



Reliability Response Guide®

and

Manager's Version Reliability Response Guide®

Instruction Manual

Collaborative Just Culture®
Collaborative High Reliability®

Version 9.2
Revised February 2025



SG Collaborative Solutions, LLC™
Designed for Impact. Powered by Partnership.

Copyright © All Rights Reserved



Preface

Introduction and Access

This instruction manual provides operational guidance on using both versions of the SGCS Reliability Response Guide™ (Full Version and Manager's Version). The manual supports SG Collaborative Solutions clients with access to the SGCS Collaborative High Reliability™ and Collaborative Just Culture™ suite of integrated products. Users must be authorized by an organization or entity under contract with SGCS.

Prerequisite: Online Training Through SGCS's Learning Management System

- *Orientation to Collaborative High Reliability Certification*
- *Principles of Reliability*
- *Performance vs. Behaviors*
- *Using the Reliability Response Guide™ (Full Version), or*
- *Using the Manager's Version of the Reliability Response Guide™*
- *Essential Supervisor Skills*
- *Case Practices (Number of practices based upon LMS Level)*

Alternate Prerequisite: *Documented attendance at Live, On-Site Training Sessions or approved hybrid training encompassing all of the above.*

Related Documents

- SGCS Reliability Response Guide™ (RRG)
- SGCS Reliability Response Guide, Manager's Version™ (MRRG)
- SGCS Collaborative Risk Review™ (CRR) Manual
- Reliability Management Team™ (RMT) Manual

Revision Date of Approval: 2024-08-13

Revised by: Paul M. LeSage

Edited by: Dale Oda, MD

Approved by: K. Scott Griffith

Signature: _____



Feedback

SG Collaborative Solutions values your feedback. Please provide general comments, along with any errors and omissions, to: info@SGCPartners.com



Table of Contents

	Preface	Page 2
	Preparing to use the Guide: Fact-Gathering	Page 4
	Peer & Organizational Perspective – Red & Blue Boxes	Page 12
	See and Understand Risk	Page 14
	Competing Priorities & Biases	Page 17
	System Reliability	Page 19
	Organizational Response: Test and Manage Potential System Reliability Improvements (FULL RRG Only)	Page 26
	Human Reliability – Performance	Page 28
	Human Reliability – Behaviors & Errors	Page 37
	Organizational Response	Page 51
	Organizational Reliability	Page 52
	Attachment A: Human Error	Page 55
	Attachment B: Bias Review Checklist	Page 60
	Attachment C: At-Risk Choice	Page 62
	Attachment D: Resource Reading List	Page 66





Preparing to Use the Guide: Fact-Gathering

Fact-Gathering

The first step in analyzing any risk event is to undertake a fact-gathering process. Good fact-gathering is not simply an objective, dispassionate collection of factual information and data – it also includes legal responsibilities, empathy, sympathy, support for staff and clients, and a host of other details. We highly recommend those using the RRG take the 1-hour course in fact-gathering, as the course material covers several very useful examples. The Fact-Gathering course is available on the SGCS LMS Platform, and access can be provided by your SG Partner or Project Manager.

Step One: Ensure Support

We must first ensure that customers, staff, family, visitors, and other involved parties receive immediate support for any physical, emotional, or psychological needs. All those involved in the risk event should be contacted as soon as possible to ensure support is arranged immediately after the risk event.

A list of available resources (e.g., Peer Support, CISD, etc.) should be readily accessible by any staff member. In addition, there should be a specific person assigned to the role of overseeing and coordinating support to confirm that it has been provided. Ensure that the appropriate Human Resources staff members and departmental leaders have been contacted in the event employees need time off work or other support.

Notifications

While support is being delivered to those who need it, ensure prompt notifications of the event are completed based on the situation. Some examples:

- **Leadership** – Departmental leaders should be notified of any event that impacts ongoing operations, staffing, or client/customer/patient risk. Directors and Executive Leadership are generally notified when emergency operations are triggered, when the organization faces potential external scrutiny from regulators and/or the media, in situations where the risk is ongoing and not yet mitigated, or in other serious circumstances (generally a list that is determined by each organization).
- **Safety Director and/or Emergency Manager** – In a severe or complex event, consult with the Safety Director or designee to see whether the incident warrants a larger, more coordinated and comprehensive response (e.g., Incident Command System). The need for an operational shutdown or a transition to limited operations should also be determined.
- **Regulator Contacts** – Incidents involving adverse events often need to be reported to external regulators or internal auditors. Fact-Gatherers are among the first to be notified of a risk event, and





must be able to identify situations which require reporting to a regulator. For example, in healthcare, many states require reporting of Serious Reportable Events (SRE) based on the National Quality

Forum List of SREs, and other serious adverse events, as well as the results of any organizational risk analysis.

Safety and Risk professionals are generally very familiar with situations that meet the thresholds for reporting and formal reporting requirements. Fact-Gatherers also must be able to identify situations that necessitate reporting to a regulator and/or a separate Federal agency, such as Food and Drug Administration (FDA) tracking medical device issues, or Department of Environmental Quality (DEQ) for aviation gas (Av-Gas) spills. They should work collaboratively with their Safety and Risk colleagues to ensure all reporting requirements are met promptly.

An example would be clinical risk reporting. An incident may meet the threshold for local or state clinical regulatory reporting, but the Fact-Gatherer may not be aware that the case requires reporting to an industrial regulator, such as State or Federal Occupational Safety and Health Administration (OSHA), Environmental Protection Agency (EPA) or the Department of Environmental Quality (DEQ).

- **Staff Contacts** – After the well-being of involved staff has been assured and they are able to participate in an analysis, they should be informed of a pending interview, and initial interviews should be scheduled with a Fact-Gatherer as soon as possible. Their managers (and, if applicable, the appropriate Labor Representative) should also be notified of the interviews (and the potential for a Collaborative Risk Review, if indicated) to ensure those individuals are available. In a Collaborative Just Culture, participation in fact-gathering and analysis should be included in a policy and/or an expectation for all staff. Leaders must support participation in Collaborative Risk Reviews (CRR) as a priority. (See the Collaborative Risk Review Manual for suggested timelines associated with staff notifications and conducting CRR's). Staff and their managers must be made aware of how important their participation in a CRR is in helping the organization see, understand, and manage risk.
- **External Support** – Every risk event is different. There may be instances when the response demands support or expertise beyond the ability of the Fact-Gatherer and/or resources of the organization to provide. When encountering those situations, Fact-Gatherers must be aware of external resources (in addition to internal departments) from various domains who may be contacted for assistance. It may be helpful to have a list of external agencies available to Fact-Gatherers for quick reference. This might include support for emergency water/food/shelter, transportation, emotional support, communication, supplies, legal assistance, etc.

Gather and Secure Relevant Items

The Fact-Gatherer must begin the process of collecting all charts, reports, electronic data, and other materials related to the event. Relevant policies and procedures should be gathered to see how they may have contributed to the risk. Fact-Gatherers should be aware of the potential for bias when conducting extensive policy review *before* initial interviews are conducted.





Appropriate people should be contacted to confirm that any equipment and data that may have been involved is secured or sequestered, including written, audio, video or digital data. This might mean storing sensitive electronic documents on a protected server separate from the organization's network, for instance. There may be times when certain equipment cannot be taken out of service (e.g., if they are necessary for continuing

ongoing operations). Taking photos may serve to illustrate issues later for others to appreciate influences from its design or issues related to dysfunction.

There may also be situations where the design or layout of the facility itself or incident location contributed to an event. Similarly, if it is not feasible for the team analyzing the event to personally view the site, it may be helpful to present the spatial issues with a diagram in order for others to have that perspective. Remember to sequester all collected documentation and equipment in a secure location, and maintain confidentiality.

Step Two: Review of Materials Collected

Review the Documentation

The initial review of most risk cases starts with analyzing reports, charts, written documentation, and digital data. Generally, starting from the primary risk (closest to the harm or risk) and working backward is the most efficient use of your time. There are exceptions, particularly related to risks the organization has seen frequently. But in most cases, working backward from the primary identified risk or event will work best. The goal is to collect as much information as possible to gain an understanding of how the system and involved humans failed to see and/or manage the risk. An initial step may be to learn how the socio-technical system was *supposed* to manage the risk, and note what conditions were different or unusual in this instance.

Be Curious and Careful

Ask a few pertinent questions to give you better overall understanding of the situation. For example:

- What else was going on at the *same time* that may have been distracting?
- Were there other demands on the system or the people that, in your opinion, may have affected the outcome or the process?
- How often do these simultaneous issues happen?

Be careful when referring to what's in a chart or written report as "facts." These should be considered *known elements* of the case (written documentation), but in many cases written documentation has been proved inaccurate before, during, or after the CRR. Most people document the information *as they perceive it*. And even machine-generated documentation, such as a monitor feeding information into a flight database or patient chart can be found inaccurate. Go in with the understanding that what you are reading may be an incomplete picture, and expect that documented times and time-stamps will not be fully accurate or synchronized.

Areas Potentially Needing Further Exploration





Check for any chart or record updates, merges/modifications, and if the report or chart is relatively consistent with the stories you have heard to this point. If there is an electronic record of who accessed the record or chart, take note of this and correlate it to any new or edited entries. If there are issues in the documentation that require further clarification, determine whether this is best done through interviews, further research, or other methods. Also, look for inconsistencies with the metrics that have been entered and any additional data you might need to provide further clarification (e.g., maintenance records, lab reports, imaging interpretations,

etc.) Check to see whether the data fields, such as gauge readings, vital signs, etc., support the narratives found in the reports and interviews.

Document the Contributors

Start with a template or clean sheet that has these categories so you reliably document contributors:

- Persons involved – this may change as you engage in discovery during your analysis.
- Risks:
 - Risks that appear to not have been seen or understood by staff involved;
 - Risks that may have been seen, but not fully understood, by staff (they knew there was a risk but did not fully understand the severity, probability, or other factors);
 - Risks that were understood to be present, but there was no way to see them (no dashboard, indicators, or other cues to indicate the risks were present).
- Competing priorities – take note of any discussion associated with staff who appear to be influenced by multiple competing goals, objectives, tasks, etc.
- System issues – those that seem evident in the report, and those that are known to be present and designed to manage the stated risks. Recall that systems can include equipment, processes, policies, and other socio-technical combinations.
- Human Performance issues – knowledge, skills, ability, proficiency issues, distractions, etc.
- Choices – violating rules, policies, best practices, etc.

Review reports and records carefully and note *Contributors* when you see them. Whether a Contributor is categorized correctly at this point is not important. Just capturing it is crucial. For example, in a report, you might find that the writer documented that she was fatigued. This likely would initially be written down as a Human Performance Factor, but you might find during further interviews that the fatigue was because of a system issue (e.g., mandatory overtime) or a personal choice (partied late before work).

Timelines and Tools





Timelines, templates, checklists, and other tools can be very helpful in understanding a sequence of events. However, users should be aware of potential drawbacks of the tools they are using. For example, templates and checklists create an incomplete picture. While they may provide reminders to assess certain items, users may be biased into not looking for other related issues.

Similarly, most timelines also carry a heavy bias – they represent only things that were thought to be relevant to the incident or risk being studied. Timelines that demonstrate only the unique times and factors in the event being analyzed, and that do not include peripheral factors, are called “Two-Dimensional” because they comprise only the times and events associated with the risk being examined. Two-Dimensional timelines

typically do not include distractions, fatigue, competing priorities, or other issues/risks being managed at the same time.

More effective, and less bias-inducing, are “Three-Dimensional” timelines. They include the relevant times and factors that appear directly related to the risk event, but also incorporate other factors that are simultaneously occurring and may have affected system or human performance. For example, in examining the timeline for an event that occurred in an Emergency Department, the initial timeline included only the times that a particular patient was seen, examined, received medications, and had interventions done. From reading the Two-Dimensional timeline, it appeared that there were inappropriate gaps between patient interventions. When a third dimension was added, which included other critical patients in the ED at the time, Radiology back-ups, later-arriving patients who were triaged as more critical, etc., a more balanced view of the operational and clinical risks became evident.

Step Three: Initial Interviews

Schedule and Prepare for Interviews

Use the list of people involved and the notes you have taken to set up any necessary interviews, as soon after the event as possible, in preparation for the CRR analysis. Be sure the people you are interviewing know the purpose of the interviews (to gather information about the event from their perspective) and that you are not trying to find fault. Plan on conducting the interviews more like a conversation over coffee than a deposition.

Setting up interviews can run the full spectrum from a quick phone call and open dialogue, to extremely difficult with a person being combative or defensive. In some cases, staff members who were involved in a risk event may be contractually required or ask to have a representative accompany them during an interview. This may be a labor association representative, or someone who can provide support while the individual relives the event during the interview. The Fact-Gatherer must be aware of both the employee’s and the organization’s rights prior to engaging in an interview with a representative present. In most cases, the representative is not allowed to answer questions for the employee, prevent the person being interviewed from answering the question, or stop the interviewer from asking a particular question – they are present to *witness* the interview and document whether the interviewer violated any of the employee’s rights.

While an employee’s refusal to consent to an interview may be considered, in some cases, a violation or insubordination, the Fact-Gatherer must remember that except in rare cases (See “Group vs. Separate





Interviews” below), the intent is to conduct interviews with empathy and curiosity. Therefore, it’s crucial to know before entering these types of interviews how to manage a situation when a witness or the employee asks questions related to specific labor laws, such as Garrity or Weingarten rights (US Law), or other rights afforded them in collective bargaining agreements. Remember, you are conducting an analysis, not an “investigation” or a deposition.

It can be helpful to call for assistance when an interviewee appears to be on guard by working your internal channels to find someone who can join the interview to help defuse some of the anxiety. If potentially severe conflicts amongst certain departments or individuals may exist, consider assigning a Mentor from the RMT to those departments/individuals who can provide guidance about the CRR process and what it is meant to accomplish.

Some organizations record interviews for accuracy. While we have no strong opinion one way or another on whether interviews are recorded, we will say that there are a few things that must be taken into consideration if you decide to record:

- Ensure you know the laws of your state or region before recording an interview.
- Be prepared to provide a copy to the person being interviewed, and/or allow them to record on their own device while you are recording on yours (this is a trust issue).
- Make sure you have a policy about where these recordings are kept, how long they are held before destruction, and who has access to the files.
- Do not keep recordings on any personal laptop or device – these should be kept only on a laptop or other device that has secure or encrypted access.

Group vs. Separate Interviews

Whenever possible, *interview teams as a group*, not individually. Having teams interview together allows members to support each other and confirm times and sequences. It generally gives a much richer and more comprehensive view of what happened. Conversely, in law enforcement interviews and most legal depositions, team members are separated to see if their stories differ. For Collaborative High Reliability, we strongly suggest you develop a more judicious approach to determining the conditions that will compel you to separate staff members for interviews.

For an open, collaborative process designed to find proactive solutions to risk, segregating the people being interviewed creates big problems. Most people’s perceptions are not completely accurate, so it is extremely rare to have everyone tell the exact same story when separated (story congruence in itself would be suspicious to a veteran investigator). It also leaves you the chore of trying to determine which version of the story is most accurate. Last, there is substantive science that shows we tend to believe people who we know and trust over people we don’t know, and that unconscious biases are powerful in forming our mental pictures from the narratives we hear.





There are, of course, some situations when separating people for the initial interviews may be appropriate or necessary. But these are usually instances involving employee conflicts, power gradients, potential reckless or higher-culpable behavior investigations, or situations where you suspect an employee is afraid to speak freely while in a group. One technique that is covered in the Fact-Gathering course is to listen and watch carefully during group interviews – if only one person is answering all the questions, and the others seem deferential or quiet, we recommend that at the end of the group interview you thank everyone, and let them know that you will be following up with individual interviews.

Tips for Interviews

- **Be perceptive during interviews:** Interviewers should watch for potential areas of conflict such as tension or finger-pointing among individuals, angry responses, or facial expressions. Sometimes, anger or frustration may be manifested by silence and withdrawal. Whatever cues are being picked up by the Fact-Gatherer that signal tension, it may be necessary to remind everyone about our goal of trying to

obtain the details of the event and not to find out who was at fault. Fact-Gatherers must also recognize if anyone is in need of support and promptly refer that person to appropriate support services. If the Fact-Gatherer senses that someone is reluctant to speak freely in the group interview, they may need to schedule a separate meeting with that individual.

- **Assign a Scribe and Secure Notes:** Document the interviews by taking good notes. It is very helpful or even necessary to assign a scribe during the interviews. Keep the notes secure and prepare to build a slide presentation for the CRR based on your interview notes as well as your review of the charts and reports. Keep your notes and presentation in a separate folder stored in a secure location before the CRR.
- **Avoid delaying the CRR:** Try not to delay the CRR because of a delayed interview. Interviews before a CRR are not always possible because of work schedules, staffing issues, other conflicting responsibilities, etc. Go forward with a CRR if there is sufficient information collected, with an understanding that others will be interviewed when possible to complete the analysis.

Tips for Managing the Fact-Gathering Process

Consider the timing of your fact-gathering efforts. The following tips have been generated by other Fact-Gatherers and are based on their experiences:

- Memories tend to fade quickly. There is qualitative and quantitative research showing people have a steep loss of memory within days, or even hours, after an event. More recent studies have shown that people forget details (or their memories change) even when related to events that evoked strong emotions. Note: Consider how quickly the National Transportation Safety Board responds to gather information after an incident.
- Misinformation is also more likely to be generated the more time that an event is talked about informally. Information from participants/witnesses quickly degrades as people are exposed to bias, media questions, and hypothetical opinions associated with “what went wrong” or “who did what.”



- 
- Equipment and physical system components are more likely to be modified, damaged, or “fixed,” either purposefully or inadvertently, as time passes.
 - Risks from continued (unexamined) operations may exist and require immediate attention, personnel, and resources.
 - There may be significant time required for the team to gather necessary information, records, equipment, and front-line interviews.
 - The psychological status of involved team members may need to be addressed, depending on the outcome and/or the situation.
 - Strong emotions often cloud the ability of those involved and the analyst team to clearly see and understand the event. You and other Fact-Gatherers will need to remain curious and objective – not upset or overly influenced by an adverse outcome.
 - Conflicts of interest among team members may need to be addressed – for example, analyst team members may have operational responsibilities or relationships with individuals involved in the risk event being analyzed.
 - Besides harm to a customer, patient or employee, there are concerns of potential harm to employees or the organization involved in a risk event. Regulatory agencies, the news media, prosecutors, and even fellow employees often engage in finding fault. Fault-finding can be important for the necessary legal, personal, and financial accountability exercises after an undesired outcome, but it rarely provides insight into proactive measures to help manage or minimize future risks. This is important for Fact-Gatherers (and Facilitators) to keep in mind.

Other Considerations

During fact-gathering and analysis, there may be materials, data, performances, or behaviors that create concerns about legal exposure to the organization or the people involved. During the fact-gathering process (records review and interviews) or while analyzing the event in the CRR (for the purpose of understanding and managing future risk), sensitive information may be uncovered and potentially used against the people involved in the event.

