PARAS PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

PARAS 0027 January 2021

Guidance for Root Cause Analysis in Aviation Security

National Safe Skies Alliance, Inc.

Sponsored by the Federal Aviation Administration

Authors

Sibel McGee, Ph.D. (PI)
Peggy McCarthy
Analytic Services Inc. (ANSER)
Falls Church, VA

Supporting Team

Evans Consulting
Falls Church, VA

Dynamis, Inc.
Fairfax, VA.

NATIONAL SAFE SKIES ALLIANCE, INC.

National Safe Skies Alliance (Safe Skies) is a non-profit organization that works with airports, government, and industry to maintain a safe and effective aviation security system. Safe Skies' core services focus on helping airport operators make informed decisions about their perimeter and access control security.

Through the ASSIST (Airport Security Systems Integrated Support Testing) Program, Safe Skies conducts independent, impartial evaluations of security equipment, systems, and processes at airports throughout the nation. Individual airports use the results to make informed decisions when deploying security technologies and procedures.

Through the POST (Performance and Operational System Testing) Program, Safe Skies conducts long-term evaluations of airport-owned equipment to track and document a device or system's performance continuously over its life cycle.

Through PARAS (Program for Applied Research in Airport Security), Safe Skies provides a forum for addressing security problems identified by the aviation industry.

A Board of Directors and an Oversight Committee oversee Safe Skies' policies and activities. The Board of Directors focuses on organizational structure and corporate development; the Oversight Committee approves PARAS projects and sets ASSIST Program priorities.

Funding for our programs is provided by the Federal Aviation Administration.

PROGRAM FOR APPLIED RESEARCH IN AIRPORT SECURITY

The Program for Applied Research in Airport Security (PARAS) is an industry-driven program that develops near-term practical solutions to security problems faced by airport operators. PARAS is managed by Safe Skies, funded by the Federal Aviation Administration, and modeled after the Airport Cooperative Research Program of the Transportation Research Board.

Problem Statements, which are descriptions of security problems or questions for which airports need guidance, form the basis of PARAS projects. Submitted Problem Statements are reviewed once yearly by the Safe Skies Oversight Committee, but can be submitted at any time.

A project panel is formed for each funded problem statement. Project panel members are selected by Safe Skies, and generally consist of airport professionals, industry consultants, technology providers, and members of academia—all with knowledge and experience specific to the project topic. The project panel develops a request of proposals based on the Problem Statement, selects a contractor, provides technical guidance and counsel throughout the project, and reviews project deliverables.

The results of PARAS projects are available to the industry at no charge. All deliverables are electronic, and most can be accessed directly at www.sskies.org/paras.

PARAS PROGRAM OFFICER

Jessica Grizzle *Safe Skies PARAS Program Manager*

PARAS 0027 PROJECT PANEL

Kristina Dores *TranSecure*
Tracy Fuller *ACTS - Aviation Security, Inc.*
Walter "Mac" Harper *Memphis International Airport*
Stephanie Lane *Dallas Fort Worth International Airport*
Stephanie Murphy *Tidal Basin Government Consulting, LLC*
Melissa Osborn *DOWL*
Teresa Scism *San Francisco International Airport*
Nikola Vucicevic *The Port Authority of New York and New Jersey*

AUTHOR ACKNOWLEDGEMENTS

The authors would like to acknowledge the assistance from those airports and aviation security stakeholders who supported preparation of this guidebook. Their helpful discussions and suggestions in individual meetings and during the validation workshop have significantly improved the content and format of the guidebook.

We also express our appreciation to Ms. Cynthia Nordean and Mr. Damian Cobey of ANSER; Mr. David Young and Mr. Alan Metzler from Dynamis, Inc.; and Ms. Tara Stearman from Evans Consulting for their support in developing the content of this guidebook.

The authors also would like to thank members of the PARAS Project Panel for their review of and feedback on previous versions of this guidebook and supporting research.

Finally, thanks are due to the PARAS Program Manager, Ms. Jessica Grizzle, for her support and guidance during this guidebook's development process.

CONTENTS

TABLES & FIGURES

EXECUTIVE SUMMARY

This guidebook was developed to provide airports with a standard root cause analysis (RCA) process to address aviation security vulnerabilities and noncompliance, and improve the effectiveness of the aviation security enterprise. Aviation security is a complex system; behaviors and outcomes observed within it emerge as a result of multifaceted and dynamic interactions among many actors, factors, and processes. In such complex systems, approaches to determine causation based on independent and linear cause-effect relationships are of limited utility, as they are not equipped to capture and convey the network of dependencies, interactions, and feedback structures that shape resulting outcomes. Recognizing this complexity, any RCA process recommended for aviation security needs to facilitate a systemic approach in which problems are examined as an integral part of a broader context, its dynamic relationships, and long-term behavior patterns. The RCA methodology presented in this guidebook is based on an expanded version of the *Current Reality Tree*, a systemic RCA method. Following this methodology and its six steps, airport security officials can trace security problems to their root causes.

Tasks necessary for the development of this guidebook were conducted in two phases. The first phase focused on the research and assessment of existing RCA methodologies, assessment of the aviation security context and the respective RCA requirements, and the design of a conceptual RCA process suitable for this domain. The second phase was dedicated to transitioning this conceptual RCA process to a practical implementation. This was accomplished by testing the designed RCA process through a participatory workshop with select airport security stakeholders. This phase concluded with the development of project deliverables, including this guidebook.

The guidebook includes five main sections:

- *Section 1: Introduction* provides an overview of the guidebook and its purpose and organization.
- *Section 2: Getting Familiar with RCA* describes RCA and discusses its role in the context of aviation security.
- *Section 3: Getting Ready for an RCA* provides airports with all the information and considerations necessary to prepare for an RCA effort.
- *Section 4: How to Conduct an RCA* presents the step-by-step RCA process along with key definitions, thinking strategies, helpful hints, activities, and examples.
- *Section 5: You Have Your RCA Results – Now What?* introduces considerations and activities that airports need to be aware of in order to leverage RCA results and transition into mitigation planning.

This RCA process can accommodate any aviation security or compliance problem, ranging from the simple to the complex. The process will deliver best results if implemented through a collaborative team approach where the perspectives of all relevant airport stakeholders are represented and synthesized.

PARAS ACRONYMS

ACRP	Airport Cooperative Research Project
AIP	Airport Improvement Program
AOA	Air Operations Area
ARFF	Aircraft Rescue & Firefighting
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFR	Code of Federal Regulations
COO	Chief Operating Officer
DHS	Department of Homeland Security
DOT	Department of Transportation
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FSD	Federal Security Director
GPS	Global Positioning System
IED	Improvised Explosive Device
IP	Internet Protocol
IT	Information Technology
MOU	Memorandum of Understanding
RFP	Request for Proposals
ROI	Return on Investment
SIDA	Security Identification Display Area
SOP	Standard Operating Procedure
SSI	Sensitive Security Information
TSA	Transportation Security Administration

ABBREVIATIONS, ACRONYMS, INITIALISMS, AND SYMBOLS

APP	Action Plan Program
ASE	Aviation Security Enterprise
CRT	Current Reality Tree
DTO	Designated TSA Official
LOA	Letter of Agreement
MOA	Memorandum of Agreement
OFC	Outcome-Focused Compliance
RCA	Root Cause Analysis

SECTION 1: INTRODUCTION


Learning Objectives

- Understand the project background and methodology
- Understand the Guidebook's purpose and structure

Determining the root cause of a problem can be a daunting task. This is especially true when operating in a complex system, addressing a difficult problem, or dealing with a combination of both. The latter is often the case with root cause analysis (RCA) for aviation security. This guidebook provides airport personnel with a standard and systematic methodology for conducting RCA, along with supporting information and tools to facilitate that process.

1.1 Project Background

Although RCA is an integral part of developing solutions to mitigate aviation security problems, there is no standard RCA process in use across airports. Consequently, assistance was needed in identifying an RCA process to meet regulatory requirements and business improvement opportunities across the aviation security enterprise (ASE). Therefore, PARAS awarded ANSER funding for the *PARAS 0027 – Guidance for Root Cause Analysis in Aviation Security* project, to produce guidance for airport security officials for conducting standard and systematic RCA.

1.2 Research Methodology

The study team designed a two-phased research approach to accomplish the objectives of this project (see Table 1). While the first phase primarily focused on the research and conceptual design of the recommended RCA process, the second phase centered on testing and refining that process with the help of practitioner feedback.

Table 1. The Research Approach

Phase 1	• Characterized the aviation security RCA context • Conducted an RCA literature review and administered targeted airport surveys • Designed the RCA process
Phase 2	• Tested the RCA process through an interactive workshop with airport security officials and stakeholders • Developed the RCA Guidebook and Executive Brief

1.3 Purpose

Airports and other regulated entities likely engage in some form of RCA for serious security problems. However, there is no standard RCA approach consistently used across all of the ASE (TSA 2020). There are two consequences of this:

1. *Variations in the quality and results from similar RCA efforts.* In the absence of a standard approach or methodology, RCA efforts often rely on ad hoc brainstorming sessions or nonsystematic procedures to collect and analyze related information. This likely results in significant variation across airports in the quality of analysis and, in turn, the respective solutions produced. A standard and disciplined approach will help airports achieve compliance and sustain the highest levels of security, and do so consistently and systematically.
2. *Inaccurate and ineffective RCAs.* Ad hoc and nonsystematic RCA is less likely to discover the true root causes of problems. Unfortunately, it is common for operators to think they know enough about a problem, skip a rigorous analysis, and rush into mitigation planning. Operators' ability to discover true cause-effect relationships and trace problems to their root causes is limited in any complex system without a robust RCA method.

Therefore, the purpose of this guidebook is to provide United States airport security officials or their designated RCA teams with a comprehensive and standard RCA methodology that can handle a range of security problems.

The ultimate outcome of any RCA effort is a better understanding of a problem along with its root causes. Although results of an RCA effort inform any subsequent mitigation planning, there are several steps between completion of an RCA and ready-to-implement solutions. Those steps are beyond the scope of this guidance. However, the guidebook does provide some high-level suggestions on how to transition into mitigation planning to facilitate the connection between the two efforts.

1.4 Using This Guidebook

Some RCA methods can appear intimidating, which can lead those conducting an RCA effort to employ a simpler, less robust approach. However, the complexity of the problem set within the airport security domain calls for a methodology sophisticated enough to accurately identify the true root cause(s). This does not mean that all RCA efforts have to be extensive, but airports require a method that can be applied to both simple and complex problems. Additionally, airports may face time constraints due to regulatory requirements or the urgency of the problem being addressed. Therefore, this guidebook is designed to present an RCA that is user-friendly, can accommodate a spectrum of problems, and can be implemented within a reasonable timeline.

Throughout the guidebook, helpful hints are highlighted and information is broken down into digestible pieces with more detailed information, tools, and examples presented in appendices for interested users.

This guidebook's sections progressively give readers the knowledge they will need to complete a successful RCA process. In addition to this introduction, the guidebook consists of the following sections:

- Section 2: Getting Familiar with RCA. The focus of this section is to provide users with a clear understanding of what RCA is and how it fits into the ASE. Furthermore, this section explains how a robust RCA capability will support an airport's decision-making in the design of risk mitigation strategies.
- Section 3: Getting Ready for an RCA. This section offers some RCA best practices and discusses the activities necessary to prepare for an RCA.

- Section 4: How to Conduct an RCA. This section gives a step-by-step explanation of how to conduct an RCA. For each step, it explains key concepts, instructions for activities, inputs, outcomes, and helpful hints. In addition, it provides a running example throughout to illustrate the progression of the methodology.
- Section 5: You Have Your RCA Results – Now What? This section will help users take the results of the RCA and guide their mitigation activities. It presents various activities that will inform mitigation design and monitor effectiveness of the solutions implemented.
- Appendices. This guidebook includes five appendices:
  - *Appendix A: Outcome-Focused Compliance* provides information on this security philosophy.
  - *Appendix B: The Iceberg Model* provides a detailed discussion of this simple but powerful systems thinking tool.
  - *Appendix C: RCA Process Quick Look* provides users with a "big picture" view of the RCA process and its steps.
  - *Appendix D: Thinking Strategy Quick Look* compiles all thinking strategies in a single-page quick reference.
  - *Appendix E: Cause-Effect Tree Example* provides an additional example of how the RCA method works using an everyday problem.

SECTION 2: GETTING FAMILIAR WITH RCA

Learning Objectives

- Understand what an RCA is and when it should be used
- Understand RCA in the aviation security context

"Getting to the root of something" is an everyday expression used to indicate that understanding the cause or source of things is important. However, this general appreciation for what lies "at the root of things" does not always translate into rigorous problem-solving efforts. This is because identifying root causes and differentiating them from other contributing factors is not always easy, particularly in the case of problems experienced in complex systems such as aviation security. This section provides an introductory overview of RCA, including its importance for aviation security.

2.1 What Is RCA and What Is It Not?

Root cause is the most fundamental cause of an undesired event, behavior, or outcome that needs to be eliminated to prevent recurrence of the associated problems.[1] A single problem may have more than one root cause. RCA is any systematic approach employed to identify the root cause(s) of problems. There is no single standard RCA methodology that is applicable or proven effective for all problems or domains. Instead, there are various methods, processes, and philosophies to conduct RCA emphasizing the needs and requirements appropriate for different disciplines and purposes.

Key Takeaway

RCA is part of a broader vulnerability management process. It generates a better understanding of problems and their root causes to inform subsequent mitigation planning.

Regardless of the field of implementation or the type of RCA method used, it is important to note that RCA is designed to attain a deep understanding of problems (in particular their root causes), and not to generate solutions. Except for very simple problems, RCA will not generate ready-to-implement solutions and will not directly translate into required mitigation activities. Instead, RCA findings serve as one of several important inputs into mitigation planning. Particularly in aviation security, it is important to recognize the separate but complementary roles that vulnerability assessments, RCA activities, and mitigation planning play in safeguarding civil aviation against threats. For best results, these activities should be conducted in ways that recognize and facilitate the inherent operational relationships between them.

[1] Theoretically, a root cause can drive both negative and positive outcomes. However, an RCA method used by airports to address security vulnerabilities and noncompliance issues necessarily deals with problems. Therefore, this guidebook focuses on root causes that lead to negative outcomes.

2.2 Understanding the Aviation Security System

Key Takeaway

Problem solving in aviation security requires a systemic RCA approach that takes a comprehensive view of problems and identifies the complex web of relationships and interactions among a large number of elements.

Aviation security is a complex system. Complex systems (e.g., natural systems, biological systems, social systems) consist of a large number of elements (e.g., parts, processes, issues, and rules), and these elements connect through multifaceted relationships and dynamic—sometimes unpredictable—interactions. Moreover, as a socio-technical system, aviation security includes a strong human element. System stakeholders (e.g., passengers, airlines, airport management, security personnel, and airport employees) are intelligent actors with free will and different missions operating within the larger system. They think about the system, learn from their actions, and adapt their behavior accordingly. This adds to the complexity of the aviation security system, as the dynamic relationships and interactions among these stakeholders and the broader security processes shape the system-level behavior and resulting problems.

Problems in complex systems are often hard to comprehend. It is difficult to understand the plethora of relationships, identify causal pathways responsible for negative outcomes, and trace them to their root causes. While many system elements contribute to the undesired outcomes, no one element or person is responsible for them alone. Moreover, although we may sense some patterns, there is limited predictability in complex systems. Even well thought-out solutions may trigger unforeseen consequences.

