COSTS & BENEFITS OF MANAGING RISK

Taking a Risk-Informed, Performance-Based Approach

By Bruce K. Lyon, N. Prasad Kadambi and Georgi Popov

RISK IS FOUND in all aspects of life. For OSH professionals, risks from workplace hazards are the primary focus. Since the emergence of the OSH Act of 1970, safety practitioners in the U.S. have been educated and trained, rightfully, to identify and correct workplace hazards and manage regulatory compliance.

However, for organizations to be successful and achieve their objectives, they must manage all risks encountered—hazard risks, operational risks, financial risks and strategic risks—while they pursue potential opportunities. OSH professionals require a wider lens that looks beyond just hazard risks and sees the aggregated risks and how they can impact the organization as well as society. Equally important is for OSH professionals to understand the need for organizations to pursue potential opportunities. This requires recognition that some risk usually accompanies any such pursuit. For an organization to successfully achieve its objectives, calculated risk must sometimes be taken. Being too risk averse can be a risk if it causes an organization to miss opportunities that would allow it to successfully compete, innovate and benefit society. Taking some risk is often necessary to achieve objectives, advance technologies and navigate through the increasingly complex world.

ANSI/ASSP/ISO 31000-2018 defines risk as the "effect of uncertainty on objectives" (p. 1). Risk's effect of uncertainty, however, has different risk sources. The American Institute for Chartered Property Casualty Underwriters, known as The Institutes, defines and categorizes these risk sources in four groups or risk quadrants (Elliott, 2017). The risk quadrants are 1. operational risk; 2. hazard risk; 3. financial risk; and 4. strategic risk.

Operational risks and hazard risks are considered pure or absolute risks, which are those that can only result in loss or negative outcomes. Financial and strategic risks represent speculative risks, which have the possibility of a positive outcome, negative outcome or both (Lyon & Popov, 2021). Figure 1 (p. 30) represents the four quadrants of risk.

For most OSH professionals, the primary focus is hazard risk. However, hazard risks do not operate in a vacuum, nor are they confined to one quadrant of risk. Hazard risks often cascade into other parts of the organization, impacting its operations, financial strength and sometimes its reputational and strategic capabilities. For example, suppose a refrigerated food storage warehouse using ammonia as a refrigerant has an ammonia release, which causes an operational risk with the

KEY TAKEAWAYS

- **In the world of enterprise risk management, are OSH professionals too narrowly focused on just the hazard risk? For an organization to successfully achieve its objectives, some level of risk in pursuit of opportunities must be taken. Being too risk averse can cause an organization to miss opportunities that would allow it to successfully compete and innovate.**
- **When accepting a level of risk to achieve an objective, the desired performance must be factored in. Defining needed performance objectives and ensuring their accomplishment as part of the decision-making process must come together in such a way that public and worker safety are always a paramount consideration.**
- **For organizations to succeed, an optimal balance between risk and opportunity is required. Achieving a risk level considered as low as reasonably practicable along with expected performance capabilities and benefits of the opportunity can be considered the art of managing risk to an acceptable level.**
- **To help organizations achieve and maintain an optimal opportunity or risk balance, OSH professionals can consider applying the principles from the risk-informed and performance-based model formulated by the U.S. Nuclear Regulatory Commission.**

SYOLACAN/E+/GETTY IMAGES

loss of refrigerant and food products. The operational risk leads to a hazard risk to workers and the local community from the toxic nature of ammonia gas. If not contained, the hazard risk cascades and escalates into a strategic risk (loss of reputation and image) and financial risk (legal and regulatory losses), as illustrated in Figure 2.

Enterprise risk management (ERM) is the concept of managing all aspects of risk—operational risks, hazard risks, financial risks and strategic risks—and considering the potential interconnectivities they bring and the overall aggregation of risk. The Risk and Insurance Management Society (RIMS, 2022) defines ERM as "a strategic business discipline that supports the achievement of an organization's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an interrelated risk portfolio." To successfully understand and manage aggregated risk, the organization must approach risk management as a fully integrated process rather than segmented into silos.

Current Challenges in Risk Oversight

As part of the International Organization for Standardization (ISO) Technical Committee (TC) 262 for risk management standards, the authors participated in an ISO task group established by TC 262 to identify the concerns and challenges facing organizations regarding ERM in preparation for the next revision of ISO 31000, Risk Management. The effort involved an in-depth review of 12 major surveys, conducted between 2019 and 2021, concerning ERM and risk oversight from affected stakeholders. Table 1 (p. 32) outlines details about the surveys.

The conclusions drawn by the ISO task group from its review of these 12 surveys indicate that:

1. ERM is typically more developed or mature in large global organizations. Significant opportunities exist for improvement in ERM and risk oversight in many small- to medium-sized organizations.

2. Many organizations still operate departmentally (i.e., in silos) and have not fully integrated risk management into their operational and strategic planning. For many organizations, their dedicated resources—whether human, technological or financial—may not be sufficient for effectively managing enterprise risk.

3. Challenges in managing risks result from interdependencies, growing complexity and rapidly changing conditions in the world. Growing complexities and changes include technology and cyber threats; environmental, social and governance concerns; and interdependencies and supply-chain risk.

4. Survey findings indicate a need for better, more effective communication of aggregated risk (combined or synergist effects) within organizations. Many organizations still use spreadsheets listing individual risks to manage and communicate risk and do not account for aggregated risks.