Concerns that the legal system, news media, or regulators may use such information against the organization or individuals may cause delays in implementing recommended strategies to improve systems, performance, or behavior. Therefore, it is vital to have Risk Management professionals, as well as Quality and Safety teams, collaborate in gathering information before a CRR. This is particularly important for public entities, where nearly every email, phone record, and calendar entry may be considered an accessible public record.

Careful review of the recommendations, and vetting them through a collaborative team approach, is the best method for ensuring effective, resilient action that safeguards protected legal information and avoids unnecessary exposure for the organization. In sensitive cases, there should be co-facilitation of the CRR



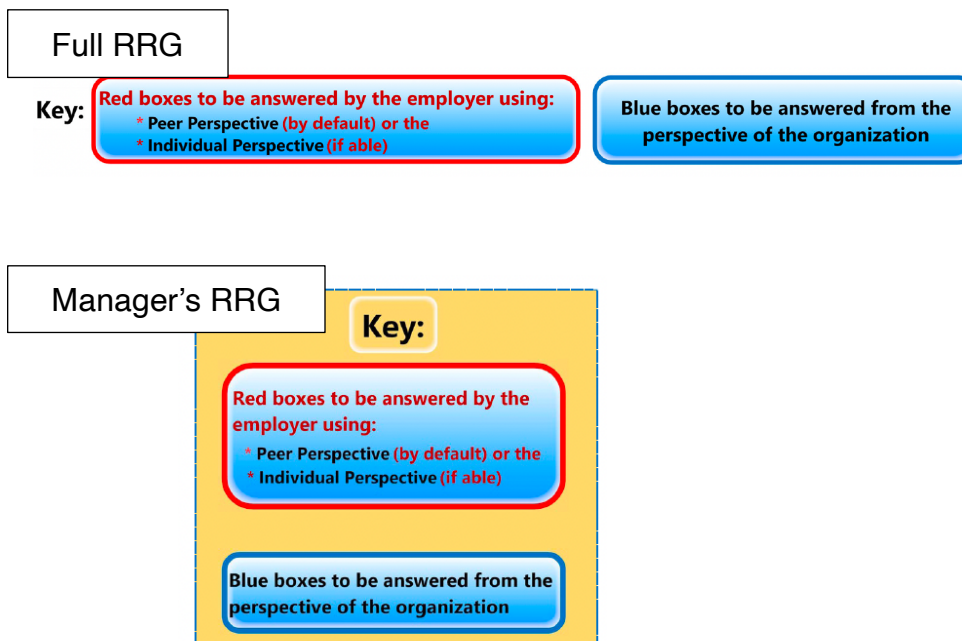
session with Risk/Quality/Safety to ensure information is managed appropriately and according to policy. In addition, all communication, slides, and other materials used for a CRR should be appropriately marked with the organization's confidentiality statements.

Ideally, you should be working with other members of your team as you gather facts and start your analysis. Multiple perspectives, when balanced, can provide optimized viewpoints and solutions. A well-structured team approach can minimize the effects of individual bias and provide more robust solution-sharing. However, collaborative work can also be challenging when multiple points of view overlap and present competing perspectives. Be aware that teams can be biased, too, and be watchful of group think and other vulnerabilities inherent in team dynamics.

Prepare your team and yourself. Be ready to listen carefully and to document what you hear. Maintain curiosity – how does this event make you feel? What judgments are you making? Imagine you are looking at a tip of the iceberg-type event and your primary goal is to see below the surface. How does this event potentially represent other unseen system, performance factor, and/or behavioral choice risks?

Peer & Organizational Perspective – Red & Blue Boxes

Peer Perspectives are Key in Understanding Risk





Why we need to understand behaviors: A fundamental concept associated with Collaborative High Reliability is the need to try to comprehend what compels and motivates people inside a system to act in a particular way. We often find leaders and managers who are reluctant or resistant to engage in any effort to *understand* a person's behavioral choices and errors. We hear them say, "They knew the rule, they knew they were breaking the rule, and they knew the consequences – why should I try to understand why?" There is a major difference between *understanding* behavior and *condoning* it. If your goal is to build a better, more effective and resilient system, you have to work hard to try to understand how, when, and *why* individuals will fail to follow rules, regulations, policies, and procedures within the system. Why didn't they see the same risk you see? Are there competing priorities, and are their priorities misplaced due to a difference in risk intelligence or risk tolerance? (See descriptions below)

Collaborative High Reliability Organizations are constantly trying to see what *compels* behavioral choices and human error. The Reliability Response Guide® uses a system of "Red & Blue" boxes to help guide you and your team's perspective. While technically *all* of the questions are answered from the perspective of the employer or their representative, the red boxes ask that you gain the perspective of those who are currently using your system and who are obligated to follow your rules, policies, and procedures. We call this the **Peer Perspective**. It is the view of front-line peers who work *within your organization, inside the same area and/or system* as the individuals who are being analyzed. It is *not* a legal "substitution test," it is *not* an exercise to determine negligence or fault, it is *not* the perspective of someone who does the same job in a different organization, it is *not* the perspective of the educator who may have trained staff members, and it is *not* the

perspective of a Supervisor or Manager who used to work the front line (or who still does). It is designed to help you establish RISK. The Peer Perspective will help you determine whether the individual(s) involved in the event are the risk, or whether you have a more widespread risk among the work group (which is likely systemic, not individual in nature).

A simple Peer Perspective can be seen when we return to the streets to examine our behaviors. As we note in the Risk section below, the law might say the speed limit is 65 MPH (104.6 KPH). Everyone knows what the rule is – it's posted. You're traveling, though, at 5-10 MPH over the speed limit. Would your peers say this is reckless behavior? What are your peers doing? Of course, they're likely going as fast or faster – so we know the Peer Perspective associated with minor speed transgressions and risk perception on the freeway simply through observation and past practice. If you were traveling at, say, 30 MPH over the limit, your peers would likely agree this is reckless, regardless of your opinion.

We recommend lots of practice with your team and your SG Partner to help you make the proper determinations related to these perspectives.





See and Understand Risk

Full RRG

1. See and Understand Risk

- Has thorough, objective fact-gathering been accomplished?
- Does the organization fully See the risk(s)? Understand the risk(s)?
- Which organizational attributes are jeopardized by the risks identified?
- Have both the **SYSTEM** and **HUMAN** contributors been identified?
- Have competing priorities and biases been identified?

Manager's RRG

1. See and Understand Risk

- Do you need assistance from a Reliability Management Team member?
- Have you gathered enough facts to begin your initial risk assessment?
- Do you fully See and Understand the risk(s) or need assistance?
- Which organizational attributes are jeopardized by the risks identified?
- Have both the **SYSTEM** and **HUMAN** contributors been identified?
- Have you identified all competing priorities and biases?

See and Understand Risk





You must first *See* and *Understand* the risk(s) that you are evaluating. This can be quite challenging due to different *perceptions of risk*. Because each individual may perceive, process, and respond to risk differently, identifying and quantifying risk can be a challenge. The following are two key concepts associated with how risk is perceived and managed:

Risk Intelligence: Risk intelligence is gained primarily through life experiences. Risk intelligence is associated with our ability to determine whether something we perceive poses a risk, the potential severity of the risk, and whether we should respond. Our risk intelligence relates to everything we do at home and at work, and it continually evolves as we gain more experience.

- Consider the first time you took a family member or friend out to teach them how to drive a car. To new drivers, everything poses a potential risk, and they have not yet built “intelligence” around how to evaluate and manage these potential risks. The more experience they gain as drivers, the more comfortable they are in managing risks, and they develop a sense of what risks need to be actively managed, and what risks can be passively managed. Importantly, risk intelligence that we have gained through experience can be accurate or it can be flawed – we can acquire the “wrong” intelligence when we have practiced something many times and believe we are safe based on never experiencing an undesired outcome. For example, you may have texted while driving many times with no adverse outcome – you know it’s against the rules, but your risk intelligence “tells” you that you are safe based on your positive experiences.
- Another example would be driving 10 miles over the speed limit on the freeway – if you are a veteran driver, based on your risk intelligence you are likely to believe this is safe. You can apply this to wearing

PPE, how often you wash your hands, or any human endeavor. Because we all have experienced life differently, nearly everyone has slightly (or even dramatic) differences in how they see various risks.

Risk Tolerance: Everyone has different tolerance for risk. Risk tolerance is considered the amount of risk that you will accept before taking some sort of action to manage or mitigate the risk. Importantly, like risk intelligence, risk tolerance is unique to every human in that not everyone will share exactly the same tolerances. The following is a way to look at risk tolerance and risk intelligence in an everyday situation:

- The *risk tolerance* of the state related to road speed is written in the law (rules) and also posted on the side of the road (signs). This is the adopted maximum level of risk that the state will accept. Consider that in a 65 MPH zone on the highway, the state allows you to go only a maximum of 65 miles per hour, and anything over that is against the law. Now consider the state in this example to be the organization you work within. The organization has SOP’s, SOG’s, policies, and posted signs that dictate the maximum risk tolerance for the organization, just like the state has laws and signs. If I want to know an *organization’s* risk tolerance, I need only look at the rule books. If I want to know how the humans see risk inside that organization, I need to look further.
- So now let’s consider the *risk tolerance* of the individuals who are responsible for enforcing the rules. For the state, this would be the state trooper, and for the organization, it’s likely you or a colleague – a leader or manager. We can probably agree that it’s unlikely a state trooper would give you a ticket for



going 67 or 68 MPH on the freeway in a 65 MPH zone. In other words, while you are clearly exceeding the *state's risk tolerance*, you are not exceeding the *state trooper's risk tolerance*. The state trooper is an experienced driver and risk manager, and his or her *risk intelligence* tells them that in most conditions, a few miles per hour over the speed limit doesn't pose a risk. You can imagine this is the same for your organization – regardless of which “rule” you apply this to, different managers, supervisors, and leaders have differing risk tolerances, and make daily decisions on which rules to enforce and at what level – just like the state troopers. And their risk tolerance is based, of course, on the previously discussed *risk intelligence* of each trooper, manager, or leader.

- Last, we would consider the risk tolerance of the individual driver on the freeway or the employee who works for your organization. Of course, by now you know that their risk intelligence and tolerance will be quite varied. This is why the first step is always an exercise in trying to *See and Understand the Risk*. This requires a discussion and collaboration on identifying the risk(s) and risk perceptions, since everyone involved is likely to see and understand them differently.

Risks to Organizational Attributes or Values: Many models of high reliability prioritize safety as the only (or primary) attribute to preserve. CHR strives to preserve multiple key attributes or values that are essential for an organization to be highly reliable including: Safety, Customer Service, Quality, Financial Responsibility, Privacy, Operational Integrity, and Equity. Consider how some of the following examples could jeopardize some of these essential attributes:

- Customer (or patient) harm
- Employee harm (physical and/or psychological)
- Visitor harm
- Negative publicity
- Harm to the organizational mission or values
- Monetary or other financial harm
- Equipment damage or destruction
- Operational disruption
- Strong mission or production values (creates safety vs. production competing priorities situation)
- Organizational and/or Individual Biases

Other Methods to Determine Risk: There are many methods for identifying risks on both individual and organizational levels. For an organization, risk can be identified through reporting, audits, observation, vulnerability assessments, quality review, actual incidents, or other methods. For example, if the wrong medication was administered, the primary risk is “Patient harm – from wrong medication administration.” If there was a motor vehicle accident (or a close call, or a driving policy violation), the primary risk is potential for



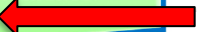
individual harm and/or property damage. In addition, try to determine whether front-line individuals might perceive a different risk than that seen by organizational leaders. For example, if the hospital keeps supplies under lock and key, a primary risk seen by *management* might be inventory control. However, the primary risk as seen by *front-line personnel* might be a negative impact on efficiency.

System and Human Contributors to Risk: Prior to your analysis, discuss what you know from the fact-gathering process. What appeared to be *systemic* contributors to the risk? What were some of the *human* contributors? The process of asking questions as you go through the RRG will help define more exact descriptions of both systemic and human risk. Listen carefully to the narrative given by those involved in the risk event. How did they perceive risks? What were the Competing Priorities?

Competing Priorities & Biases

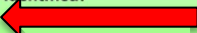
Full RRG

1. See and Understand Risk

- Has thorough, objective fact-gathering been accomplished?
- Does the organization fully See the risk(s)? Understand the risk(s)?
- Which organizational attributes are jeopardized by the risks identified?
- Have both the **SYSTEM** and **HUMAN** contributors been identified?
- Have competing priorities and biases been identified? 

Manager's RRG

1. See and Understand Risk

- Do you need assistance from a Reliability Management Team member?
- Have you gathered enough facts to begin your initial risk assessment?
- Do you fully See and Understand the risk(s) or need assistance?
- Which organizational attributes are jeopardized by the risks identified?
- Have both the **SYSTEM** and **HUMAN** contributors been identified?
- Have you identified all competing priorities and biases? 





Competing Priorities: Are there competing organizational priorities influencing these risks and the way they are perceived and managed? We should always have an interest in the organizational or personal *incentives* that compel behavioral choices. Socio-technical science has shown, over and over again, that people make choices based on bounded rationality – what do they perceive as the highest utility, best immediate benefit, and what is their risk perception? For most people, this is associated with the “goals and objectives of the day.” What needs to be completed today in order for me to meet the organization’s production targets, and for me to feel like I fulfilled my job’s objectives?

- Incentives induce behavior, and if we understand what front-line operators are thinking during a decision process, we can better understand organizational and individual risk, where these views intersect, and where they depart from one another. It’s important to recognize we are not *condoning* any behaviors at this point – we are only trying to *understand* what may have compelled or incentivized a particular behavioral choice. Think of it as trying to view the situation through the “lens” or eyes of the people who are doing the work and managing the risks at the front line.
- Humans are rarely driven to action solely by rules – they are compelled by perceptions of risk, a sense of mission and by their operational goals. Individuals often will say that something “made” them make a particular choice. When safety and quality rules affect production and mission goals, it’s more likely that the individual felt *compelled* or *influenced* to make a choice based on a production incentive or goal they perceived as having a greater importance than safety. Their *risk intelligence* told them this was the best choice, and their *risk tolerance* has been modified by repetitive positive feedback associated with meeting goals.
- Two of the most common competing priorities are Production and Safety. People will trade safety where they do not perceive risk in order to meet production or operational goals that are reinforced by the organization. Besides Production and Safety, other common competing priorities are *Efficiency*,

Privacy, Financial Targets, and Empathy. When examining risk, it is helpful to understand that humans don’t see “one risk” or “one rule” at a time. Normal daily operations involve a complex mix of policy, practice, experience, and production goals. One thing to keep in mind – generally, the only person who comes to work every single day with safety “top of mind” is the Safety Officer. Everyone else is there for a different reason.

- One last note on Competing Priorities – listen carefully when people explain “What they normally do.” You will often find what we call “Overt” and “Covert” messages. In many organizations, the “Overt” message is that “Safety is our number one priority.” However, the “Covert” message received at the front line is that the organization rewards throughput and production – the mission goals. We often even do annual employee evaluations where we reward employees for meeting production and project goals, but these same evaluations rarely reward meeting safety goals. What “message” is most prevalent at the front line? In one example, an EMS agency regularly discussed response time objectives with their crews, including rapid hospital turnaround times, how long it took to get to a deployment post location, etc. However, the only time they discussed driver safety was when they received a complaint related to





an employee's driving. The company would say that "safe driving" is more important than speeding to arrive at scene within the allotted time frame. However, their "Covert" messaging, what they cover in day-to-day conversations with crews, is that the real priority is response times.

Biases: Openly discuss any Systemic and Human biases that might influence the decision process. *We highly recommend that the team uses the SGCS "Bias Review Checklist," which is Attachment "B" to this guide.* One way to help manage bias is to evaluate your risk incident using counterfactuals. Counterfactuals are often used by those of us who conduct a lot of Collaborative Risk Reviews. It involves inserting "counterfactuals," or different information, into the story at important points to test the objectivity of the group. Common counterfactuals involve changing the outcome of the incident from a harmful one to no harm, changing the age and/or experience level of the involved parties, changing the race, insurance, housing status, or medical history of those involved, and adding or removing certain human performance factors. These exercises help the group examining the risk see whether their opinions hold up under varying circumstances, and they assist the group in identifying risks associated with equity, systemic bias, economic factors, and educational levels.

There are many, many different biases, but consider these common ones prior to, and during, your analysis:

- Structural Biases, Implicit and Explicit Biases.
- Undesired Outcomes (Outcome Bias).
- Hindsight Bias (tendency to view events as predictable or obvious).
- Manager's Bias (everyone knows the rules...), and your own Personal Experience Bias.
- Fundamental Attribution Bias (tendency to overestimate character or personality as a contributor and underestimate systemic or situational influences).
- History Bias (positive or negative) that may be associated with previous performance or behavior issues related to the individuals who are involved in the risk being examined.

System Reliability

2. System Reliability

Assess Current System Design

What Systems are in place to manage these risks?

- What are the macro-systems?
- What are the sub-systems?

Assess Current System Design





What Systems are in place to manage the specific risk being discussed? At this point, you need to identify exactly what the system is, and we have introduced the terms “*Macro System*” and “*Sub-Systems*.”

Macro System: The Macro System consists of various *Sub-Systems*. The Macro System is the entirety of the system in place to manage a particular risk. For example, for in-hospital medication administration, the Macro System may include 20 to 35 *Sub-Systems*, starting with the physician ordering the medication, to the pharmacy receiving the order, compounding the medication, packaging and labeling it, transporting it to the floor, placing it into an Omnicell™ or Pyxis™, and the steps a caregiver takes to administer the medication.

Initially, when examining risk, we take the entire *Macro System* through the Reliability Response Guide (RRG). Once we have found areas of vulnerability or non-resilience, we would analyze those *Sub-Systems* in more depth by taking each *Sub-System* and looking at it individually.

Sub-Systems: As described above, the *Sub-Systems* are those parts of the Macro System that work together to manage risk. *Sub-Systems* are typically policies, procedures, technology, software, hardware devices, and other components that are integrated to form a series of steps an individual navigates to perform a task that has risk. For example, starting your car, performing an MRI, giving medication, and landing a plane all involve multiple *Sub-Systems*. Importantly, not all *Sub-Systems* inside a Macro System need to be resilient – as a matter of fact, that’s likely not possible logistically or financially. While it is certainly desirable to put resiliency into upstream *Sub-Systems*, (e.g., checking two patient identifiers before creating a wrist band that will be scanned for many procedures or treatments downstream) due to the heavy reliance on human performance and behavior, and the potential for error to occur at any level, we should try to ensure the *Sub-Systems* are more *resilient* as they get closer to the risk being managed.

System Responsibility: Most systems within our organization are the responsibility of the organization and the leadership. Most of the equipment we use in our jobs, including hardware, information technology, operational gear, PPE, and policies are provided by the organization, and the organization bears the responsibility for maintenance and operational performance.

Some systems, though, are *nothing more than behavioral expectations* that have been set forth in a policy, procedure, or guideline. *Prescriptive* rules, for example, tell us not only *what* to do, but they tell us *how* we are

expected to do the task. If people are flying airplanes, driving ambulances, or administering medications, individuals are subject to behavioral expectations that they likely did not design themselves, and that they are expected to follow. The individual is a human component in an *organizational*, socio-technical system.