Because of these tendencies, problem solving in complex systems such as aviation security require *systemic* RCA approaches. Systemic RCA approaches view problems as part of a greater system and require assessing the full spectrum of contributing elements and their causal mechanisms. As part of this holistic look, airports must thoroughly investigate and understand the broader context in which a problem presents. For example, depending on the problem, an airport may need to review the annual FAA airport certification safety inspection (14 CFR § 139) results and post-inspection briefing to airport management to consider the broader operating context and potential solutions available. Without a comprehensive and systemic approach, it is difficult, if not impossible, to identify root causes and, in turn, identify effective mitigation strategies for better outcomes in complex systems.

2.3 Aviation Security Problem Types

Key Takeaway

The RCA process in this guidebook is intended for security vulnerabilities and cases of noncompliance.

The RCA process presented in this guidebook is designed to address two types of aviation security problems: (1) vulnerabilities and (2) noncompliance (see Table 2). Accidents or broader safety issues, which are also among common aviation problems, require different RCA processes and will *not* be effectively addressed by this method.

Table 2. Types of Problems Addressed in This Guidebook

Vulnerability	• "A physical feature or operational attribute that renders an entity open to exploitation or makes it susceptible to a given hazard" (TSA 2019b). • TSA emphasizes that a vulnerability is not regulatory noncompliance; a threat to transportation security is considered a vulnerability prior to the occurrence of any regulatory noncompliance related to that vulnerability.
Noncompliance	• Noncompliance refers to the failure of regulated entities (e.g., airport operators, aircraft operators, indirect air carriers, foreign air carriers, flight training providers, and cargo screening facilities) to fulfill a known security requirement outlined in transportation security regulations. • Airports are under direct obligation to address cases of regulatory noncompliance to maintain TSA approval of their security programs (TSA 2019b, 1).

Regulatory requirements are in place to ensure widespread application of remedial practices for well-known vulnerabilities that have been extensively examined. Therefore, addressing noncompliance cases often requires implementing the regulation in question without an extensive RCA effort. However, if an airport experiences repeated issues of noncompliance in the same area, an RCA effort may be required. Similarly, in cases where an airport experiences a disruption in compliance as a result of an unexpected failure in a specific process, training, technological application, or the complex interactions among them, RCA can help identify failure points or causes for such disruption.

In contrast, vulnerabilities almost always require a rigorous RCA effort as they present novel and unique security problems with limited operator understanding of their cause-effect relationships and underlying dynamics. Solutions to these problems are unknown at the time of an RCA, and airports conduct an RCA to better understand the source of the problem so that they can identify and implement appropriate solutions.

2.4 When Do I Conduct an RCA?

Not all problems necessarily require RCA. When determining the need for an RCA, airport security officials need to consider the following factors: (1) the complexity of the problem, (2) the significance of the problem, (3) the persistency of the problem, and (4) existing policy requirements. The next sections will describe these factors in more detail.

2.4.1 The Complexity of the Problem

It is common to differentiate between types of problems based on their complexity (Snowden and Boone 2007):[2]

[2] Snowden and Boone also talk about chaotic problems. However, RCA is not appropriate in the context of chaotic problems, as response efforts often address a crisis situation and decision-making often focuses on urgent mitigation steps.

1. *Simple problems* involve few variables with relatively static and linear cause-effect relationships that are obvious or already known. These types of problems can often be addressed without an RCA or much expertise by simply applying known best practices (e.g., training requirements for airport employees to ensure consistency in quality of service).

Key Takeaway

Airport security officials need to consider four things when determining if an RCA is needed:

1. Complexity of the problem
2. Significance of the problem
3. Persistency of the problem
4. Existing policy requirements

2. *Complicated problems* include more variables and more relationships. The relationships and interactions between variables involved are reproducible and still largely predictable. Cause-effect relationships are either already known or can be identified with careful observation, application of expertise, and some assessment. There may not be ready-to-go solutions, but they can be developed once cause-effect relationships are identified (e.g., intrusion detection system failure). Complicated problems will likely require a formal RCA effort, depending on the scope of the issues involved and the extent of cause-effect relationships

3. *Complex problems* are dramatically different from simple and complicated problems. They often refer to unique situations that involve an extensive number of variables (e.g., actors, factors, and processes) with high levels of dynamic interconnectivity. The relationships between variables change over time, so the resulting behavior is difficult to predict. Complex problems always require a rigorous RCA effort since cause-effect relationships are not known and are difficult to identify even with expertise (e.g., preventing unauthorized individuals and items from entering restricted areas; and facilitating intelligence and information sharing between TSA, airports and law enforcement for accurate and timely airport employee and vendor vetting). Solutions are implemented, but their impact should be monitored so that the mitigation strategy can be adjusted as needed.

In sum, complicated and complex problems often require an RCA effort to reveal extensive cause-effect relationships and identify true root causes.

2.4.2 The Significance of the Problem

In addition to the nature of a problem, operators need to consider the impact of a problem when deciding whether an RCA is needed. This impact includes not only assessing consequences of that problem in different areas of a system or organization, but also assessing potential negative side effects of superficial analysis and ineffective mitigation strategies. In situations where these assessments indicate high risks, a rigorous RCA effort is required.

2.4.3 The Persistency of the Problem

Problems that recur despite repeated mitigation attempts are resistant to policy responses and necessitate a rigorous RCA effort. Such situations indicate an incomplete understanding of a problem. The resulting ineffective or partial fixes do not target the right elements of that problem, and mitigation efforts are easily defeated (Sterman 2006; Meadows 2008).

2.4.4 Existing Policy Requirements

The principal mission of the ASE is to protect the nation's civil aviation mode of transportation to ensure freedom of movement for people and commerce. In fulfilling this mission, the ASE leverages a complex security system that comprises legal regulations and supporting programs, processes, and practices. As the lead regulatory agency in the ASE, TSA guides collective security management efforts and interacts with a range of regulated entities that collectively protect the civil aviation system. Recently adopted by TSA, an overarching philosophy known as Outcome-Focused Compliance (OFC) informs this security system (see Appendix A). As a collaborative security philosophy, the primary goal of OFC is to "increase partnership [of TSA] with industry stakeholders, mitigate vulnerabilities, obtain compliance, and sustain the highest levels of security through shared outcomes" (TSA 2019b). RCA is a critical enabler of key OFC activities. For example, the Action Plan Program (APP), the most novel practice of the OFC program, "provides an opportunity for eligible parties and TSA to discuss and reach an agreement on corrective actions to address the root cause(s) of any security vulnerability or noncompliance . . . and resolve [it] with administrative action instead of a civil enforcement action" (TSA 2019b). Any eligible party who commits to this process must conduct an RCA, document results, and indicate the identified mitigation plan and timeline within the subsequent action plan. In other words, the RCA process presented here will function as part of a larger aviation security system, and can be a critical enabler of the related vulnerability management processes.

2.5 How Does RCA Benefit Aviation Security?

Effective problem-solving requires addressing not just any cause, but the root cause(s) of a problem. Unless there is a clear understanding of root causes of a problem, it is impossible to determine necessary changes in behaviors, processes, or practices. As a result, there is a risk of implementing flawed or partial solutions. Doing so in complex systems like aviation security can lead to serious consequences:

1. *Exacerbated Problems.* Focusing mitigation strategies on superficial analysis of symptoms leads to a phenomenon known as "fixes that fail." Even though addressing symptoms may temporarily alleviate the situation, the problem itself is not actually cured; because the underlying cause(s) are not removed, the problem reappears. In the long run, the superficial solution can cause the original problem to become worse or can create new problems (Kim 1992; Meadows 2008).
2. *Lost Opportunity for True Solutions.* Superficial solutions result in what is known as "shifting the burden." Owing to the temporary improvement in the problem situation, operators experience an illusion of victory, thinking the problem is fixed. This sense of success curbs motivation for discovering the true long-term solutions. Moreover, in some cases, quick solutions can generate side effects, hurting the system or organization's own capacity for lasting solutions (Kim 1992; Meadows 2008).

Both scenarios are unacceptable in aviation security, where a failure can have significant implications for everyone involved. Therefore, a key goal for problem-solving efforts in the aviation security domain is to ensure that scarce resources are not wasted on continually "fighting fires" but instead are invested in corrective strategies that address the true root causes. This is the best way to prevent problems from recurring or new problems from emerging.

Key Takeaway

Without an in-depth understanding of problems and their root causes, aviation security officials cannot identify effective and lasting solutions.

SECTION 3: GETTING READY FOR AN RCA


Learning Objectives

- Understand RCA good practices
- Understand how to prepare for an RCA:
  - Identify information/data needed for the RCA
  - Scope the RCA
  - Manage the RCA

Committing to the right mindset and taking the time to do proper planning can help ensure a successful RCA. This section discusses those practices and preparatory activities to help airport security officials get ready for an RCA.

3.1 RCA Best Practices

Embracing the following key principles and good practices will increase the chance that this effort will produce accurate and helpful results. In aviation security, this is especially important because inaction or ineffective strategies can have serious repercussions.

Key Takeaway

Airports can enhance their RCA efforts by:

- Making RCA a positive part of organizational culture
- Conducting RCA as a team
- Including diverse perspectives
- Familiarizing the RCA team with key concepts and steps
- Examining all aspects of the problem
- Expecting iterations in RCA

3.1.1 Make RCA a Positive Part of Organizational Culture

The RCA process will not get the attention and rigor it needs if stakeholders do not value it as a necessary and useful activity. Each of the airport's security stakeholders should see RCA as a key tool to achieve the airport-wide security mission. Changing attitudes toward RCA and convincing everyone about its practical utility may not happen overnight—particularly in organizations where stakeholders see RCA as a hunt for "the guilty." The following actions can help create an "RCA-positive" culture:

- Establish RCA as a routine part of the broader quality management process.
- Implement RCA in a collaborative fashion.
- Communicate to airport security stakeholders that root cause(s) often have less to do with individual behaviors and more to do with underlying systemic structures and processes, as well as cultural perspectives that generate those individual behaviors.
- Encourage airport leadership to outwardly show their support for RCA efforts through consistent messaging about the importance and purpose of the RCA efforts; authorizing all necessary resources, time, and access; rewarding related efforts and service; and, finally, showing the practical relevance and utility of RCA findings by disseminating results and acting based on RCA insights.

3.1.2 Conduct RCA as a Team

Although an RCA effort can be conducted by a single person, a collaborative effort will achieve the best outcomes; no single person can reasonably be expected to have the complete view of a large system or

the full dynamics pertaining to a complex problem. This is often true in aviation security, where the elements of the problem and solution may be spread across various organizations and functions. In addition to input from different perspectives, group interaction facilitates brainstorming and collaborative discussion, which can surface new ideas and produce unique questions and insights. The team can harness different thinking styles and levels of analytic sophistication to produce results that are more robust in nature and increase confidence in the findings. If RCA cannot be conducted in-person, airports should consider leveraging virtual platforms and their collaboration tools to facilitate group activities.

3.1.3 Include Diverse Perspectives in RCA Teams

Diverse perspectives may be the most critical principle for a systemic RCA process. The role stakeholders play in a system shapes not only how they define the problem, but also how they determine effective and acceptable solutions. Although stakeholders may have a good understanding of their part of the system, they view the rest of the system from their own perspective only. As a result, no one stakeholder has the "big picture" view of the entire system or all issues, processes, and behaviors that contribute to the same problem. For example, those who are not directly charged with security, such as baggage handlers or airline representatives, may have valuable insights about a security issue. Capturing a complete picture of a problem or system requires the collection and synthesis of different perspectives so that all issues, some of which can only be observed or experienced in a specific functional or physical area of the system, can be considered in the RCA effort. When establishing an RCA team, consider technical expertise, staff positions (levels of responsibility), gender, race, age, and other diversity elements that may be relevant.

3.1.4 Familiarize the RCA Team with Key Concepts and Steps

Ensuring that team members have the same level of understanding of RCA concepts and processes will improve the efficiency and effectiveness of RCA activities. Some RCA concepts, such as recognizing the difference between causality and correlation or root causes and symptoms, can be challenging for personnel who are new to this type of analysis.[3] In addition, a deeper understanding of how the process is supposed to work will reduce meeting times as well as make the time spent more productive. Accomplishing this can be as simple as handing out this guidebook as pre-reading prior to the first meeting. Another approach could be designating a specific person to become an "RCA expert," and then having that person teach the rest of the team the RCA methodology prior to the first meeting. The good news is that the more an airport conducts RCA using the methodology presented in this guidebook, the more proficient the team will become. RCA training will then only be necessary for new stakeholders joining the RCA team.

3.1.5 Examine All Aspects of the Problem

For a robust RCA, the RCA team should examine the problem of interest by assessing all relevant issues and forces across the system. Taking a holistic approach is particularly critical for problems generated in complex systems such as aviation security. These problems are produced by causal interactions and relationships among many stakeholders, factors, and processes, potentially from different parts of an airport, working together dynamically. Therefore, the RCA team should avoid looking at a problem as a snapshot in time and space, and instead strive to attain a big picture understanding. For example, is the problem an isolated incident or part of a greater trend? Is it specific to one functional area or influenced by other functional areas and related processes within the airport?

[3] For definitions of these terms, see Section 4.

3.1.6 Expect Iterations in RCA

For some problems, the RCA may follow a straightforward sequence of steps. Other problems, however, may dictate that the RCA team repeat some steps. Any RCA process is dependent on not only the nature and complexity of the problem, but also the amount of information gathered about it. Identifying a complete set of cause-effect relationships without all the data upfront may be particularly difficult for complex problems. But as the RCA team works through the process and gains a deeper understanding of the problem, it might need to refine previously developed results and incorporate newly discovered cause-effect relationships. Rather than being a sign of an ineffective process, these types of revisions indicate a normal evolution of the team's understanding of the problem. Ultimately, this demonstrates progress toward the identification of more accurate and nuanced root causes.

3.2 Planning for the RCA

Prior to conducting the RCA, airport personnel need to implement various planning activities to ensure that the RCA effort will be completed in a timely and effective manner.

Key Takeaway

Airports can plan for their RCA by conducting the following activities:

- Collect preliminary information
- Scope the RCA effort
- Manage the RCA effort by:
  - Identifying stakeholders
  - Identifying the RCA team
  - Determining the schedule
  - Determining the budget/ resource requirements
  - Determining a communications strategy
  - Gathering meeting materials

3.2.1 Collect Preliminary Information

Once a vulnerability or noncompliance is identified, airport personnel should start collecting as much information as possible to properly frame and understand the problem. Initially, this information will help determine if an RCA is required. Then, if it is decided RCA is needed, this preliminary information will help the RCA team scope the RCA process, identify relevant stakeholders, and provide a foundation for defining the problem to be examined. Types of information can include:

- Test results (i.e., joint, self or covert testing, self-audits)
- Vulnerability assessment or inspection reports
- Risk management documentation (e.g., threat assessment and risk register)
- Functional SOPs
- System documentation (e.g., process charts, schematics, diagrams, and hardware/software specifications)
- Staffing (e.g., schedules, shifts, and roles/responsibilities)
- Training documentation (e.g., curriculum, requirements, objectives, and records of attendance)
- Federal policy, regulations, and laws
- MOUs, memorandums of agreement (MOA), and letters of agreement (LOA)

3.2.2 Scope the RCA

Scoping the RCA will require consideration of the type of problem being examined and the related operational issues within an airport so that the RCA team can properly gauge the time and resources required. Table 3 presents questions to consider when scoping the RCA.

