BENCHMARK ESG™ | Gensuite®

ISO 31000 RISK MANAGEMENT: FRAMING A PROCESS FOR MANAGING RISKS & GUIDING INTERNAL & EXTERNAL AUDIT PROCESSES

WHAT'S INSIDE

FOREWORD FROM GENSUITE PARTNER

By: Tjeerd Hendel-Blackford, Head of Thought Leadership, Enhesa

We live in an increasingly risk adverse, and risk aware society. The role of corporate risk executives and managers has evolved over time to cover all the potential risks a company may face. Financial, insurance, human rights, cyber security have been the 'traditional' focus of the risk function in most organizations. However, environmental, health and safety (EHS) risks have gradually become incorporated into the wider holistic risk management programs. Similarly, over the years we have worked with multinationals around the world, we have seen the language that is used by EHS professionals change over time. In the past, when we spoke to EHS executives their main concern was enforcement and specifically the fines that they might have to pay for a non-compliance. This is still a concern (a risk!), of course.

Enhesa conducted a survey in 2017 around the costs of non-compliance, and around 74% of the 50 EHS executives we surveyed had incurred an enforcement penalty of some kind in the previous 5 years. A quarter of those had had one just in the previous year. However, the terminology that we now increasingly hear from within organizations has moved beyond the costs of (non)compliance this and now focuses on:

- **Business Continuity.** Managing EHS to avoid operational shutdowns, lost-time injuries or fatalities is a critical aspect of keeping business operations running smoothly. However, we see these concerns raised increasingly in an overall operational risk management context. The risk of disruption to supply chains from the enforced shutdown of a plant or process has many and varied business implications.

- **Corporate Governance.** EHS risks are increasingly a part of overall robust and responsible corporate governance. How you company conducts itself and how it is perceived by the outside world are increasingly vital elements of risk management in our social-media driven world. We have seen studies that indicate that a third of the overall costs associated with a non-compliance incident are related to lost opportunities – resulting from loss of market share or a damaged reputation.

- **Risk Management.** Potential damage to the environment or people are inherent and high-profile risks that all companies face. Yet, surprisingly, when we talk to risk management associations or professionals, the risks presented by EHS have only quite recently started being considered as part of a company's overall risk management – which has historically tended to focus on financial, insurance or cyber and security risks. In fact, as well as avoiding risks, proactive EHS risk management can also proactively help to make cost-savings, in terms of reduced insurance premiums.

So managing EHS as part of an overall risk management system is imperative to business. It is no longer a silo and an overhead. This is also relevant as it is the intended aim of ISO 31000 (and the more EHS focused ISO 14001 and ISO 45001) management system to embed the management of risks into the very fabric of an organization's business strategy.

INTRODUCTION TO ISO 31000 RISK MANAGEMENT AND THE GENSUITE RISK MANAGEMENT PROCESS

Risk management comprises of the processes and procedures designed to promote a healthier, safer, and more environmentally-sound workplace, and compliance with laws and regulations enforced by agencies. It's important for several reasons. Business owners and executives want to run a responsible and safe operation, for the sake of their brand's reputation, their employees' safety and the operations of their companies. ISO 31000 helps accomplish just that. It is a set of standards relating to risk management established by the International Organization of Standardization (ISO).

ISO 31000 provides a universally recognized set of principles and guidelines on risk management. Organizations employing risk management processes can use these guidelines to replace their myriad of existing complex standards and methodologies to reduce organizational risk.

ISO 31000 has three main sections. It starts by listing a set of management principles. Use these principles to guide your organization of your risk management framework. Then use the framework to guide the management of your risk management process. Together these three sections make up ISO 31000's guideline, to ultimately help your organization form a risk management program.

Risk management programs, like that provided by Benchmark ESG™, are critical foundations in the continued management of risks for environment, health and safety (EHS). Meet ISO 31000's risk management guidelines and your organizational needs. With comprehensive auditing and compliance software application suites for incident management and training solutions, Benchmark ESG™ is your one-stop shop for risk management.

PRINCIPLES OF ISO 31000

Risk Management establishes and sustains value. To establish and sustain value, risk management must be tied to organizational objectives and then be analyzed. The ISO 31000 principles can help organizations improve their risk management and auditing processes.

- Risk Management establishes and sustains value. To establish and sustain value, risk management must be tied to organizational objectives and then be analyzed.

- Risk management is an integral part of all organizational processes. Risks impact everyone within an organization. Make sure to get all levels involved in the risk management process to prevent and manage them better.

- Risk management is part of decision-making. Risk management decision-making involves identifying risks and planning actions to manage, assess and prioritize them.

- Risk management explicitly addresses uncertainty. Risk management technology must be embedded in business processes where decisions are made with uncertainty. Such technology must be intuitive and easy to use to help users make informed decisions.