However, there are times when individuals “own” or are responsible for the system being examined. In these situations, we have *autonomous* rules where we tell people *what* to do, but we do not provide any detail on *how* to accomplish the work – therefore the individual must have their own autonomous system in place to manage risk.

An example would be common policies related to time and attendance. While you may have rules outlining what an individual does once they get to work (how to check in, accessing certain restricted areas, etc.) your time and attendance policy is generally considered *autonomous* – the individual enjoys autonomy on how they will comply. The organization’s expectation is that employees show up for work ready and on time. You really

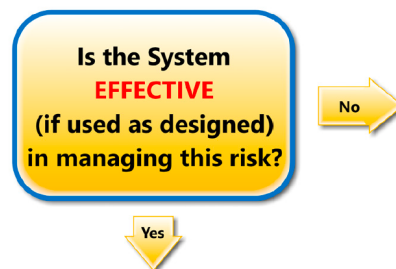


don't care *how* they do it – and in those situations, the individual would be responsible for the “system” to manage the risk of not showing up on time. It would be *their* morning schedule, *their* vehicle or transportation choices, *their* alarm clock, etc.

Here is an example: An individual doesn't arrive at work on time as stated in the policy. Remember, we always start with the risk: What's the *risk* of not showing up on time? This is where we often see confusion – managers and supervisors will say that the risk of not arriving on time is that the individual will be punished, lose their job, get their pay docked, etc. Those are not the risks of not arriving on time – those are the *consequences* we have decided are *organizationally appropriate* for not meeting the expectation. The *risks* of not showing up on time are associated with potential negative impacts on production, co-workers needing to stay overtime, customer service, finances, etc. Managers and supervisors should know the difference, so they can help the employee see and understand the risk, then follow up with what consequences may be in place for further violations.

Can you and your team think of other “autonomous” rules or risk management systems where the individual, not the organization, is responsible for the system? These are common for physicians, well-trained and educated experts, contracted repair professionals...what other situations are there?

Is the System Effective if Used as Designed?



If the current system is used as designed, is the system *effective* in managing the risk being evaluated? Look at the color key at the top of the page in the RRG. The box is outlined in blue, therefore this question is asked from the perspective of the organization – the entity responsible for the system. In asking this question, we seek to understand if the system is effective in managing the identified risk(s) if the individual operating the system used it as *designed* and *followed the policies*.

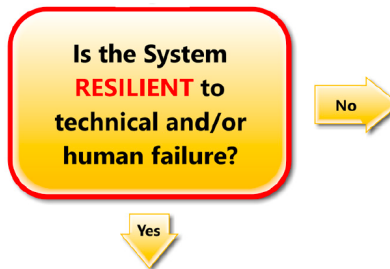
Let's use a medication administration example, and a policy (sub-system) that requires a double check. The risk being managed is patient harm from giving an incorrect medication or dose. The system requires a redundant check, and the policy states the individual needs to find an equally trained person to conduct the check. If the individual followed the rule and conducted an appropriate double-check, would that effectively manage the risk of giving the wrong dose?

The answer is likely “yes,” a redundant check would *effectively* manage this risk, and you would then continue to the next question below it in the box outlined in red: “Is the System Resilient to technical or human performance issues?”



If the answer to the “effective” question is “No”, move to the right in the RRG to the box titled “*Examine Factors Influencing System Performance*” and consider system improvements.

Is the System Resilient to Technical and/or Human Failure?



These include both system and human failures. System failures might be technical, such as hardware, software, or policies and procedures. Human failures might be gaps in knowledge, skills, abilities, and proficiencies (KSAPs), or behavioral choices and/or human errors. Note that this box is outlined in red. If you reference the key again at the top of the RRG, you’ll note this is asked from the Peer Perspective. Generally, this means from the perspective of the peer group that will be directly using and affected by the system. To mitigate a manager’s bias, the employer should look carefully for data or indications from the front line to inform this perspective. This question is intended to help you see if your system is vulnerable to *human performance, policy violations, equipment failure, etc.*

For example, consider the sub-system above where we had a policy requiring a redundant check. For some work environments, such as an airplane flight deck or pediatric oncology pharmacy, we know from experience that redundant checks are frequently performed as required because the front-line operators see *risk* in not following the policy. Not a *consequence*, like punishment, but real *risk* that requires a second human check. Their risk intelligence informs them that secondary checks are important due to the high risk and the potential severity of the outcome. However, even in these cases, redundant checks can lack resilience. Often, they can be easily bypassed with no adverse consequence.

One of the easiest and most common examples for us to see “effective” vs. “resilient” systems is something we come across nearly every day – a traffic intersection with a stop sign:

- What are the risks associated with not stopping? (Injury, damage, etc.)
- What is the Macro-System? (A series of Sub-Systems that are visual, requiring some cognitive awareness)
- What are the Sub-Systems? (White stripe on the road, red octagonal sign that says “Stop,” perhaps a flashing red light above)
- Is the system **effective** in managing the risk of damage and injury if used as designed? (Yes, if we use it as designed, and follow the rules, it’s effective in managing the risks)



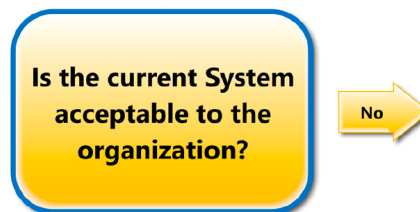
- Is the system **resilient**? (No, I can make an error and inadvertently drive through the stop sign, I can make a poor choice and drive through the intersection without stopping, or the sign could be knocked over and be unseen by the motorist – a systemic failure)

One way to understand resilience is to ask questions designed to probe for areas of vulnerability. These should be directed to those who do the actual work, as well as members of your Reliability Management Team. Here are some examples:

Are there *competing priorities* that influence human behavior around the system? Would production metrics or operational goals be adversely affected if individuals strictly followed all safety rules and procedures, and adhered to all system requirements? In other words, am I being measured regarding production goals, and can I speed up production by avoiding some basic safety rules?

Does the system have a single point of failure? Is it vulnerable to a human making one error, or is the system resilient *in depth*? Are there recovery options? Can the system manage peak operational demands? The best systems have a high probability of managing risk and a relatively low front-line production impact. In other words, the safety and/or quality process does not adversely affect the efficiency of operations.

Is the Current System Acceptable to the Organization?

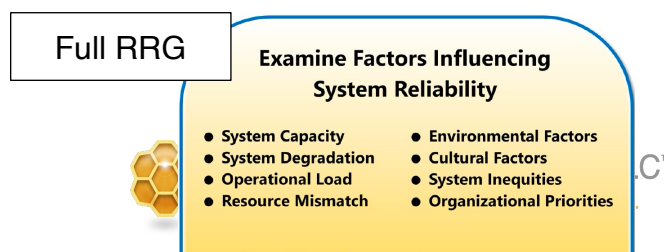


If the answer to the resiliency question is “yes”, the system is both *effective* and *resilient*, the next question asks *is the current system acceptable to the organization*? It is uncommon to find Macro Systems and Sub-Systems that are both effective and resilient at every level. If the answer to this question is “yes,” the system is acceptable, go to the Human Reliability section (back page of the RRG) and continue there. If the system is effective, but you’re still not comfortable with the level of resilience, continue to re-design the system.

Remember that every system has limits – making something as safe as reasonably practicable means that you have achieved the best you can do considering the resources and equipment available, and the limits of the humans operating the system. In addition, there are no system improvements that you can suggest that don’t carry their own risks! Your suggested improvement might affect the budget, the operational efficiency, or create

unseen risks that can be hard to manage. Always ask the group, particularly those operating on the front line, how the suggested system improvement might introduce additional risks or operational impediments.

Examine Factors Influencing System Reliability





Manager's RRG

Examine Factors Influencing System Reliability & Consider Recommending Improvements:

- Can the system contributor(s) to the risk be removed?
- Can the system be re-designed to better manage risk?
- Does the suggested redesign create competing priorities or add additional risk in other areas?

The list in this box (in the full RRG) is not meant to be comprehensive, but to generate discussion about what factors may be influencing the effectiveness and resiliency of the Macro Systems and Sub-Systems. Most systems, after they are initially designed, are modified over time or are allowed to “flex” to adapt to new production pressures. We *rarely* re-design an entire system when production goals are reset – we often just expect the current system to continue working as originally designed. This list represents known issues that affect socio-technical systems and that have been identified as contributors to system failure:

System Capacity: The system was originally designed and staffed for a stated capacity, but over time the demand on the humans and the system has increased. This is commonly seen in healthcare and maintenance environments, when resources get stretched as volume increases, and we don't recognize the effects until there is a breaking point.

System Degradation: Systems degrade over time, even when regular maintenance is performed. Every Macro System and Sub-System has an associated inherent failure rate – we should recognize that systems degrade and fail, regardless of our interventions and how well we predict operational demand. If you have identified that the system has degraded, the Reliability Team might ask, is it temporary? Would an intervention fix the system? Is it worth it? In other words, is the inherent failure rate acceptable to the organization? What's the rate and severity? Are there other system issues that have a higher potential failure rate and should be first in line for added resources?

Operational Load: Similar to System Capacity, above, operational load is often thought of as a sudden, unexpected peak problem rather than something that creeps up on us over time. In other words, a mass casualty event, an unexpected or rare influx of demand, etc.

Resource Mismatch: This is an issue we see in two different areas. First, is the human working within the system capable of handling the complexity and operational demands? Do they have the right Persona





Performance Factors – KSAPs and cognitive/physical abilities? Second, is the system itself overmatched? Was it designed for the load it is currently serving?

Environmental Factors: Internal and external environmental factors can negatively affect our system. These could be environmental issues that were unanticipated during the design, that have evolved over time, or that were sudden and unexpected.

Cultural Factors: Systems are usually a product of the dominant culture where they were developed. We rarely re-evaluate our systems to ensure they meet minimum expectations for privacy, access, religious beliefs, cultural norms, grieving, family access, and other important factors.

System Inequities: The systems we have developed and used for years often have embedded beliefs, processes, policies, and/or expectations that are not equitable for all people. For example, discharge instructions that are printed only in English, pre-procedure instructions that are opaque, confusing, legalistic, or single-language, barriers to access for people with disabilities, elderly, financially vulnerable, or houseless, and structural racism are but a few of the inequities we should look for when examining our systems.

Organizational Priorities: Every organization shifts priorities based on mission, goals, and risk perception. Was the organizational focus somewhere else? Were they pushing production and not paying attention to safety? Was there a particular organizational initiative that took priority over the system and risk being examined?

Consider System Improvements

Once your team has discussed the factors that may be influencing system performance, you should have a sense of what system improvements might build resilience.

Can the system contributor to the risk be removed? We ask this question to determine whether the system component that presents risk can be removed without adversely affecting safety or operations. It is rare that we can remove a system contributor to risk without implementing another, new or modified system component, but at times it is possible. For example, if there is a rug causing a tripping hazard, and the rug is for cosmetic purposes, can it be removed and would that mitigate the fall risk? Can you transfer that patient needing a rare specialty intervention to another facility that performs the procedure regularly? These are difficult questions because you might be replacing one risk with another. *Nothing is risk-free*, so you have to balance the conversation: What risk are you willing to accept? How about the customer? What would the potential failure rate be of your suggested intervention?

Can the System be Re-designed to Better Manage Risk? Can You Strengthen or Implement New Sub-Systems?

- 
- **Barriers:** A barrier is anything we put between the operator and the risk. Healthcare examples would be gloves, mask, and eyewear; for firefighters it could be turnouts, hoods, and helmets; for EMS it might be floor latches that keep gurneys in place, etc. While technically policies and signs are barriers, remember to evaluate your system suggestion against the “Strong, Moderate, Weak” tool to help you determine the proactive power of the method being discussed. Recall that signs and policies may be effective if used as designed, but they are not typically resilient and make weak barriers.
 - **Redundancies or Backups:** A backup or parallel component is a “belt and suspenders” approach. There are technical backups and behavioral backups. A technical backup is one that is provided by a machine or system, such as airbags and seatbelts. A behavioral backup example would be a double-check requirement. Be aware that human redundancy requirements are often weak systems in that they adversely impact operations and/or production. To ensure compliance with redundant checks, people must first “see and understand” the risk of non-compliance.
 - **Forcing Functions:** Examples of forcing functions would be the need to apply the brake before you can shift a vehicle from neutral, the need to put your personal ID into the Pyxis™ system before the door to the narcotics will open, the need to push down on a child-proof cap before you can twist open a medication container, etc. Typically, forcing functions tend to be resilient, in that they are generally designed to protect against inadvertent errors by requiring an additional step (for safety) in order to proceed.
 - **Recovery Options:** A recovery option is something that typically allows the initial error to occur but offers the operator a recovery option before there is an undesired outcome. Recovery option examples would be fire sprinkler and alarm systems, the “rumble strips” along highways, the computer reminder “are you sure you want to delete that?” and other similar strategies.

Is there another system strategy available? There are many other system design features that are unique to a certain system or domain. This is a good place to brainstorm other system methods that might mitigate future errors, or that might make the job easier for the front-line operator.

Once you complete the System Improvements section and find that you *cannot* make an improvement or are satisfied with the current system, you would proceed through the “No” box at the bottom of this section and continue with *Human Reliability* on the reverse side of the RRG. In some cases, no system design improvements are available or affordable, and we rely on compliance behaviors within the existing system. If the system improvement questions are answered in the affirmative, and you propose new system features or address actors that influenced your system performance, test your proposal by moving to the next section.





Organizational Response: Test and Manage Potential System Reliability Improvements (FULL RRG Only)

(NOTE: This section is not in the Manager's Version RRG because generally, those testing organizational improvements are not directly involved with feasibility, cost, and measurement activities, as are the Reliability Team Members and other organizational SME's)

Organizational Response Test and Manage Proposed System Reliability Improvements

Review Proposed System Re-Design for:

- **EFFECTIVENESS and RESILIENCE**
- Estimate of lower probability of risk
- Possible adverse operational impact to organizational attributes and/or priorities
- Feasibility and cost
- Ability of the organization to see, understand, and manage these risks
- Ability to monitor and measure results

Now review your team's suggested improvements. First, determine the probability that the proposed system re-design strategies will be both *effective* and *resilient* in managing the risk. Recall not every Sub-System needs to be resilient! Discuss whether you believe this strategy will lower the probability of future risk.

Have possible adverse operational impacts and costs been considered and deemed acceptable? This is one of the most important and valuable "High Reliability" questions you can examine, and the team should ask front-line people who are doing the work (or who will be responsible for operating the new Sub-System, following the new policy, or whatever mitigation strategy was proposed). This question will help you determine if the suggested strategy will create additional *Competing Priorities*. Will the new strategy create more work? Interrupt workflow? Create the need for more resources? Have you conducted a time-study to ensure your estimates are accurate? Don't be that organization that says, "it'll only take a few more minutes." Front-line staff don't generally have additional minutes in their day. Are you creating risk in another area as front-line staff may be required to find another work-around?

If the system re-design strategies have a *high probability of managing the risk*, and a *low adverse operational impact*, escalate for implementation, assessing feasibility and cost.

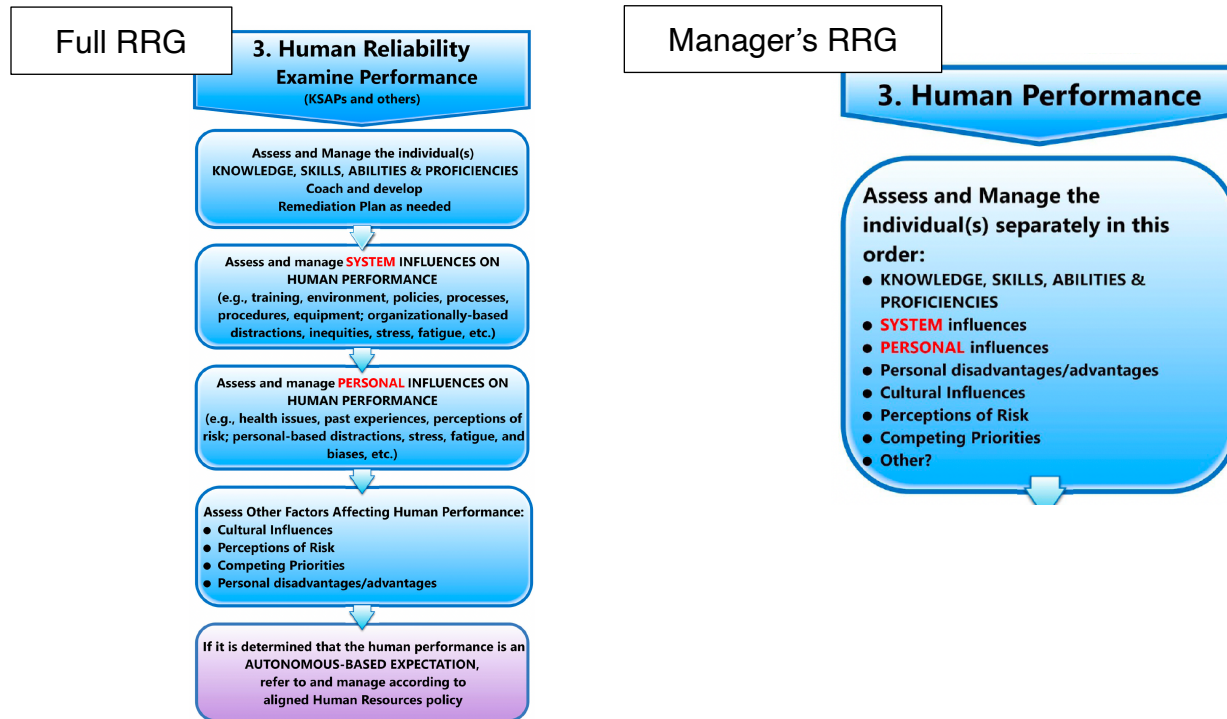




Follow your internal processes for changing the system – use Organizational Planning departments, Lean Processes, etc., as needed to coordinate efforts. Integrate system re-design strategies with organizational improvement and individual behavioral expectations. Coordinate the integration of your new system expectations with any required procedures or behavioral expectations. Consider impacts on different work areas within your system and how the organization will be able to monitor and measure results to know whether the new system is meeting expectations.



Human Reliability – Performance



Examine and Manage the Factors Influencing Human Performance

After you have assessed perceptions of risk, the system factors that influenced system performance (and the humans operating it) and identified competing priorities, you are ready to focus on Human Performance Factors (HPF) within the system. **Remember, you are assessing risk, not fault, during this exercise.**

Note – if you are not readily familiar with these terms and how to define a *Human Performance Factor* vs. a *Behavioral Choice*, review the SGCS online LMS Library titled “Performance vs. Behavior.” It is important to understand that HPF should not be addressed with punitive action – they should be managed through remediation. Human Performance Factors are associated with elements that influence our cognitive and/or physical performance. HPF cover a wide range of variables, and they can have many different sources of origin.

System-influencing HPF are those resulting from a systemic and/or organizational origin. This could be inadequate organizational training programs, work-related distractions, mandatory overtime causing fatigue, and many other variables.