Table 3. Considerations for RCA Scoping

Problem Characteristics	▪ Is the problem straightforward? Do you know the source of the problem or is it unclear (i.e., cause-effect relationships are unclear or unknown)? ▪ What type of problem do you have? Is it a vulnerability or a noncompliance issue? ▪ What is the extent of the problem? Which/How many functions/departments/organizations are affected, or is the problem system- wide? ▪ What is the nature of the problem? Is it complicated or complex? ▪ How persistent is the problem? Is the problem an isolated incident or part of a trend? ▪ What is the impact of the problem? Will it result in a loss of life/assets? Is there an economic impact? Does it impact other functions?
Operational Issues	▪ Is the RCA required or optional? ▪ What is the level of support for this RCA in your airport? ▪ What is the availability of potential RCA team members? ▪ What is the airport's level of RCA readiness? Is there an RCA process in place? What is the level of experience within the RCA team? ▪ What will the impact of this RCA effort be on normal operations? ▪ How much time is available? Is there a time constraint on this RCA effort? What is the budget for this effort?

3.2.3 Manage the RCA Process

The following planning activities will facilitate effective RCA management:

- *Identify Stakeholders:* Stakeholders can include entities (individuals, departments, or organizations) who are actively engaged in or are the beneficiaries of the functions, processes, or assets that are at risk or are not working properly.
- *Identify the RCA Team:* An RCA team is composed of those people who will conduct the RCA. Within the team, an individual should be designated as the primary facilitator or RCA manager. This person could be from the responsible entity, a security expert, someone properly trained in the RCA process, or someone with the necessary subject-matter expertise for examining the problem. The rest of the team will comprise a subset of stakeholders identified as relevant to the problem. In addition, there may be stakeholders with relevant technical expertise who are not part of the RCA team but may be brought on as needed for targeted consultation.
- *Determine the Schedule:* The scope of the RCA process, external time constraints (e.g., APP requirements and normal operations), and stakeholder availability will shape the number and duration of meetings required to complete the RCA. In addition, data collection methods (e.g., individual interviews, focus groups, virtual meetings, surveys, etc.) and timelines should be built into the RCA schedule. If necessary, time should be included in the schedule for the RCA team to get familiar with key RCA concepts and develop a general understanding of the RCA process.

- *Determine the Budget/Resource Requirements*: The team should determine the resources necessary to conduct the analysis. The resources required for an RCA will vary based on the complexity and pre-existing understanding of a problem, the number of stakeholders involved, and their understanding of the RCA process.
- *Determine a Communications Strategy*: The RCA team should decide the method and frequency of communication between team members and between the team and airport leadership (and TSA if needed). This is particularly important for RCA processes that require virtual meetings or have an extensive number of stakeholders. This requirement also includes determining how and in what format the RCA team will document and disseminate findings. A more detailed discussion of dissemination of RCA findings is presented in *Section 5: You Have Your RCA Results – Now What?*
- *Gather Meeting Materials*: For RCA team meetings, printed copies of any documentation that will support the RCA process (e.g., assessment reports, process documents, etc.) should be made available. Meeting rooms should include white boards, sticky notes, and writing materials, and be large enough to accommodate the team size. Computer access during meetings may facilitate collaboration, documenting results, or modeling the problem of interest. If RCA team meetings must be virtual, the team should use a collaborative conferencing system and make sure that this system is tested over the airport network before the meeting.

SECTION 4: HOW TO CONDUCT AN RCA

Learning Objectives

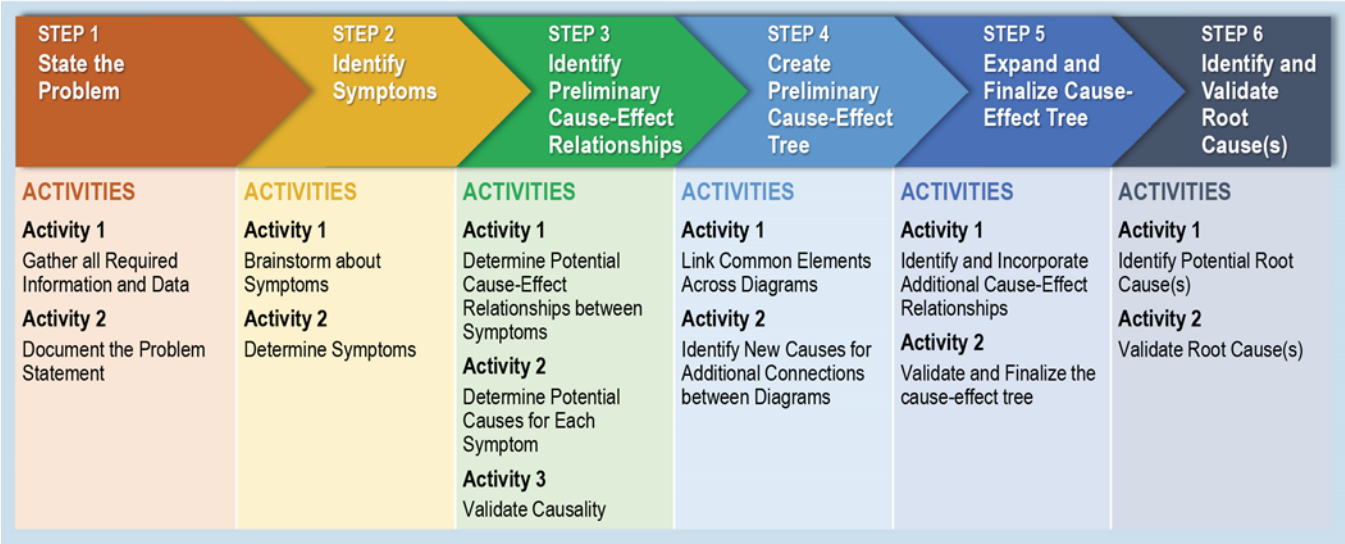
- Understand key RCA concepts and thinking strategies
- Write a problem statement
- Create a cause-effect tree
- Identify root cause(s) using a cause-effect tree

4.1 RCA Process Overview

The RCA methodology presented in this guidebook largely draws upon the *Current Reality Tree* (CRT) method (Adams et al. 2004; Walker and Cox 2016; Burton-Houle 2001; Taylor and Ortega 2003; Vorne 2020), which captures complex cause-effect relationships and can identify multiple root causes. CRT was chosen after an extensive literature review and assessment of available open-source RCA methodologies. Although the presented RCA method follows the overarching process of CRT, it has been expanded based on considerations and insights from the broader field of *systems thinking*[4] to meet the requirements of aviation security.

As shown in Figure 1, the RCA methodology described in this section consists of six steps:

Figure 1. RCA Methodology



Although these steps are presented here in the form of linear tasks, insights discovered during the process may naturally feed into multiple steps. Moreover, implementation of these steps is expected to occur iteratively rather than conclusively, as the RCA team's evolving knowledge about the problem and related dynamics may require revisiting previously completed steps, as discussed in Section 3.1.

[4] *Systems thinking* is the broader discipline associated with systems theory and related approaches to understanding and solving complex problems. For a more detailed discussion of this field and its principles and concepts, see Sterman (2000), Meadows (2008), and Boardman and Sauser (2008).

4.2 RCA Process Presentation Format

This guide presents the RCA Steps in a standard format. Information about each step is organized into the following six sections for a user-friendly layout and reference:

- Where are you in the RCA process?

The graphic at the beginning of each step orients the user about the specific step relative to the rest of the process.

Users can also find a quick-look reference in Appendix C that provides a big-picture view of the RCA process and its steps.

- What will you need?

Provides users with inputs (e.g., information and resources) needed for each step.

- What will you do?

Describes what the RCA team will accomplish during each step.

- What is the end product?

States the output expected from each step.

- What do you need to know to complete this step?

DEFINITIONS

Explanations of RCA concepts that are important to understand when completing the RCA step.

THINKING STRATEGIES

Logic and brainstorming tools that can be used by the RCA team to complete the RCA step.

Users can also find a quick-look reference in Appendix D that includes all thinking strategies.

HELPFUL HINTS

Tips that will assist the RCA team to more effectively and efficiently complete the RCA step.

Sidebar

Provides detailed elaboration on a critical tool or analytic principle

Activities

Each step is broken down into analytic activities, and each activity is broken down into discrete actions that the RCA team will complete.

- ### Example

Illustrates how each step works in the context of a notional airport employee vetting problem. Rather than a real-life problem with factual details, this example is included only as a prompt to think through requirements of each step. Therefore, the example is not meant to be exhaustive in its problem inquiry or identify actual root causes. As a snapshot at a specific point in time, some causes provided in the example may not be relevant to all airports or may be overcome by recent policy and regulatory updates.

Step 1: State the Problem

Where are you in the RCA process?

What will you need?

- ☐ Supporting information and data collected during RCA planning
- ☐ Meeting materials
- ☐ Meeting time and location

What will you do?

The RCA team will write the problem statement that will guide the rest of the analysis process.

What is the end product?

The end product of Step 1 is a clear and concise problem statement that captures the nature of the identified vulnerability or noncompliance being examined. The problem statement can also include a paragraph describing additional details about the problem.

What do you need to know to complete this step?

DEFINITIONS

Problem Statement

The problem statement is a brief and articulate description of an undesired issue to be addressed or a condition to be improved upon.

HELPFUL HINTS

- A problem statement should not include solutions or possible mitigation actions.
- An effective problem statement synthesizes data collected from all stakeholders related to the issue being addressed.
- Ensure that your problem statement captures a discrete problem.
- If, during this process, you discover that the issue examined is a series of related problems, develop multiple problem statements and associated cause-effect trees. You may need to adjust the RCA process and team arrangements (i.e., a separate team on each problem or the same team considering all problems) to accommodate this situation. During Step 5, the RCA team should bring related analysis efforts together to ensure that the overall RCA effort maintains a systemic perspective.

- Although the problem statement itself needs to be brief and concise, rich details from interviews and surveys can be included in the description paragraph (e.g., details on time, location, impact, and process specifics). Such details will provide a good starting place for the subsequent RCA process steps.
- This is a really important step as a common understanding of the problem statement among team members is important for the overall RCA process. However, it can be conducted virtually or combined with the next step for efficiency purposes.

What makes an effective problem statement?

A problem statement should be a concise, clear expression and can include the following details:

- A brief description of the ultimate negative outcome/effect
- Where the problem is occurring (e.g., which process and where in the process?)
- The timeframe over which the problem has been occurring
- The size or magnitude of the problem (if available, related metrics can document the gap between current performance and the performance target)
- If an issue of noncompliance, the related regulation
- Why this is a problem (what its impact is)

Step 1, Activity 1: Gather All Required Information and Data

1. Collect all relevant information about the identified noncompliance or vulnerability.
2. Combine the information collected during the RCA planning phase with observations and ideas gathered through interviews or surveys with relevant stakeholders.
3. Define as a team critical terms or concepts involved in the problem (e.g., how does an airport define restricted areas?)

Step 1, Activity 2: Document the Problem Statement

1. Write a problem statement. See sidebar for characteristics of an effective problem statement.
2. Write a paragraph to describe the details about the problem; include agreed upon definitions of key or ambiguous terms.
3. Agree as a team on the official problem statement.

Example

An example problem created to illustrate the RCA steps pertains to vetting of airport employees. Using this example, a problem statement and a brief description is provided below.

Problem Statement: Airport workers are not always adequately vetted.

Description: Over the past three years, there were five security incidents that involved airport workers. Preliminary investigations indicated that the vetting process missed some concerning issues about these workers. This is an undesired condition as these employees may pose an insider threat (e.g., unauthorized access to secure areas and smuggling of prohibited items into the airport).

Step 2: Identify Symptoms

Where are you in the RCA process?

What will you need?

- ☐ The problem statement
- ☐ Supporting information and data
- ☐ Meeting materials (sticky notes, large wall or board, etc.)
- ☐ Meeting time and location

What will you do?

The RCA team will brainstorm about the conditions that indicate there is a problem.

What is the end product?

Five to eight clear and concise statements capturing the identified symptoms.

What do you need to know to complete this step?

DEFINITIONS

Symptom

Easily seen or felt conditions, events, or behaviors that indicate a problem

HELPFUL HINTS

- All RCA team members should be included in Step 2.
- If the RCA is conducted virtually, the team should utilize a virtual whiteboard to capture brainstorming results. The designated lead for the RCA team should facilitate the discussion, visually documenting and synthesizing symptom ideas.
- If the RCA team is not able to identify five to eight symptoms, it may be necessary to conduct an outreach to additional airport staff who are involved in problem-related activities or testing/audit activities that revealed the security problem, or to other technical experts.
- Ensure that there is a clear and defensible explanation about why each symptom is an important indication of the problem.
- Allow everyone in the team to articulate opinions and observations.
- Do not conclude this step with more than eight symptoms. Too many symptoms will make the rest of the process more difficult to manage.

Symptoms vs. Root Causes

It can be hard to differentiate between *symptoms* and *root causes*. For example, bad grades are a symptom of poor student performance; fever is a symptom of an infection; and withdrawal from once-pleasurable activities is a symptom of depression. Many problem-solving efforts rely on symptomatic solutions to address these immediate issues. But symptoms are nothing more than an indicator of a deeper issue. Root causes are the real reasons that drive a problem. For example, poor time management may be a root cause of poor student performance; bacteria may be a root cause of an infection; and marital problems may be a root cause of depression.

Step 2, Activity 1: Brainstorm Symptoms

1. Brainstorm as a team about possible symptoms of the problem and capture each on a sticky note. See sidebar for an explanation of the difference between a symptom and a root cause.
2. Attach sticky notes to a large board or wall where everyone can see the information. If available, include in the symptom statements quantifiable information to indicate prevalence or importance (e.g., percentage, numbers, and years).
3. Display all suggested symptoms for consideration during this activity without any concern for the overall number of symptoms or significance.

Step 2, Activity 2: Determine Symptoms

1. If you have more than eight symptoms, reduce the number of symptoms using the following techniques:
   a. Evaluate each symptom by its relative perceived importance to the problem.
   b. Combine similar statements into a single symptom.
   c. Divide comprehensive statements into two symptoms.
2. Develop a justification for each symptom in the list.
3. Document symptoms on sticky notes with clear and concise sentences.
4. Gather symptoms that are determined to be less critical, or potentially duplicative, and place them in a "parking lot" in case they are needed during the subsequent steps.

Example

In the example problem, five potential symptoms are identified and placed on sticky notes (Figure 2).

Figure 2. Step 1: Symptoms

Step 3: Identify Preliminary Cause-Effect Relationships

Where are you in the RCA process?

What will you need?

- ☐ The problem statement
- ☐ Five to eight symptoms
- ☐ Supporting information and data collected
- ☐ Meeting materials (sticky notes, dry erase board, etc.)
- ☐ Meeting time and location

What will you do?

The RCA team will begin developing the cause-effect tree by (1) determining the relationships, if any, between symptoms; and (2) brainstorming and documenting potential causes for each symptom.

What is the end product?

The initial cause-effect diagrams that show (1) the relationships between symptoms and (2) relationships between the initial causes and the symptoms.

What do you need to know to complete this step?

DEFINITIONS

Cause-Effect Relationship

A relationship where occurrence of one thing (the cause) leads to the occurrence of another thing (the effect), indicating a causal connection between the two.

Causation

Causation denotes relationships that are substantiated by a reasonable explanation or theory that occurrence of one thing (cause) leads to occurrence of another thing (effect).

