COSMOS
Navigate the Compliance Universe

Compliance Today - April 2021
Root cause analysis and corrective action plans

By Cornelia M. Dorfschmid, PhD, MSIS, PMP, CHC

Cornelia M. Dorfschmid (cdorfschmid@strategicm.com) is Executive Vice President, Strategic Management Services, LLC.

One reason for an increased or renewed interest in root cause analysis (RCA) in the compliance community may be due to the recently updated U.S. Department of Justice (DOJ) guidance entitled *Evaluation of Corporate Compliance Programs*.[1] In the guidance revision issued June 2020, the DOJ states: "To determine whether a company's compliance program is working effectively at the time of a charging decision or resolution, prosecutors should consider whether the program evolved over time to address existing and changing compliance risks. Prosecutors should also consider whether the company undertook an adequate and honest root cause analysis to understand both what contributed to the misconduct and the degree of remediation needed to prevent similar events in the future." DOJ further states that "a hallmark of a compliance program that is working effectively in practice is the extent to which a company is able to conduct a thoughtful root cause analysis of misconduct and timely and appropriately remediate to address the root causes." DOJ would assess effective compliance programs with respect to the organization's internal investigations and emphasizes RCA importance in the response to investigations: "Have the company's investigations been used to identify root causes, system vulnerabilities, and accountability lapses, including among supervisory managers and senior executives? What has been the process for responding to investigative findings? How high up in the company do investigative findings go?"

Clearly, RCA is an integral part of an effective auditing and monitoring element of the compliance program and the techniques related to the audit and investigation processes, as has been raised in the U.S. Department of Health & Human Services Office of Inspector General (OIG) and Health Care Compliance Association's (HCCA) *Measuring Compliance Program Effectiveness: A Resource Guide*[2] to measure compliance program effectiveness. The guide was issued in March 2017 as an outcome of an HCCA-OIG Compliance Effectiveness Roundtable. It points out the depth of and breadth of RCA and proper integration into corrective action plans as part of effectiveness criteria.

Not surprisingly, conducting an RCA may also be considered by internal review organizations that conduct claims, arrangements reviews to assess systemic error patterns, or be required in corporate integrity agreements with quality-of-service–, patient safety–, or software systems–related reviews of entities that settled with the government and are subject to external monitoring or review. In the context of corporate integrity agreements or integrity agreements, the independent reviewer typically needs to report the reasons for errors and patterns noted in billing and coding system(s) or report on any patterns of errors or weaknesses in arrangement systems. In corporate integrity agreements with quality control systems, quality review systems, and quality assurance program requirements that mandate reviewing, tracking, and completing root cause analyses of potential and identified issues, it is critical that such root cause analyses are actually conducted and done well. Quality-of-care incidents must be effectively reviewed and root cause analyses completed.

In certain auditing activities, RCA can also be beneficial. In process audits and systems reviews that focus on risk and internal controls, auditors typically must understand why processes do not work and why internal controls

are not functioning as they should—they need to find the gaps. RCA is then especially advantageous when auditors find out that the implemented control activity or monitors do not operate effectively. In a new system deployment, or during the pre-implementation phase, an RCA can be helpful to weed out systemic weaknesses that lead to malfunction.

Healthcare is increasingly integrated through advances in health information technology. Many medical and care delivery systems talk to each other through ever more sophisticated technology; keeping internal systems well controlled through setting compliance controls will be a consideration for effective and mature compliance programs. Getting to the root causes of compliance failures or violations will likely take a multidisciplinary approach and involve all parts of a system: people, policies, technology, corporate structure, communication channels, and the like. Understanding the basis and effective use of RCA should be part of the compliance officer's tool chest.

What is root cause analysis?

Two aspects are worth remembering with respect to root cause analysis: it is all about (i) *systems* and not isolated incidents and (ii) the *prevention* of the same system failures or errors through remediation and corrective action. And that means the goal is to control the system well and improve its quality. This is similar to the human body, which is a complex system that, if injured or ill, typically has the best chance of a cure with a proper diagnosis (knowing what and why) rather than a mere identification of symptoms. Root cause analysis gets to the bottom of the problem. However, the team or auditor that conducts the root cause analysis must not just find the contributing factors. ("Contributing factors – situations, circumstances or conditions that collectively increased the likelihood of an incident. By itself a contributing factor may not have caused the incident, but when they occur at the same time, the probability an incident will occur increases.")[3] They need to dig deeper. It means weeding out the very fundamental causes that affect the undesired outcome. As every gardener knows, the weeds (undesired outcome, pattern) will grow back unless all of the root is extracted and the garden prepared so that it cannot grow back, and that is not always easy. Neither is root cause analysis. It can be time consuming and costly and typically involves input from operational departments. And these departments are busy. Therefore, the compliance office needs to use RCA wisely.