Personal-influencing HPF are those resulting from factors that are beyond the organization's control and are generally within the scope of the individual being examined. These could include health issues, personal

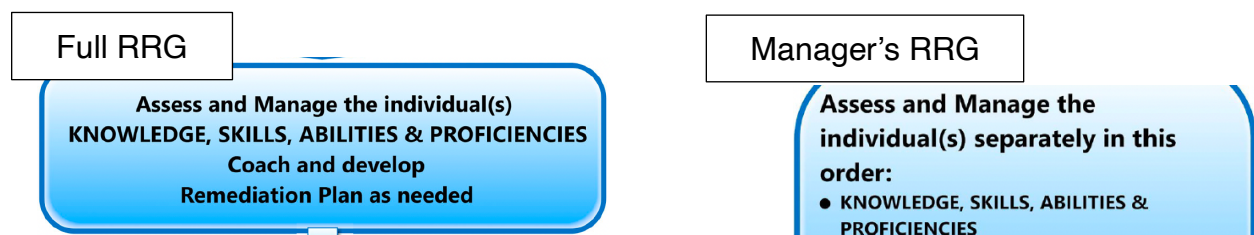
distractions or stress, fatigue due to poor off-duty choices or illness, and other factors. HPF can also have *cultural* origins. For example, sensitivities to power gradients and perceptions of risk can vary significantly between people from differing cultural backgrounds.

Key Point: There can be gray areas where HPF can appear to overlap with Behavioral Choices. In all cases, collaboration is important – discuss with your team – and ask whether remediation or performance improvement, which is designed to address and minimize these factors, is the appropriate course of action. When in doubt, we suggest your team first consider the issue to be HPF-related and see if a remedial plan manages the risk.

Do not produce a risk analysis or Collaborative Risk Review report or summary that indicates an individual (or a group) needs additional “Training.” This is a common fallback used in after-action reports, and it is non-specific, often unnecessary, and/or addresses the wrong type of training that is needed. See the descriptions below under Knowledge, Skills, Abilities, and Proficiencies, and ensure that your remediation plan has specific, achievable, measurable objectives that are related to the specific area (or areas) needing improvement. In other words, what *specific* type of training is needed, and why?

Also, recall that in your analysis of a risk or an event, it is common to have multiple people (i.e., actors) involved, and also for those actors to make more than one choice that may have added risk. You should run each individual actor through the Human Performance Factors analysis.

Assess the Individuals’ Knowledge, Skills, Abilities, and Proficiencies



Let's review what these terms mean. We will use a few examples to illustrate the points.

Knowledge: Knowledge is the information necessary to perform the job. What are the job requirements requiring *knowledge*? (Education, didactic training, etc.). How does the employee prove they have the knowledge? Often, this is a degree, certificate, course completion record, or other official documentation. Knowledge can be transferred in many ways, but typically is didactic, classroom- or online-based, and follows an established curriculum with required reading and comprehension.

- Your child gains the knowledge to drive a vehicle when they read the DMV and car manuals.

- 
- A physician, nurse, or paramedic gains specific knowledge by taking various courses in school.
 - A pilot gains knowledge of aircraft systems and flight rules by attending school and reading.

If there is a **Knowledge** issue, the remedial response – or Performance Improvement Plan (PIP) – would typically address the necessary minimum training or education in order for the person to learn the required information. We recommend that you don't develop a remedial plan requiring classroom or online training unless your evaluation demonstrates that the individual lacks the knowledge needed for the job. Remember, just because someone doesn't follow a procedure doesn't mean they need "retraining" on the procedure itself – they may know it well and have reasons for choosing not to follow it verbatim. Plans that address Knowledge should include, at a minimum:

- Specific examples of where the individual appeared to lack the knowledge (time, date, circumstances);
- Reference the job requirements and/or training manuals showing the minimum required;
- Resources available to the individual (online, books, courses, etc.);
- The expected length of time given to complete the learning;
- Any Mentors or Training Staff who can be of assistance;
- Regular check-in points during the learning process to ensure progress;
- Expected metrics at each check-in and to successfully complete the remediation.

Skills: Specific physical or cognitive tasks expected of an individual's role. They are usually associated with direct performance metrics, but may also include experiential skills like "situational awareness." What *skills* are required upon hiring? What skills must be developed? In high-risk domains, skills are often first practiced in labs, simulators, classrooms, and other direct-observation settings where instructors can monitor progress and technique.

- Your child develops the skill to drive when you allow them to practice with you in the car (or they attend a driving school and terrify a stranger instead).
- A physician, nurse, or paramedic gains specific skills such as IV insertion, medication administration, ECG interpretation, and airway management techniques by practicing on cadavers, medical mannequins, and in some cases actual patients under the direct supervision of an instructor.
- A pilot gains skills by flying in a simulator but also starts with smaller aircraft under the direct tutelage of a Certified Flight Instructor.

If there is an identified **Skill** problem, the remedial plan (or PIP) should address practical applications. Skills are hard to learn by watching a video or PowerPoint – one must *practice*. Your plan should include, at a minimum:



- 
- Specific examples of where the individual appeared to lack the skills needed (time, date, circumstances);
 - Reference the job requirements and/or training manuals showing the minimum required skill level;
 - Resources available to the individual (skill labs, simulators, instructors assigned to the PIP);
 - The expected length of time given to master the skill (or a specific number of successful completions, regardless of the time it takes to demonstrate they have achieved expectations);
 - Any Mentors or Training Staff who can supervise the practice and be of assistance;
 - Regular check-in points during the learning process to ensure progress;
 - Expected metrics at each check-in and to successfully complete the remediation.

Abilities: What *abilities* are required for the job? Recall from the videos that ability is the capacity to put your knowledge and skill to work in the *actual environment*. Ability is usually proved by passing a minimum competency assessment, which may include both knowledge and skill testing to a standard. Ability might be confirmed in many domains through the issuance of a license, certificate, or other accepted documentation. Individuals can have the Knowledge (they can recite the book), they might possess the basic Skill (they can start an IV on the rubber arm), but they may not be able to demonstrate competency in the actual environment or when under evaluation.

- Your child proves their ability to drive a vehicle when they receive their driver's license.
- A physician, nurse, or paramedic proves their Ability through licensing and certifications that were achieved by meeting minimum competencies associated with the domain.
- A pilot proves their ability when they receive a pilot's license and specific qualifications for the type of aircraft they wish to fly.

If there is an identified **Ability** problem, the remedial plan (or PIP) should address the minimum required knowledge and skill set, and the expectations of how these are applied in the actual work environment. Proof that one has the Ability to do a specific job should be evaluated by comparing the formal minimum requirements against actual performance and developing a plan to address the "gap." Your plan should include, at a minimum:

- Specific examples of where the individual appeared to lack the defined abilities (time, date, circumstances);
- Reference the job requirements and/or training manuals showing the minimum required abilities (these are often found in licensing, certification, or training course documentation);
- Resources available to the individual (Mentors, materials, etc.);



- 
- Working under the supervision of Mentors or Training Staff in the actual or simulated work environment;
 - The expected length of time given to prove the ability (or a specific number of successful evolutions in the actual or simulated work environment, under the eye of a Mentor or Coach);
 - Any Mentors or Training Staff who can be of assistance;
 - Regular check-in points during the learning process to ensure progress;
 - Expected metrics at each check-in and to successfully complete the remediation – include the minimum standard, and ensure you have an approved method for measuring this.

Proficiency: When is someone considered Proficient? Proficiency is a different measurement altogether. Individual *Proficiency* is rarely measured on a regular basis outside of the commercial aviation industry. Unlike commercial pilots, who have to demonstrate their knowledge, skill, ability, and *proficiency* under various flight circumstances and be certified in specific aircraft types on an annual basis, most other professionals (healthcare, EMS, manufacturing, dispatch, etc.) are not regularly cognitively and/or physically evaluated once they have a license or certificate. They more than likely have to meet *recertification* or *re-licensure* requirements, but those are usually associated with continuing education opportunities and are generally not high-fidelity practice scenarios with “pass/no pass” outcomes.

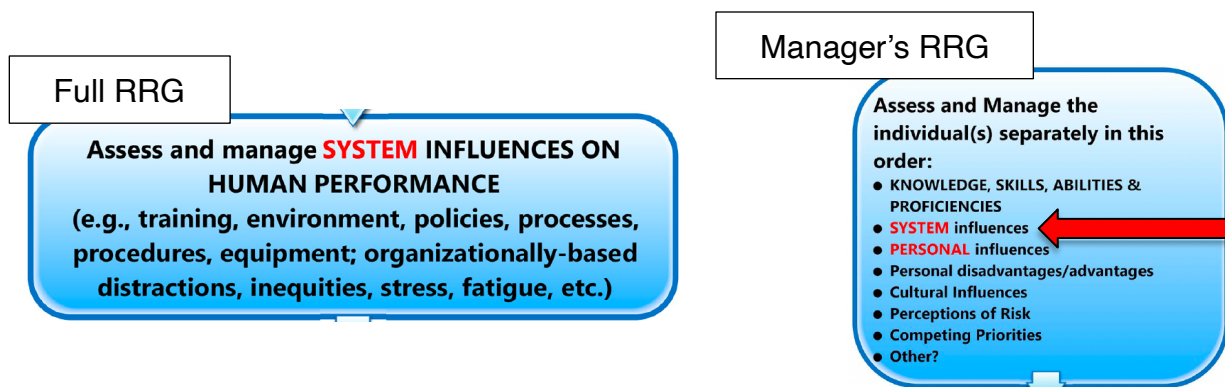
Proficiency is usually associated with an individual (or a team) gaining experience under various working conditions, over time, with different environmental and operational influences. Proficient operators are generally continual learners, and demonstrate the capability to adapt and learn as their profession changes, as technology transforms their work, and as socio-technical systems evolve around them. Because our organizations rarely regularly update job descriptions and expectations to include the advancements associated with every job, and many of these descriptions include only minimum competency levels, developing a remedial plan (or PIP) to address Proficiency can be fraught with complications.

When facing a situation where an individual appears to have the KSA’s, but not the “P,” more work is required. In addition, bias can easily be introduced to the process, where senior operators in the domain can have proficiency expectations that are rarely stated, never measured, and remain somewhat ambiguous (e.g., “You’ll know it when you see it”). Remedial plans and PIP’s must be based on documented, measured criteria. This requires a team of people that can analyze the current domain in our organization, including the expectations that exceed any standards set forth in a job description. Be prepared to defend your Proficiency criteria with measurable metrics and proof others are meeting those standards. Manage bias by including a wide range of experience, not just experts on your team.

- Your child is Proficient in driving a vehicle when they have mastered different driving conditions, including adverse weather, mechanical breakdowns or system failures, city and mountainous driving, distractions associated with passengers, etc.

- Physicians, nurses, and paramedics are considered Proficient after spending time in their domain and demonstrating proof of successfully responding to a wide variety of situations that require adaptation, new knowledge, collaboration, management of ambiguity.
- Commercial pilots are tested at least annually on Proficiency! While their license and qualifications demonstrate their *Ability* to fly certain aircraft, they have to prove to a third party (Evaluator) that they can manage multiple different emergency scenarios, including but not limited to mechanical failures, adverse weather situations, passenger and/or crew issues, etc.

Assess and Manage System Influences on Human Performance

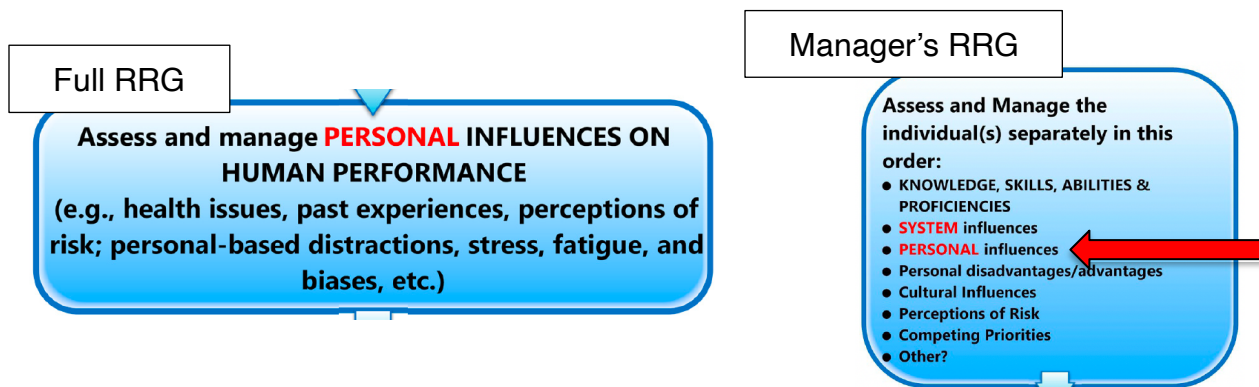


Next evaluate whether there were *System* issues that affected Human Performance. If you find an issue here, the *Organization* is generally “responsible” for the factor affecting performance *and* for the fix – not the individual. If you have already done a comprehensive job assessing the System (the first page of the RRG), you will likely find these questions relatively easy to answer – and you may have already developed a plan to address them. This is one reason for assessing System Reliability before Human Reliability – you gain context into how the human performed before addressing minimum performance expectations.

- **Training:** Is there training the *organization* should have provided but did not? Was the training provided but ineffective? Examples would be newly introduced equipment with insufficient training, IT programs without the appropriate or comprehensive training, poor or no emergency vehicle operator training, etc.
- **Environmental:** Are there environmental or noise issues causing distraction, affecting cognitive performance, that are system-driven problems? Examples could be noise, weather, etc.
- **Inequities:** Are there inequities in the system? On the front page, under “Examine Factors Influencing System Reliability,” you were asked to carefully examine the system for structural or other system-related inequities. It can be extremely helpful to have guidance from a professionally trained individual when examining these particular factors, because they are easy to overlook with the untrained eye.

- **Fatigue or Stress:** Are there *system* issues driving fatigue or stress? Examples could be mandatory overtime, rotating work schedules from day to night shift, etc.

Assess and Manage Personal Influences on Human Performance



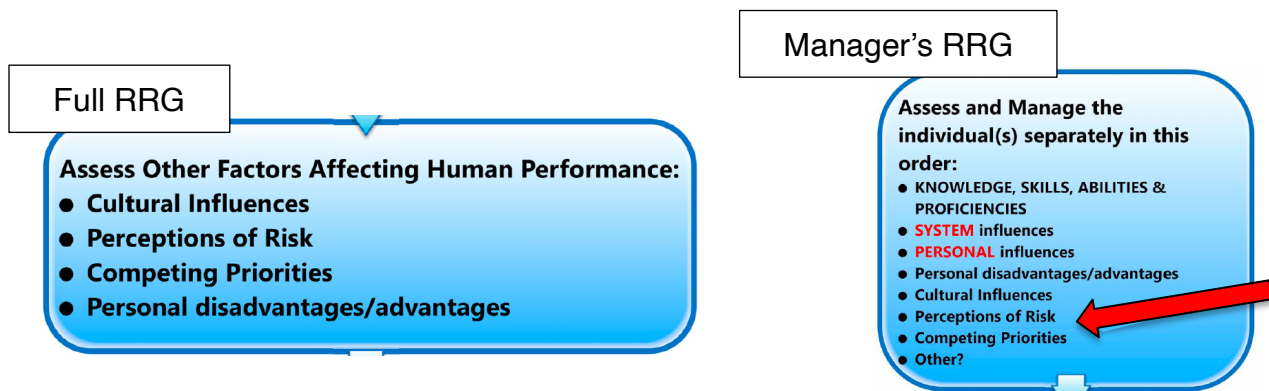
After addressing System influences on HPF, we ask whether there were *personal* influences that affected Human Performance. If you find an issue here, the *individual being assessed* is generally responsible for the factor affecting performance *and* for the fix – not the system or organization. These are factors we expect the individual to manage themselves. Keep in mind, some of these are sometimes not readily controlled or managed, such as “level of experience” or “personal health,” and you may find system influences as well. In these cases, the organization generally has a responsibility to *identify* the issue and *clarify how it affects performance*, but the organization typically does not take responsibility for *managing* the issue – this is considered an individual responsibility. The level of engagement or responsibility varies widely by organization, and you are advised to contact your Human Resources professionals if you have any questions.

- **Health, Personal Stress, Personal Fatigue:** Are there health influences, personal stress, or personal fatigue that may be affecting their performance? Examples would be medical issues or medications that affect cognition, insomnia, stress related to family or marital problems, etc. These are best managed by helping the individual identify them, pointing out how they are affecting at-work performance, and directing the person to the appropriate organizational resources such as Employee Assistance Programs, Human Resources, etc.



- **Level of Experience:** Is there an identified lack of experience that may have affected performance? Lack of experience is one of the personal, “individual” performance factors that is hard to control. Experience is gained, of course, through exposure to the work, and if this is a new employee or the individual is new to the process, errors associated with inexperience are to be expected (and hopefully managed in the system). If the organization has a responsibility here, it might be associated with ensuring the individual gets the exposure and mentorship they need to gain the appropriate level of experience.
- **Cognitive or Physical Capacity/Ability:** Does the individual have the cognitive capacity for the job? This is often closely associated with a defined lack of “Ability” in the KSAs described in the first box above. Some people work better in areas where the work is evenly paced, non-stressful, and predictable, and others thrive in ambiguous, complex, changing environments. One is not better than the other – they just demonstrate abilities that are valued in different parts of the organization, and at times we find that we have mismatched a human within a system.
- **Biases:** Are there personal biases that may influence human performance? For example, implicit bias is commonly misunderstood and rarely effectively captured during a risk analysis. As noted above, until the team is adept at seeing and understanding these biases, having a professionally trained individual assist the team with guidance in this area is recommended.

Assess Other Factors Affecting Human Performance

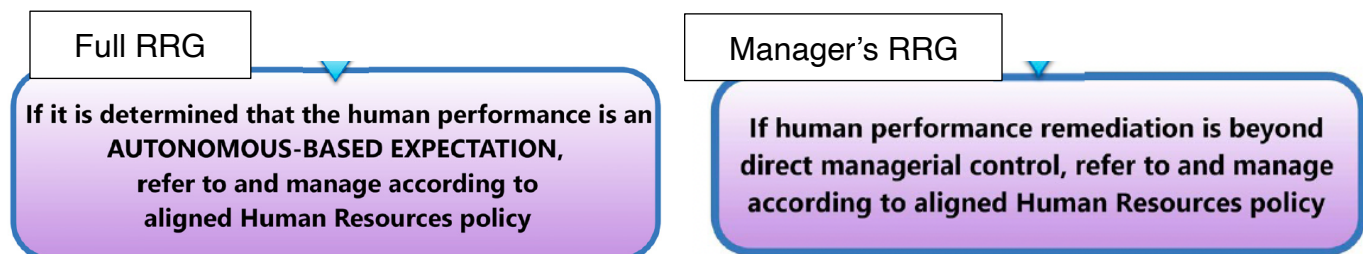


This section asks us to review any other issues that might affect human performance. Our own personal biases (many of which we may be unaware of) can affect the way we assess these factors. Like all the sections in the RRG, this is best done with a diverse team to minimize bias.