5. Better or increased board oversight in risk management and strategic planning are needed, especially at the board level. There are concerns that boards are not always receiving the risk-based information necessary to adequately oversee risk. Findings also indicate that boards spend little time discussing reported risk when they discuss the strategic plan. This finding indicates a need for more direct accountability of senior management for risk oversight.

6. As a result of the findings, there is an overall need for more structured risk-informed decision-making and including risk-informed and performance-based practices within organizations and their management systems.

The authors' key takeaway from these findings is that there appears to be a need for a more risk-informed, performance-based approach to decision-making and managing risk.

Risk, Opportunity, Performance & Uncertainty

Since risk, opportunity, performance and uncertainty are interrelated and often intertwined, a clear understanding of these terms and their relationships is needed in the decision-making process.

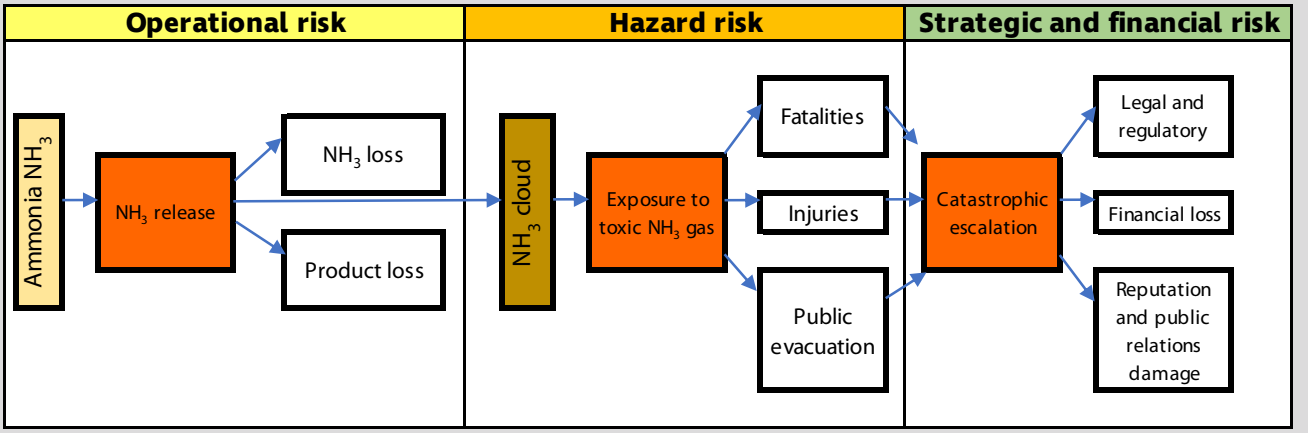
First, risk and opportunity must be recognized as being mirror opposites or two sides of the same coin. While there are many varying definitions found in standards and applications, risk is simply the chance for something bad to happen or the "potential for adverse outcomes" (Lyon & Popov, 2022, p. 19). Organizations and people do not necessarily want more risk, however, some risk must be taken to pursue an opportunity, meet a performance goal or achieve an objective. Conversely, opportunities can be defined as the potential for favorable outcomes. They offer the chance for desired achievements, gains or other benefits. In addition, just as risks are associated with taking an opportunity, risks also exist from missing an opportunity. The art of achieving an optimal balance requires decision makers to be well-informed of both the risks and opportunities involved.

While risks present the potential for adverse outcomes, so do the failures to accomplish specific performance objectives. Performance is a modulating factor requiring levels of performance of specific activities to accomplish defined objectives. Performance can be described as an expression or measure of how well a particular subject is doing compared to established criteria. For instance, success in a particular area may be represented by performance measures focused on the completion of specific tasks and their efficiency level, timeliness factors, costs factors or other measures. These may be considered as outputs of the activity in that area. However, from an enterprise perspective, it may be important to differentiate such outputs from the outcomes that matter to the whole organization. The economic health of the organization may depend on defining such performance criteria up front during the decision-making process, along with methods for measuring and monitoring such performance. This approach of differentiating between the output in one area from the impact that it has in the broader picture, which is the outcome, avoids suboptimization. Suboptimization can occur if management mistakenly thinks that success in one area represents the whole picture.

FIGURE 1
QUADRANTS OF RISK

Uncertainty, strongly linked to probability or likelihood, can be described as the "lack of knowing outcomes" (Lyon & Popov, 2022, p. 20). There are four types of uncertainty: 1. epistemic uncertainty, or a condition where there is a lack of relevant knowledge of the system; 2. aleatoric uncertainty, or a condition where a random, unpredictable nature exists surrounding the system; 3. linguistic uncertainty, or a vagueness or ambiguity

FIGURE 2
EXAMPLE OF CASCADING RISK



inherent in spoken languages; and 4. decision uncertainty, or uncertainty associated with value systems, professional judgment, company values and societal norms (ANSI/ASSP/ISO, 2019; Lyon, 2022). ISO Guide 73, Vocabulary for Risk Management, defines uncertainty as the "state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence or likelihood" (ANSI/ASSP, 2011). This definition assumes that correction of the deficiency of information will reduce or eliminate the uncertainty. However, for aleatory type uncertainties that are unpredictable or random in nature that cannot be reduced with additional information, a risk-informed and performance-based approach can add value (U.S. NRC, 2012).