There are many versions of definitions of root cause analysis, all saying similar things. Here are a few examples of definitions:

"Root Cause Analysis is a collective term for a number of structured methods that competent authorities, management and control staff as auditees and audit bodies as auditors can use to assist in identifying the underlying factors which lead to the occurrence of an issue."[4]

"A root cause analysis allows an employer to discover the *underlying* or *systemic*, rather than the *generalized* or *immediate*, causes of an incident. Correcting only an immediate cause may eliminate a symptom of a problem, but not the problem itself."[5]

"Root cause analysis is defined as the identification of why an issue occurred (versus only identifying or reporting on the issue itself). In this context, an issue is defined as a problem, error, instance of noncompliance, or missed opportunity."[6]

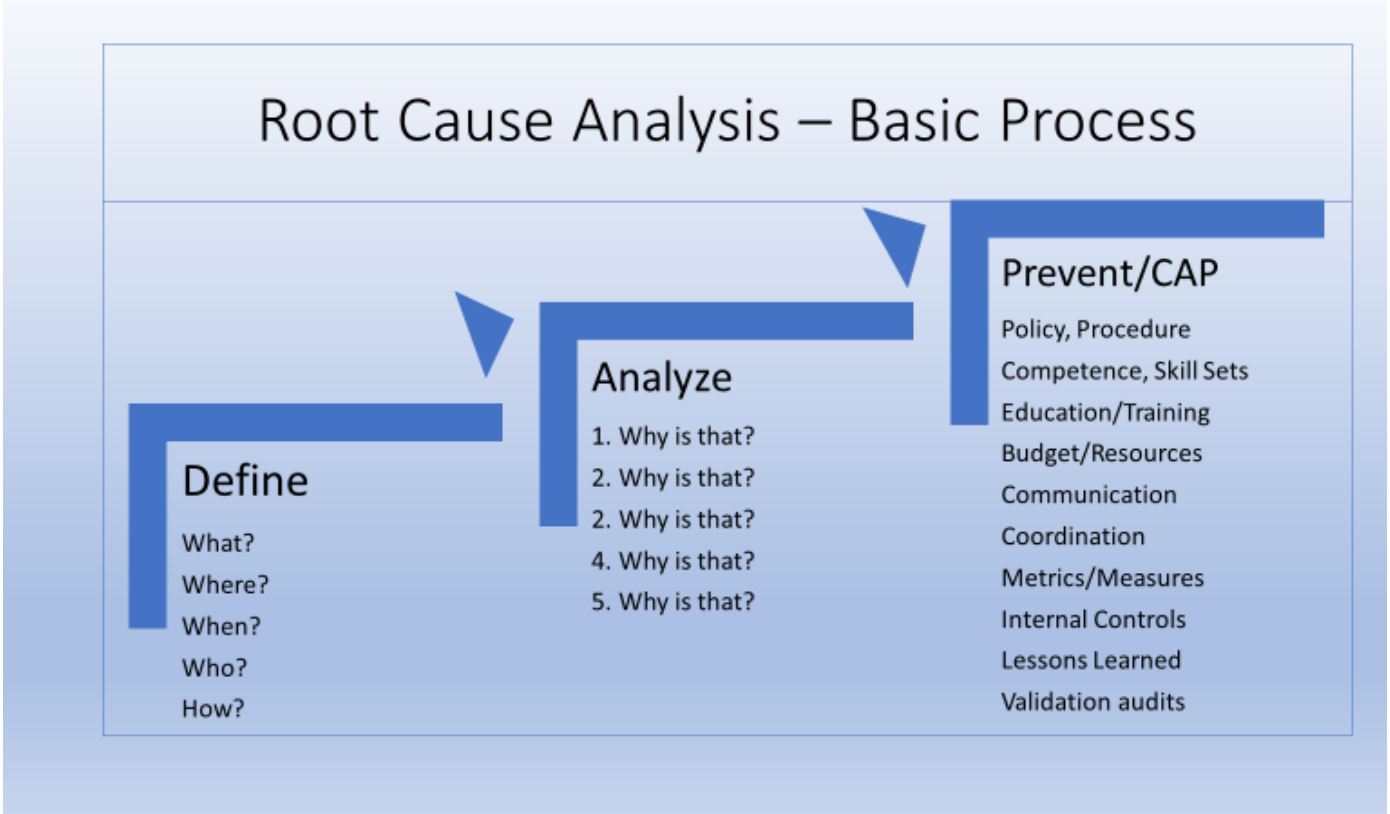
All these definitions suggest that root cause analysis is about system failures and error or noncompliance detection and preventive corrective action techniques. Root cause analysis allows us to find out the underlying causes for the outcomes and effectively prevent repeat failures or noncompliance. It comes from systems analysis in industrial engineering that examines systems to detect and prevent faulty products. It is often used in

quality management and safety systems but can be applied to any system, including systems on both the administrative and clinical side of healthcare. If conducted correctly, root cause analysis will allow you to fully understand *why* something happened. That puts you in the best position to make corrective action plans, as necessary.