- **Cultural Influences:** This is non-specific for a reason: These could be organizational in nature, family related, connected to religious beliefs, associated with the person’s country of origin and/or traditions, or many other factors. If your team identifies a factor here, proceed carefully with expert advice on how these factors should be managed at the Individual, System, and Organizational level.

- **Perceptions of Risk:** Hopefully, you discussed individual perception of risk when you first started under the “See and Understand Risk” section. Is there a way to align the individual’s risk perception and tolerance with yours? Can you increase their risk intelligence around a certain issue? If not, how would you best manage their perception of risk? Also – discuss when the *organizational* responsibility to outline, define, and set limits on risk tolerance ends, and where *personal* responsibility begins. Some individuals might pose a risk themselves and might be unable to see this.
- **Competing Priorities:** It is likely you already defined these when you started. Just review – have you determined how you will address these? Recall this is a crucial issue, in that **Priorities** drive behavioral choices! And **understanding** these can help you build a more resilient system.
- **Personal Advantages/Disadvantages:** It is likely that structural and individual advantages contribute to risk in many situations. For example, houseless individuals rarely have personal physicians, often lack prenatal care, commonly have limited or no access to a pharmacy for daily medications, and lack transportation options to access care. Strongly consider using a counterfactual exercise to “test” your system for inequities – run the same risk through the exercise, but substitute an individual from a disadvantaged group, or a different race or ethnicity or financial status. Again, we recommend you undertake these exercises with a trained individual when first collaborating and discussing these risks to avoid unintended conflict.

Is the Human Performance an Autonomous-Based Expectation?



What does this mean? When we hire contractors, subject-matter experts, and/or professionals on a contract basis, we often define a “Scope of Work” and a set of minimum performance expectations for the contractor and/or subcontractors. We are not in control of the contractor’s KSAP, cognition, or personal factors such as their health or fatigue. If your team has identified Human Performance Factors associated with individuals who are part of your system, but over whom you have no direct organizational control, these are commonly called “Autonomous-Based Performance Factors.”

In addition, you have some rules, policies, and procedures that, as we described earlier, are “autonomous” and not prescriptive. Time and Attendance, some operational rules, and some clinical procedures are not highly prescriptive and we assume the individual has certain KSAPs due to the education, training, and experience it took to get the job in the first place. In these situations, the team must evaluate who is responsible for the Human Performance Factors, and for any remedial efforts. Is it an individual responsibility? An organizational



one? Does the responsibility belong with a professional membership entity or educational source, such as a college program?

Other examples would be non-employee physicians, non-employee subcontractors (trades, IT, etc.), and others who are not under the management or direct control of the Human Resources team.

When you find problems with Autonomous-Based HPF, work with your Human Resources team and with the organizational leadership who is responsible for ensuring individual and contractor performance, and develop an appropriate management plan consistent with your policy and culture.

Human Reliability – Behaviors & Errors

Full RRG

4. Human Behaviors

Manager's RRG

4. Human Reliability Examine Behaviors (choices and errors)

Examine and Manage Behaviors (Both Choices and Errors)

Note: *The Standards of Behavioral Review used in the RRG represent proven methods and strategies that have been demonstrated successfully in multiple high-consequence industries. These standards are for internal use only to assist in the management of risk and to determine organizational response to identified human performance and behaviors. These terms bear no relation to and do not represent legal standards of review.*

In this section, your team will evaluate the quality and effect of behaviors on the risks being examined. In your analysis of a risk or an event, it is common for there to be more than one individual involved, and for an



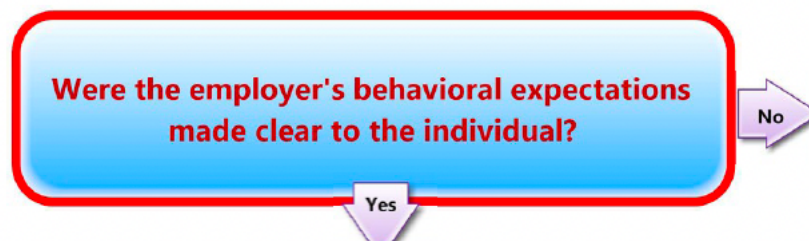
individual to make more than one choice or error that added risk. You must run *each individual actor* through the Performance and Behaviors sections of the RRG, and if a single actor made more than one choice (for example, did not follow two rules), *each choice* is separately run through the Behaviors section. While initially learning the process, this seems laborious and time-consuming, however, it will become much easier with practice and as you collaborate with your team. There is simply no other way to maintain reliability in your analysis.

For example, if “Actor #1” did not follow the rule to wear a seatbelt and did not stop at an intersection, both of those would be separate assessments under Section 3b – the Behaviors column. Your team might find that the employee’s failure to wear a seatbelt was a “Reckless Choice” or even “Justified,” depending on circumstance, and that running the stop sign was a “Human Error” or a “Reckless Choice.” In this way, you identify and manage *every* risk associated with the choices and performance factors surrounding a risk or event.

We are providing a method to see and understand risk from the *Peer Perspective* as well as the *Organizational Perspective*. When evaluating behavior from the peer view, do not refer to external or internal “best practices.” Do not substitute yourself for the individual being examined. Do not use proxies from outside your organization. You are not trying to find *negligence* or *fault* – which might require an “outside” or “best practice” view – you are trying to See and Understand Risk *inside your organization*, and you can do that effectively only if you use your own culture – the Peer Perspective – to examine behaviors.

Refer to the key on the front page of the RRG if you need a reminder about the color of the boxes in this section. Red boxes are asked using the “Peer Perspective” or the “Individual Perspective,” and blue boxes are answered from the “Organizational Perspective.”

Were the Employer’s Behavioral Expectations Made Clear to the Individual?



Note this is a “Red Box” question, and it is answered from the Peer Perspective. Take note of the examples below about what that means – it can be helpful when applying the perspective to other “Red Box” questions in the RRG. This is a Yes/No question, and while that’s the way the RRG is written for clarity, it can present a challenge in actual practice. For example, if you ask me, “Do you understand our expectations?” and I say “Yes,” you may not really know whether I do – we could be thinking of two completely different expectations. It’s often best to keep questions *open-ended*. Ask something like, “In these circumstances, or in this situation, what do you believe you are expected to do?”

If using the Peer Perspective you find the individual (and peers) don’t understand the expectations, this likely presents an organizational risk. Usually this means the supervisor or manager needs to clarify expectations





with the entire work group as well as with the individual. If the Peer Perspective indicates that the behavioral expectations are clear and understood, you continue through the RRG to the next question.

Example – “No, the expectations were not clear from the Peer Perspective”:

- A nurse trainee was brought into the office and told that her behavior was being questioned – she had been practicing with another new nurse, using a piece of equipment to determine blood glucose levels. During their practice session, they punched the wrong button and inadvertently uploaded one of their own blood glucose readings into a patient’s chart. While they quickly fixed the error, two different policies were apparently violated – Policy #1 was that nurse trainees were supposed to ask permission from their mentor or nurse educator prior to practicing with any equipment. Policy #2 was that they were expected to operate medical equipment in a manner that was safe to the patients.
 - Clearly, the violation of Policy #2 was an error, not a choice. They certainly did not choose to upload the wrong information into the chart. For analysis purposes, the Policy #2 review would look something like this:
 - ▶ Did they understand the expectation to operate equipment in a manner to not cause harm?
 - Yes (Peer view)
 - ▶ Was there a policy, procedure, guideline, or process to manage this risk?
 - Yes (Organizational view)
 - ▶ Was it possible to follow the policy, and not cause harm to the patient?
 - Yes (Peer view)
 - ▶ Was this an inadvertent error, or a choice?
 - This was inadvertent – it is an error (Peer view). However, move to the box on the right that provides some guidance on a response. Examine system, performance, and behavioral contributors to the error. Well, we’re not sure about the system, but if it allows this type of error, perhaps there should be additional capture opportunities. What about Human Performance? Certainly nurse trainees do not have the full breadth of KSAP’s – they are *trainees*. The additional performance factors of stress and inexperience also come into play. How about Behaviors that contributed to the risk? Well, there was that Policy #1 that stated they should be asking permission from an educator or a mentor – and they did not, so this behavioral choice was a contributor to the error. Let’s take that choice through the Behavioral Assessment:
 - ▶ Policy #1 states they should have asked permission from a mentor or a nurse educator.

► Did they understand the expectation to operate equipment in a manner to not cause harm?

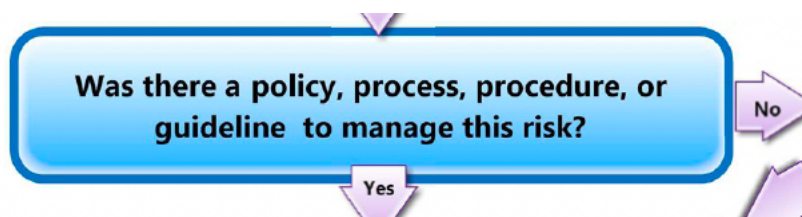
■ They both said “No.”

- This answer confounded the Nursing Supervisor. However, instead of checking with peers (other nurse trainees), the Nursing Supervisor asked the *Nurse Educator* about the policy. The Nurse Educator told the Supervisor that “They all know that rule; I teach that on the third day of orientation,” and even sent the slide to the Supervisor. This is *not* a “Peer View.” This is a “Management View,” and while it might indicate *fault*, it did not find *risk*. Ready to punish the nurse trainees, the Supervisor first asked for some assistance from HR. The HR Representative, trained in CJC and CHRO, told the Nursing Supervisor that she had obtained the information from the wrong source. The HR Representative suggested that the Nursing Supervisor randomly ask 5-10 nurse trainees (there were over 40 at the time), “Can you walk me through what you are supposed to do when practicing with a piece of equipment?” Not one of the nurse trainees was able to answer correctly – the “Peer View” demonstrated that the RISK in this case was no one knew the policy. Had the employer punished the two nurse trainees, they would not have mitigated the risk!

Example – “Yes, the expectations were clear from the Peer Perspective”:

- Let’s take the *exact same* case – nothing changes, except when the Nursing Supervisor checks with the nurse trainee’s peers, and asks “Can you walk me through what you are supposed to do when practicing with a piece of equipment?,” most of them answer *correctly* – they describe how they are to ask a mentor or the educator for permission. This demonstrates that the individual’s answer, “Yes” or “No,” is not really applicable – what is relevant is what the Peer Perspective demonstrates. In this example, the nurse trainees answered “No,” they did not understand the expectations, but the Peer Perspective proved otherwise – so for now, these two employees are the risk, and the Nursing Supervisor continues on down the RRG to the next question.

Was There a Policy, Process, or Procedure to Manage the Risk?



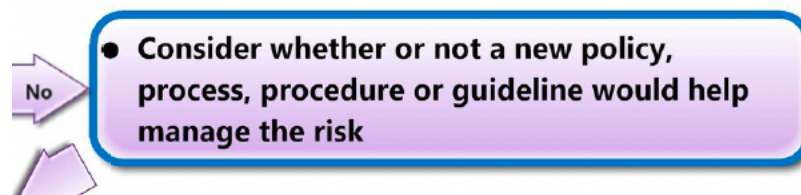
This is one of only two “Blue Box” or “Organizational Perspective” questions that are asked when analyzing behavioral risk. Because it simply seeks to determine whether the organization has a policy, process, procedure, or guideline in place to manage the risk, it should be answered by someone with knowledge of the policies that are in place to manage risk in the work environment being analyzed. It can be a specific policy or procedure (such as a medical protocol) or it can be an autonomous expectation (“Be professional”). If the answer is “Yes”, ensure you, as the manager or supervisor, know what the policy is, and ensure that the policy is relevant, up to date, and accurate for the risk that is being examined. If it’s an open-ended expectation (such as “Be professional”), validate your perception of that expectation first with HR or other peers. If the policy or



procedure refers to indefinite standards (such as “Frequently” or “Often”), ensure you have metrics that validate your assumptions.

We commonly find teams referring to policies or procedures that don’t say what staff actually *thinks* they say. Policies or procedures are often not as clear as leaders believe, developed and written during earlier operational phases, related to outdated equipment or practices, overly ambiguous, or have other issues. Always examine the policies and procedures you are referencing to ensure you are assessing the correct expectations.

If the answer is “No” and no current policy, procedure, or guideline exists, then:



You should discuss and consider: “If we put a policy in place, will it help manage the risk, and what other organizational values will be impacted?” In other words, if you suggest a new or revised policy, run that policy through the *Effective* and *Resilient* system questions of the RRG so you have no false expectations associated with the need for a policy or how it might manage the risk proactively. Many times, we see organizations adding procedures that include new steps in a process – extra “capture opportunities” or double-checks. These rarely hold up over time unless the organization either adds operational resources or reduces operational load.

If you simply add more steps without modifying the production expectations, the employee has to take shortcuts elsewhere in order to meet production – you have now created a new Competing Priority!

If the team does a careful review, the organization is satisfied with the policy or procedure in place, and the policy or procedure does not create new competing priorities, you continue to the next question.

Was It Possible to Follow the Policy, Process, or Procedure, or to Meet the Expectation?



Note this is another “Red Box”, or Peer Perspective question. This question seeks to understand whether it was *logistically* or *physically* possible to follow the rule or meet the expectation. Not *inconvenient* at the time, but impossible under the circumstances. Examples would be policies that dictate using particular equipment and that equipment is not available; policies or procedures that are outdated and refer to notifications or steps

that include staff no longer with the organization; and most commonly, procedures that dictate calling a supervisor or other person for guidance, and that individual is not available.

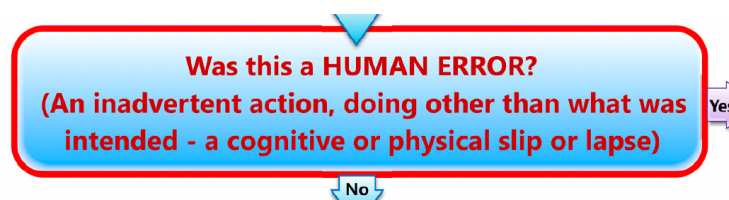
- Review reasons why it was impossible to follow under these circumstances and consider whether adding exceptions are warranted

If deemed “impossible,” there is a significant risk involved – the staff know the expectation to follow a procedure or policy, there is a procedure or policy written and available, but for some reason the materials, people, or system to comply is not readily available to the staff. One classic example is the “Lock-Out, Tag-Out” procedure used in most industries when staff members have to enter a dangerous environment where equipment is operating, or who have to maintain equipment that can be remotely turned on while they are conducting repairs. A Lock-Out, Tag-Out process usually includes locks that will physically lock out the “On” switch, colored tags to show it is locked out, checklists to ensure everyone is accounted for, and other items. If the Lock-Out, Tag-Out equipment is present in, say, a safety locker and someone has to go get it, that’s inconvenient, but no matter how busy you are, it’s likely “Possible” to get the equipment and follow the rule. However, if the individual goes to the safety locker and some or all of the necessary equipment is missing, it would be physically impossible to follow the rule. While this is a simple example, you and your Reliability Team can discuss others in your own work environments.

One of the steps we recommend when proposing a new policy or procedure is to send it out in draft form first, and ask the people who will be expected to follow the policy or procedure if they can think of times where it might be impossible to follow the rule. You might be surprised at the feedback.

If the answer is “Yes,” it was possible to follow this policy, process or procedure (or meet the expectation), proceed to the next question.

Was This a Human Error?



Determining Human Error is a “Red Box,” or Peer Perspective. In the taxonomy of Collaborative Just Culture (CJC) and Collaborative High Reliability, there are only “Errors” and “Choices” at this point. There is no using the term “Mistake,” as the term *mistake* is ambiguous. Is a mistake truly an inadvertent error, or is it a poor choice that we now regret? Politicians and other high-profile people are infamous for acting poorly or choosing poorly, and when called out or caught, they apologize for their “mistake.” If during your fact-gathering or





interviews someone says they made a mistake, clarify: Was what they did truly inadvertent – a slip or a lapse – or was it a choice they now recognize as the wrong one?

In our experience, people will use all sorts of justifications for their poor choices. In one case, an individual made an obviously poor choice – not an inadvertent error, yet they called it an “error in judgment.” You can expect some of these types of justifications, and this is why collaboration is such an important part of the review and analysis process – the variations in perspective provide valuable balance to decision-making.

Choices and Errors are managed differently in CJC, so the distinction is important, yet there are circumstances where the Peer Perspective can be difficult to determine. Yet if you get the initial decision wrong about whether something is a choice or an error, as long as you stay true to the CJC taxonomy, you’ll neither likely drift far from a proper risk mitigation strategy, nor will you usually wrongfully punish someone. Let me give you an example:

An EMS organization has a policy that Medics must “Drive with due regard considering the road and traffic conditions,” and this is further defined as not allowing any unit to travel more than 10 MPH over the posted speed limit. One of the units was involved in a motor vehicle crash, and the internal data recorder showed it was traveling at 12 MPH over the posted speed. During the Collaborative Risk Review, the Reliability Team was split on whether this was an error or a choice. Let me demonstrate how they responded to the questions under the Behavioral Review section of the RRG:

- Did the Medics understand the expectations to drive with due regard and that this limited them to 10 MPH over the limit? This is a Peer Perspective question, and their answer was “Yes.”
- Was there a policy or procedure to manage the risk? This is answered from the Organizational Perspective, and they answered “Yes.”
- Was it possible to follow the rule? That means, was it possible to drive with due regard in this situation and maintain a speed at or below 10 MPH over the posted limit? This is another Peer Perspective, and the answer was again “Yes.”
- Was driving at 12 MPH over the limit a choice, or an error? This is where the debate started. Keep in

mind, we are talking about a *2 MPH differential*, not 12 MPH – since the driver is allowed 10 MPH over the limit, the variance is a mere 2 MPH. The driver stated during the interview he was aware he was “about 10 over,” but was carefully watching other traffic and was unaware he had drifted 2 MPH over the allowed speed. He said it was inadvertent, a slip, and most of the team agreed with that perspective. However, others were stuck on the choice – “He was conscious of the fact he was exceeding the limit.”

These are important discussions, but for the sake of analyzing risk, can be rather frustrating. When a team is stuck on a particular answer, the best resolution is to play it both ways – call it an error and determine what you’d do to mitigate the risk, then go ahead and call it a choice and continue down the RRG. See where you end up – and in most cases, your risk mitigation strategy will be identical!



The lesson here is don't get too fixated on what "box" you land in during a Behavioral Review. Instead, compare risk mitigation suggestions and strategies. If these mitigation strategies differ significantly, your team has more work to do – but if your team arrived at nearly identical mitigation strategies through different paths, that's not an issue.

So, how was the speeding Medic issue resolved? First, the team agreed that a 2 MPH variance is far different than, say a 10 or 20 MPH variance. While the Peer Perspective confirmed it would be easy to slip up and go 12 MPH over the limit when you are trying to stay at 10 MPH, considering all the distractions of driving in traffic with lights and siren, the 2 MPH variance over what was allowed could easily been inadvertent – an error. They also agreed that had the driver been going 10 or 20 MPH over the allowed speed (which would translate to 20 or 30 MPH over the *posted* speed), regardless of what the driver said, this would be a choice – not an inadvertent slip or lapse.

