Session No. 687

Top 10 Reasons Organizations Don't Perform Good Risk Assessments

Bruce Hollcroft, CSP, ARM, CHMM
Hays Companies
Portland, Oregon

Bruce Lyon, CSP, P.E., ARM, CHMM
Hays Companies
Kansas City, Missouri

Introduction

Organizations face a range of risks every day that can impact their ability to reach certain business objectives. Risk assessment is an important and sophisticated tool used to assess an organization's risks so that the organization can mitigate and manage risks to an acceptable level.

This paper will describe the top 10 reasons organizations *fail* to identify their most significant hazards and greatest risks, and perform good risk assessments. The overall objective of this paper is to describe how to improve risk assessment methods based on *ANSI/ASSE Z590.3-2011; Prevention through Design* and *ANSI/ASSE Z690.3-2011; Risk Assessment Techniques* standards, and nearly 60 years of combined experience of the two presenters.

The top 10 reasons organizations fail to perform good risk assessments are discussed below

Number 10: Failure to P:erform a Risk Assessment

In many cases, risk assessments are simply not performed by an organization. There are many reasons organizations do not perform risk assessments (RA). Some of these reasons may include:

- A belief that the organization has adequately assessed risk by informal means.
- A reliance on insurance alone to manage risks.
    - It's been the authors' experience that there are organizations that leave the risk assessment process to their insurance provider's risk control service to identify hazards and make recommendations for improvement rather than perform internal risk assessments.
- A misconception that simple hazard identification and correction methods are adequate.
- A lack of knowledge, and/or resources to perform a risk assessment internally.

In the U.S., many organizations rely on checklist inspection methods that focus on regulatory compliance and prescribed hazards and conditions to evaluate workplace safety and health. Unfortunately, these 'inspection' type methods do not provide a real measure of risk.

In a webinar hosted by ASSE, "Prevention through Design: Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes," November 30, 2011, one of the webinar facilitators, Bruce Main, quoted a study conducted by Owens Corning indicating that 65% of serious incidents had no previous risk assessment.

British Petroleum's internal investigation team of the Deepwater Horizon accident (i.e., "Deepwater Horizon Accident Investigation Report," September 8, 2010, page 36) concluded that one of the eight key causes to the accident was that no risk assessment was performed of the cement slurry barrier application. The report stated, "The investigation team has not seen evidence of a documented risk assessment regarding annulus barriers." The accuracy of cement slurry barriers was described as "critical" in the report, yet no formal risk assessment was performed.

An organization should have a strategy for determining where, when, and how risks need to be assessed as outlined in ANSI Z690.3, Risk Assessment Techniques (p.12). Some basic criteria for establishing the need for risk assessment includes:

- existing or new project/tasks that have not had a formal risk management process to identify the principle risk management issues;
- when there are a number of risks present or introduced that make it necessary to apply risk priorities in an organized way;
- when there is a risk that could have serious consequences, and where control measures are unclear; and
- where there is a planned change to equipment, machinery or a particular process (as outlined in ANSI Z10, 5.1.2, Design Review and Management of Change.)

Lack of proper risk assessment can lead to the most catastrophic results and is the Number 10 reason organizations do not perform good risk assessments.

Number 9: Failure to Define the Context and Objectives of the Assessment

Without a guidance system, the risk assessment may wander aimlessly and far from its intended purpose. A good risk assessment starts with establishing the objectives and context by defining basic parameters, scope, and criteria.

The purpose and scope of a risk assessment should be determined by those who are going to use the resulting information to make informed decisions. The purpose should be stated as concisely as possible with care given to avoiding complex statements. The purpose should then be written so everyone on the team can continuously refer to it in order to stay focused and avoid wandering too far from the intended goal. The following might be an example of a good purpose statement, but even in this statement words like "emergencies/disasters" and "impact" many still need to be more precisely defined.

"The purpose of this risk assessment is to determine the potential emergencies/disasters that could have the most impact on the organization."

