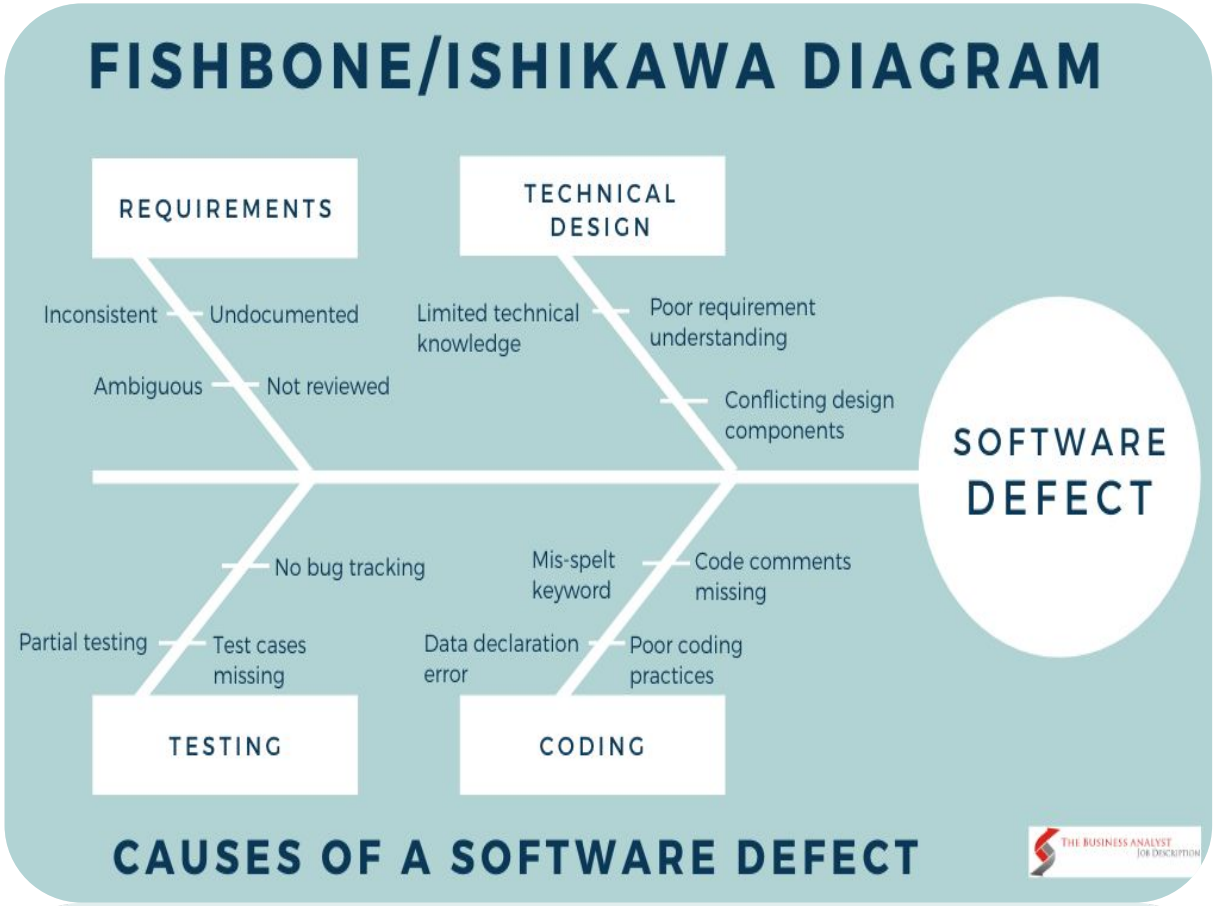
  As a result of the problem:

- Preventive actions: Monthly maintenance to ensure proper functioning and reliability of machines. In addition, the responsible authorities were instructed to carefully follow the monthly maintenance recommendations for each machine and document the data in the monthly maintenance report.
- Corrective actions: Balance the mixer blades and replace the bearings.Thus, as we have just seen in the example above, the systematic implementation of the FMEA method has led to an increase in the durability of the machine, as well as to an increase in the overall productivity of the production unit.

FISHBONE DIAGRAM / CAUSAL DIAGRAM (CED)

One of the most widely used tools for conducting a comprehensive root cause analysis is the **Ishikawa diagram, fishbone diagram, or Cause-effect diagram (CED).** This tool is used in situations where the root cause is completely unknown. Cause-and-effect diagrams reveal "all" potential root causes associated with a particular problem from the very beginning of the analysis.

- **Example:** A good example of root cause analysis using the Fishbone method is the information technology (IT) industry.



ANALYSIS OF RESULTS

When conducting a thorough root cause analysis, specific recommendations should be taken into account. The implementation of these best practices ensures that the root cause of the problem is identified and helps to identify specific and sustainable corrective actions.

- Focus on fixing the actual cause of the problem, not its symptoms.There may be several root causes that may be interrelated.Methodically solve the problem in order to find specific causal evidence supporting the claims about the root cause.
- The people involved in the analysis should have in-depth knowledge of the various RCA methods and their application.
- The identified root cause must have the consensus of the team involved in the analytical activity.When determining the solution to the problem, the cost of implementation should be taken into account.
- Recognize the fact that solving the root cause can have cultural consequences, and its implementation may face resistance from the affected people.
- Visualization of your data - visualization helps in quick analysis and investigation.
- The whole process should be moderated by a facilitator with significant experience in conducting and managing RCA.

DETERMINING THE SCOPE OF POSSIBLE USE OF THE RESULTS

Root cause analysis is undoubtedly a highly recommended practice for conducting multidimensional analysis when something goes wrong within a certain process. The success of **RCA** depends on how effectively the root cause of the problem is identified.Since studying the problem in all aspects can help to identify the root cause, **RCA** always encourages its users to ask a lot of questions and collect as many points of view as possible. Then each of these points of view is investigated and analyzed to identify all the possible causes of the problem.There are various types of tools and methods used to analyze root causes.

These methods help businesses resolve complex and confusing situations by finding the best possible solutions. Although one person can independently analyze the root causes, in most cases a team approach is correct. Regardless of the industry, the possibilities of applying root cause analysis are limitless, as it can help enterprises effectively prevent the recurrence of failures and anomalies along with a significant increase in the efficiency of business processes.

THANKS FOR ATTENTION!

LIST OF RESOURCES

- https://blog.rsisecurity.com/six-steps-to-effective-root-cause-analysis/
- https://www.youtube.com/watch?v=6wt8Mm7HsXE
- https://www.corelan.be/index.php/2013/07/02/root-cause-analysis-integer-overflows/
- https://cambridge-intelligence.com/root-cause-analysis-timeline/