Next, team members who determined it was an inadvertent error moved over in the RRG to assess the contributors – where it says to examine System, Performance, and Behavioral contributors. They determined that the Medic did neither see nor understand the risks of going 2 MPH over the allowable speed, and that one system contributor is the placement of the speedometer and the other equipment in the cab of the unit. They also determined that the Human Performance Factors of stress, distractions, and some equipment-based issues (viewing the speedometer requires taking your eyes off the road and the mobile data computer maps) were contributors, and their recommended mitigation strategies were to look into heads-up speed displays on the units and to provide some system-wide coaching during their annual driver training about how easy it is to misjudge speeds in distracting environments.

The team members who remained convinced it was a choice then continued through the RRG. Was speeding above the allowed limit Justified under the circumstances? They answered "No." This brought them to asking whether traveling at 2 MPH over the allowance was At-Risk or Reckless. Well, had the variance been 10 or 20 MPH over, the Peer Perspective would likely be Reckless – however, at only 2 MPH over, the Peer Perspective concluded that this was At-Risk Behavior. The Medic made a choice that increased risk where risk was unrecognized, and he mistakenly believed himself to be justified. What was their risk mitigation strategy? Because if it's At-Risk, the assumption is that other peers are likely making the same choices and not seeing the risk. The mitigation strategy was to look into heads-up speed displays on the units and provide some system-wide coaching during their annual driver training about how easy it is to misjudge speeds in distracting environments. This would be the exact strategy as if they had decided it was an inadvertent error.

So, the conclusion is that collaboration is important, and the most important part of your analysis is collaborating and agreeing upon risk mitigation strategies – not on "labeling" behaviors as Errors, At-Risk, etc.

If choosing "Yes," it was an Error, your team's analysis goes deeper. Recall that in CJC, Human Error cannot be a sole "Cause." Human error is a consequence – a consequence associated with risk perspectives, system issues, performance factors, and yes, other choices.



- 
- 
- Support and encourage the individual
 - Examine System, Human Performance, and behavioral contributors that may have led to this error
 - Evaluate both System and Human reliability strategies

For example, an individual could run a stop sign inadvertently – they did not see the sign, and there might be system contributors (poor sign placement), human performance factors (inexperience as a driver), and behavioral choices (texting while driving, speeding) that contributed to the action. In this case *running the stop sign* itself was an *error* – it was *inadvertent* – but the contributors could include *choices* that were likely either at-risk, reckless, or higher culpability, depending on the Peer Perspective.

Key Point: Human Error is common, and it can be difficult to navigate all the contributors. It is strongly suggested that if you determine Human Error was involved, go to “**Attachment A: Human Error**” attached to this instruction manual. This Human Error guide provides examples of contributors, scenarios, and documentation tips.

Does the Organization Believe This Was a Justifiable Choice?



When evaluating this question, it can be enlightening to ask the individual(s) involved what values they were supporting when they made their choice. What did they perceive as the greatest risk at the time? If they thought their choice of action had a higher value than the policy, procedure, or process that was in place, ask them to explain their thinking.

For example, let's use a hypothetical case where there is a Lock-Out, Tag-Out policy that is supposed to be followed any time someone goes into a machine to clean it, repair it, or conduct maintenance. For worker safety, it's critical that every step in the Lock-Out, Tag-Out process be followed using a detailed checklist. But what if an employee fell into the machine and was unconscious and not breathing, or severely bleeding? Say the Lock-Out, Tag-Out process takes 20 minutes to complete as designed. Would you be justified in hitting an emergency stop button and jumping in to save the person? If you do, and save them, you're a hero. If you do the same thing and become injured or die, your decision would be viewed differently. So these "Justifiable" decisions have to be made by running counterfactuals – pretend there was no good or bad outcome, just a duty. What are the risks of acting outside the rules vs. inside the rules? You must be willing to accept the risks

before making a determination: Don't pretend saying "Yes" or "No" to this question eliminates risk – it won't – your decision will only shift the risks. Because either way you answer, remember there is residual risk. There are times when the rule doesn't fit, and a higher value is in place; and there are times when there is a higher requirement to follow the rule, but a perceived obligation to act differently pulls at our moral fiber and sense of what is right or wrong.





So there are no right or wrong answers here, just perceptions of risk, policies, duties, and the obligations we have to our fellow humans. Remember, this is a “Blue Box” question, which means it is answered from the perspective of the *Organization*. Do you, representing the organization enforcing the rule, believe that the individual’s choice overrode the requirement to follow the policy, process, or procedure? In other words, if these two values were to collide again in the near future, what would you want other individuals to do – follow the rule or make a similar choice?

NOTE: With all behaviors that are evaluated using the Collaborative Just Culture (CJC) process, one should never go straight to the “Behavior Column” of the RRG and start analyzing specific policy or procedural violations. All behaviors are to be evaluated in the context of CJC - so Risk, Competing Priorities, Systems, and Human Performance should be considered prior to assessing behavioral expectations.

One of the most common debates in any organization is the concept of “Justifiable” in the context of Time and Attendance policies. When is someone “justified” in showing up late, or failing to arrive at all when scheduled? Let’s run some scenarios to help you gain some clarity around the issues.

First, an important reminder about how you apply policies and procedures: There are two basic types of policy in any organization – **Autonomous** and **Procedural**. Policies that are **Procedural** tell employees what to do, and also describe, often in detail, *how* to comply. Policies that are **Autonomous** tell employees *what* to do, but leave it up to the employee regarding the how – *in other words, with autonomous policy, the employee “owns” the System they use for compliance, and the Human Performance Factors as well.*

In most cases (but not all), *Time and Attendance policies are **Autonomous***. The organization does not care *how* the employee gets to work on time – they just set an expectation for the start of a work shift. Whether the employee takes a bus, a personal vehicle, or rides horseback, the organization has neither the responsibility for the system the employee uses to arrive, nor are they concerned whether the employee knows how to operate their personal system (drive the car, catch the bus, ride the horse, etc.).

Because every organization expects some systemic failure, whether the system is managed by the company or by the employee, most entities give employees an acceptable “Failure Rate” for their systems when enforcing autonomous policies. In many organizations, for Time and Attendance, employees are given a certain number of unexcused absences in a rolling time period. For example, “three unexcused absences in a rolling nine-month period” specifically outlines the organization’s acceptable rate of failure. Any number above three would be an unacceptable rate of failure in the eyes of the organization, and there would likely be punitive consequences.

Because the employee “owns” their System *and* their Human Performance for arriving at work on time, *most* reasons employees miss work are *not* considered “Justifiable” behavior. Instead, they are personal System or

Human Performance failures, counted against the employee’s “Failure Rate.” There is a common misperception that excuses such as illness or vehicle malfunctions are “Justified,” since they appear to be random and out of the employee’s control.





However, for a Time and Attendance failure to be considered “Justifiable,” the reasons for the employee’s failure to arrive at work on time must be more than just random and somewhat out of their control. To be considered “Justified,” the circumstances typically need to be beyond their control, *and/or an unusual and unexpected circumstance, and/or support the values of the organization*. For Time and Attendance violations, these are typically *unanticipated* and *uncommon* situations. Normal illness and vehicle breakdowns might be random, and may not be fully in the employee’s control, *but these are anticipated situations*.

The employee’s system should anticipate these types of disruptions, and the organization’s rate of failure should as well.

Examples of Time and Attendance violations that are *not typically* considered “Justified:”

- My car broke down, would not start, had a flat tire. (It’s the employee’s system, they own the failure rate; if this starts happening often, it is their responsibility to find a different mode of transportation.)
- I missed my bus. (Take Uber, plan accordingly to have a back-up system, etc.)
- My child, spouse or significant other, parent, dog, cat, pet tiger is sick. (Again, it’s the employee’s system, the human performance factors are their responsibility, they own the failure rate. If this is occurring often due to chronic illness or other circumstance, it usually does not become “Justified,” but does require the Manager or Supervisor to explore options with Human Resources and the involved employee.)
- My alarm clock, phone, personal assistant did not wake me on time. (Same story – these systems are the responsibility of the employee, and the failure rate is designed to accommodate a few systemic failures.)
- My day-care provider was sick, closed, etc., or school had a late start. (Not usually Justifiable – these are anticipated situations related to child care and must fall within the acceptable failure rate.)

Time and Attendance Violations that might be considered “Justified” and not count against the employee’s Failure Rate:

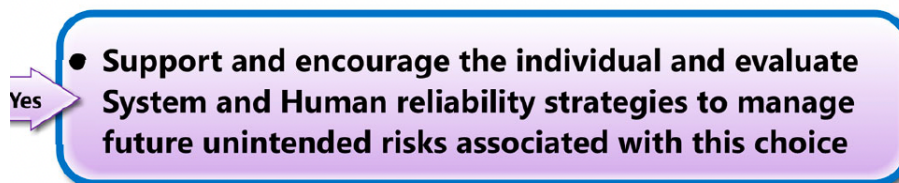
- On the way to work, I came across a motor vehicle accident and stopped to render emergency care. (The Manager or Supervisor might ask for some sort of proof, depending on the circumstances or the number of times this has occurred with this employee. But for most organizations, this behavior supports their values and is a justifiable reason for being late.)
- The bridge between my house and the office washed out last night. (In some circumstances, if there were alternate ways to get to work, the employee would be allowed this as a Justifiable absence for the first day – from then on, they would be expected to find alternatives.)
- A man on my bus collapsed, and we stopped so EMS could render aid (or I did CPR, etc.)



- The City Bus System serving my neighborhood is extremely poor – there is only one bus in the morning, and its arrival is often unpredictable. (The organization would hopefully assist the employee in finding alternatives – this would likely be more strongly considered if the employee was a low-wage worker unable to afford a personal vehicle expense, rather than a higher-paid employee who has more options.)

As always, “Justifiable” behavior is based on the organization’s risk tolerance, the risks associated with “justifying” the behavior vs. enforcing the policy, and the specific circumstances that are being evaluated. Always consider the risk you are accepting when you determine that a particular behavior is justified because you are trading one risk for another. There are no “risk-free” options!

If you, as an employer, regulator, or other rule-enforcer want to answer “Yes,” the choice was a Justifiable action, make sure you are talking with a peer and someone from HR and Operations to ensure you are supporting the *organization’s* value, not just a *personal* value. *Collaborate for consistency*. If you answer “Yes,” then:

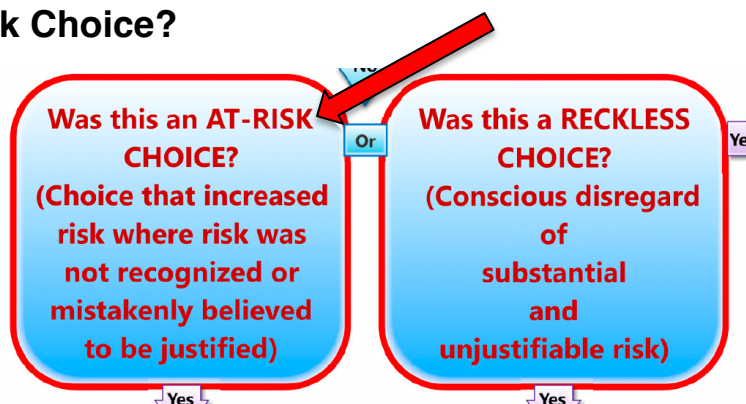


Consider:

For the individual: Support the person, and examine strategies to manage future unintended risk around the decision. In addition, determine whether the situation has a high probability of repeating itself, and/or whether the potential risk associated with the individual’s choice is tolerable. If there is a high probability of recurrence and/or the consequences are significant, educate other individuals about the risks as soon as necessary and consider system enhancements.

For the system: Assess the operational tolerance for the risks involved – both the immediate risk of not following policy, and the “value” risk if you direct them to follow policy next time in the face of the conflicting values. If “No”, the choice was *not* Justified from the perspective of the organization, move to the next question related to At-Risk and Reckless Choices.

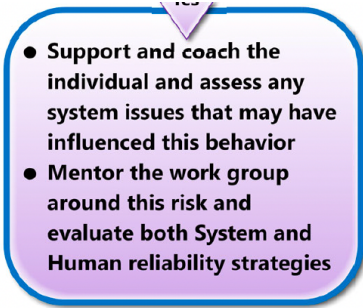
Was This an At-Risk Choice?





An At-Risk Choice is a conscious choice that increased risk where risk was not recognized, and/or the individual mistakenly believed the choice to be justified. Did the *individual* believe they were making a safe choice? Do you believe they did *not* recognize a risk? Would the individual say they thought they were justified in doing what they did, or in not doing what they were supposed to do, according to the policy, process, or procedure?

If the *individual* answers “Yes”, they did not recognize risk or believed themselves justified, you are not finished evaluating this behavior. At-Risk Choice is ***not an individual perception***, but a ***peer perception of risk***. Your team then has to ask, “What would other, similarly situated individuals *in our organization – in that department or work unit* – have done? What are they doing now?”

- 
- Support and coach the individual and assess any system issues that may have influenced this behavior
 - Mentor the work group around this risk and evaluate both System and Human reliability strategies

If others are doing the same thing, it is likely an At-Risk Choice – and the risk is not isolated to the employee you are examining, but also resides within the work group, and perhaps the managers as well. Your team should use objective data – video, audits, etc. – in determining the peer perspective. Try not to rely on asking others anecdotally what they would do, as this is generally inaccurate, particularly if the event had an undesirable outcome. If the answer is “Yes,” your team believes the behavior was At-Risk, consider:

For the individual: Generally, for At-Risk behavior, we coach the person, discussing the organizational risk tolerances, behaviors that are expected in the future, and potential consequences for not changing behavior. However, *before taking any action whatsoever*, look in the individual’s Human Resources file and/or training file for previous actions, including coaching or corrective action. If the individual has been coached for At-Risk behavior within the previous 12-18 months, the behavior may be considered “repetitive” and may require a more substantive response to change behavior (such as progressive discipline). Make sure to check your HR policies and/or labor agreements to ensure you clearly understand what constitutes “repetitive,” and how far back you can go into an individual’s record.

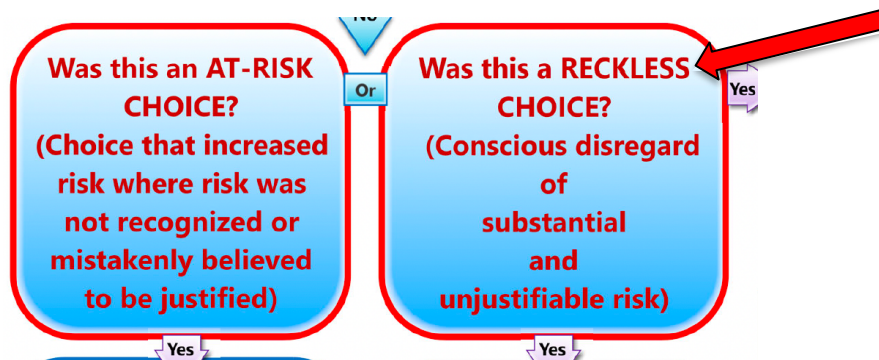
When coaching, focus attention on any competing priorities or system influences that may have been driving these behavioral choices. Help the individual understand how you want them to deal with those competing priorities and ask them how the system might be modified to make it easier for them to comply. Note the coaching in your manager’s file.

For the system: While it is important to coach the individual about risk tolerances and priority conflicts, it’s also crucial that you address how you expect them to deal with the priority conflicts within the system when they occur. Note the coaching in your Manager’s notes, and make sure you follow up with the remainder of the work group. Address the competing priorities you think are driving the behavior within the work group and address any system issues that might be involved.

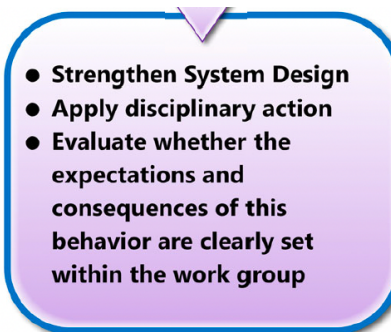


Key Point: At-Risk Choices are also common, and coaching effectively is both science and art. It is strongly suggested that if you determine At-Risk Choices were involved, go to “**Attachment C: At-Risk Choice**” attached to this instruction manual. This attachment provides examples of coaching techniques, scenarios, and documentation tips.

Was this a Reckless Choice?



A Reckless Choice is a conscious disregard of a substantial *and* unjustifiable risk. Although it's a high bar, behaviors such as lying, drunk driving, and showing up to work under the influence of intoxicants are *generally* found to be reckless choices. However, jumping to conclusions is dangerous, and this is an area where it can be helpful to recall you are not necessarily *condoning* behavioral choices, but trying to *understand* them.



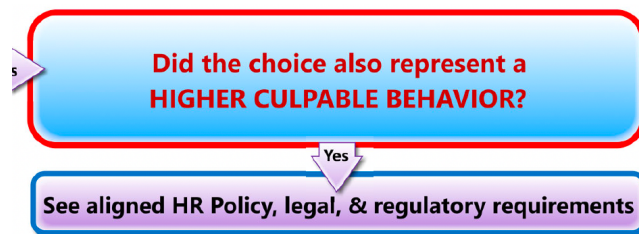
If you believe the behavior was reckless, you must understand the effectiveness of strengthening system design (barriers, redundancies, and recoveries), versus employing only punitive deterrents such as progressive discipline. You and your team should be confident that applying corrective action to both the system and the individual will *proactively* manage this particular risk. If you don't think the system is safer after applying corrective action, you may have placed too much emphasis on the individual component.

If you believe the behavior was reckless, follow the organization's progressive discipline or corrective action policies. Typically, you start with the least punitive available step to initiate a change in behavior, but every organization has their own determinants associated with the severity of a risk and the subsequent consequences for the individual.



Key Point: If you choose “Reckless Choice,” are you relatively certain you have proactively managed the risk by strengthening system design and applying punitive measures? Have you minimized this risk to an acceptable level for the organization? By calling the behavior reckless, you are generally making the determination that the individual is a risk – their Reckless Choice placed the organization, themselves, or others at risk and, most important, their *peers* would see their behavior as both a substantial risk and unjustified. Discuss with your team, and ensure your assessment will withstand a TRIAD review.

Did the Choice Represent a Higher Culpable Behavior?



Higher Culpable Behavior is often what we describe as “beyond reckless.” It can be criminal in nature, and may fall into categories such as assault, theft, inappropriate and/or unwanted sexual contact, harassment, menacing, stalking, intimidation, and other serious transgressions. If you believe there is Higher Culpable Behavior involved, we recommend that you do not manage this at the local Supervisor and/or Manager level! Instead, consider the following steps:

- If necessary for the immediate safety of co-workers, clients, or others, contact law enforcement;
- Immediately contact your Human Resources team for advice;
- Follow your chain of command to ensure the appropriate levels of management are involved;
- In cases of suspected Higher Culpable Behavior, with very few exceptions the employee should be placed on immediate suspension and removed from the work environment. Ensure you have the proper support, and strongly consider steps to secure the employee’s passwords, access badges or keys, accounts, laptops, and other work materials prior to placing them on leave to ensure they are unable to present further risk to the organization and staff while analyzing their behaviors.
- Contact any regulatory authority as required by local and state statutes;
- Work with HR and other key leaders to develop any necessary internal and/or external messaging;
- Ensure to communicate who the key contact is for both internal and external questions and demands for materials, access, or other needs.