Communicating the purpose and scope to the risk assessment team should include a common understanding of the terminology to be used. For example, when using qualitative risk analysis, a clear explanation of the terms used and their meaning should be defined, communicated and understood by the assessment team and management (ANSI Z690.3, p. 18).

Determining the scope of a risk assessment can be even more complicated than the purpose, but it is just as important to the success of the risk assessment. Every successful risk assessment needs a tightly defined beginning and end so the team is not tempted to take it further than it is intended to go or make it too complicated. For example, the risk assessment of potential emergencies/disasters might need some limitations. Should the risk assessment be limited to emergencies/disasters at facility sites or include events offsite? Should it include natural, man-made, or technological emergencies/disasters, or all of them? Setting the scope too narrow might prevent a hazard and the resulting risk from being identified and assessed, or setting it too broad could prevent the risk assessment from getting to the real purpose. Again, it is important to get input from those who will be using the risk assessment to make decisions.

Number 8: Failure to Understand Organization's Acceptable Risk Level

Organizations need to define tolerance levels for risk and incorporate into the risk assessment process. Otherwise, "paralysis by analysis" will take effect, wasting time and resources on acceptable risks, and possibly stall or short-circuit the process.

In Fred Manuele's article "Acceptable Risk; Time for SH&E professionals to adopt the concept" published in *Professional Safety*, May 2010, he suggests that safety professional have not yet fully embraced the concept of acceptable risk. It is the authors' experience that some organizations promote "Zero Risk/Zero Accidents" as their primary safety and health goal. The fact is that there will always be some residual risk. Organizations with such goals should take heed. As described in ANSI Z10, Appendix F, safety and health management goals should be specific, measurable, actionable, realistic and time-oriented (or SMART). A goal of "Zero Risk" is not realistic, and should be redefined to an achievable and acceptable level for the organization.

What is an achievable and acceptable level of risk? ANSI Z690.3 explains that the potential for harm must be reduced until the cost of further reduction is disproportionate to the benefit gained; to the level of "as low as reasonably practicable" (ALARP). Prior to risk assessment, an organization should clearly establish its own acceptable risk or ALARP level. The criteria used to determine ALARP should include cost/benefit analyses of risk and their treatment, and include a stratification of risk levels. (ANSI Z690, p. 21)

Number 7: Failure to Assemble the Best Team to Perform the Risk Assessment

Depending on the scope of the assessment, a team of objective, knowledgeable, experienced and complementary personnel should be composed. Unfortunately, some risk assessments are performed with a less than objective viewpoint, and a single perspective.

Sometimes risk assessments are performed just to get them documented in order to meet some internal or external requirement. These are often performed by limited teams and may be led by a dominant individual who is primarily focused on getting it done. Experience has shown that this leads to incomplete risk assessments, where some of the hazards are not identified and risks are not fully assessed.

Teams of three to 10 competent members seem to work well. Teams in this size range usually offer enough perspectives on a risk assessment, but are not too big to manage and keep focused. The team members should be selected based on their knowledge, experience, and commitment to the effort, and will vary depending on the hazards and risks being assessed. A good risk assessment of a product might include representatives from research and development, design, engineering, production, quality, legal, sales, service, risk management and safety. A transportation risk assessment might include a driver, routing/scheduling, DOT compliance, service and maintenance, risk management and safety. It can be a good idea for these team members to go back to their departments and solicit input if the process is not confidential; external parties can often make significant contributions to the risk assessment.

Risk assessments are excellent opportunities for employee involvement, which is key to the success of any safety effort. Employee involvement is required by all health and safety management system standards, such as ANSI Z10, OSHAS 18001, and OSHA VPP. It is also a requirement by some state OSHA regulations and specific regulations such as process safety management (PSM). Most importantly, employee involvement leads to a better risk assessment.