Correlation

Correlation refers to the simultaneous presence of two things where the existence of one is not causally dependent on the other.

THINKING STRATEGIES

Cause-Effect Relationship Conditions

In a suspected cause-effect relationship, the following three conditions must hold (Chambliss and Schutt 2006):

- *Covariation*: Whenever the cause occurs, the effect must also occur (i.e., if A then B).
- *Temporal Precedence:* The cause must occur before the effect (i.e., A occurs before B).
- *Control for Third Variables:* There must be no plausible alternative explanation indicating a third variable is causing the effect (i.e., other potential variables are identified and ruled out in favor of A causing B).

Five-Whys

Ask the question of "why?" five or more times to progressively identify deeper forces that are related to a problem: Why did A (effect) occur? Because of B (cause). Why did B (effect) occur? Because of C (cause). Why did C (effect) occur? etc.

Causality Rule

A change in a variable (cause) necessarily leads to a change in another variable (effect). There is a causal link between the two variables. If A (cause) THEN B (effect) or A THEREFORE B.

Tautology Rule

A change (effect) in a variable occurs as a result of a change in another variable (cause). B (effect) BECAUSE A (cause).

HELPFUL HINTS

- All RCA team members should be included in Step 3.
- If this step is conducted virtually, the team should come up with a digital way of building a cause-effect tree using a collaborative online platform.
- If the RCA team is not able to identify relationships between symptoms, it may be necessary to conduct an outreach to additional airport staff who are involved in problem-related activities or testing/audit activities that revealed the security problem, or to other technical experts.
- When identifying causes, consider all key aspects of an organization/process to capture a diverse set of issues, forces, and dynamics.
- When identifying relationships, avoid using correlations. Remember that if there is no logical explanation about causality between two things, their simultaneous existence cannot indicate a causal relationship.
- Do not be afraid of erasing and restarting. Activities 1 and 2 are iterative and can be repeated until the team feels comfortable with the causal relationships established.

Causation vs. Correlation

While conducting RCA, it is particularly important to differentiate between causal and correlative relationships. When A and B are causally related, a change in A will necessarily produce a change in B, causing its current state.

Correlation, on the other hand, measures merely the strength and direction of a relationship between A and B without necessarily indicating why the relationship exists. While presence and consistency in the relationship between two things may indicate a causal connection, it is also possible that a third variable may be causing both of the original variables. Alternatively, correlation may result from random chance if there is no meaningful explanation for the observed relationship.

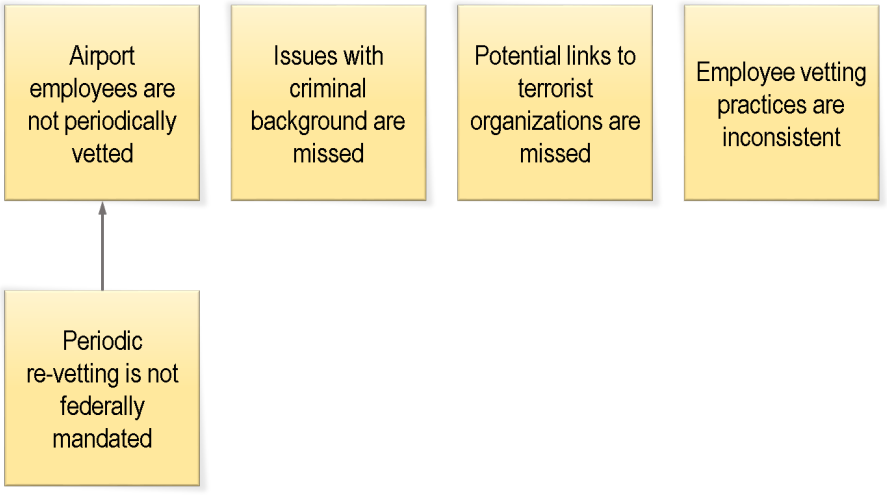
Step 3, Activity 1: Determine Potential Cause-Effect Relationships between Symptoms

1. Pair up each of the symptoms and see if any of them are causally related. See the sidebar to understand the difference between causation and correlation.
2. Place the sticky notes representing causes at the bottom and sticky notes representing the effects at the top.
3. Draw arrows between related sticky notes. Arrow heads should point from the cause to the effect in each pair.
4. If no relationships are identified between symptoms, skip this activity and continue with Activity 2.

Example

In the example problem, the only causal relationship identified is between the lack of a federal mandate on periodic re-vetting and the subsequent result of airport employees not being re-vetted periodically. Other symptoms are determined to have no causal relationship to each other (Figure 3).

Figure 3. Step 3, Activity 1: Causal Relationship



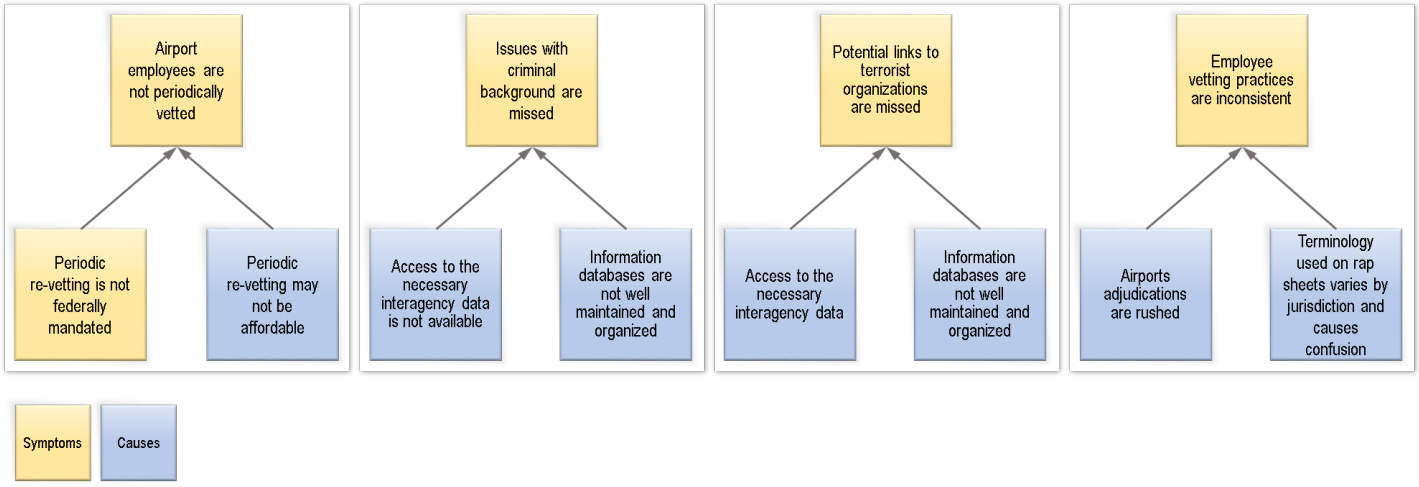
Step 3, Activity 2: Determine Potential Causes for Each Symptom

1. Brainstorm to suggest causes for each symptom, thinking about the question of "what conditions, factors, or behaviors may lead to this effect?" Using the Five-Whys technique may be helpful to progressively dig deeper in the cause-effect chains. See Thinking Strategies for more information on the Five-Whys.
2. Document each new cause identified with a sticky note. Consider using different colored sticky notes to differentiate between symptoms and causes.
3. Draw arrows between sticky notes to capture suspected causal relationships and form an individual diagram for each symptom.
4. Since the team considers each symptom in isolation at this stage, there may be common causes across symptoms and related diagrams. In such cases, create duplicate sticky notes to denote the same cause.

Example

In the example problem, some symptoms have common causes (Figure 4). The lack of access to some interagency data makes it hard to uncover criminal and terrorism-related issues during the employee vetting process.

Figure 4. Step 3, Activity 2: Symptom Causes



Causality Validation

There are two tests that can be used to validate causality. Both of these tests are designed to externalize and validate the logic contained in the suspected causal relationships and should be referenced by the RCA team during all steps:

- *Causality Rule:* If A (cause) THEN B (effect) or A THEREFORE B.
- *Tautology Rule:* B (effect) BECAUSE A (cause).

Each cause-effect relationship should be stated out loud, both in direct and reverse order, for the logic to become more accessible for the whole team to assess and critique.

Step 3, Activity 3: Validate Causality

1. Validate each cause-effect relationship using simple logic tests. See the sidebar for more information on causality validation.
2. Document the validated cause-effect relationships as individual diagrams. Remember that some causes and effects may be part of multiple diagrams.

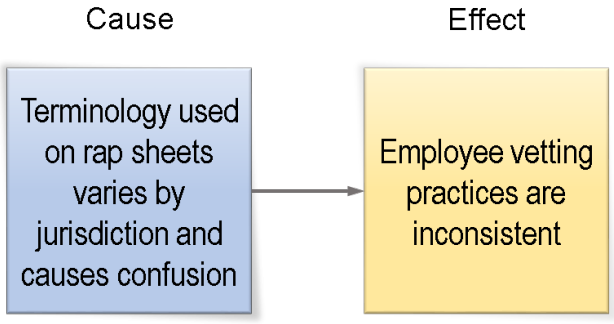
Example

One of the causal relationships supporting Symptom 4 can be validated by stating the following (Figure 5):

- (A) Terminology used on rap sheets varies by jurisdiction and causes confusion, THEREFORE (B) employee vetting practices are inconsistent.
- (B) Employee vetting practices are inconsistent BECAUSE (A) terminology used on rap sheets varies by jurisdiction and causes confusion.

Both of these statements sound logical, indicating a plausible relationship, therefore the causal relationship between the two things are considered verified.

Figure 5. Step 3, Activity 3: Causal Validation



Step 4: Create The Preliminary Cause-Effect Tree

Where are you in the RCA process?

What will you need?

- ☐ The initial cause-effect diagrams created in Step 3
- ☐ Supporting information and data
- ☐ Meeting materials (sticky notes, dry erase board, etc.)
- ☐ Meeting time and location

What will you do?

The RCA team will merge individual cause-effect diagrams into a preliminary cause-effect tree.

What is the end product?

A preliminary cause-effect tree.

What do you need to know to complete this step?

DEFINITIONS

Cause-Effect Relationship

A relationship where occurrence of one thing (the cause) leads to the occurrence of another thing (the effect), indicating a causal connection between the two.

Cause-Effect Tree

A specific diagramming technique that helps map causes and effects associated with a problem in the form of a tree. The tree graphically represents the hierarchy of causes and the flow of relationships toward their effects. Cause-effect trees are usually read from the bottom up using if-then statements in a logical format.

Causal Chain

A stream of cause-effect relationships in which a cause leads to an effect, which then becomes a cause for another effect, and that effect becomes a cause for another effect.

Intermediary Cause

An intermediary cause facilitates the causal connection between two things. It is often necessary in cases where a relationship between two things is not direct and therefore requires a lengthy explanation.

THINKING STRATEGIES

There are two thinking strategies that the RCA team can use to identify new causal relationships:

The Clarity Rule

There may be cases where there is a causal link between two things (A and B) but a third thing (C, the intermediary factor) needs to intervene to facilitate the causal flow between A and B. In other words, A and B are not directly related but have a causal relationship through C (i.e., A→C→B). This strategy helps the RCA team identify indirect relationships (e.g., education and income are linked if you are gainfully employed).

The Cause Insufficiency Rule

There may be cases where an effect will only occur if all causes are present simultaneously. This is shown in the cause-effect tree as a circle (i.e., ellipse) placed around arrows directed to that effect. This strategy helps the RCA team to identify relationships where multiple causes need to be present for the effect to occur (e.g., becoming a professional athlete is a result of talent, hard work, and opportunity).

HELPFUL HINTS

- To facilitate identification of new causes, consider all key aspects of an organization/process to capture a diverse set of issues, forces, and dynamics (e.g., policy, budget, schedule and culture).
- If the team has a hard time identifying new causes, it may be necessary to conduct additional research to include supplementary stakeholder interviews.

Using Thinking Strategies

For the Clarity Rule: If A (cause) THEN C (intermediary cause) THEN B (effect).

For the Cause Insufficiency Rule: If A (cause) and B (other suspected cause), THEN C (effect); or A and B THEREFORE C.

In a cause-effect tree, a circle around respective arrows that lead from causes to the effect represents this conditional relationship.

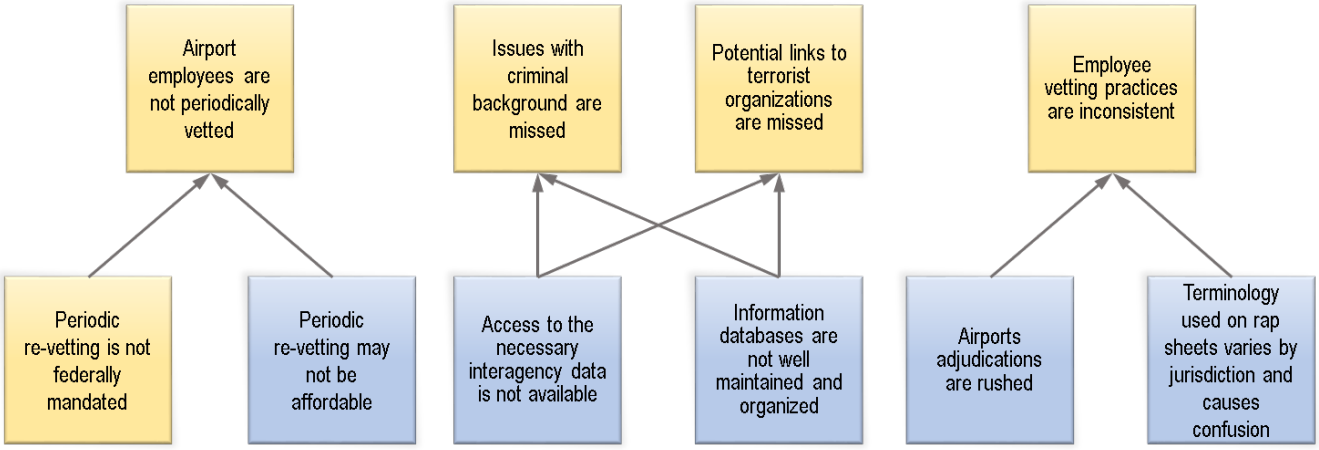
Step 4, Activity 1: Link Common Elements Across Diagrams

1. Identify common sticky notes (i.e., causes and effects) across diagrams. It is not unusual at this stage of the effort to see a single cause driving effects in multiple diagrams, or an effect from one diagram serving as a cause for an effect in another diagram.
2. Merge individual cause-effect diagrams into a single cause-effect tree by linking the common causes and effects.
3. Eliminate duplicate sticky notes and rearrange remaining ones to ensure related sticky notes are near each other on the board.
4. Draw arrows between the related sticky notes to capture their causal relationships.