Organizational Response

5. Organizational Response Manage System and Human Contributors

Organizational Response

The Organizational Response column provides tips for system and individual intervention as you work through the Behavioral Choice column. As mentioned in the Human Error section, a key tip is to remember that the “box” you land in under “Examine Behaviors” is less important than the *response* that is chosen. For example, you could have members of your team debating whether someone clearly knew the expectations or made an At-Risk Choice. If your team agrees that the appropriate response would be to coach the individual about the expectations and look for system issues, you have achieved a successful outcome.

Do not think you have to label the behavior. Again, this is neither a fault-finding or labeling exercise, nor do you take an individual through this process to determine what action to take (coach or punish, for example). This is not a Human Resources tool to help you decide what to do. That would be an incorrect use of the High Reliability model, which is designed to determine risk, discuss potential proactive interventions, and manage the socio-technical system.

If, during the risk analysis, you and your team determine that remediation, coaching or corrective actions would mitigate future risk, make the appropriate recommendations.



Organizational Reliability

6. Organizational Reliability

- Has the organization provided a balanced response to both **SYSTEM** and **HUMAN** contributors?
- How will the organization see, understand, and manage these risks moving forward?
- Is this approach sustainable? Can it be monitored and measured?
- What other related risks should be seen, understood, and managed?

Once finished evaluating Systems, Human Performance and Behaviors, it's time to evaluate your approach and make recommendations:

- Does the organization now fully see and understand the risks?
- Do you feel the organization has taken a balanced response to both System and Human contributors to the risk? Re-check your biases and discuss among your team whether you feel the actions taken (System, Human) have a good chance of mitigating future risk.
- How do the individuals within the system see and understand risk?
- Have you examined the systems, performance factors, and behaviors that contributed to the risk?
- Have you set clear expectations?
- Have you documented your findings and your coaching?
- Have you managed the competing priorities for the people involved and their peers?
- Have you addressed or suggested system improvements, sent them to the appropriate person, and followed up to see whether they are being planned?

- Have you created an effective remediation plan if needed for Human Performance (both personal and organizational)?
- Is the approach sustainable? Can it be monitored and measured?
- Are the recommended system changes *aligned* and *integrated* with your Reliability System?
- Determine the relative proactive strength of the recommendations. Review the Proactive Strength section of the Collaborative Risk Review Manual and discuss where your proposed remedies may leave the organization vulnerable.

STRONG <i>System Focused</i>	• Effective Automation • Failsafe Mechanisms • Forcing Functions • <i>Resilient</i> Lean Design	• Improved Devices, Usability Tested • Optimal Process Redesign • Architectural Improvements • High Fidelity Capture Opportunities
MODERATE <i>Human Performance Focus</i>	• High Fidelity Simulation • Checklist/Cognitive Aids • Reduce Distraction • Increase Detectability	• Eliminate “Look & Sound Alike” • <i>Optimized</i> Redundancy • Standardize Equipment/Processes • Team & Communication Training
WEAK <i>Behavior Focus</i>	• Classroom Training/Ed. • Additional Double Checks • Additional Documentation • Warnings & Signs	• Safety Bulletins, E-Mails • New Written Procedures • Highly Detailed Processes • Memos, Policies, Best Practices

Evaluating the Risk Mitigation Strategy

Determining the relative proactive strength of a recommended action is an important exercise. In many cases, organizations opt for the easy fix – more training, memos, e-mails, posting a sign. While weak, behavior-focused methods are certainly reasonable responses and even domains that are consistently highly reliable use them, such as the commercial aviation industry, these should not be the default reactions to any analysis. Instead, gauge the short-term, long-term, and residual risks. None of the behavioral responses in the table above will be effective in the long term – people forget, time passes, signs get ignored, e-mails are read and deleted, new policies become part of the huge online resource pool.

Note that the effectiveness of a response is closely associated with the Sequence of Reliability. The strongest responses are those that involve capture opportunities, forcing functions, or other systemic changes, particularly those that are designed around predictable human performance and behaviors. These also tend to be the most expensive and operationally disruptive – hence, an organization needs to balance the appetite for





residual and continued risk, and the costs associated with occasional unwanted risk events, against the cost and disruption associated with a strong systemic fix.

The next most reliable responses are those associated with improving the cognitive and physical performance of the humans in the system. Realistic simulation, reducing distractions, addressing fatigue and mental capacity, and building ardent team communication skills have moderate to high proactive mitigation probability,

are often less expensive than structural system changes, and have an additional benefit of improving employees' work experience.

Our advice is to apply what your collaborative efforts have determined to be the best, most actionable response, and to ensure the organization has a systematic, executive process for evaluating the suggested remedies, resourcing them, and providing feedback.

Many organizations that have a Collaborative Risk Review process also have a method for ensuring mitigation strategies or remedies are appropriately evaluated. This often means that an executive team, with the powers to budget and/or allocate funds, reviews the recommendations on a regular and timely basis, and provides feedback. In several organizations that we work with, this Executive Risk Review Committee is given three choices when presented with risk mitigation options:

1. Accept the recommendation as presented and provide the necessary resources to implement, monitor, and measure the results.
2. Reject the recommendation and *accept the risk!*
3. Send the recommendation back for more research. This response, in many organizations, is allowed to occur only once – this forces the organization to make a decision to either resource the mitigation strategy, or accept the risk for the near future until some other strategies are developed (or until another risk event occurs).

Determining Residual Risk

Organizations often use what we call a two-dimensional tool to evaluate risk. With only two measurements, Probability (or often, Frequency) and Severity, these have green, yellow, and red boxes that are supposed to visually indicate the potential risk.

High Reliability requires not a two-dimensional evaluation, but four dimensions:

- Potential Severity and/or Operational Disruption
- Frequency (can also be Probability and/or Likelihood)
- The Organizational Ability to Respond and Recover
- Time (usually the length of time the risk will be present)





In the Collaborative Risk Review Manual and the Reliability Team Manual, these are described in more detail, with examples of four-dimensional risk tables, including applications. In addition, your SG Partner can provide examples where organizations have used these strategies, not just organizationally, but to help determine who analyzes a risk event.

Attachment A: Human Error

Support, Determine Cause, Mitigate

Why This Strategy?

In most instances, no one is more focused on understanding and correcting the contributors to an error than the individual (or individuals) directly involved. When someone commits a human error (an *inadvertent* slip or lapse), we need an approach that maximizes our learning from the event, and one that also provides a redemptive pathway for those involved.

What we want is a compassionate response; however, it is more than extending compassion or empathy. The person who committed the error needs to understand clearly what happened. They should realize that another careful, competent person could also have made the same error under similar circumstances. And while they need to hear that they will not be punished for the *error itself*, we caution that CJC is not a “non-punitive” approach – it is an approach that values justice and fairness. So while the error itself is not punished, there are instances where individuals made At-Risk or Reckless choices that contributed to the error – clearly defining these during the CRR process is an important part of ensuring a safe, fair, and accountable culture.

For example, if I ran a stop sign because I didn’t see it, that would likely be an inadvertent error. However, if I was texting on my phone, and that distracted me, I might be held accountable for the At-Risk or Reckless choice to text and drive – but in a CJC, not for running the stop sign. We understand that this does not always align with what the legal world would do, because the legal system often bases the severity of the response on the outcome. If you hit someone in the crosswalk when you ran the stop sign versus just driving through it and creating a risk, the legal system would see those differently and respond based on the severity.

When to Use This Strategy

When a human error has been identified, engage the individual who committed the error as soon as possible.

Steps

- **Determine who will conduct Fact-Finding.** People who have committed a Human Error may feel





badly for the outcome and may be fearful that they will be punished for their inadvertent action. Although anyone can support the individual, it will be more meaningful if their Manager or Supervisor offers them support and reassures them. If you feel that you cannot support the individual because you are uncomfortable, angry, or unsure of how to approach them, ask someone else to support the person.

- **Make it private.** When possible, take the person to a quiet and private space where you can discuss the issue, offer reassurance, and ask open-ended questions whenever possible.
- **Help the person understand what happened.** Go through the events as they are known to you. Don't assume causal connections. Use known facts. Try not to ask "yes" or "no" questions. Build a timeline and get individual input on what System issues may have contributed to the error. Ask whether their experience had anything to do with the error, or whether education and training around the issue are adequate. Were there any other things that may have contributed to the Human Error, such as fatigue, stress, or distraction? Why?
- **Listen.** Be curious. Give the person your undivided attention. Be focused on them, and mindful of what they are saying.
- **Ask:** Do they need assistance? Support? What would they need to regain their sense of safety?

Gather Key Information

See if the individual can provide some insight into the following:

1. **Were there things within the System that may have contributed to the error?**
 - a. For example:
 - i. Equipment interface
 - ii. Alarms
 - iii. Ineffective barriers
 - iv. Confusing packaging
 - v. Unclear policy or procedure
 - vi. Cultural "norms"
 - b. If "Yes," determine if the System issue presents an *immediate* risk. If it does, contact your Supervisor and the Safety Officer. Take the equipment out of service, if possible, or discuss an immediate risk mitigation strategy.



- 
- c. If not an immediate risk, but the System issue has the likelihood of causing further Human Errors or issues, complete a Safety Report and ensure follow-up.

2. Were there any contributing Human Performance Factors? Also try to determine whether these are personal or system-driven. For example, if fatigue is mentioned, is the person working mandatory OT, or did the individual stay up late last night at a concert?

a. Examples of Human Performance Factors:

- i. Level of Knowledge, Skill, Ability, or Proficiency (See the earlier section on KSAP)
 - ii. Cognitive or physical performance and ability
 - iii. Familiarity with the process in question (level of experience)
 - iv. Fatigue, stress and/or distraction
 - v. Cultural influences
- b. If “Yes,” write down how these were managed by the individual, and/or where they had particular difficulty (Example: “The individual was under significant time pressure to complete the assigned task, was distracted by other demands, and missed Step Seven in the process...”)

3. Were there any Behavioral Choices that may have increased risk?

- a. Did they engage in choices that increased risk? (Failed to follow a good procedure, engaged in a short cut, displayed a bad attitude, etc.).
- b. Did they engage in a choice that may have caused distraction? (Cell phone conversation, multi-tasking, etc.).
- c. If “Yes,” ask yourself: Was there a *behavioral expectation, policy, process, or procedure* that they did not comply with?
- d. If “Yes,” take the individual through the “Behaviors” column of the RRG to properly evaluate the risk.
- e. Do not “conflate” issues. Do not combine behaviors. Take each one through the RRG to determine where risk lies.

Once your interview and analysis are complete, SUMMARIZE:

1. Your report should include:

- a. ***Any System Influences that contributed to the Human Error.***

- 
- i. Each System issue should be identified, and each should have an appropriate risk mitigation strategy outlined. Collaborate with front-line people, Risk Management, and others to identify and advance any System recommendations that have a high probability of mitigating future risk and have a low operational impact.

b. *Any Human Performance Factors that are the responsibility of the individual?*

- i. If “Yes,” it is the employer’s responsibility to outline remedial improvement steps (or a Performance Improvement Plan) that will address any KSAP deficiencies, cognitive issues, or other individual performance that falls below the standard for the person’s position. PIP’s should include, at a minimum:
 - The minimum required performance standard
 - Examples of substandard performance
 - Suggested steps necessary to achieve minimum required performance
 - A timeline for improvement, including metrics
 - A schedule of “check-in” dates when a Supervisor or Training Officer will check the metrics and discuss progress
 - Consequences associated with a failed PIP (e.g., extension, termination, re-assignment, etc.)

c. *Any Behavioral Choices that increased risk.* Your report should document whether these were At-Risk or Reckless Choices, as objectively determined using the RRG Guide.

- ii. **Each Behavioral Choice should have a recommended action.** For example, if the choice was At-Risk, the recommendation should include coaching the individual for the At-Risk Choice and addressing any value conflicts or System issues that may have contributed to the At-Risk Choice.
- iii. If the individual made a Reckless Choice that contributed to the Human Error, the Corrective Action Plan or Process should always be separated from any Performance Improvement Plan that might be associated with task or cognitive performance (see below references to PIP).

2. Repetitive Human Errors

- a. Human Errors should be managed as they occur. In instances where an individual makes repetitive human errors, the PIP and/or corrective action plan should define very measured steps for improvement and should clearly identify consequences for not performing up to





standards. Repetitive errors do not have to be “the same error type” to be deemed repetitive. For example, an individual may make several errors associated with a lack of situational awareness. These should be clearly defined, but they can be grouped as an example of failure to perform at a required cognitive level. Work with your HR and Education departments to ensure the correct steps are taken toward the individual’s success (or potential separation for failure to perform).

Example Only (Operational):

Human Error Scenario

A bio-med technician is performing regular maintenance on a cardiac monitor and defibrillator. The maintenance procedure stipulates that the technician bench-test the batteries, and that any battery that fails on the first test must be replaced. Batteries are in short supply due to a backlog at the manufacturer,

and they often fail the first test but pass the second test without difficulty. The maintenance technicians have developed a practice to test batteries twice instead of once – and if they pass the second test, batteries are returned to service (but a notation is made that they be replaced at the next service).

The bio-med technician has a battery that fails the first test, and he sets it aside for a second test. He is then distracted by two urgent repair requests and returns to his test bench three hours later. He mistakenly places a “Tested – Passed” sticker on the failed battery and places it back into service. The battery fails during a patient resuscitation, and tests show it was bench-tested only once and failed.

Summary

The bio-med technician had a responsibility to complete the testing procedure as designed. This was a behavioral expectation, he understood the expectation, there was a policy in place that required the technician to properly test the equipment, it was possible to follow the policy, but he did not *choose* to place a failed battery back into service. It was deemed a Human Error. When the Human Error analysis was completed, it found:

- **System Contribution** – Batteries are in short supply because of a vendor issue.
- **System Contribution** – The bench-test area is not laid out in a way that minimizes the chance of error. It is easy to confuse batteries that are awaiting testing with batteries that have already been tested.
- **Human Performance Factor** – The technician was distracted by two urgent requests for service.
- **Behavioral Choice** – The technician chose to not place the battery out of service immediately per protocol. This was deemed an At-Risk Choice, because it was found that other technicians had developed and used the same method to keep equipment in service.





The Final Action Report would:

- Address the system issue, if possible, with a recommendation about how to mitigate future risks. Suggestions might be to discuss the backlog with the vendor, talk with Engineering about the test procedure, and re-design the workspace.
- Coach the technician for his At-Risk Choice about the work-around, but also look at the competing values and incentives for the behavior (safety vs. production). Communicate with other technicians regarding your future expectations and discuss how to mitigate the System issues that are driving the behavior.
- Recommend that when technicians are called away, they first organize their work site to minimize the chance they will miss a step upon returning to the testing and maintenance process.

Attachment B: Bias Review Checklist

Bias Checklist for Collaborative Risk Reviews

For further details on these questions, please reference the Bias Assessment Guide in the CRR Manual.

Seeing and Understanding the Risk (of Biases)

Biases in Team Members *Analyzing the Risk Event (Assessing Ourselves)*

- **Fact-Gathering**
 - ▶ Completed? Countervailing evidence being considered?
- **Sequence of Reliability**
 - ▶ Utilized the RRG? Behavior first (blame) avoided?
- **Personal Biases**
 - ▶ Outcome over/underwhelming? Individual responsibilities? Similar cases recently?
- **Psychological Safety**
 - ▶ Input from everyone? Dissenting opinions considered/explored?



Biases in Individuals *Involved in the Risk Event (Assessing Others)*

- **Different Cultures Involved?** (or different demographic groups)
 - ▶ Risk Perception of staff/patients toward that culture? Perception of RMT members?

System Reliability (Managing Structural Biases)

- **Effective/Resilient in managing risk *for other cultures or demographic groups*?**
Consider System access, Communication, Education/Training, Policies, Metrics for different cultures
 - ▶ System differences for different cultures? Why or why not?
 - ▶ Challenges for different cultures to engage with the healthcare system?
 - ▶ Information, instructions/signs accessible and decipherable for different cultures or disadvantaged people?

Human Performance Factors (Influence of Biases)

- **KSAPs – Potential Biases during assessment of KSAPs?**
 - ▶ KSAP challenges for different cultures?
 - ▶ KSAPs related to bias and discrimination awareness?
- **System Influences**
 - ▶ Challenges for customers and staff from different cultures?
 - ▶ System/sub-systems to aid customers and staff from different cultures?
- **Personal Influences**
 - ▶ Culture (or demographic group) of the individual and/or their experiences?
 - ▶ Status of customer or staff in the organization or the community?
 - ▶ Relationship or experience of team members to the people involved?
 - ▶ Potential benefits or risks of CRR results to team members?
- **Cultural Influences**
 - ▶ Diversity of the work force and/or the community?

- 
- ▶ Biased attitudes/beliefs about different cultures?
 - ▶ Hierarchy (or Power Gradient) in the work unit?

Human Behavior (Related to Biases)

- Clear understanding of discriminatory actions or words?
- Possible to not be biased? e.g. personal relationship
- Inadvertent Discrimination? (**Implicit Bias**)
- Choice to Discriminate? (**Explicit Bias**)
- Justifiably biased? e.g. discriminatory treatment needed to manage a risk

Counterfactual Statements

A Counterfactual Statement is one which specific detail(s) are altered to lessen the likelihood of a particular bias.

If answers to any of the questions above suggest a potential for bias, have we tested our assessment using a Counterfactual Statement?

Attachment C: At-Risk Choice

Effective Coaching

Why This Strategy?

Coaching is an effective method when an individual is unable to see the risks associated with their behavior. It is not punitive, the first coaching is not placed in the person's HR file, and the goal is to increase the individual's awareness around risk. However, the Manager should make a note in the Manager's record that coaching took place, just as the Manager should note when an individual exhibits positive behavior or performance.

When to Use This Strategy

When an At-Risk Choice has been identified, engage the individual who demonstrated the behavior as soon as possible.

Steps

- **Determine who will do the coaching.** Generally, the best coaching comes from peers who see risk. However, because At-Risk Choice is often a shared conduct within a work group (many are doing the





same thing), it is most often going to be the immediate Supervisor or Manager of the individual who conducts the coaching. Coaching is most effective when the person coaching has direct experience around the individual's task, workload, and the risks involved, and when the person coaching has demonstrated in the past that they want the individual to succeed.