When considering whether a particular risk is acceptable to the organization, the as low as reasonably practicable (ALARP) concept should be considered. The ANSI/ASSP Z590.3-2021 prevention through design standard defines ALARP as "that level of risk which can be further lowered only by an increase in resource expenditure that is disproportionate in relation to the resulting decrease in risk" (p. 12). The balance between the opportunity and the risk as well as the level of uncertainty should be considered when making decisions (Figure 3, p. 32); this can be described as the benefit or cost factor.

While risks present the potential for adverse outcomes, so do the failures to accomplish specific performance objectives.

Management Systems & Risk Metrics

The risk management principles, framework and process described in ANSI/ASSP/ISO 31000-2018 (Figure 4, p. 33) are designed to provide an organization an iterative and integrated approach to managing risk effectively within its management system. This integrated approach enables decision makers to make more risk-informed decisions and reduce or manage risk while achieving their objectives.

While ANSI/ASSP/ISO 31000 is not a management systems standard, it is designed to be integrated into an organization's management systems. One of the standard's guiding principles is continual improvement, which is achieved through a plan-do-check-act model (Figure 5, p. 34).

Performance evaluation, or the check component, is essential in the plan-do-check-act management system model. Consideration of risks and opportunities, as well as information on the performance and trends in monitoring and measurement results, are the inputs for management to make informed decisions as part of the continual improvement process (ASSP, 2020).

Key Performance Indicators

Key performance indicators (KPIs) are a set of specific, quantifiable measures that an organization tracks to gauge performance over time. To be effective, KPIs must be tied to the related objectives in the risk management process. They should be used to determine progress in achieving strategic and operational goals, and to benchmark an organization's position or performance in comparison to baselines, internally or externally. The measurement of performance allows an organization to estimate its performance in comparison to its expected performance in support of the organization's strategic objectives (ASSP, 2020). When selecting KPIs, an understanding of the organization's mission, goals and objectives, as well as what is currently measured related to achieving its related objectives, are needed. KPIs will vary by organization as well as department or business unit. For each selected KPI, the desired target and the baseline should be established. Performance measures can be input-based or leading indicators, while others may be outcome-based or lagging indicators. A combination of indicator types is often needed and may include those identified by ASSP TR-31010-2020, which include:

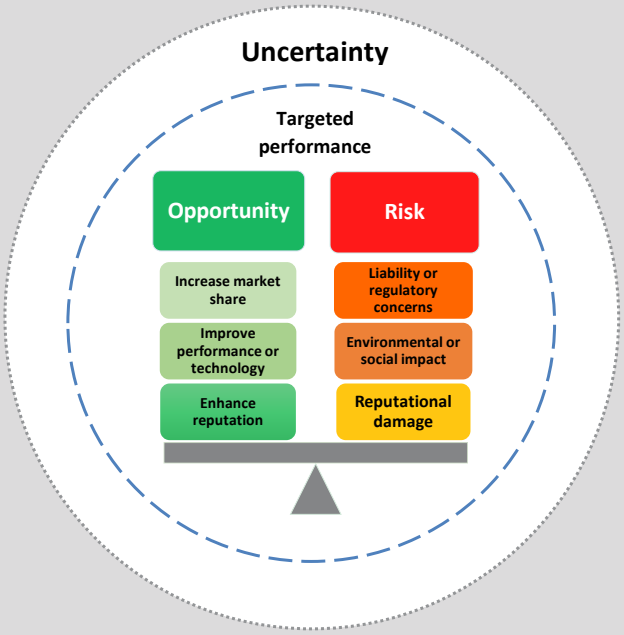
- Qualitative or subjective measures, signal words and descriptions.
- Quantitative or objective measures such as percentages, numbers and ratios. Often qualitative and quantitative indicators are used together to provide a more holistic picture of performance.
- Input-based or action measures that are designed to achieve a desired outcome, sometimes called leading indicators. Input-based measures are activity-oriented measures that signal a

TABLE 1
ISO TC 262 SURVEY RESULTS

Survey	Source	Sample	Year
2020 Study of Advancements in Enterprise Risk and Governance	Columbia University School of Professional Studies	150 global practices leaders	2020
2020 The State of Risk Oversight	North Carolina State University	450 CFOs	2021
The State of ERM in Canada	Conference Board of Canada, Global Risk Institute, CPA Canada	160 Canadian organizations	2019
EY Four Ways to Advance Risk Oversight	Ernst & Young Global Ltd.	500 global CEOs and board members	2019
PwC Risk Management Leaders Insights	PricewaterhouseCoopers	106 risk managers	2021
PwC 24th Global CEO Survey	PricewaterhouseCoopers	5,050 global CEOs	2021
WEF 16th Global Risks Report	World Economic Forum	Global stakeholders	2021
Airmic Top Risks and Trends 2020	Airmic Corp.	U.S. stakeholders	2020
Deloitte 12th Global Risk Survey	Deloitte	57 global financial institutions	2020
Evolving Practices in Enterprise Risk Management Survey Summary Report	American Productivity and Quality Center	229 U.S. organizations	2021
RIMS 2020 Enterprise Risk Management Benchmark Survey	Risk and Insurance Management Society	300 global organizations	2020
Federal Enterprise Risk Management 2020 Survey Results	Association for Federal Enterprise Risk Management	37 federal organizations	2020

FIGURE 3
BALANCING OPPORTUNITY & RISK

Balance between opportunity and risk to achieve performance in uncertain conditions.



change in performance. Input-based measures indicate changes in improvement in the process and detect changes that require adjustment. Input- or action-based KPIs might include quarterly evaluation of the assessment process, number of process improvements completed per month, or number of emerging risks identified prior to any incidents in a year.