Basic steps of root cause analysis

Every root cause analysis must tackle three basic steps: define, analyze, and prevent the failure or adverse outcome of the system.

Figure 1: Basic steps



Definition of the problem

As the first step, we need to understand exactly *what* happened, where it happened, who was involved, how long it was going on, and what company services and goals and objectives were affected. One needs to get the full picture of the unfavorable outcome, compliance violation, or faulty product or service.

Analysis of the problem

In this second step, we analyze the problem and look at the process that led to the faulty product, compliance violation, or undesired outcome of the process. This can be a costly and time-consuming endeavor, especially when we thought solid procedures and controls were already in place but we found that the process still failed more than once. In this second step we ask the *whys*, which typically involves looking at procedures; policies; mechanical and software systems; communication processes; environment; enforcement; and, importantly, interviews with staff and employees that operate the processes on a daily basis.

As controls may have failed or not worked effectively, people that run operations need to be queried. However,

this is best done in a collaborative and nonconfrontational manner, avoiding the blame game. Staff and leadership, some of whom may ultimately have contributed to the faulty outcome, need to be held accountable, but that can be visited in the third step. First, we need to find out why the problem persists. Oftentimes when systems and people (e.g., in areas such as contracting, revenue cycle, patient access, care delivery, enrollment, billing, coding, sales and marketing, clinical trials) do not communicate well, systems fail, and that puts the organization at risk. Compliance officers may want to conduct interviews and inspections at operational departments and talk with frontline staff to find out why the failure, errors, or compliance violation happened. Asking the five whys[7] or conducting cause–effect diagramming are methods to get to some answers and are techniques for this second step, but even going through a prescribed checklist or expected workflow may do.

Prevention through corrective action planning

Once the problem is identified and the causes are well understood, *preventive* corrective action planning (CAP) can occur. In this phase, the proactive changes to the quality of the system are made. That means the vulnerabilities that put the system at risk of faulty outcomes can be fixed. The risk of system failures is typically associated with several vulnerabilities, where each one could lead to nonperformance or failure, hence a corrective action plan likely also involves a variety of actions, such as new policies or modified desk procedures, along with staff education and training; addition of skill sets/hiring; addition of enforcement and incentive programs; software modifications and configuration changes; new metrics; adding triggers or alerts (e.g., error rates, accuracy rates, thresholds); increased budgets; and production system improvements through change in design. The focus is on prevention through process improvement. Validation testing that the implemented corrective action plans work consistently may also be part of this step.

Some techniques

Techniques for root cause analysis vary, and only a few can be discussed here. Root cause analysis is a rigorous exercise. The following techniques are examples and are particularly useful in the analysis part.

- **Answering the five whys**: The five whys[8] is a method that is attributed to Sakichi Toyoda, the founder of Toyota. Asking why the failure occurred five times was believed to be a simple method to get to the root cause. Although the number five is arbitrary, the idea is that the more you ask *why* a problem is occurring, the more different answers are likely to lead to the root cause.

- **Ishikawa "fishbone" diagram**: A cause-and-effect diagram[9] that shows the various factors that lead to the system failure. More than one cause can be identified that way. Many examples of this type of process analysis can be found online, often used as part of quality management. It tries to ask what happened, why it happened, and what can be done to stop it from recurring. It illustrates that many reasons can cause an ultimate outcome and that curing one *or* the other alone may not do the job. Basically, it suggests getting the whole picture.

- **Failure Mode and Effects Analysis**: "Failure Modes and Effects Analysis (FMEA) is a systematic, proactive method for evaluating a process to identify where and how it might fail and to assess the relative impact of different failures, in order to identify the parts of the process that are most in need of change."[10] It is considered particularly useful in new processes prior to implementation.

- **The Pareto principle**: Pareto analysis is linked to the 80/20 rule (i.e., the idea that 80% of problems are often the result of just 20% of causes).

- **Logic/event trees**: These integrate probability analysis into a branching of events.