- **Make it private.** When possible, take the person to a quiet and private space where you can coach the person.
- **Lead with your intentions.** Always let the person know, from the very first, that your intention is to discuss a potential (or actual) risk, to increase the individual's understanding of the risk, and that there is no intention to be punitive.
- **Use facts.** Be specific about the observed behavior. Don't use general terms. Make sure they are listening and that they understand. Describe the observed behavior, the risks involved, the expected behavior, and the consequences of non-compliance. Have them repeat back what the risks are, and what their expected behavior is. Always ask them what System issues and values might have driven their choice: "What makes it difficult to follow the policy/process?"
- **Create an understanding of the risk(s) involved:** Use specific examples of real or potential risk, if available. Discuss risk in real, not abstract terms. Risks to organizational values, to people (patient or individual harm, harm to teams, harm to organizational culture), to financial health, and to organizational and/or personal reputation may be involved. If so, describe how an At-Risk Choice could lead to harm.
- **Specifically address other incentives or values that you believe may have led to the At-Risk Choice. This is a critical step.** People are often driven to shortcuts and/or At-Risk Choices because they perceive one value (for example, production) may be more important than another (a safe practice). If you address only the expected behavior without addressing the workplace conflicts or system difficulties, the person is likely to be frustrated. For example, if there is a production or privacy issue that is driving the behavior, ensure that you address how the individual should address those values in the future when they conflict with what you are telling the individual is the primary value.
- **Example:** "While I recognize that the safety protocol requiring a redundant check slows down our patient care process and interferes with other people's work process, I need you to follow the redundant check process because the risk to the patient if we get this wrong is just too great, and the frequency that we administer this drug is relatively high. So the redundant check is a primary value. In the future, when production or the pace of work conflicts with our safety protocol, please let me know so we can address the system influences that are driving this issue. Additionally, if you have suggestions for a method that might meet our safety goals, but that would not impact work pace or production, I'd love to hear it."



- 
- **Gain their assistance:** Ask them if they will assist you in letting others know about the risks associated with the behavior. If it is a widespread practice deviation, offer to bring the staff together to discuss the issue. Ensure the individual knows that it is your intention to address the behavior with other staff members if you believe it is widespread or common.
 - **When appropriate, make a note in your Manager's record of the date and the type of coaching that took place.**

What This Might Look Like:

At-Risk Choice

An individual forgets to restock a unit with critical medications after an emergency transport. The crew is supposed to fill out an inventory form after each run, and contact the field supervisor if they are low on a particular medication or supply item. The medication that was not restocked is needed for the next emergency call, and after the crew uses what's in the drug box, they find they have no second dose available in the unit. The patient is delivered to the hospital with suboptimal treatment.

An incident analysis determined that the person made a human error by forgetting to complete the restocking of the ambulance. It is determined that there were personal performance factors in play (distraction), but it is also found that the individual made a *Behavioral Choice that led to increased risk* (failure to use the required inventory checklist after every call).

When taking the person through an evaluation of their behavior related to the policy, you find that they chose not to follow the checklist. You determine that the behavior was not "Justified" and do the "At-Risk" behavior analysis. You find that their choice was At-Risk, not Reckless, because many other individuals are not taking the time to complete the inventory, and production pressures push people to get their unit back in service rapidly after every call. You are curious why this is a shared (and not individual) behavior, and find that the individual involved, along with her peers, believe the checklist slows their turnaround time at the hospital, and that they have been counseled in the past for extended turnaround times.

When You Call the Person into the Office

- Lead with your intention: "My intention this morning is to discuss with you a choice you made that increased risk for our patients and our organization. You are not in trouble and this is not punitive, but I'd like to raise your awareness about risk, clearly state our expectations for future behavior, discuss potential consequences, and to ask you how we might work together to mitigate future risks."
- "We want to explain the concept of At-Risk Choices. An At-Risk Choice is one where there is an organizational risk for real or potential damage or harm, but the risk is not seen by the person involved. The individual thinks they are safe. We all engage in At-Risk Choices of some sort, and my intention today is to discuss with you an At-Risk Choice that we identified in our recent analysis of the missing medication incident."
- "Your decision to not use our inventory checklist is not in compliance with policy XYZ. I have reviewed





the policy, and I believe it is current and relevant to the situation.”

- “We are curious as to whether there is anything that makes it difficult for you to follow this rule. What kinds of things in our system might be contributing to your choice?”
- “We expect that in the future, you will use the inventory checklist that we have provided. The risk for our organization and for our patients is just too great.”
- “You mentioned that people feel pressured to get back in service, and to shortcut the process. I can understand that view, and let me discuss with my boss what I might do to relieve some of those pressures or to change the perception. If you have any thoughts about how we might do this, please share them with me.”
- “Would you be willing to discuss with your peers the risks associated with not completing the checklist, and to provide me feedback about how we might make this process easier, or how we might keep our turnaround times reasonable while still ensuring we have adequate inventory?”
- “The consequences of repetitive At-Risk Choice could likely be corrective action. We’d like to avoid that at all costs.”
- “Can you please tell me what you just heard about At-Risk Choices, about our expectations about using the checklist, and about the risks involved if you continue the behavior?”

Repetitive At-Risk Choice:

- Have you documented previous coaching?
- Have you ensured that the individual understands how you (the employer) see risk and what the consequences are?
- Have you addressed any issues *within the system* that might be driving the behavior?
- Have you made sure that you, the Manager or Supervisor, have communicated expectations about the risk to the individual and to other peers within that work group?
- If “Yes” to the above:
 - Depending on the risk and the individual’s previous behavioral record, consider coaching again and re-emphasizing expectations.
 - Ensure that your obligations as a Manager (communicating risk to the work group and addressing System issues and Conflicting Values) have been completed.
 - If “Yes,” consider progressive discipline as needed to change behavior.





Attachment D: Resource Reading List

Collaborative High Reliability & Collaborative Just Culture

- ***The Leader's Guide to Managing Risk: Griffith, K. Scott***
 - ✦ The sentinel view on how Collaborative High Reliability and Collaborative Just Culture became the premier method for analyzing and managing risk, by Scott Griffith, former pilot for American Airlines and one of the founders of SG Collaborative Solutions.

Decision-Making, Error Analysis, Human Factors, Human Performance

- ***Range – Why Generalists Triumph in a Specialized World: Epstein, David***
 - ✦ An excellent book on why individuals and teams benefit from diversity in skill and thought.
- ***Thinking, Fast and Slow: Kahneman, Daniel***





- ✦ A sentinel view of how our mind works, and a necessary read for people trying to understand the human decision-making process. High Reliability is based on a clear understanding of decision-making under time pressure, and there is, as of this evaluation, no better resource to explain the process.
- **Noise: Daniel Kahneman**
 - ✦ An educational view of how the “noise” of too much information can obscure the “signal.” The Signal to Noise Ratio (SNR) is commonly discussed when looking at human factors. This book helps to understand how easily we can be influenced by noise and miss the signal.
- **The ETTO Principle – Efficiency Thoroughness Trade-Off: Hollnagel, Erik**
 - ✦ A study of how we trade accuracy for speed.
- **The Limits of Expertise: Rethinking Pilot Error and Cause: Dismukes**
 - ✦ A good analysis of all the human, systems, and performance factors that play into our becoming “experts,” what those limits are, and why we should always be learning.
- **Safety-I and Safety-II: The Past and Future of Safety Management: Hollnagel, Eric**
 - ✦ Eric’s sentinel book about safety management introduced a new term that is now commonly used – “Safety I and Safety II.” This is an excellent primer on why prevention and proactive management is the future of safety. Safety 1 is primarily old-school accident investigation, whereas Safety 2 is focused on contributors, mitigating risk proactively, and managing systems better to make them more resilient.
- **The Intelligence Trap: Why Smart People Make Dumb Mistakes: Robson, David**
 - ✦ An interesting book on Human Error and poor decision-making. A quick read, a little repetitive.
- **The Power of Habit: Charles Duhigg**
 - ✦ Want to break a habit? This book will show you how that’s done, but more important, it demonstrates how we get stuck in patterns of thinking and operation that can be harmful and risky.
- **The Design of Everyday Things: Norman, Don**
 - ✦ An analysis of design features, and how marketing drives more about design than human factor usability. A little repetitive, but you’ll never look at a doorknob the same way again.
- **User Friendly: How the Hidden Rules of Design are Changing the Way We Live: Kuang, Cliff**
 - ✦ Another systems design book, but probably more in line with understanding intuitive design and how human factors should play a stronger role.
- **Safety II in Practice – Developing Resilience Potential: Hollnagel, Eric**
 - ✦ The author expands your understanding of how to integrate Safety II methods, how to test for resiliency, and other skills. A good read for the budding expert in Safety II science.





- **Sources of Power: Klein, Gary**
 - ✦ A sentinel work on how individuals make decisions under time pressure. Gary introduces us to the concept of “Naturalistic Decision-Making” and “Recognition-Primed Decision Making.” If you want to know how firefighters, paramedics, trauma surgeons, critical care nurses, and others make decisions every day, and how these might be looked at differently in the calm aftermath of hindsight bias, this is an excellent read.
- **The Challenger Launch Decision: Vaughn, Diane**
 - ✦ Diane introduced us to the term “Normalization of Deviance” in this book. While in retrospect critics have criticized some of its accuracy related to events, it is nonetheless an excellent analysis of complex systems run by complex and pressured humans and how things can easily drift from safety toward production goals.
- **The Book of Why – The New Science of Cause and Effect: Pearl, Judea**
 - ✦ A journey through cause and effect analysis.
- **Risk-Based Thinking – Managing Uncertainty: Muschara, Tony**
 - ✦ A good read for those who want to better understand risk and risk analysis. This and the next book (Against the Gods) are must-reads for those working to develop expertise in how we see and understand risk.
- **Against the Gods – The Remarkable Story of Risk – Bernstein**
 - ✦ Not just a good analysis of the history of risk perception and management, but Bernstein uses stories to get the message across. Good analogies and an excellent read on risk.
- **Human Judgment and Social Policy – Irreducible Uncertainty: Hammond, Kenneth**
 - ✦ While this is an older book, and trends toward the academic, it is a sentinel work on how humans make decisions, and the difference between analytic decision making and naturalistic decision making. Probably not for the novice, but those of you gaining expertise will see many references here that will peak your interest.
- **Brain Rules: John Medina**
 - ✦ Medina writes well, uses stories, and shows us how the brain works both for and against us.
- **A Deadly Wandering: Richtel, Matt**
 - ✦ This is an unusual addition to the list, but is added to entice those wanting to face and manage their biases. The book is a true story, based on a tragic car crash involving the use of intoxicants. The author intentionally switches between the aggrieved family of the victims and the perception of the driver charged with the crime. Just as you decide “who you’re for,” the author pulls you in a different direction. I recommend this for those who have to facilitate.



- 
- ***The Human Contribution: Reason, James***
 - ✦ One of James Reason’s sentinel works on human performance within systems. Some of the ideas are old and no longer valid, but it will give you a good historical background on why so many systems are still not resilient.
 - ***Intuition at Work: Klein, Gary***
 - ✦ The author of Sources of Power dives deeper into human intuition. Maybe not for the novice, but for those interested in developing some expertise around human decision making and intuition, this is a good read.
 - ***Judgments Under Uncertainty – Heuristics and Bias: Kahneman, Slovic, Tversky***
 - ✦ An older and academic book, but amazingly relevant when it comes to human reliability. Kahneman wrote “Thinking, Fast and Slow,” and Tversky was a lifelong collaborator with him. This book is pretty amazing in its depth.
 - ***Medical Error and Patient Safety – Human Factors in Medicine: Peters, George***
 - ✦ A little simplistic in its conclusions compared to other texts on this list, but it emphasizes the importance of good systems and system design in healthcare, using examples.
 - ***The Multitasking Myth: Loukopoulos, Loukia***
 - ✦ A book that proves the title using science and great examples – it’s a myth, we don’t multi-task. A good reference if you are doing workload studies and human performance analysis.
 - ***Uncontrolled: The Surprising Payoff of Trial and Error: Manzi, Jim***
 - ✦ A journey into some studies and real-life examples of how “perfect is often the enemy of good enough.” Trial and error, within reason, prevails over long-term analysis paralysis.

Communication, Culture, Risk, Change Strategies

- ***The Person You Mean to Be: How Good People Fight Bias: Chugh, Dolly***
 - ✦ An amazing book about inequity, bias, and how systemic and structural biases have affected us in many ways. If you are charged with any type of incident or risk analysis, or part of a reliability team, this is a must-read.
- ***The Failure of Risk Management: Why It’s Broken and How to Fix It: Hubbard, Douglas***
 - ✦ A book that emphasizes why the reactive risk-management process used for years needs to change to a more proactive model. Supports many of the Safety I and Safety II concepts, from a different voice and perspective.
- ***Pre-Accident Investigations: Conklin, Todd (PLUS: Available Podcast on iTunes)***
 - ✦ Like other reads we have given you, it’s about proactive and “Safety II” strategies. The gift here





is that Todd is a very curious, creative guy and a great listener. His podcast is amazing – every week, you’ll hear safety, risk, and quality discussions from different people. Importantly, they offer different and at times divergent perspectives. I highly recommend Todd’s material.

- ***Risk Intelligence: Dylan Evans***

- ✦ A must-read for Reliability Team members. The best description yet on Risk Intelligence and Risk Tolerance and why our ability to See and Understand risk is so diverse. It gives us crucial insight into why we see risk that others don’t. This is required reading if you want to really understand how to understand risk in a high reliability sense.

- ***Mistreated – Why we Think We’re Getting Good Healthcare: Pearl, Robert MD***

- ✦ Robert does an excellent job of outlining the systemic failures of the healthcare system.

- ***Being Wrong: Adventures on the Margin of Error: Kathryn Schulz***

- ✦ A very good book to read if you’d like to understand the cognitive dissonance that comes with being wrong. Those who interview people in risk analysis or investigative situations should read this book.

- ***Understanding Patient Safety, Second Edition: Wachter, Robert***

- ✦ Dr. Wachter is on-target with many suggestions (and stories) on how we can make our healthcare safer. Many are structural things that you will see in your own facility if you work in any aspect of healthcare (although if you’re not in healthcare, you’ll probably never go to the hospital again after reading this book).

- ***Beyond the Checklist – What Healthcare Can Learn from Aviation: Gordon, Mendenhall***

- ✦ A good book on checklist development, but more important, on the WHY behind good checklists.

- ***Command and Control: Eric Schlosser***

- ✦ A frightening, cannot-put-it-down book about multiple failures in the so-called high-reliability world of nuclear weapons and the military. It’s a real story, though you’ll wish it weren’t.

- ***The Digital Doctor: Wachter, Robert***

- ✦ A journey through the positives and negatives of a digital medical world.

- ***Resilience Engineering: Hollnagel, Erik; Woods, David***

- ✦ Another book if you’re becoming an expert on resilience. This is a good study on how best to design around human factors and expected human behaviors to make a system more resilient.

- ***Safety Differently: Dekker, S.***





- ✦ A good Safety II book by one of the early Just Culture theory practitioners.
- ***Mistakes Were Made, But Not by Me: Tavris***
 - ✦ The sentinel book on cognitive dissonance. It's short, but a tough read given all the dissonance, crime examples, etc.
- ***The Creative Destruction of Medicine: Topol, Eric***
 - ✦ For when you have the time, an interesting read on what could be done to change healthcare in order to make it safer and more efficient. Some excellent ideas (and some far-fetched ones, politically), but worth the time if you are reaching for something to stimulate thought.
- ***Influence: Robert Cialdini***
 - ✦ Read this book before you buy your next car, or go for your next promotion. Cialdini has likely done more research on influence, and how we influence each other (often unknowingly), than anyone else. This is a mandatory read for professional leaders.
- ***Social Intelligence: Goleman***
 - ✦ Want to better understand the person who has technical expertise but maybe some toxic personal tendencies? Is this you? Read this book for some ideas on how to become more socially intelligent.
- ***Sensemaking in Organizations (Volume 1 and Volume 2): Weick***
 - ✦ Weick was an original thinker in the High Reliability space. This is an early book on High Reliability and how people and organizations make sense of risk, accidents, production values, and other things that drive risk.

CRM, TEM, SMS, Situational Awareness

- ***The Culture Code: Secrets of Highly Successful Groups: Coyle, Daniel***
 - ✦ A good read on successful team building. But you first need some leadership skills.
- ***Safety Management Systems in Aviation: Halford, Carl; Goglia, John***
 - ✦ More of a textbook than anything, but if you need to understand or implement a Safety Management System, this will give you all the information you need.
- ***Managing the Unexpected-Sustained Performance in a Complex World: Karl Weick***
 - ✦ Another early High Reliability book by Weick, he discusses the ways organizations can manage unexpected outcomes, using very good examples.
- ***Crew Resource Management - Principles and Practice: LeSage, Dyer, Evans***
 - ✦ Using stories at the beginning of every chapter, this textbook was designed to introduce the





reader to the values of CRM, and the many problems commonly encountered in trying to change a culture and/or attitudes. Aimed mainly at firefighters, paramedics, and air medical, but anyone can learn from the examples.

- ***Safety at the Sharp End: Rhona Flin, Paul O'Connor, Margaret Crichton***
 - ✦ A solid book on Safety II principles, and what safety really means at the front line rather than in the board room. A must-read for risk managers and safety managers.
- ***Situational Awareness: Paul Kraig***
 - ✦ Straightforward, textbook-type and short, covers principles of situational awareness in aviation. A bit overly simplistic if you're an expert in human factors, but a good read if you're just learning the concepts.
- ***Beyond Aviation Human Factors: Maurino, Reason, Lee***

Incident Investigation, Information Analysis, Safety Strategy Discussions

- ***Weapons of Math Destruction – How we Misuse and Misinterpret Data: O'Neill, Cathy***
 - ✦ A great book on how data is usually manipulated with the end in mind, and how to carefully and expertly deduce what might be behind the math. If you analyze data in the risk, quality, or safety realm, you need to read this book (or chance making many of the same errors).
- ***Root Cause Analysis: Improving Performance for Bottom-Line Results, FIFTH EDITION: Latino, Mark***
 - ✦ As you know, we don't do Root Cause because so much of it is based on the highly flawed "5-why's" model. However, this book introduces a more modern approach that is worth reading about, and if you have already read about Safety II, you'll see some proactive ideas.
- ***Trapping Safety into Rules – How Desirable or Avoidable is Proceduralization: Bieder, Corinne, Bourrier, Mathilde***
 - ✦ While this starts out like a textbook, and it's a hard book to find, it is an amazing view of how strict adherence and reliance on policy and procedure is in itself a huge risk. I encourage everyone who wants some expertise around reliability and systems to read this, and I believe it should be *mandatory* reading for *anyone who writes rules*.
- ***Left of Bang: How the Marine Corps Combat Hunter Program Can Save Your Life: VanHorne***
 - ✦ Great discussion on how and why to invest in proactive management and preparation rather than a singular focus on responding to crisis.
- ***Breakthroughs in Decision Science and Risk Analysis: Louis Anthony Cox***
 - ✦ A more scientific read (have coffee), but a valuable resource on decision-making and risk.
- ***The Field Guide to Understanding Human Error, 3rd Edition: Dekker, Sidney***





- ✦ An interesting book from Sidney, who was an early adopter of the Just Culture concepts.
- ***Principles of Risk Analysis: Decision Making Under Uncertainty: Yoe, Charles***
 - ✦ More recent studies and discussion on Hollnagel and Kahneman and Tversky's early work.
- ***STPRA and Complex Socio-Technical Modeling: Australian DOD: Qureshi, Zahid***
 - ✦ Another explanation of STPRA, using language that most of us can understand. Find this online.
- ***Measure What Matters: Doerr, John***
 - ✦ If your company considers OKR's a key part of their operation, you need to read this book.

For additional resources please contact:

Paul LeSage: Paul@sgcpartners.com

K. Scott Griffith: Scott@sgcpartners.com

or info@sgcpartners.com

Notes