•Process measures used in measuring and evaluating process efficiency or productivity.

•Output-based metrics or result measures that are produced from the inputs or actions taken in terms of numbers and percentages. Examples of output-based metrics might include the number of new engineering controls implemented because of risk assessments, the conformance rate of control implementations, and the percentage of employees trained as risk assessors because of a risk assessment training initiative.

•Outcome-based or result measures that produce numbers indicating the level of success, sometimes referred to as lagging indicators. Outcome-based measures are used to analyze events, successes or failures, and results or trends to determine whether the process is effective and working. Examples of result-type KPIs include the number of close-call incidents per quarter, number of corrective actions successfully completed, average number of days to complete corrective action and incident rate numbers.

For KPIs to provide value, they must be tied to a specific business objective and measurable. While KPIs should be standardized, they should have some flexibility or ability to adjust with changes.

Key Risk Indicators

In addition to KPIs that focus on performance measures, a need for indicators of risk also exists. Key risk indicators (KRIs) are measures that provide detection and identification of emerging or developing risks and are used to determine when such risks require assessment. In a way, KRIs provide an early warning of new risks that have reached a level of concern. As noted in ASSP TR 31010-2020, KRIs are used in developing strategies for the identification, assessment and management of new risks such as root-cause analyses and causal-factor analyses of previous incidents.

Monitoring Risk

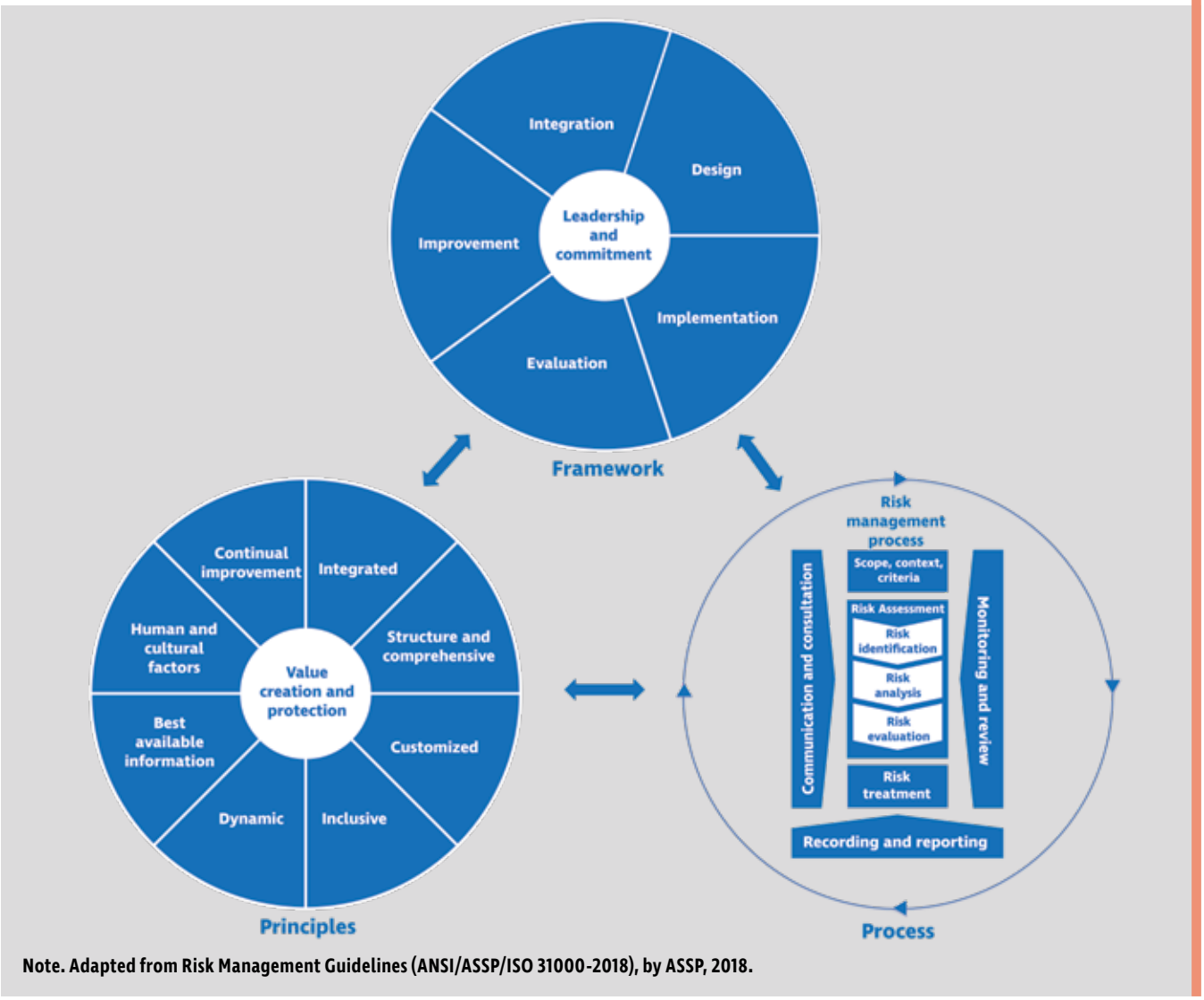
Since risk is dynamic, there is a need for ongoing monitoring of risk in an organization. Measures associated with the effects of implemented decisions or risk treatments as well as KPIs and KRIs should be monitored and evaluated to determine whether desired results are being achieved or whether adjustments are needed. If unintended effects occur, specific adjustments can then be determined and made.