Example

In the example, individual diagrams can be connected through common causes as shown in Figure 6:

Figure 6. Step 4, Activity 1: Common Elements



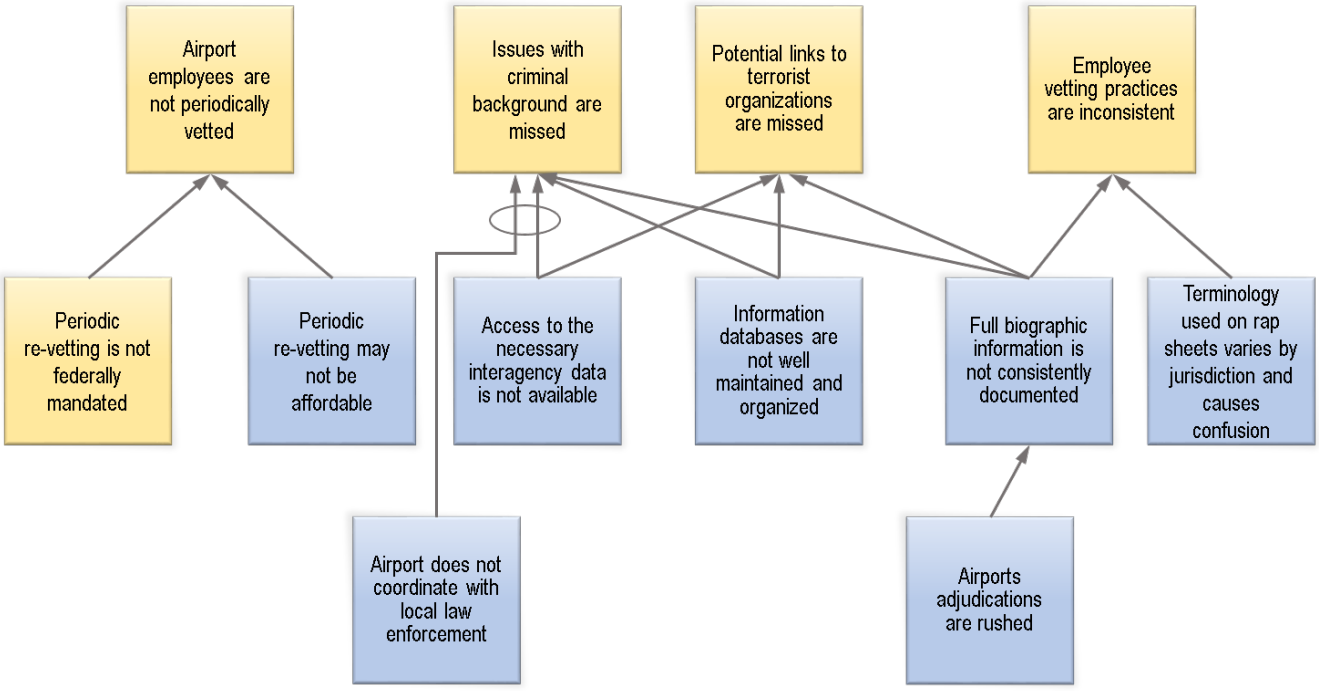
Step 4, Activity 2: Identify New Causes for Additional Connections between Diagrams

1. Brainstorm additional causes that can create new connections between elements of the developing cause-effect tree. Consider intermediary causes that may be required to establish additional causal connections. See sidebar above for using the Clarity Rule.
2. Document the new causes on sticky notes and add to the cause-effect tree.
3. Draw arrows between related sticky notes.
4. Identify effects that are conditional on the simultaneous presence of multiple causes. See the sidebar above for using the Cause Insufficiency Rule to facilitate this process.
5. Document any new causes on sticky notes and add to the cause-effect tree.
6. Draw arrows between related sticky notes, adding circle(s) around arrows to represent conditional relationships.

In the example below (Figure 7), the addition of a new factor regarding inconsistent documentation of biographic information not only clarifies the relationship between rushed airport adjudications and inconsistent vetting practices, but also facilitates additional relationships to other diagrams (i.e., the inconsistent documentation of full biographic information curbs criminal background checks as well as checks on potential links to terrorist organizations).

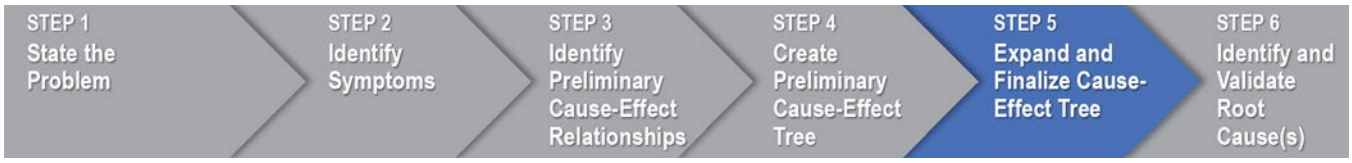
Additionally, an example of the Cause Insufficiency Rule is added to the emerging cause-effect tree. The lack of access to the necessary interagency data is, by itself, not sufficient to cause the effect of "issues with criminal background are missed." But when it happens together with the lack of airport coordination with local law enforcement, criminal issues are missed during the vetting process. This relationship is represented with a circle around the arrows leading from the two causes to the effect.

Figure 7. Step 4, Activity 2: Additional Causes



Step 5: Expand and Finalize the Cause-Effect Tree

Where are you in the RCA process?



What will you need?

- ☐ The preliminary cause-effect tree created in Step 4
- ☐ Supporting information and data
- ☐ Meeting materials (sticky notes, dry erase board, etc.)
- ☐ Meeting time and location

What will you do?

The RCA team takes the cause-effect tree to the next level by going below the surface to explore deeper forces and dynamics that drive the problem. A key part of this step is to identify and incorporate additional cause-effect relationships pertaining to these deeper forces and dynamics.

What is the end product?

A finalized cause-effect tree for the identified problem statement.

What do you need to know to complete this step?

DEFINITIONS

Feedback Loop

A closed circle of causes and effects interacting whereby a variable affects another variable and that variable affects another variable and so on with the last variable feeding into the original variable, closing the loop.

THINKING STRATEGIES

There are several thinking strategies that the RCA team can use to identify new causal relationships:

The Clarity Rule

There may be cases where there is a causal link between two things (A and B) but a third thing (C, the intermediary factor) needs to intervene to facilitate the causal flow between A and B. In other words, A and B are not directly related but have a causal relationship through C (i.e., A→C→B). This strategy helps the RCA team to identify indirect relationships (e.g., education and income are linked if you are gainfully employed).

The Cause Insufficiency Rule

There may be cases where an effect will only occur if all causes are present simultaneously. This is shown in the cause-effect tree as a circle (i.e., ellipse) placed around arrows directed to that effect. This strategy helps the RCA team to

identify relationships where multiple causes need to be present for the effect to occur (e.g., becoming a professional athlete is a result of talent, hard work, and opportunity).

The Additional Cause Rule

There may be cases where an effect is driven by multiple causes, but the occurrence of the effect is not conditional on all causes being present at the same time. The more causes that are present, the stronger the effect becomes (Walker and Cox 2006). This strategy helps the RCA team to identify alternative causes that can create the same effect (e.g., lung cancer can be a result of genetic predisposition, chemical exposure, first/second-hand smoking, or air pollution).

The Cure of the Effect

Considering a particular effect, the team can ask "If all listed causes were removed, would the effect/issue in question disappear?" This strategy will prompt the team to think about conditions under which the effect can still exist. For example: If you take away ineffective training and a broken x-ray machine, will the problem of prohibited items in secure areas exist? What else may cause prohibited items to enter into the secure areas?

The STEEP Factors

STEEP is a thinking framework that is used to identify external factors that impact the course of an organization or issue (Szigeti et al. 2011). These factors are organized into five domains: social, technological, economic, environmental, and political. This strategy helps the RCA team take a comprehensive approach and consider diverse domains and related factors to identify causes for a problem of interest (e.g., student performance may be a result of several factors from different domains: *social* – peer network and school culture; *technological* – availability of electronic learning tools; *economic* – family income and school funding; *environmental* – community income level and crime rate; and *political* – school district policies, regulations, and teaching methods).

The Iceberg Model

The Iceberg Model is a thinking framework that argues that what we can see and readily know about a problem is no different from the tip of an iceberg—only a small portion of the entire situation. In this model, there are four layers of a problem or situation: observed events, behavior patterns, system structures, and mental models. This strategy helps the RCA team gain a deeper understanding of the problem and its root causes with each layer (e.g., *event* – School A achieved poor scores in standardized tests in X year; *pattern* – School A has not been doing well in its standardized test scores for the past decade; *system structures* – teachers, learning methods, school funding, and regulations are not well aligned; *mental models* – school administration and student body do not prioritize standardized test performance). See Appendix B for a more detailed discussion of the Iceberg Model and its insights.

HELPFUL HINTS

- All RCA team members should be included in Step 5.
- If the RCA team is not able to identify additional causes and effects to expand the emerging cause-effect tree, it may be necessary to conduct an outreach to additional airport staff who are involved in problem-related activities or testing/audit activities that revealed the security problem, or to other technical experts.
- The RCA team can consider conducting a literature review to survey previous research and established empirical knowledge and evidence to identify additional causes (i.e., events, conditions, or behaviors) that may be important in explaining certain outcomes.
- There is often a trade-off between the depth and breadth of a cause-effect tree. While more detail reveals rich information about the problem, too much detail can curb the team's ability to manage the resulting RCA effort. Striking a balance between these two conflicting objectives is critical for an effective RCA.
- Given that a cause-effect tree's primary utility is to provide a big-picture view of a problem, the RCA team should include only those causes that can help explain the problem and make a significant difference in terms of its scope and severity.
- Ensure consistency across the cause-effect tree in terms of levels of details (i.e., explanation of one causal chain should not be more detailed than other causal chains). However, the RCA team may choose not to delve deeper in certain causal chains if doing so is not expected to generate valuable insights. For example, exploring causes about issues that an airport cannot control (e.g., regulatory requirements) or phenomena that do not require further explanation (e.g., holiday season and weather conditions) will not reveal insights useful for the RCA.
- If during Step 1 – State the Problem the RCA team identified related problems and developed separate cause-effect trees for each problem, those trees should be linked together during Step 5 to achieve a systemic view.
- Developing a complete cause-effect tree takes time and several iterations. Manage participants' expectations to ensure they take revisions as part of the discovery process rather than signs of confusion and lack of understanding.

Using the Iceberg Model

Consider the following questions:

- *System Structures Level:* How are various parts of the organization/process connected? Are there relationships—or lack thereof—between policies, processes, practices, and stakeholders that can help explain the problem or its symptoms? Are there problems with decision-making, flow of information, or resources? Are there healthy or perverse incentives in the organization promoting a particular behavior or outcome?
- *Mental Models Level:* How do stakeholders think about key processes and requirements related to the problem? What role do stakeholders' views play in the problem? Are there certain assumptions or biases that prevent desired outcomes?

Identifying Feedback Loops

Problems generated by complex systems often have cause-effect relationships that include feedback loops. The size of a feedback loop depends on the issue and its underlying dynamics. The smallest feedback loops include two elements (i.e., A leads to B and B, in turn, leads to A). Alternatively, a feedback loop can include several elements, with the last element feeding back to the original element that started the cause-effect chain (e.g., A leads to B, B leads to C, C leads to D, and D leads to A).

Step 5, Activity 1: Identify and Incorporate Additional Cause- Effect Relationships

1. Brainstorm new causes that need to be added to the cause-effect tree for a more complete understanding of the problem.
2. Use the thinking strategies presented above. See the sidebar on how to use the Iceberg Model.
3. Document the new causes on sticky notes and add to the cause-effect tree.
4. Draw arrows between related sticky notes.
5. If the RCA team worked on multiple, related problems and developed separate cause effect trees, identify common elements to link these trees to achieve a systemic view and complete account of the overarching problem.
6. Examine the relationships within the cause-effect tree and identify any feedback loops. See the sidebar for a discussion of feedback loops.

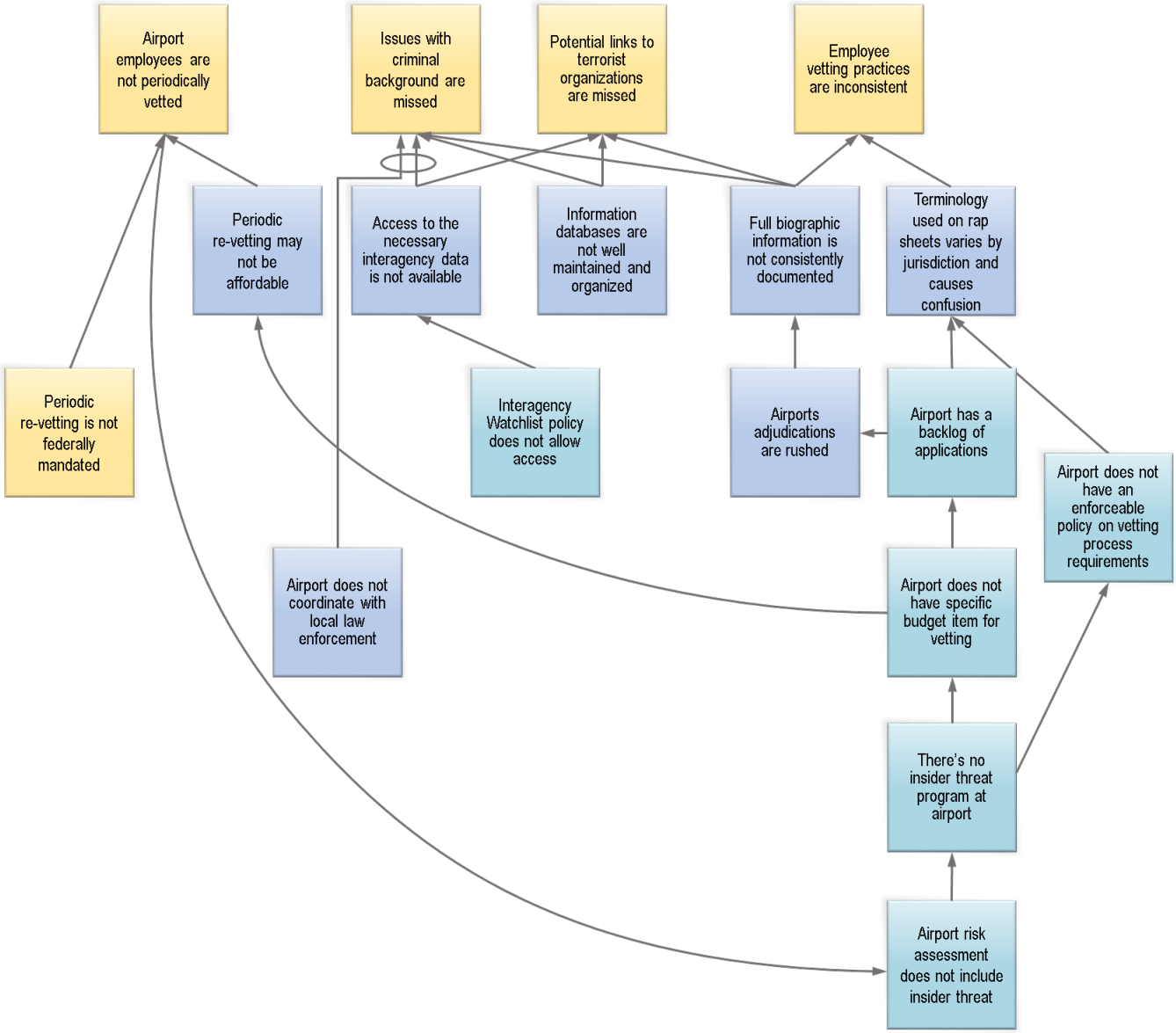
Step 5, Activity 2: Validate and Finalize the Cause-Effect Tree

1. Narrate the cause-effect tree as a team, walking through all cause-effect relationships.
2. Ensure that everyone on the team is comfortable with the tree and agrees that the relationships represented are defensible and pass the validation tests discussed in Step 3, Activity 3.
3. Update the cause-effect tree as necessary.
4. Agree as a team that this version of the cause-effect tree will be used to identify root cause(s) in the next step.