- Checklists
- Brainstorming

Benefits and documentation

The benefit of root cause analysis is that it can prevent or eliminate nonperformance and, hence, wasteful processes. It is best applied when system failures are discovered or suspected and not when isolated incidents or mistakes are discovered. Not every single overpayment error in a claims audit or a missing signature in an arrangements review may trigger a full-blown root cause analysis. However, if a pattern of error or noncompliance is suspected, it may be considered. Sometimes set error rates and accuracy rates serve as monitors or thresholds and, when exceeded, trigger root cause analyses and full-blown audits.

No matter what method or technique is used to conduct the root cause analysis, results need to lead to action, typically management action. That often involves requests for additional resources/budget to fix an issue. Therefore, the documentation of the RCA must be credible and convincing. It must explain what exactly happened and why recommendations and suggested corrective action plans are reasonable and leaders can expect no recurrence. It is important to document the steps and fully explain what causes were found and what remedy is suggested. It is best to keep methods simple and documentation straightforward. This is especially important if reports are made to boards and governing bodies. If there is no convincing reason(s) why the failure happened, they may not see the connection between the ultimate root cause and compliance violation or faulty outcome and question whether it was not just an isolated incident.

Tips to conduct root cause analysis

Compliance officers may consider the following areas for probing and identification of potential vulnerabilities when conducting a root cause analysis. Probing into these areas to discover why a billing process, security management process, patient admission, or discharge process has not conformed or failed should be well documented and solicit input from various stakeholders, including line staff but not limited to only those directly involved. It is best to get broad perspective. RCAs should be well planned out so that people are available for review/interview and budget and timelines can be met. Remediation suggestions and ideas may often arise right at the discussion with operational staff involved. Again, a nonconfrontational and collaborative approach will work best.

Communication

Many compliance professions would agree that half of the problems are often simply due to communication failures. Examples are numerous. For example, departments are not sharing information efficiently or timely with each other, or there is not enough cross-departmental discussion or committee. Software systems are not integrated well or at all to communicate electronically, and hence manual handovers/input led to error. Contracting is decentralized, and local facilities do not report contracts routinely to legal. Management by email fails to get important messages or information through to all stakeholders; overflowing mailboxes prevent effective dissemination and people taking note.

Competence/skill sets

Reasons can fall into the area of competence and skill sets. While policies and procedures may be well done and available, staff simply do not have the competence to execute. In situations where budget cuts for training, staff shortage, high turnover, or missing onboarding protocols are areas of concern, competence and skill sets may be sought out.

Education and training

Education and training of staff in written guidance and protocols is an obvious area to look into. Following up on why training and refreshers did not work whenever repeat violations occurred may come into play. The quality and frequency of training, the lack of participation, and nonenforcement of missed training should be checked. The best training does not help if someone gets a free pass and misses crucial information that ultimately leads to a series of violations. For example, in marketing and sales and contracting with providers, it is important that the Anti-Kickback Statute and Stark Law compliance are taught and enforced by supervisors.

Supervision

The best policies and procedures are not effective if supervisors do not understand, follow, or enforce them with their staff. Problems in supervision may also reflect a weak corporate culture. Supervision/supervisors can bring numerous issues to light, with wide-ranging potential. Probing *why* in this area, for instance, may point to allegations of retaliatory practices, lack of rule following, or lack of mentoring and support during onboarding.

Guidance (policies and procedures)

Compliance officers understand the importance of clear and available written guidance and procedures that are well disseminated and explained. This is an obvious topic for a *why*.

Coordination

Poor coordination is often closely related to communication weaknesses. If new projects or initiatives are not coordinated well across departments, they may create compliance gaps. Reasons for compliance failure can be found when querying interviewees and procedures on coordination across departments during planning, rollout, etc.

Resources (budget/personnel)

Lack of sufficient resources and budget can lead to shortcuts and lack of available knowledgeable staff to execute and audit operational processes. Has the number of certified coders been reduced, and coding errors increased? Have audit staff been overwhelmed with audits related to COVID-19 issues and not been available for areas where system errors were not caught? Has training been cut because of resources being reassigned or insufficient? Including resources into framing a *why* will be helpful.

Incident response systems

If patterns of error or noncompliance persist and become systemic, it may be worthwhile asking whether incident response systems are in place and complaints/reports are being followed properly. Are hotline or compliance complaints processed timely? Are resolutions to complaints effectively communicated? Are the right people available to respond to reported incidents? Are they applying proper investigative techniques?