Decision Models for Managing Risk

As a part of managing risk, decision makers are required to consider and evaluate alternatives in values of probabilities and consequences, variations of risk factors, options and trade-offs, and uncertainty. More information on developing and selecting decision models can be found in Section 6.2 of ANSI/ASSP/ISO 31010-2019. Decision analysis provides insight into how the defined alternatives differ from one another and provides a basis for considering new and improved alternatives (ANSI/ASIS/RIMS, 2015). Two decision-making models used in managing risk are briefly described: the U.S. Coast Guard's risk-based decision-making model and the U.S. Nuclear Regulatory Commission's (NRC) risk-informed, performance-based model.

FIGURE 4

ISO 31000 PRINCIPLES, FRAMEWORK & PROCESS



Note. Adapted from Risk Management Guidelines (ANSI/ASSP/ISO 31000-2018), by ASSP, 2018.

U.S. Coast Guard Risk-Based Decision-Making Model

One model referenced in ASSP TR 31010-2020 is the risk-based decision-making process. Developed in the late 1990s by the U.S. Coast Guard, the risk-based decision-making model can be used to organize information about possible unwanted outcomes into an orderly structure that helps facilitate decision-making and more informed management choices (Macesker et al., 2002). The model provides a systematic, structured way of making informed decisions by reducing uncertainty regarding the effects and outcomes of the selected decision. The model takes into consideration key questions about risk relating to the decision to be made including: 1. what can go wrong; 2. how severe the potential outcome is; 3. how likely it is to occur; 4. if the risk is acceptable or unacceptable; and 5. if the risk requires reduction.

In the risk-based decision-making model, the context is first determined regarding the type of decision to be made, the objective to be achieved, and the KPIs and KRIs that are tied to the objective. Once the decision and context are defined, the associated risks are assessed with the outputs used in making the decision. The final decision is then implemented and monitored for effectiveness.

Figure 6 (p. 35), adapted from ASSP TR 31010-2020, illustrates the relationship between the KPIs and KRIs and the risk-based decision-making process steps. More information on this model can be found in this article's reference list.

NRC's Risk-Informed Performance-Based Model

A second approach developed by NRC in the late 1990s is the risk-informed and performance-based (RIPB) model. While the model was developed for the nuclear energy industry, the basic principles are sound and can be applied to other applications. The RIPB model essentially is the practice of assessing the risks and the potential for benefits to achieve an optimal balance in the decision-making process to improve outcomes. Risk information gathered from risk assessments is used in allocating resources to achieve performance objectives. NRC states that the objectives of RIPB methods are to:

Enable risk insights, engineering analysis and judgment including the principle of defense-in-depth and the incorporation of safety margins and performance history to be used to:

•focus attention on the most important activities;

•establish objective criteria for evaluating performance;

•develop measurable or calculable parameters for monitoring system and licensee performance;

•provide flexibility to determine how to meet the established performance criteria in a way that will encourage and reward improved outcomes; and

•focus on the results as the primary basis for regulatory decision making. (U.S. NRC, 1999)

The terms "risk-based" and "risk-informed" appear similar, however, there are some distinctions. According to NRC, the term "risk-based" implies that decisions depend only on quantitative results and that experience shows that decision-making often requires more than just quantitative data. "Risk-informed," as described by NRC, is a more encompassing term referring to both quantitative data and qualitative information important to the decision being made. NRC describes the term "risk-informed" to mean that an organization has taken the potential for adverse outcomes into account when it undertakes activities to obtain beneficial outcomes. The term "risk-informed" generally connotes that a combination of quantitative and qualitative decision-making approaches is employed to assign resources appropriately toward the outcomes.

In terms of outcomes and performance, a hierarchical relationship exists. Outcomes that drive performance can have complex characteristics that reflect performance over a wide range. Overall performance is determined by the resulting outcomes from associated activities directed at achieving specific performance objectives. Therefore, overall performance is represented by a structure that is composed of a logical arrangement of relationships and dependencies among performance objectives (Kadambi, 2005).

The term "performance-based" is frequently equated with "outcome-oriented." The implication is that activities are undertaken by an organization to achieve performance objectives that are projected to accomplish specified beneficial outcomes. The contrast to be made is with a compliance-oriented process in which activities comply with process requirements, and it is explicitly or implicitly assumed that beneficial outcomes will follow. A problem arises if effectiveness of the process is not sought using the right parameters. Experience has shown that mere compliance with detailed process steps may not accomplish outcome objectives. It is generally more effective to have evidence of achievement of the outcome objectives as being more important than merely complying with process requirements.