Example

As illustrated in Figure 8, several new causes and related effects (displayed as light blue sticky notes) are added to the cause- effect tree, providing a more complete account. There is also a newly discovered feedback loop: the lack of periodic re-vetting contributes to the exclusion of the insider threat from this airport's risk assessment. Without periodic re-vetting, related problems would remain unknown and unaddressed in the risk assessment process.

Figure 8. Step 5: Additional Causal Relationships



Step 6: Identify and Validate Root Causes

Where are you in the RCA process?

What will you need?

- ☐ The finalized cause-effect tree created in Step 5
- ☐ Supporting information/data
- ☐ Meeting materials (colored markers, wall or large board, copy of the cause-effect tree for each team member, etc.)
- ☐ Meeting time and location

What will you do?

The RCA team will examine the developed cause-effect tree to identify root cause(s) for the problem.

What is the end product?

Validated root cause(s) for the identified problem and supporting information for use in required reporting.

What do you need to know to complete this step?

DEFINITIONS

Root Cause

The most fundamental cause of an undesired event, behavior, or outcome that needs to be removed to prevent recurrence of the associated problems.

Causal Pathway

A specific causal chain that traces a problem or an undesirable outcome to its root cause.

THINKING STRATEGIES

There are several thinking strategies that the RCA team can use to identify and validate root causes:

The Cure of the Effect

The RCA team walks through entire causal pathway(s) associated with potential root cause(s) and ensures that, in the collective judgment, the removal of the identified root cause(s) would eliminate the problem and related issues. This strategy helps the RCA team to identify and validate potential root causes.

The 70% Test

A rule of thumb to determine the right root causes is to see if the root cause in question connects to approximately 70% of the original symptoms identified during

Step 2 (Walker and Cox 2006). This rule applies to all cases, regardless of whether there is one or multiple root causes. If there are multiple root causes, all root causes combined should account for 70% of the symptoms and, if they are addressed, almost all—if not all—associated symptoms must disappear.

Explanatory Depth

Root causes are often found at the bottom two layers of the Iceberg Model (i.e., system structures and mental models). This strategy prompts the RCA team to check for the last time to see whether they sufficiently unpacked the dynamics about the problem to identify the true root causes. For example: Is there one level below the current causes included in the causal pathways that can help explain the problem? Is there another condition, issue, behavior, or way of thinking that can account for one or more of the causes at the bottom of a causal pathway?

HELPFUL HINTS

- Ensure that the RCA effort identifies root causes that are relevant to the lowest applicable layer of the Iceberg Model. This does not mean that an RCA should always trace things back to mental models (i.e., culture, biases, organizational philosophy, and various assumptions). Mental models can explain many complex problems, but there are also cases in which it is the poorly designed or aligned system structures that are creating operational problems.
- There may be multiple root causes for a problem.
- In the case of multiple root causes, the RCA team must analyze relationships between these root causes and discuss implications. Mitigation strategies for lasting change may require simultaneous targeting of these root causes.

How do you know this is a root cause?

Root causes must be specific and actionable; that is, they represent underlying issues (i.e., factors, conditions, behaviors, and processes) that contribute to the problem and can be changed through action.

For example, human error (e.g., a linebacker keeps missing tackles) is often not a root cause as it is not clear and specific. An RCA team needs to dig deeper into the conditions and processes that contribute to the human error to establish a specific, actionable root cause (e.g., the defense does not practice proper tackling techniques). These conditions and processes must be established as root causes to identify effective mitigation actions.

Step 6, Activity 1: Identify Potential Root Causes

Review the cause-effect tree to identify critical causal pathways.

Trace the critical causal pathway by using a different-color marker and circle potential root causes for visibility. Usually, root causes are at the bottom of a causal pathway, denoting the first cause that triggered the subsequent effects, with the last one being one of the original symptoms identified in Step 2. See sidebar about how to identify potential root causes.

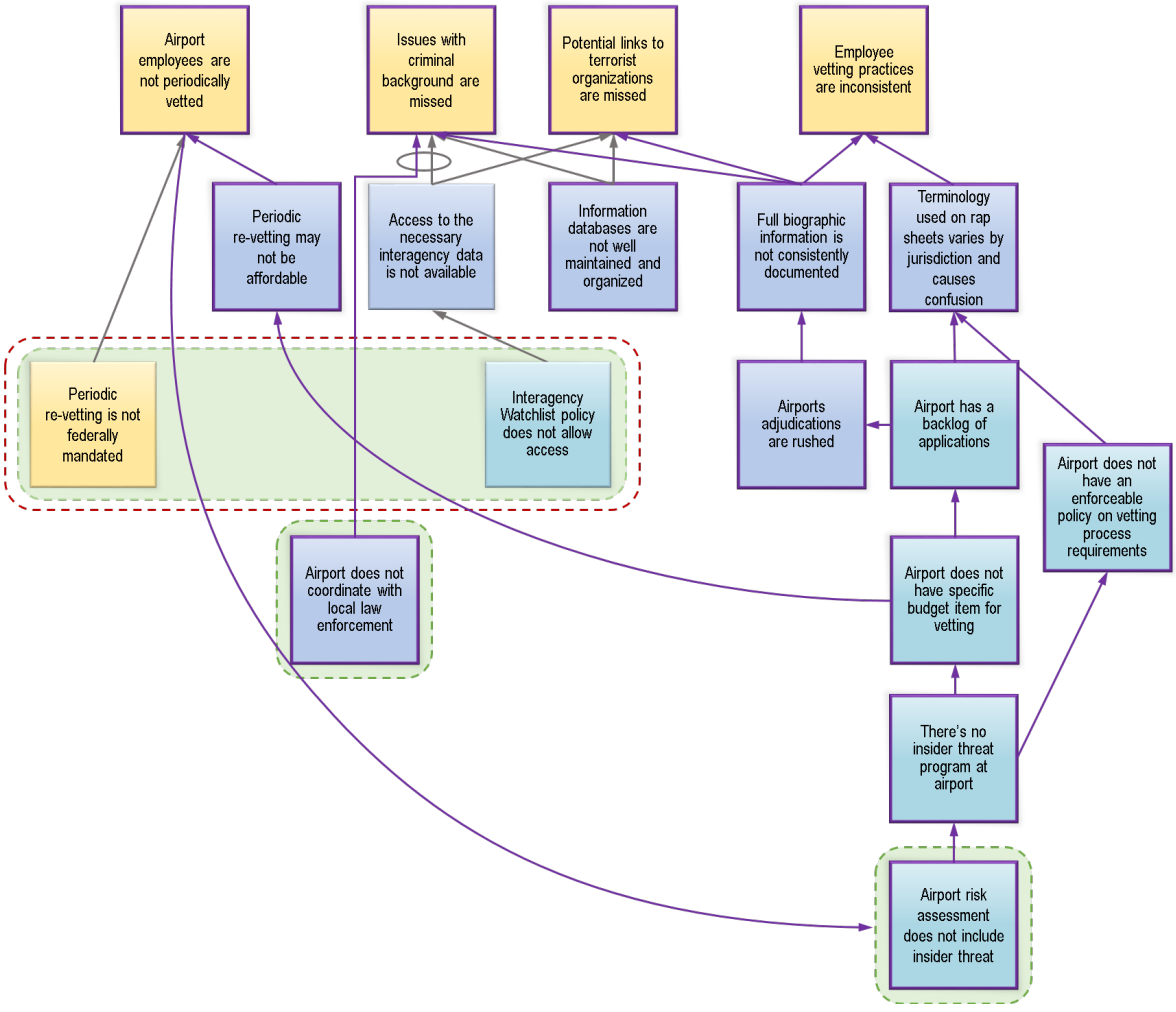
Example

In Figure 9, critical causal pathways associated with the identified potential root causes are marked using a purple highlighter.[5] The potential root causes for the airport employee vetting problem are enclosed in green boxes.[4] The cause-effect tree revealed four potential root causes, shown enclosed in green boxes:

- The exclusion of the insider threat from airport risk assessment
- The lack of airport coordination with local law enforcement
- The lack of a federal mandate for re-vetting of airport employees
- The lack of permission per Interagency Watchlist Policy for access to relevant databases

The last two root causes are beyond any airport's control to fix; they are shown with red dashed lines for clarity. The remaining two root causes are within this particular airport's control to address.

Figure 9. Step 6, Activity 1: Critical Pathways and Root Causes



[5] Note that the cause-effect tree presented here is relatively simple due to the limited information used to illustrate a notional security problem. In a real-world problem, more information would be collected and a greater number of issues and associated relationships would be documented. The methodology presented here is equipped to handle more complex problems, and will typically produce more extensive and complex cause-effect trees. The same set of rules outlined in this guidance can be used regardless of the complexity of the problem.

Why should you validate the root cause(s) outside the RCA team?

All cause-effect trees incorporate biases and perceptions of their creators (Walker and Cox 2006). Review of the cause-effect tree and designated root causes by person(s) external to the RCA team can help incorporate different perspectives and reduce systemic bias. Any resulting discrepancy should be resolved through additional sessions and iteration by the team of the respective RCA steps as necessary.

Step 6, Activity 2: Validate Root Causes

1. Validate the potential root causes as a team using root cause validation strategies such as Cure of the Effect, the 70% Test, and Explanatory Depth.
2. If additional conditions are identified under which a problem can endure, related causes and effects should be incorporated into the cause-effect tree following the previously discussed steps. Then Step 6 should be repeated to determine root causes in the updated cause-effect tree.
3. If needed, conduct a targeted external outreach to those airport staff who are knowledgeable about the problem, work in the related departments, or are technical experts, to help validate the root causes identified. See the sidebar for more information.
4. Agree as a team on the final root causes and denote them clearly in the cause-effect tree.
5. Document the cause-effect tree for follow-on efforts (e.g., take a picture of the board and replicate the cause-effect tree digitally).
6. Develop a narrative explanation/rationale for the causal link between the problem and its root causes.
7. Identify and compile all supporting materials, such as written documentation, graphics, process charts, SOPs, audio and video recordings, electronic data, and photographs.

Example

In the example problem, the elimination of the identified root causes with appropriate mitigation actions would remove all subsequent negative effects, eliminating the majority of the symptoms within this airport's control. Given that there are two root causes not controlled by the airport, some of the forces driving this problem may persist, but it would not be due to any noncompliance or security vulnerability caused by this airport's own processes or actions. Such situations indicate a collaborative problem-solving effort is needed with external entities and agencies.

While conducting root cause validation (e.g., using Explanatory Depth), the RCA team in this example might consider whether the insider threat is rooted in a cultural bias toward employees (i.e., a general belief that employees cannot be security threats, or that real security threats are created by external forces) or empirical evidence and trends. If it is the former, the airport can include an additional cause in the cause-effect tree to capture this cultural factor/condition to meet the explanatory depth test discussed above. Inclusion of this cause in the cause-effect tree would also be critical to inform subsequent mitigation planning, as it would likely include activities to promote a cultural shift in the mindset of airport operators.

SECTION 5: YOU HAVE YOUR RCA RESULTS – NOW WHAT?

- Document and present results of the RCA
- Identify leverage points
- Understand how to use RCA results during and beyond mitigation

Once the RCA is concluded, there is still a significant amount of work that needs to be completed in order to mitigate or eliminate a noncompliance or vulnerability. After the RCA is complete, it is important to continue to engage all stakeholders and provide transparency regarding the way in which the RCA results feed into any subsequent mitigation design and planning. This openness also allows widespread access to and reflection upon the RCA findings, solidifies the culture of teamwork, increases a sense of ownership of the problem, and facilitates buy-in for recommended mitigation actions. The RCA team will also want to refer back to the plan for disseminating the RCA results that was developed during RCA planning.

The following activities provide a general overview of tasks to be completed as the airport transitions into mitigation planning.

5.1 Create an RCA Results Package

The RCA results package contains information that was generated during the RCA effort. This information will help the RCA team justify and disseminate RCA results and facilitate the broader airport efforts to transition into mitigation planning. The RCA package should include a clear, concise statement that accurately captures the root cause(s). In addition, the RCA team should write a description that tells the story of how the problem is connected to the identified root cause(s) through respective relationships and interactions included in the cause-effect tree. This documentation should also include the final version of the cause-effect tree, as well as any supporting materials collected during the RCA process, to facilitate meetings with stakeholders inside and outside an airport.

5.2 Identify Leverage Point(s)

RCA results help airports make the most informed decisions to effectively address a vulnerability or noncompliance. However, root causes identified at the end of an RCA process may not lead directly to mitigation actions. At this point, the airport personnel need to consider where the airport has leverage in the cause-effect tree to remove the root cause(s) identified so that the problem is eliminated.

Key Takeaway

While root causes drive problems, leverage points indicate where airports can intervene to address those root causes. When identifying leverage points, airports need to consider:

- Root causes
- Potential impact
- Control

A leverage point is a place or point in a problem where action can be taken to address root cause(s) and initiate lasting change within the respective system or organization (Meadows 2008). The identification of leverage points requires consideration of three things. Places in a system where all three considerations are met are ideal places to act in order to address a problem. These considerations are:

1. *Root Cause(s).* Leverage points in a system or problem may either coincide with or be closely related to root causes through cause-effect relationships. Therefore, root causes are good places to start in identifying leverage points.
2. *Potential Impact.* Although there may be multiple leverage points in a system, they may have varying levels of impact (Meadows 2008). As a rule of thumb, a cause with multiple effects often indicates a place where action can bring about positive change that ripples through the system, eliminating a number of related negative issues. As such, leverage points that have many arrows coming out of them (indicating their ability to influence different parts of the system) often indicate an opportunity for high impact.
3. *Control.* Leverage points are also places where a decision-maker has control to intervene or implement response strategies to address a problem. In other words, some root causes may not be places where action can be taken, others may not promise large-scale influence in the system, and still others may be beyond a decision-maker's control to induce change (e.g., federal regulations, human nature, or external forces).

5.3 Identify, Implement, and Monitor Corrective Action(s)

After leverage points are identified, airports should determine corrective actions or mitigation strategies to eliminate a noncompliance or vulnerability. The following activities should be conducted:

- *Identify Corrective Actions*. To improve the odds of curing a problem, airports should target the highest-impact leverage point(s) that are within their control. Although high leverage points are preferred, low leverage points also have value. For example, mitigation efforts targeting high-impact leverage points may take time to plan and implement; therefore, while working on such mitigation activities, airports may want to implement fixes involving low leverage points for short-term improvement. For leverage points that are beyond an airport's control, joint mitigation strategies through collaboration with external stakeholders should be explored.
- *Coordinate with TSA (if applicable)*. If the RCA is part of an APP, the airport will meet with the Designated TSA Official (DTO) to determine whether proposed mitigation actions are commensurate with the noncompliance or vulnerability. During these discussions, the airport must be prepared to discuss the results of the RCA and provide any supporting materials that justify conclusions. Supporting materials can include all written documentation, audio and video recordings, electronic data, and photographs that demonstrate the noncompliance or vulnerability. At the conclusion of the meeting, TSA and the airport should reach agreement on the root cause and the mitigation measure(s) to be implemented in the Action Plan. After agreeing upon the root cause and corrective actions, the DTO will create and send to the airport the Action Plan Letter, which details the corrective action(s) agreed upon by the parties during the meeting(s) (for more information, see the TSA Action Plan Program, issued June 26, 2019)[6].
- *Implement Corrective Actions*. Before implementing corrective actions, the airport should do proper implementation planning to include roles and responsibilities, an implementation schedule with milestones and conclusion dates, and supporting elements that may be required, such as changes or additions to policy, processes, training, staffing, or budget.
- *Monitor Implementation Results.* Once a corrective action has been implemented, the airport should assess whether the action has actually resulted in elimination or mitigation of the vulnerability or noncompliance. This can be accomplished through testing, a vulnerability

[6] https://www.tsa.gov/sites/default/files/action_plan_program.pdf

assessment, or a simple verification process if the issue is a basic noncompliance situation. This activity also acts as the final validation step for the RCA if it demonstrates that addressing the designated root cause(s) got rid of the problem. If the problem still exists despite the corrective action, the RCA team should reexamine the problem by rethinking the root cause(s), seeking more impactful leverage points, or collecting additional information about the problem to revise the cause-effect tree.