- Risk management is systematic, structured and timely. To remain consistent with risk management to ensure a safe and sound workplace, you must have a process in place for managing risks, such as weekly checks, mitigation plans and a plan of action that addresses risks.

- Risk management is based on the best available information. Industries are moving towards the continuous monitoring of risks. Risk solutions need to be flexible and allow users to enter risk data in real-time, ensuring that information is always up-to-date.

- Risk management is tailored. Each company is unique and each risk management solution should be too. Every company has a unique set of risks so finding a solution that can be customized to meet your organizational needs is critical.

- Risk management takes human and cultural factors into account. Ensure you invest in risk management software that doesn't require on-going maintenance, has consistent customer support and can support a global team, while customizing to your business needs.

- Risk management is transparent and inclusive. Risk management software should be scalable and affordable. This includes a single sign-on license so that the solution is easily accessible across the organization and an integrated solution with auditing, compliance and incident management to help make risk-based decisions even more informed.

- Risk management is dynamic, iterative, and responsive to change. Business changes, so the technology you use needs to change with it.

- Risk management facilitates continual improvement of the organization. To facilitate continuous improvement, risk management needs to get out of the risk function and into the hands of end users where it can be used in decision-making across the organization.

FRAMEWORK OF ISO 31000

The purpose of the risk management framework is to assist with integrating risk management into activities and functions – particularly those related to environment, health, and safety (EHS). The effectiveness of risk management will depend on integration into governance and all other activities of the organization, including decision-making.

LEADERSHIP & COMMITMENT

- Aligning risk management with strategy, objectives and culture of the organization
- Issue a statement or policy that establishes a risk management approach, plan or course of action
- Make necessary resources available for managing risks
- Establish the amount and type of risk that may or may not be taken

INTEGRATION

- Determine management accountability and oversight roles and responsibilities
- Ensure risk management is part of, and not separate from, all aspects of the organization framework

DESIGN

- Understand the organization and its internal and external context
- Articulate risk management commitment and allocate resources
- Establish communication and consultation arrangements

IMPLEMENTATION

- Develop an appropriate implementation plan including deadlines
- Identify where, when and how different types of decisions are made, and by whom
- Modify the applicable decision-making processes where necessary

EVALUATION

- Measure framework performance against its purpose, implementation and behaviors
- Determine whether it remains suitable to support achievement of objectives

IMPROVEMENT

- Continually monitoring and adapting the framework to address external and internal change
- Take actions to improve the value of risk management
- Improve the suitability, adequacy and effectiveness of the risk management

PROCESS OF ISO 31000

The risk management process involves the systematic application of policies, procedures and practices to the activities of communicating and consulting, establishing the context and assessing, treating, monitoring, reviewing, recording and reporting risk.

1. COMMUNICATION AND CONSULTATION

- Bring different areas of expertise together for each step of the RM process
- Ensure different views are considered when defining risk criteria and evaluating risks
- Provide sufficient information to facilitate risk oversight and decision making
- Build a sense of inclusiveness and ownership among those affected by risk

2. SCOPE, CONTEXT AND CRITERIA

- Define the purpose and scope of risk management activities
- Identify the external and internal context for the organization
- Define risk criteria by specifying the acceptable amount and type of risk
- Define criteria to evaluate the significance of risk and to support decision-making

3. RISK ASSESSMENT

- Risk identification to find, recognize and describe risks that might help or prevent achievement of objectives and the variety of tangible or intangible consequences
- Risk analysis of the nature and characteristics of risk, including the level of risk, risk sources, consequences, likelihood, events, scenarios, controls, and their effectiveness
- Risk evaluation to support decisions by comparing the results of the risk analysis with the established risk criteria to determine the significance of risk

4. RISK TREATMENT

- Select the most appropriate risk treatment option(s)
- Design risk treatment plans specifying how the treatment options will be implemented

5. MONITORING & REVIEW

- Improve the quality and effectiveness of process design, implementation and outcomes
- Monitor the RM process and its outcomes, with responsibilities clearly defined
- Plan, gather and analyze information, recording results and providing feedback
- Incorporate the results in performance management, measurement and reporting activities

6. RECORDING & REPORTING

- Communicate risk management activities and outcomes across the organization
- Provide information for decision-making
- Improve risk management activities
- Provide risk information and interacting with stakeholders

HOW TO GET STARTED: ISO 31000 GUIDELINES OVERVIEW

The most recent 2018 draft of the ISO 31000 risk management document has removed much of the complex language. It includes improvements, such as the importance of human and cultural factors in achieving organizational objectives and also placing an increased emphasis on the risk management decision-making process.

ISO 31000 defines a total of eight key terms, including the definition of risk as “the effect of uncertainty on objectives”. This definition is clarified by stating that risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.