The scope and application of RIPB methods should be determined on a case basis. In general, RIPB methods are resource intensive because they demand broader and deeper understanding of the organizational culture and management commitment for improved outcomes. Compliance with prescribed process requirements is generally less demanding and easier to verify. However, if the focus is on effectiveness, it becomes more important to look for congruence between the results of process compliance and outcome objectives.

The limitations of RIPB methods lie in the level of effort being commensurate with potential benefits. Careful assessment of the level of effort and the level of detail to be pursued makes achievement of success more likely.

The main benefits of RIPB methods accrue from a strategic perspective. A focus on outcomes generally leads to consistency in alignment of activities and decision-making within an organization. In addition, a risk-informed and performance-based approach helps accommodate innovation and new technology.

For the nuclear energy industry, NRC recommends that an integrated risk-informed decision-making model be incorporated into the risk management framework. The approach shown in Figure 7 consists of five principles that are executed within the framework toward an outcome considering the risks, safety and performance (ANS, 2020). The principles are:

1. Current regulations met: As a minimum, applicable regulations are met.

2. Defense-in-depth consistency: The consistent, effective use of layers of controls or defense-in-depth is a key requirement. Such a layered approach to implementing controls supports the resilience of the organization to unexpected challenges.

3. Maintenance of safety margins: Information about the most important safety margins relevant to a given decision is used.

4. Risk-informed analysis: Insights from the analysis including qualitative and quantitative information are used to set priorities and allocate resources.

5. Performance monitoring: Parameters associated with outcome and performance objectives are closely monitored.

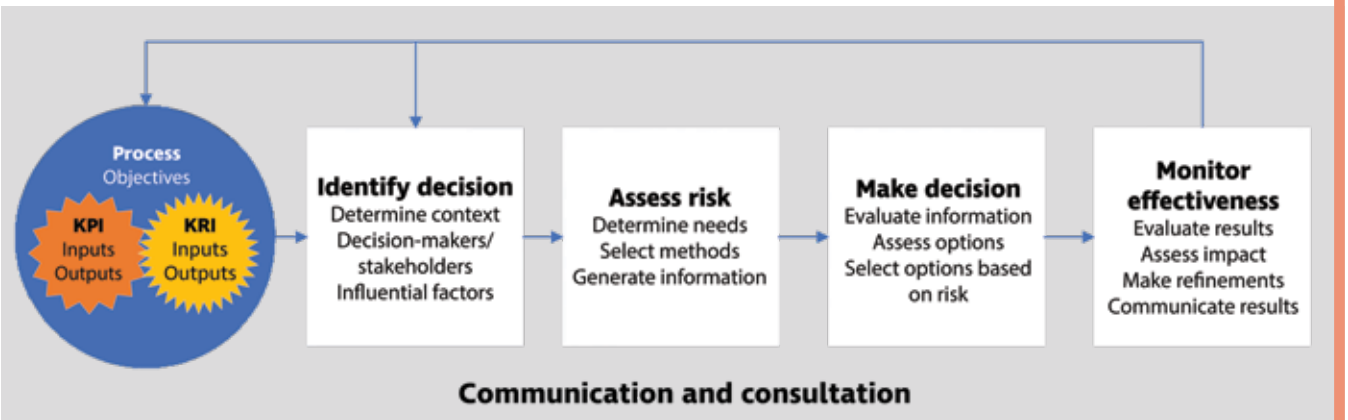
NRC has been a leader in developing the ideas central to RIPB concepts into tools and methods based on an evolution of regulatory practices away from those that were strictly compliance oriented. NRC has expressed the importance of having the licensee (entity that has been granted license to use radioactive materials) take responsibility for the safe use of potentially hazardous radioactive materials. Licensees have the primary responsibility for safety, with NRC having the role of verifying that applicable rules and regulations are followed. During the 1980s and 1990s,

FIGURE 5

PLAN-DO-CHECK-ACT MODEL

Note. Adapted from Occupational Health and Safety Management Systems: Requirements with Guidance for Use (ANSI/ASSP/ISO 45001-2018), by ASSP, 2018.

FIGURE 6
RISK-BASED DECISION-MAKING PROCESS



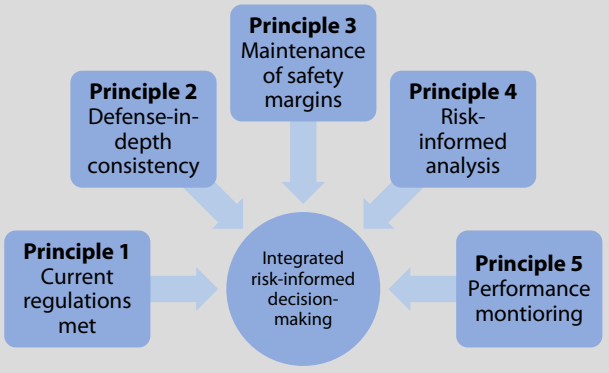
Note. Adapted from "Risk Management: Techniques for Safety Practitioners" (ASSP TR-31010-2020 Technical Report), by ASSP, 2020.

compliance orientation was seen to have become counterproductive. A realization that too much emphasis on compliance detracted from licensees taking full responsibility for safety led to the highest levels of NRC directing the staff to adopt a more performance-based approach. However, the challenge was that accountability to the public could not be decreased by licensees or the NRC. The result led to the group issuing the "White Paper on Risk-Informed and Performance-Based Regulation" (known as the RIPB white paper), providing more direction to NRC staff and regulated industry (U.S. NRC, 1999).