5.4 Learning from the RCA Activities

Although each RCA effort is conducted for a specific problem, the experience may help identify insights that go beyond that problem. After an RCA is completed, the RCA team should consider holding a hotwash meeting to discuss things that went well and areas that need improvement. The insights can be documented in an after-action report.

Additionally, periodic trend analysis across all conducted RCAs can identify patterns in root causes or types of problems. Such higher-level assessments can provide strategic clues about the broader operational health and effectiveness of an organization. For example, if multiple RCAs are concerned with a seemingly recurring problem, this may indicate a failure in identification of true root causes.

Similar problems may indicate the presence of a much broader systemic issue, requiring a more comprehensive assessment. This type of trend analysis may also reveal that a specific part of a process or organization is highlighted by multiple RCAs, which may require further investigation into that aspect of the system.

REFERENCES

Adams, M., M. Kiernele, L. Pollock, and T. Quan. 2004. *Lean Six Sigma: A Tool Guide.* Colorado Springs: Air Academy Associates.

Boardman, John, and Brian Sauser. 2008. *Systems Thinking: Coping with 21st Century Problems.* Boca Raton, Florida: Taylor & Francis Group.

Burton-Houle, T. 2001. *The Theory of Constraints and Its Thinking Processes*. The Goldratt Institute.

Chambliss, Daniel F., and Russell K. Schutt. 2006. *Making Sense of the Social World: Methods of Investigation*. 2nd ed. Thousand Oaks, California: Pine Forge Press.

Federal Aviation Administration. 2020. "What is Part 139? Part 139 AirportCertification." Accessed November 2020. https://www.faa.gov/airports/airport_safety/part139_cert/what-is- part-139/

Kim, Daniel. 1992. "Guidelines for Drawing Causal Loop Diagrams." The Systems Thinker, Leverage Networks. https://thesystemsthinker.com/guidelines-for-drawing-causal-loop-diagrams-2/.

Meadows, Donella H. 2008. *Thinking in Systems: A Primer.* White River Junction, Vermont: Chelsea Green Publishing.

Snowden, David, and Mary Boone. 2007. "A Leader's Framework for Decision Making." *Harvard Business Review* 85: 68–76, 149. Accessed October 2020. https://hbr.org/2007/11/a-leaders-framework-for-decision-making.

Sterman, John D. 2000. *Business Dynamics: Systems Thinking and Modeling for a Complex World*. New York: McGraw Hill.

Sterman, John D. 2006. "Learning from Evidence in a Complex World." *American Journal of Public Health* 96: 505–514. https://ajph.aphapublications.org/doi/pdfplus/10.2105/AJPH.2005.066043.

Systems Innovation. 2018. "Iceberg Model Explained." https://systemsinnovation.io/post/iceberg-model-explained/.

Szigeti, H., M. Messaadia, A. Majumdar, and B. Eynard. 2011. "STEEP Analysis as a Tool for Building Technology Roadmaps." Paper presented at the International Challenges e-2011 Conference, Florence, Italy.

Taylor, Lloyd J., and R. David Ortega. 2003. "The Application of Goldratt's Thinking Process to Problem Solving." Paper presented at the Allied Academies International Conference, Academy of Strategic Management.

Transportation Security Administration. 2019a. "Outcome-Focused Compliance" brochure. Accessed February 2020. https://drive.google.com/file/d/0Bx9D-qebvaRBT25wcEpGQ0dETkk/view.

Transportation Security Administration. 2019b. "TSA Action Plan Program." Accessed February 2020. https://www.tsa.gov/sites/default/files/action_plan_program.pdf.

Transportation Security Administration. 2020. Action Plan Program Industry Review Townhall Meeting Discussions, TSA Headquarters, February 25, 2020.

Vorne. "Theory of Constraints." Accessed February 2020. www.leanproduction.com/theory-of-constraints.html.

Walker. E. D., and J. F. Cox. 2006. "Addressing Ill-Structured Problems Using Goldratt's Thinking Processes: A White-Collar Example." *Management Decision* 44, no. 1: 137–154.

APPENDIX A: OUTCOME-FOCUSED COMPLIANCE

Outcome-Focused Compliance (OFC) is a security management approach recently adopted by TSA. Different from TSA's traditional, penalty-focused, civil-enforcement framework, OFC is a collaborative security philosophy. The primary goal of OFC is to "increase partnership [of TSA] with industry stakeholders, mitigate vulnerabilities, obtain compliance, and sustain the highest levels of security through shared outcome" (TSA 2019b). To improve transportation security, OFC focuses on three things: outcome, partnership, and innovation. Accordingly, OFC relies on best practices from transportation industry stakeholders, TSA field and headquarters offices, and other initiatives to achieve and sustain the highest compliance and security outcome (TSA 2019a). The focus on partnership involves efforts to collaboratively identify and mitigate security problems. Finally, OFC promotes sharing of information and lessons learned that help develop innovative and proactive solutions without legal enforcement measures.

The partnership element is the key driver of OFC activities. Therefore, in addition to the traditional enforcement tools (i.e., oral or written counseling and administrative action to include warning notices and letters of correction, legal enforcement action, and referral for criminal prosecution), OFC provides transportation security stakeholders with the following collaborative tools and programs to promote joint identification and mitigation of security problems (TSA 2019b):

- *Industry reviews* provide industry stakeholders with various opportunities to get together with TSA so that they can provide input to ongoing OFC-related processes, share feedback and information to identify root causes of security problems, and develop solutions jointly.
- *Risk ranking* is an OFC practice that aims to prioritize security requirements so that more critical risks are addressed first in recognition of time and resource limitations.
- *Self-audits and testing* (to include both self and joint testing) are concerned with identification of security problems. While self-audits are conducted to evaluate compliance and overall effectiveness of security management, testing is carried out to ensure effectiveness of security measures.
- *Voluntary disclosure* promotes industry stakeholders to notify TSA of instances of security noncompliance, to jointly address the security issues without the burden of a legal enforcement process. The voluntary disclosure procedure involves an eligible party notifying the DTO about the noncompliance and then following up within 7 days with a report that includes a description and summary of the noncompliance, a description of the immediate action taken, and a summary and analysis of supporting material.
- The *Action Plan Program* (APP) is the most novel practice of the OFC program. It serves as the main implementation tool of the OFC security paradigm, whereby transportation security stakeholders collectively address security problems identified and conveyed through the other tools discussed above (i.e., industry reviews, risk ranking, self-audits, self and joint testing, and voluntary disclosure). As such, action plans are greatly emphasized, sometimes leading to the misconception that they are same as the broader OFC program.

  APP "provides an opportunity for eligible parties and TSA to discuss and reach an agreement on corrective actions to address the root cause(s) of any security vulnerability or noncompliance with TSA's security requirements, which qualifies for this program, and resolve that vulnerability or noncompliance with administrative action instead of a civil enforcement action" (TSA 2019b). APP, once agreed upon by TSA and the eligible party, documents the problem, the results of root cause analysis conducted by the eligible party, and the agreed-upon mitigation

actions along with a binding schedule. APP and the related process rely on voluntary participation by eligible parties based on the incentive that such participation allows resolution of security problems without a traditional civil enforcement process and, as such, without a violation history. In the APP process, eligible parties can "offset potential civil penalties with investment and without a formal adjudication of regulatory violations" (TSA 2019b).

APPENDIX B: THE ICEBERG MODEL

The Iceberg Model is a simple systems thinking tool that helps with examining a problem comprehensively and across time to identify potential root causes. It utilizes key RCA concepts discussed in this guidebook, portraying their inherent relationships. Based on an analogy, the Iceberg Model argues that what we can see and readily know about a problem is no different from the tip of an iceberg—only a small portion of the entire situation. Consequently, this initial understanding may not be representative of the true nature and magnitude of the problem. The latter requires seeing what is below the surface. Similar to an iceberg, "a large percentage of what is going on in our world is hidden from view, and the Iceberg Model tries to make this explicit by depicting it as a series of layers that sit beneath the everyday phenomena observed" (Systems Innovation 2018).

According to this model, there are four levels of abstraction about a problem or a situation:

- **The first level of the model, Events,** represents conditions, behaviors, and outcomes that we can easily observe in our everyday lives. As such, they are the visible portion of the iceberg. Events tell us the state of things; when we get a sense that things are not working as they should, we refer to one or more events as symptoms to substantiate our perceptions. For example, a conversation between a couple of friends about current gas prices indicates event-level information exchange. High gas prices are undesired events/outcomes that consumers complain about and are symptomatic of a deeper problem. Event-level thinking can only help us answer the question of "*what happened?*" and keeps us acting in a reactive mode.
- **The second level of the model, Patterns of Behavior,** is the first layer beneath the water line. It refers to trends in cause-effect relationships that you can notice only when you look across a number of events (i.e., observations). If the same or similar events are recurring, it indicates that these events are related rather than being isolated incidents, and rely on the same cause-effect relationships. A comment about increasing gas prices when there are political tensions in world affairs relies on this type of an observation, indicating a pattern. This level of thinking allows us to answer the question of "*what has been happening?*" Having patterns of behavior-level understanding of issues allows us to predict the related trends and act accordingly.
- **The third level of the model, System Structures,** refers to causal relationships between key system elements and how they work jointly, producing patterns and events that we observe. System structures can include elements such as institutions, policies, rules and laws, social and cultural norms, distribution of power and resources, and governance practices. Combined, they shape incentive and sanction structures in a system and help us explain why things (i.e., events and behavior patterns) happen the way they do. Therefore, system structures often are good starting places to look for root causes of problems. For example, gas price fluctuations are ultimately a manifestation of our dependence on fossil fuels that are more readily available in different parts of the world. Understanding the consequences (i.e., effects) of structures can help us identify leverage points in a system/problem and design new structures that are more aligned with our desired outcomes.
- **The fourth level of the model, Mental Models,** refers to individual perspectives and worldviews about how the world works. Mental models are an amalgamation of our beliefs, values, attitudes, experiences, and assumptions. We may not be always aware of our mental models or their constitutive elements, but they subconsciously shape the way we think about things and justify the structures we put in place or the way we behave within them. Mental models are often associated with the ultimate root causes of complex problems. For example, our dependence on fossil fuels may be produced by our mental models that value the privacy and

comfort of private vehicles or deemphasize the importance we attach to developing alternative fuel sources. This level of abstraction helps us answer the question of "*what keeps the system/structures in place?*" Mental models represent the most impactful leverage point in a problem, as shifting mental models can help transform a system or organization along with its outcomes.

In sum, the Iceberg Model makes the point that generating system-wide, lasting change requires moving lower in the level of abstraction when trying to understand and resolve complex problems. The event-level thinking can address only symptoms of a deeper problem, producing quick fixes with short-term improvements. Pattern-level thinking, while representing a deeper level of understanding, does not go sufficiently below the surface to uncover real causes, falling short of providing cures to complex problems (e.g., stockpiling fuel before an anticipated political or economic crisis). Complex problems are often caused by deeper forces that are situated at the structure or mental model level. RCA efforts need to understand the full spectrum of cause-effect relationships within a problem and identify causal pathways that trace problems to their root causes. Mitigating actions must target the root causes found at the lowest possible level (given resource feasibility and mandate of the intervening agency) to ensure effectiveness of solutions.

APPENDIX C: RCA METHODOLOGY QUICK LOOK

1 State the Problem

ACTIVITIES

Activity 1

Gather all Required Information and Data

1. Collect all relevant information about the identified noncompliance or vulnerability.
2. Combine the information collected during the RCA Planning Phase with observations and ideas gathered through stakeholder interviews or surveys.

Activity 2

Document the Problem Statement

1. Write a problem statement.
2. Write a paragraph to provide available details about the problem.
3. Agree as a team on the official Problem Statement.

THINKING STRATEGIES

None

OUTPUT

Problem Statement

2 Identify Symptoms

ACTIVITIES

Activity 1

Brainstorm about Symptoms

1. Brainstorm as a team about possible symptoms of the problem and capture each on a post-it.
2. Attach all suggested post-it notes to a large board or wall where everyone can see the information

Activity 2

Determine Symptoms

1. If you have more than 8 symptoms, reduce the number of symptoms.
2. Develop a justification for each symptom in the list.
3. Document each symptom on a post-it note with a clear and concise sentence.
4. Gather symptoms that are determined to be inaccurate, less critical or potentially duplicative and place in a "parking lot.

THINKING STRATEGIES

None

OUTPUT

5-8 symptoms

3 Identify Preliminary Cause-Effect Relationships

ACTIVITIES

Activity 1

Determine Potential Cause-Effect Relationships between Symptoms

1. Pair up each of the symptoms and see if any are causally related.
2. Place the post-it notes representing causes at the bottom and post-it notes representing the effects at the top.
3. Draw arrows between related post-its. If no relationships are identified between symptoms, skip this activity and continue with Activity 2.

Activity 2

Determine Potential Causes for Each Symptom

1. Brainstorm to suggest causes for each symptom.
2. Document each new cause identified with a post-it.
3. Draw arrows between post-it notes to capture suspected causal relationships and form an individual diagram for each symptom.

Activity 3

Validate Causality

1. Validate each cause-effect relationship using simple logic tests.
2. Document the validated cause-effect relationships as individual diagrams.

THINKING STRATEGIES

- 3 Cause-Effect Relationship conditions
- Five-Whys
- Causality Rule
- Tautology Rule

OUTPUT

Initial Cause-Effect Diagrams

4 Create Preliminary Cause-Effect Tree

ACTIVITIES

Activity 1

Link Common Elements Across Diagrams

1. Identify common post-it notes (i.e., causes and effects) across diagrams.
2. Merge individual cause-effect diagrams into a single cause-effect tree by linking the common causes and effects.
3. Eliminate duplicate post-its and rearrange remaining ones to ensure related post-its are nearby on the board.
4. Draw arrows between related post-its.

Activity 2

Identify New Causes for Additional Connections between Diagrams

1. Brainstorm additional causes that can create new connections between elements of the developing cause-effect tree.
2. Document the new causes on post-it notes and add to the cause-effect tree.
3. Draw arrows between related post-its.
4. Identify effects that are conditional on simultaneous presence of multiple causes.
5. Document any new causes on post-it notes and add to the cause-effect tree.
6. Draw arrows between related post-its adding circle(s) around arrows in the cause-effect tree to represent conditional relationships.

THINKING STRATEGIES

- Clarity Rule
- Cause Insufficiency Rule

OUTPUT

Preliminary Cause-Effect Tree

5 Expand and Finalize Cause-Effect Tree

ACTIVITIES

Activity 1

Identify and Incorporate Additional Cause-Effect Relationships

1. Brainstorm new causes that need to be added to the cause-effect tree using thinking strategies..
2. Document the new causes on post-it notes and add to the cause-effect tree.
3. Draw arrows between related post-its.
4. Examine the relationships within the cause-effect tree and identify any feedback loops.