The new version of ISO 31000 is shorter than the earlier 2009 version, and presents a high-level overview of risk management and how a risk management program can be implemented. ISO 31000 states that managing risk is based on the principles, framework and process described in the guidelines, which has been outlined in the above sections.

It also states that these components might already exist in full or in part within an organization, but they might need to be adapted or improved so that risk management is efficient, effective, and consistent.

ISO 31000 states that the guidelines should be used by people who create and protect value in organizations by managing risks, making decisions, setting and achieving objectives and improving performance. The guidelines are applicable to all types and sizes of organizations and relevant to all external and internal factors and influences. ISO also states that managing risk assists organizations in setting strategy, achieving objectives and making informed decisions.

ISO 31000 GUIDELINES

RISK MANAGEMENT PRINCIPLES

- Develop an approach that is structured and comprehensive
- Make sure it's effective
- Make sure it's dynamic
- Make sure it's customized

RISK MANAGEMENT FRAMEWORK

1. Plan the establishment of a risk management framework
2. Show leadership by making a commitment to risk management
3. Make your personnel responsible managing risk
4. Design your organization's risk management framework
5. Implement your unique risk management framework
6. Evaluate the performance of your risk management framework
7. Improve the performance of your risk management framework

RISK MANAGEMENT PROCESS

1. plan the establishment of a risk management process
2. Discuss risks and get feedback from your stakeholders
3. Define scope, context, and the criteria you intend to use
4. Conduct risk assessments whenever necessary
5. Treat the risks that affect the achievement of the objectives
6. Evaluate and improve your risk management process
7. Record and report on your risk management activities

IMPLEMENT GENSUITE RISK MANAGEMENT PROGRAM

HOW BENCHMARK ESG™ CAN HELP: RISK MANAGEMENT AND AUDITING SOLUTIONS

A risk management solution can help to achieve the ISO 31000 guidelines and the three fundamental areas within it. See below for the Benchmark ESG risk management solution programs to help improve organizational needs.

AUDIT & COMPLIANCE ASSURANCE

Audits and corrective actions made easy with Audit Management software that simplifies regulatory compliance audits, inspection and follow-up processes.

INCIDENT MANAGEMENT

Reduce workplace accidents and injuries with Benchmark ESG™ Incident Management Software to track incidents from occurrence to closure.

CHANGE MANAGEMENT

Execute change more confidently with Benchmark ESG™ Change Management software to manage processes, compliance and risks from operational change.

SAFETY PROGRAMS & PROCEDURES

Reduce safety risks and incidents with Benchmark ESG™ Safety Management Software.

TRAINING COMPLIANCE

Structure and deliver regulatory and best practice training to reduce risk and enhance productivity with Benchmark ESG™ Training Management Software.

CASE STUDY: PROVEN RISK & AUDITING MANAGEMENT SOLUTIONS FOR FOLLOWING ISO STANDARDS

CURRENT GENSUITE SUBSCRIBER MAINTAINING CERTIFICATION

Overview

A behavior-based approach to safety drives employee engagement, identifies greatest behavioral safety risks and helps one nationally recognized food retail and distribution company meet 100% of safety observation targets.

Business Profile

- U.S.-based food retail and distribution company servicing over 300 locations
- Annual revenue of 16 billion USD and 70,000 employees
- Operates over 2+ million square feet of grocery and non-food warehousing

Application Highlight

Benchmark ESG's Safety Observations application enables company employees to observe and track safe and at-risk employee behaviors using custom observation forms.

- Provides a single platform to house safety observation forms and checklists
- Ability to customize risk categories and associated behaviors specific to each site
- Data mines safety observations to identify risks and drive safety improvements
- Identify top 5 at-risk behaviors

Better Together: Risk Management & Occupational Safety Management

Benchmark ESG offers proven IT solutions for risk management and Environmental, Health & Safety (EHS). These solutions allow companies and organizations to gain certification to both ISO 45001 for Occupational health and Safety Management and ISO 31000 for Risk Management.

JOIN THE BENCHMARK ESG™ SUBSCRIBER COMMUNITY

Interested in joining the Benchmark ESG subscriber community? As a subscriber, you'll gain access to additional perks like training sessions through Benchmark ESG University as well as the benefits of having a 24/7 team of experts ready to help you whenever you need it most. Plus, our annual Benchmark ESG Conferences are made just for our subscribers so we can learn how to improve our solutions to meet their needs.

Sharing best-practices, providing feedback on existing features and dreaming up new software solutions is what makes our company grow into the future. If you're looking to get started, our software experts can help you decide the best application module for your team. You can even try Benchmark ESG solutions absolutely free with our demo through Benchmark ESG READY. Interested in making the switch to our software solutions? Now is the perfect time!

The first 6 MONTHS are on us!

If you are switching from an eligible competitor, we're happy to take care of the first 6 months of your operating and service costs!