The RIPB white paper describes the terms and characteristics that should be observed in the outcome of the application within a wide range of contexts. As the RIPB white paper was issued by the highest-level authority in the regulatory agency, it carries the power of setting a standard demanding conformance.

As a result, NRC developed NUREG/BR-0303, Guidance for Performance-Based Regulation, based on the RIPB white paper (U.S. NRC, 2002). This document provides a structure and processes to implement performance-based safety. The methodology is general enough that it can be used by OSH professionals as another tool in the toolbox for a wide range of applications involving hazardous materials and operations.

FIGURE 7
INTEGRATED RISK-INFORMED DECISION-MAKING



Note. Adapted from "An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to Licensing Basis," by U.S. NRC, 2018.

Conclusion

Organizations must manage all risks encountered (i.e., hazard risks, operational risks, financial risks, strategic risks) while pursuing opportunities and achieving their objectives. For an organization to successfully achieve its objectives, calculated risk must sometimes be taken. To help organizations accomplish this, OSH professionals must be prepared to look beyond hazard risks and see the aggregated risks and their potential impacts. This requires recognition that some risk usually accompanies opportunities.

OSH professionals can assist organizations in establishing a more risk-informed and performance-based approach to decision-making by applying the basic principles found in the RIPB model. These include:

- defining the performance-based objectives and related KPIs and KRIs
- establishing the decision context and information needs
- assessing the aggregate risks and their potential impacts
- providing the necessary information to make the decision
- ensuring that legal and regulatory requirements are met
- implementing a layers-of-controls approach that achieves and maintains ALARP
- maintaining acceptable safety margins
- monitoring performance and adjusting as needed to meet objectives
- communicating performance and risk with affected stakeholders

For an organization to achieve its objectives, there are occasions where certain opportunities and associated risks must be considered. Being able to make such decisions in an informed way that balances the benefits (opportunities) and the costs (risks) allows an organization to be innovative, competitive and resilient. By helping organizations incorporate and integrate RIPB principles into their ERM framework and decision-making process, OSH professionals can increase their value, importance and worth. PSJ

References

American Nuclear Society (ANS). (2020). Introduction to implementation and assessment of safety for risk-informed and performance-based technical requirements in non-light water reactors (Draft report revision 1).

ANSI/ASIS International/Risk and Insurance Management Society Inc. (RIMS). (2015). Risk assessment (ANSI/ASIS/RIMS RA.1-2015). RIMS.

ANSI/ASSP. (2011). Vocabulary for risk management (National adoption of ISO Guide 73:2009; ANSI/ASSP Z690.1-2011). ASSP.

ANSI/ASSP. (2021). Prevention through design guidelines for addressing occupational hazards and risks in design and redesign processes (ANSI/ASSP Z590.3-2021). ASSP.

ANSI/ASSP/International Organization for Standardization (ISO). (2018). Risk management principles and guidelines (ANSI/ASSP/ISO 31000-2018). ASSP.

ANSI/ASSP/ISO. (2019). Risk management—Risk assessment techniques (ANSI/ASSP/ISO 31010-2019). ASSP.

American Productivity and Quality Center (APQC). (2021). Evolving practices in enterprise risk management: Survey report. https://bit.ly/3shI9Zp

ASSP. (2020). Technical report: Risk management—Techniques for safety practitioners (ASSP TR-31010-2020).

Beasley, M.S., Branson, B.C. & Hancock, B.V. (2020). *2020 the state of risk oversight: An overview of enterprise risk management practices* (11th ed.). North Carolina State University, Poole College of Management. https://bit.ly/3Fq0M2s

Bone, J. (2020). 2020 study of advancements in enterprise risk and governance. Corporate Compliance Insights. https://bit.ly/38eg4v7

Côté-Freeman, S. (2019). The state of ERM in Canada: A benchmarking study. The Conference Board of Canada, Chartered Professional Accountants of Canada and the Global Risk Institute in Financial Services. https://bit.ly/39xfqJu

Deloitte. (2020). *Global risk management survey* (12th ed.). https://bit.ly/3P7mAES

Elliott, M.W. (2017). *Risk management principles and practices* (2nd ed.). The Institutes.

Fox, C. (2021). 2020 enterprise risk management benchmark survey. RIMS. https://bit.ly/3shIcEz

Fox, C.R. & Ülkümen, G. (2011). Distinguishing two dimensions of uncertainty [Working paper]. In W. Brun, G. Keren, G. Kirkebøen & H. Montgomery, *Perspectives on Thinking, Judging and Decision-Making*, Universitetsforlaget. https://bit.ly/38uX7ol

Franco, E.G., Kuritzky, M., Lukacs, R. & Zahidi, S. (2021). The global risks report 2021 (16th ed.). World Economic Forum. https://bit.ly/3sJRB7Z

Gluckman, P. (2016). Making decisions in the face of uncertainty: Understanding risk. Office of the Prime Minister's Chief Science Advisor. https://bit.ly/3kJCqHI

Graham, J. (2020). Top risks and megatrends 2020: Airmic annual survey report. Airmic. https://bit.ly/39y36ca

Hester, P. (2012). Epistemic uncertainty analysis: An approach using expert judgment and evidential credibility. *Journal of Quality and Reliability Engineering, 2012*, Article 617481. https://doi.org/10.1155/2012/617481

Hubbard, D.W. (2009). *The failure of risk management: Why it's broken and how to fix it*. Wiley.