Activity 2

Validate and Finalize the cause-effect tree

1. Narrate the cause-effect tree as a team, walking through all cause-effect relationships.
2. Ensure all the cause-effect relationships represented are defensible and pass the validation tests discussed in Step 3, Activity 3.
3. Update the cause-effect tree as necessary.
4. Agree as a team this version of the cause-effect tree will be used to identify root cause(s) in the next step.

THINKING STRATEGIES

- The Clarity Rule
- The Cause Insufficiency Rule
- The Additional Cause Rule
- The Cure of the Effect
- The STEEP Factors
- Iceberg Model

OUTPUT

Cause-Effect Tree

6 Identify and Validate Root Cause(s)

ACTIVITIES

Activity 1

Identify Potential Root Cause(s)

1. Review the cause-effect tree to identify critical causal pathways.
2. Trace the critical casual pathway by using a different color marker and circle potential root cause(s) for visibility.

Activity 2

Validate Root Cause(s)

1. Validate the potential root causes as a team using root cause validation thinking strategies.
2. If needed, incorporate any additional conditions under which a problem can endure and the related causes and effects into the cause-effect tree.
3. If needed, conduct a targeted external outreach to additional airport staff to help validate the root causes identified.
4. Agree as a team on the final root cause(s) and denote clearly in the cause-effect tree.
5. Document the cause-effect tree (e.g. take picture or digitally re-create).
6. Develop a narrative explanation for the causal link between the problem and its root cause(s).
7. Identify and compile all supporting materials.

THINKING STRATEGIES

- The Cure of the Effect
- The 70% Rule
- Explanatory Depth

OUTPUT

Validated Root Cause(s)

APPENDIX D: THINKING STRATEGY QUICK LOOK

Causality Rule	Cause-Effect Relationship Conditions	Tautology Rule	Five-Whys	Cause Insufficiency Rule	Additional Cause Rule
A change in a variable (cause) necessarily leads to a change in another variable (effect). There is a causal link between the two variables. If A (cause) THEN B (effect) or A THEREFORE B.	In suspected cause-effect relationships, the following three conditions must hold: • *Covariation:* Whenever the cause occurs, the effect must also occur. (i.e., if A then B) • *Temporal Precedence:* The cause must occur before the effect. (i.e., A occurs before B) *Control for Third Variables or Non-Spuriousness:* There must be no plausible alternative explanation indicating a third variable is causing the effect (i.e., other potential variables are identified and ruled out in favor of A causing B)	A change (effect) in a variable occurs as a result of a change in another variable (cause). B (effect) BECAUSE A (cause).	Ask the question of "why" five or more times to progressively identify deeper forces that are related to a problem. Why did A (effect) occur? Because of B (cause). Why did B (effect) occur? Because of C (cause). Why did C (effect) occur? etc.	Effect is due to multiple causes and those causes need to all happen for the effect to occur. If A (cause) and C (cause) THEN B (effect).	Effect is due to multiple causes, but those causes do not need to all happen for the effect to occur. Presence of one of the causes is sufficient for the effect to occur. B (effect) may occur due to A (cause) OR C (cause) OR D (cause).
STEP 3	STEP 3	STEP 3	STEP 3	STEP 4 and STEP 5	STEP 5

Clarity Rule	The STEEP Factors	Iceberg Model	Cure of the Effect	Explanatory Depth	The 70% Test
A variable may be related to another variable through an indirect relationship. An intermediate variable connects the two variables. A(cause)→C (intermediate cause)→B(effect).	When identifying causes, consider factors from five overarching domains: social, technological, economic, environmental and political.	When identifying causes, consider the four layers of a problem: observed events, behavior patterns, system structures, and mental models. Root causes are often found in system structures and mental models.	Considering a particular effect, ask "if all listed causes were removed, would the effect/issue in question disappear?" Will B (effect) still occur if A (cause) and C (cause) are removed?	To determine the right root causes, see if the dynamics about the problem have been sufficiently unpacked in reference to system structures and mental models (from Iceberg Model).	To determine the right root causes, see if the root cause in question connects to approximately 70% of the originally identified symptoms.
STEP 4 and STEP 5	STEP 5	STEP 5	STEP 5 and STEP 6	STEP 6	STEP 6

APPENDIX E: CAUSE-EFFECT TREE EXAMPLE

This example illustrates how the RCA methodology presented in this guidebook works using an everyday problem.

STEP 1: STATE THE PROBLEM

The RCA team considered the problem of weight gain during winter months. After some internal discussion, the team developed the following problem statement. The description includes additional details about this problem, such as the amount of weight gain experienced on average.

Example: Weight Gain during Winter Months – Step 1

Problem Statement: People usually gain weight during the winter season.

Description: On average, people gain an additional 10% of their body weight during winter months. This has physical and mental health repercussions.

STEP 2: IDENTIFY THE SYMPTOMS

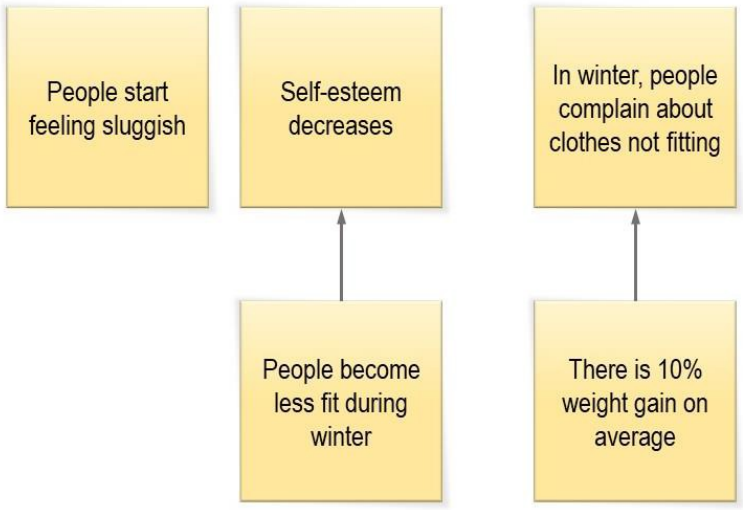
The RCA team identified five symptoms for the problem of weight gain during the winter months. They put symptoms on sticky notes and placed them on the board where everyone can see.

Example: Weight Gain during Winter Months – Step 2

STEP 3: IDENTIFY PRELIMINARY CAUSE-EFFECT RELATIONSHIPS

During Step 3/Activity 1, the RCA team identified only two relationships between symptoms. Decreasing fitness levels during winter decreases self-esteem. Also, the 10% weight gain causes people to complain about their clothes not fitting.

Example: Weight Gain during Winter Months – Step 3, Activity 1



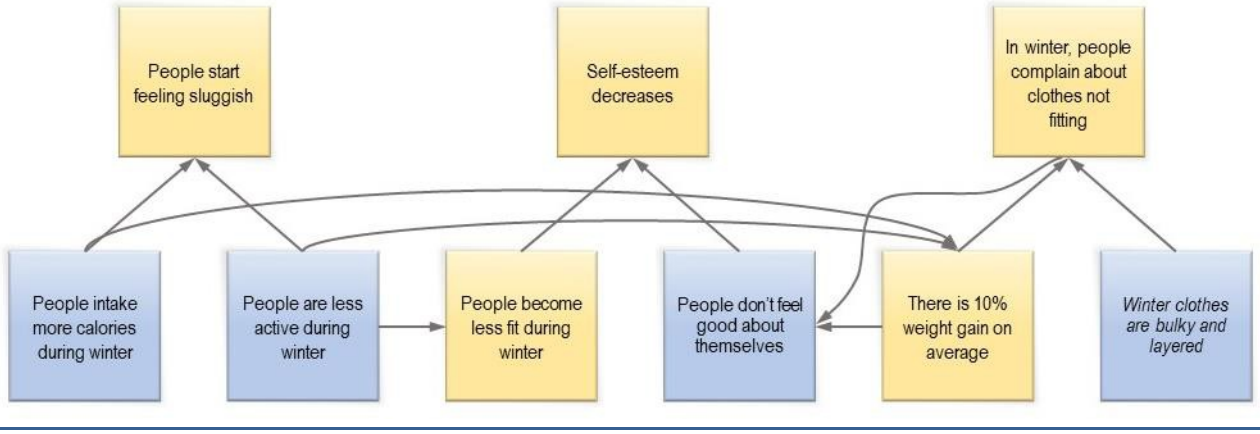
During Step 3/Activity 2, the RCA team identified some causes for the symptoms. People start feeling sluggish because they take in more calories and are less active during winter months. As people become less fit and don't feel good about themselves, their self-esteem decreases. Also, the 10% weight gain and bulky winter clothes cause people to complain about their clothes not fitting right.

STEP 4: CREATE THE PRELIMINARY CAUSE-EFFECT TREE

During Step 4/Activity 1, the RCA team looked into linking common elements across diagrams. There were no common elements.

During Step 4/Activity 2, the RCA team identified new causes to facilitate additional connections between diagrams. They discovered that less activity during winter leads to decreased fitness, allowing the team to make connections between these two diagrams that were previously not linked. Similarly, 10% weight gain causes people to not feel good about themselves. There was also a causal connection between people's clothes not fitting right and people feeling less good about themselves. Finally, the team identified a couple of causal connections between the first and the third diagrams: increased calorie intake and less activity leads to 10% weight gain during winter months.

Example: Weight Gain during Winter Months – Step 3, Activity 1



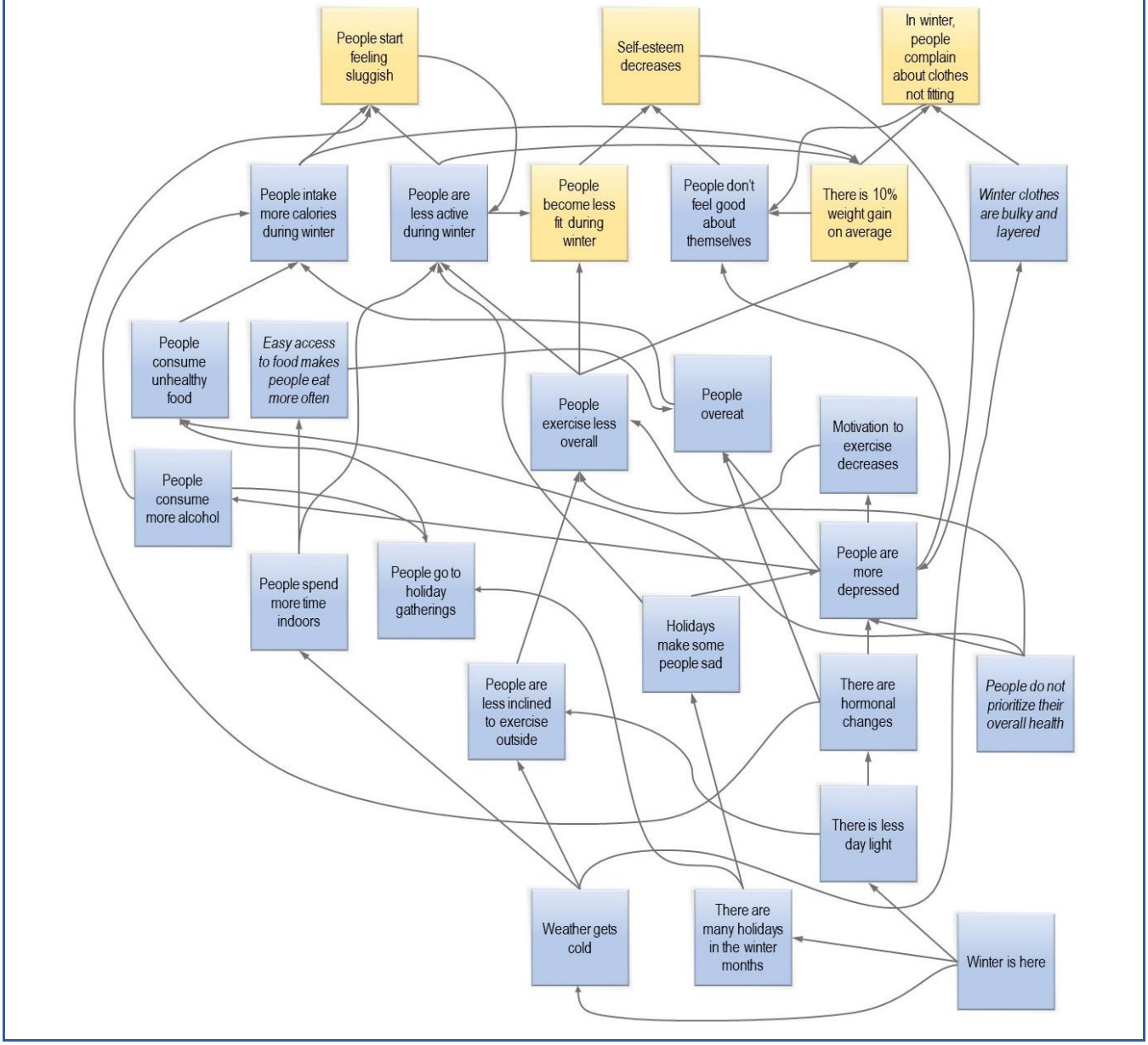
STEP 5: EXPAND AND FINALIZE THE CAUSE-EFFECT TREE

During Step 5/Activity 1, the RCA team identified and incorporated additional cause-effect relationships using a number of thinking strategies. Using the clarity rule, the RCA team decided that people eat more unhealthy food during winter months because of the holidays. But to make the connection, they had to add an intermediary cause: going to holiday gatherings. Holidays in winter cause people to go to holiday gatherings, which encourages increased consumption of unhealthy foods.

Also, during this activity the RCA team referenced the Iceberg Model to make sure they considered factors pertaining to the lowest layers—system structures and mental models. After some discussion, they decided that both consumption of unhealthy food and declining exercise levels tie back to how people prioritize their physical and mental health. It is this mental model that shapes people's everyday choices about what they eat and what they do to stay healthy.

During Step 5/Activity 2, the RCA team validated and finalized the cause-effect tree.

Example: Weight Gain during Winter Months – Step 5, Activity 1



STEP 6: IDENTIFY AND VALIDATE ROOT CAUSES

In Step 6/Activity 1, the RCA team reviewed the tree to identify potential root causes. Three were identified, one of which was subsequently deemed out of their control: people not prioritizing their overall health (surrounded by a green box), people going to holiday gatherings (surrounded by a green box), and the winter season (surrounded by a green box and red dashed lines). Winter appears to be the driver of most of the effects on this cause-effect tree, but there is not much people can do to change the fact that they will experience winter each year. However, seeking actionable points in the lower stream of the cause-effect tree, the RCA team determined that people can change how they handle holiday gatherings (by changing their food consumption behaviors) and their priorities in life (by putting more emphasis on being healthy, and adopting practices that can improve their overall physical and mental well-being). There are other actionable points in the cause-effect tree, but finding root causes that are actionable and located in the lowest possible parts of the cause-effect tree is the key, as any change made in those points will drive the subsequent effects on the tree, leading to the largest possible impact.

In Step 6/Activity 2, the RCA team validated root causes through internal discussion and external outreach as necessary, and then used a purple highlighter to designate the final root causes and associated critical causal pathways.

Example: Weight Gain during Winter Months – Step 6, Activities 1 & 2