Number 6:Failure to Use the Best Risk Assessment Technique(s)

Properly matching the right technique to the exposure is vital in achieving the results desired. Many types of risk assessments are not well understood, or used. Experience is important in proper selection and application. In some cases, it may be necessary to use more than one method.

There are many different types of risk assessment techniques, some complex (quantitative) and specific, and others more basic (qualitative) and broad in their application. ANSI Z690.3 describes 31 different techniques (p. 22-25), while ANSI Z590.3 features eight. Three risk assessment techniques are highlighted in ANSI Z590.3 as being more practical for most risk situations: preliminary hazard analysis and risk assessment; the what-if/checklist analysis methods; and failure mode and effects analysis (FMEA). Some techniques have specific applications. For instance, hazard analysis and critical control points (HACCP) is often used in food and beverage processing.

The technique selected should be justifiable and appropriate for the situation, provide useful results, and be traceable, verifiable and consistent. Selection criteria should be based on the "defined context and objectives of the assessment" (Reason Number 9) and would take into consideration:

- type and range of risks
- potential magnitude
- degree of experience
- available data
- regulatory

It may be necessary to use more than one assessment tool in some cases. For example, brainstorming techniques to develop a list of concerns and qualified risks, followed by a breakdown of each concern, using a cause-and-effect analysis or fishbone diagram.

The assessment and its output should be consistent with the risk criteria established in the scope and purpose of the assessment. Annex A of ANSI Z690.3 provides an extensive "Comparison of Risk Assessment Techniques," which lists each techniques application, and attributes to help make the proper selection.

Number 5: Failure to be Objective and Unemotional in the Risk Assessment Process

An objective, experienced facilitator can help the risk assessment stay focused on the purpose and goals, and remain objective. Sometimes the members of the risk assessment team can be too close to the situation or a past experience to be objective. A reality check from an experienced facilitator can help maintain the objectivity of the risk assessment process.

If members of a risk assessment team have a memorable experience that is fresh in their minds, the real potential frequency and severity can be greatly exaggerated in their opinions. Experiences such as reading a dramatic article, hearing a dynamic speaker or a seeing a recent news feature can also skew the members' perception. In addition, everyone has their own issues that they tend to over-value. This can interfere with the process, especially if it comes from a member with a strong personality.

The effects of a less than objective team member can be moderated by a good, well-rounded risk assessment team, or an experienced facilitator. The right comparisons can be made, and questions can be asked to bring the perception back into line with reality. This must be done with much care and consideration as to not discredit or alienate the member with a strong position on an issue.

Number 4: Failure to Identify hazards that Create Risks and See Combined Whole-System Risk

If a hazard is not recognized or simply missed, the resulting risk is not assessed. Reasons assessors fail to identify specific hazards are many. An individual's experience and background will influence the direction and focus of the risk assessment. If the organization does not use a diverse team to capture a broader spectrum of risks (Reason Number 7), the assessment is left to the individual risk assessor's comfort level with certain types of exposures (i.e., machine guarding, electrical, ergonomics, industrial hygiene, and so on), limiting the results. Depending on the complexity of the situation, this can create a false sense of risk management, with critical risks remaining unidentified and untreated.

Equally important is the potential effect of combined risks being missed. Risk assessors that identify, and catalog individual hazards as line items in their assessments, may miss the potential for certain risks occurring together, creating synergistic effects. For instance, certain combinations create greater risk, such as cold temperatures and vibration causing soft tissue damage (ANSI Z590.3 7.4.5). Whole-system risk must be considered, not just individually, to properly manage risk.

Number 3: Failure to Consider the Hierarchies of Control and Prioritize Based on Risk

Personal protective equipment (PPE) and administrative measures should not be the default choice. Although they may be the easiest to implement, they are the least effect and reliable. Failure to apply the hierarchy of controls properly will often result in a failure to control the risk as low as reasonably practicable (ALARP). Organizations should have a strategy for prioritizing control measures based on risk level and degree of exposure to optimize efforts and resources.