ISO. (2019). Space systems—Probabilistic risk assessment (PRA; ISO 11231:2019).

ISO/International Electrotechnical Commission (IEC). (2014). Safety aspects—Guidelines for their inclusion in standards (ISO/IEC Guide 51:2014). ISO.

Kadambi, N.P. (2005). Performance-based (risk-informed) regulation: A regulatory perspective. *Nuclear Technology, 149*(1), 110-121. https://doi.org/10.13182/NT05-A3583

Klemash, S., Lee, J. & Smith, J. (2020). Four ways to advance risk oversight: Global board risk survey 2021. Ernst & Young Global Ltd. Retrieved on Jan. 5, 2022. https://go.ey.com/3wE5DKV

Lyon, B.K. (2022). Uncertainty and residual risk [Manuscript in preparation]. In J. Haight (Ed.), *The Safety Professionals Handbook* (3rd ed.). ASSP.

Lyon, B.K. & Popov, G. (2021). *Assessing and managing risk: An ERM perspective*. ASSP.

Lyon, B.K. & Popov, G. (2022, March). On the concept of risk, uncertainty and black swans. *Professional Safety, 67*(3) 18-23.

Macesker, B., Myers, J.J., Guthrie, V.H., Walker, D.A. & Schoolcraft, S.G. (2002). *Principles of risk-based decision making.* ABS.

PricewaterhouseCoopers (PwC). (2021a). CRO and risk management leaders: Latest findings from PwC Pulse Survey. Retrieved on Jan. 5, 2022. https://pwc.to/3wHcl1n

PwC. (2021b). 24th annual Global CEO survey: U.S. findings. https://pwc.to/3MSvUu8

PwC and Committee of Sponsoring Organizations of the Treadway Commission (COSO). (2004). Enterprise risk management: Integrated framework: Executive summary, framework, September 2004. https://bit.ly/3LRmGOT

RIMS. (2022). What is enterprise risk management (ERM)? https://bit.ly/3P0t2xh

Sylvis, K., Fisher, D. & Fletcher, K. (2020). Federal Enterprise Risk Management 2020 survey results. Association for Federal Enterprise Risk Management. https://bit.ly/3vPAun8

U.S. Nuclear Regulatory Commission (U.S. NRC). (1999, March 1). Staff requirements—SECY-98-144—White paper on risk-informed and performance-based regulation. https://bit.ly/3wEw6YP

U.S. NRC. (2002). Guidance for performance-based regulation [NUREG/BR-0303]. https://bit.ly/3KLcAh7

U.S. NRC. (2012). A proposed risk management regulatory framework [NUREG-2150]. https://bit.ly/3vZMD9v

U.S. NRC. (2018). An approach for using probabilistic risk assessment in risk-informed decisions on plant-specific changes to the licensing basis [RG 1.174, revision 3]. https://bit.ly/3lEx54V

Cite this article

Lyon, B.K. & Popov, G. (2022, June). Costs and benefits of managing risk: Taking a risk-informed, performance-based approach. *Professional Safety, 67*(6), 29-36.

Bruce K. Lyon, P.E., CSP, SMS, ARM, CHMM, is vice president of risk management services for Brown & Brown. He is chair of the ISO 31000 U.S. TAG, vice chair of ANSI/ASSP Z590.3, advisory board chair to the University of Central Missouri's (UCM) Safety Sciences program, and vice president of the board of directors for BCSP. Lyon is coauthor of ***Assessing and Managing Risk: An ERM Perspective***, ***Risk Management Tools for Safety Professionals***, and ***Risk Assessment: A Practical Guide to Assessing Operational Risk***. He holds an M.S. in Occupational Safety Management and a B.S. in Industrial Safety from UCM. In 2018, he received the CSP Award of Excellence from BCSP. Lyon is a professional member of ASSP's Heart of America Chapter and a member of the Society's Ergonomics and Risk Management practice specialties.

N. Prasad Kadambi, Ph.D., is a nuclear safety expert with more than 50 years' experience in government, private sector and academia. He is chair of the American Nuclear Society's Risk-Informed and Performance-Based Principles and Policy Committee. He has served the U.S. Nuclear Regulatory Commission for 26 years. In retirement, Kadambi runs a consulting practice with locations in the U.S. and India.

Georgi Popov, Ph.D., CSP, QEP, SMS, ARM, CMC, FAIHA, is the interim chair of Safety Sciences at UCM. He is coauthor of ***Assessing and Managing Risk: An ERM Perspective***, ***Risk Management Tools for Safety Professionals***, and ***Risk Assessment: A Practical Guide to Assessing Operational Risk***. Popov holds a Ph.D. from the National Scientific Board, an M.S. in Nuclear Physics from Defense University in Bulgaria, and a post-graduate certification in environmental air quality. He graduated from the U.S. Army Command and General Staff College in Fort Leavenworth, KS. Popov is chair of ANSI/ASSP Z590.3 and vice chair of ISO 31000 U.S. TAG. He is a professional member of ASSP's Heart of America Chapter and a member of the Society's Risk Management Practice Specialty. In 2017, Popov received ASSP's Outstanding Safety Educator Award.