Accountability/corporate responsibility

Accountability and corporate culture are topics that can lead to explanations. If compliance is not enforced or leadership is not held accountable, problems and errors may persist in spite of the best written policies and training.

Corporate culture/environment

-

Corporate culture is an area to probe for, especially when potential double standards, challenges in leadership, a weak infrastructure of the compliance program, possible fear of retaliation, and similar issues are suspected.

Lessons learned

Lessons learned is an important element of sharing experiences beyond a small group of auditees or those affected by an adverse event or failure. Others can benefit from insights of an audit or remediation effort. Are "lessons learned" exercises being done at all? Could repeat patterns have been avoided if they were done?

Risk management

Lastly, checking for the presence and sophistication of an annual centralized risk assessment process that matches the complexity and size of the organization is an area to query. Are the right people conducting risk assessments and risk management processes? Are they using the appropriate tools and engaging all those who need to be involved? Is risk prioritization working? Has the compliance violation been the result of risk acceptance or just inadequate prioritization? Are risk remediation efforts scheduled but dragged out and delayed/not completed? These are just a few questions related to this area.

The topics above and any additional issues can easily be put into a simple template for use with root cause analysis (see Table 1). The topic(s) can be checked off, indicating what underlies the formulation of questions and answers to the whys and helps with the analysis. Alternatively, the list of topics can be simply used as a separate checklist/cheat sheet to help with interviews, investigations, and formulating questions.

	1	2	3	4	5
Coordination					
Competence/skill set					
Education/training					
Supervision					
Guidance/policies and procedures					
Coordination					
Resources					
Incident/response system					
Accountability/corporate responsibility					
Corporate culture					

	1	2	3	4	5
Lessons learned					
Risk management					
Identify (What happened?)					
Analyze (Why?)					
Prevent/remediate/ CAP activity					
CAP assigned to					
Due date					

Table 1: Simple root cause analysis template

Conclusion

New compliance officers may want to get more educated on ways to conduct root cause analysis and how best to record their efforts to complete one. They may want to liaise with internal audit, health information technology, patient safety, information security, quality assurance, and improvement functions or departments—or those involved with the International Organization for Standardization and The Joint Commission certifications who may already be more familiar with root cause analysis. Ultimately it is a useful and needed type of analysis when systemic patterns of error are suspected or have occurred, and the quality of systems need to be improved. As DOJ and OIG expect these techniques to be available and used in compliance programs, it is a must to get oriented on how to best use them and evidence such usage as needed.

Takeaways

- Root cause analysis (RCA) is a must for effective compliance programs.
- RCA is for assessing quality of systems and patterns and prevention.
- RCA relies on three steps: definition, analysis, and preventive corrective action planning of a system failure.
- Functional and operational departments in their quality assurance and process improvement initiatives use RCA (e.g., for the International Organization for Standardization and The Joint Commission certification).
- Fishbone diagrams and cause–effect diagramming are typical RCA activities.

1 U.S. Dep't of Justice, Criminal Div., *Evaluation of Corporate Compliance Programs* (Updated June 2020), http://bit.ly/2Z2Dp8R.
2 HCCA-OIG Compliance Effectiveness Roundtable, *Measuring Compliance Program Effectiveness: A Resource Guide*,

March 27, 2017, http://bit.ly/2V8dajN.
3 QAPI, "Guidance for Performing Root Cause Analysis (RCA) with Performance Improvement Projects (PIPs)," Centers for Medicare & Medicaid Services, last accessed January 26, 2021, https://go.cms.gov/3ceDeRV.
4 National Audit Systems Network, *Root Cause Analysis, Version 1*, November 2016, https://bit.ly/3aaMpQD.
5 Occupational Safety and Health Administration and U.S. Environmental Protection Agency, "The Importance of Root Cause Analysis During Incident Investigation," fact sheet, October 2016, https://bit.ly/3qYtXkK.
6 The Institute of Internal Auditors, "Practice Advisory 2320-2: Root Cause Analysis," December 2011, https://bit.ly/3iPzUO6.
7 "Five whys," Wikipedia, last edited September 15, 2020, at 06:14 (UTC), http://bit.ly/3a2xaJo.
8 QAPI, "Five Whys Tool for Root Cause Analysis," Centers for Medicare & Medicaid Services, last accessed January 26, 2021.
9 QAPI, "How to Use the Fishbone Tool for Root Cause Analysis," Centers for Medicare & Medicaid Services, last accessed January 26, 2021, https://go.cms.gov/2Mx4eBm.
10 "Failure Modes and Effects Analysis (FMEA) Tool," Institute for Healthcare Improvement, last accessed January 26, 2021, https://bit.ly/30sRFnW.