The Prevention through Design (PtD) standard, Z590.3 addresses the hierarchy of controls and selecting and implementing the risk reduction and control methods. The risk assessment standard, Z690.3 also covers controls assessment. Both require consideration of the hierarchy of controls on initial risk assessment and subsequent risk assessment after the implementation of controls. The hierarchy of controls, in order from most effective to least effective, are:

1. Elimination
2. Substitution
3. Engineering Controls
4. Warnings
5. Administrative Controls
6. Personal Protective Equipment (PPE)

Applying the hierarchy of controls properly should become second nature for every safety professional and standard practice for organizations. It serves to assess risk more accurately and continuously improves controls.

Number 2: Failure to Perform Risk Assessment during the Design/Redesign Phase

The *ANSI/ASSE Z590.3-2011; Prevention through Design* (PtD) standard emphasizes the importance of using risk assessment during this crucial stage. As obvious as this seems, it is still rare for organizations to perform a thorough risk assessment during design and redesign phases.

The National Institute of Occupational Safety and Health (NIOSH) Prevention through Design (PtD) initiative states on its website: “One of the key elements of this standard is that it provides guidance for ‘life-cycle’ assessments and a design model that balances environmental and occupational safety and health goals over the life span of a facility, process or product. The standard focuses on the four key stages of occupational risk management. The pre-operational, operational, post incident and post-operational stages are all addressed within,” The fact that operations, equipment, and products have a ‘life-cycle,’ and that risk may change during various stages of the cycle, should be considered in the risk assessment.

Unfortunately, many organizations do not even think about assessing risk during design and redesign stages, resulting in a lost opportunity for significant cost savings and risk mitigation. Instead, they wait to address risks after final completion or installation and, many times, not until an incident or significant loss occurs.

Risk assessment at the design/redesign phase may be the most overlooked risk management tool available to organizations. Organizations should make risk assessments a standard practice during the design and redesign phase.

Number 1: Failure to Communicate Before, During and After the Risk Assessment

Successful risk assessment is dependent on effective communication with stakeholders before, during, and after the process. Anything less will result in a less effective risk assessment outcome. A good risk assessment will involve stakeholders throughout the process and seek their input. Stakeholders will include internal personnel, but may also include customers, investors, partners, suppliers and vendors.

NASA’s Space Shuttle Columbia explosion on February 1, 2003, which claimed seven lives, was determined by the investigation board to be partially due a lack of effective communication of critical safety information. The synopsis of the Report of the Columbia Accident Investigation Board concluded that organizational causes including lack of communication contributed to the incident.

> Cultural traits and organizational practices detrimental to safety were allowed to develop, including: reliance on past success as a substitute for sound engineering practices..., organizational barriers that prevented effective communication of critical safety information and stifled professional differences of opinion; lack of integrated management across program elements; and the evolution of an informal chain of command and decision-making processes that operated outside the organization’s rules. (p. 9)

Communication is a provision of both ANSI Z690.3 and ANSI Z590.3. Communication is also required by virtually all of the national and international health and safety management standards, such as ANSI Z10, OHSAS 18001 and OSHA VPP, but it is seldom done well. As a result, poor communication is often identified as a major contributor to poor outcomes such as accidents.

As with many other functions within organizations, people should make it a priority to communicate effectively when performing risk assessments. Those involved in the risk assessments should think about who could help them do the risk assessment more effectively. For example, they could ask others within their own departments for input. Alternatively, they should think about who might be interested and benefit from the risk assessment that is being performed and let them know the outcome.

Summary

Safety professionals should have a firm understanding of the risk assessment methodology and techniques described in ANSI/ASSE Z590.3 and ANSI/ASSE Z690.3, and avoid these common “Top 10” failures. Well-executed risk assessments enable organizations to make the right decisions, protect their assets, and properly manage their risks as they operate, grow and improve their businesses.