SafetyInfo

Vol. No. 13 Issue No. 05 *Fortnightly, Free soft copy* 1st March 2022

ISO 31000:2018 – Risk Management

ISO 31000 defines risk as "the effect of uncertainty on objectives." Those risks are expressed in the form of risk sources, potential events, their related consequences, and the likelihood of them occurring. Naturally, leaders and employees within a business want a process to run as completely and as smoothly as possible. This means no defects, no injuries, and no downed equipment during processing hours. Predicting those risks, however, can be incredibly difficult without the right strategy in place.

This article will go over the importance of following best practice methods for risk management in addition to the excellent guidance ISO 31000 provides on how to run these types of programs.

What is ISO 31000?

Managing risk within a business is critical to be able to make the right decisions, achieve any objectives, and promote productivity. There are always both internal and external risks that put pressure on a business whether they are aware of them or not. Because of that difficulty, ISO 31000 was created.

Consisting of a framework for implementing, maintaining, and improving risk management tactics for businesses, ISO 31000 was meant to be inclusive. This standard is for all levels of businesses, individuals, and even small groups looking into creating their own risk management program.

The three different parts that ISO 31000 provides guidance on include management of risks, the relationship between leadership and employees, and a general direction to follow when it comes to risk management. These characteristics are driven by the following primary concepts:

- **The principles** of risk management must be considered when the company is beginning to lay out it's individualized framework and unique process. Risk management principles exist to provide guidance on managing uncertainty.

- **The framework** exists to help facilities implement their own risk management program into daily activities. Successfully implementing this part of the risk management strategy heavily relies on top management buy in as well as stakeholder participation.

- **The process** is where the nitty gritty stuff happens. It is the application of company policies and procedures to work towards monitoring and reporting risk. It can be applied at any level of the business structure and heavily relies on decision making.

Risk management is impossible without all three of these concepts and their individual focuses. With that being said, each of those three core concepts will be gone over in more depth as this article progesses.

The Principles of Risk Management

Managing uncertainty is essential to be successful in taking the right amount of risk, as well as utilizing the right kind of risk. To do so, becoming familiar with the eight principles of ISO 31000 must be step number one. The eight principles of risk management hold value creation and the protection of that value at its core. Those principles include:

1. **Integration** – To be successful, risk management must be integrated into all existing business operations. There is no action without risk.
2. **Structured** – Having a structured and comprehensive approach to risk management means formulating a plan and having all the information ready to go.
3. **Customized** – ISO's 31000 framework as well as the processes the company employs must be customized to their needs. There is no one size fits all option for risk management. A risk management program for office work is going to be wildly different from a risk management program for a car manufacturing plant.
4. **Inclusive** – It's not just the company itself that takes care of a risk management program, all stakeholders must also be involved. It's a team effort!
5. **Dynamic** – This means being proactive and responding to changes by first detecting or anticipating a problem before it reaches catastrophic failure rates.
6. **Accountable** – Staying knowledgeable about any limitations the process may encounter because of a lack of available information is incredibly important for risk management programs.
7. **Considerate** – Out of all the stages within a risk management program it is important to put people first. Your employees, stakeholders, and customers are relying on a final item that brings forth value. Controlling those risks is one of the primary reasons why good product is delivered.
8. **Continuously Improving** – By learning and experiencing the current risk management strategy, you will always be finding areas that need improvement. Acting upon that improvement completes the risk management cycle, bringing your company that much closer to a safer and more perfect process.

The above principles must be considered first before drafting the company's framework for managing risk.

Understanding the ISO 31000 Framework

The purpose of the ISO 31000 framework is to help companies integrate risk management into their daily activities. It must be remembered that each of the pieces of an ISO 31000 framework for risk management make up a rough guideline. This is because there is no one-size-fits all with risk management, every company is different.

The components of a risk management framework are as follows:

- **Leadership and Commitment** – Ensure risk management is integrated into all activities. Leaders can demonstrate their commitment by customizing their unique framework, managing risk efforts with the right resources, and keeping everyone involved accountable.

- **Integration** – Put in the effort to understand the organization's structure and context for risk management. In terms of integration, risk management must be a part of the organizational purpose, governance, leadership, commitment, strategy, objectives, and operations. It is necessary for companies to be dynamic in terms of integrating risk management practices.

These next four components of the ISO 31000 framework are often linked to the Plan, Do, Check, Act cycle. However, ISO refers to it as the Plan, Implement, Measure, Learn system.

- **Design** – Understand fully both the internal and external context of the company's purpose and where risk is involved.

- **Implementation** – Decision-making takes high priority during implementation. This involves developing a plan, identifying when and where decisions are made, and understanding how to manage risk.

- **Evaluation** – Periodically measuring the performance of the risk management framework against indicators, behavior, plans, and its purpose is necessary for decision-making that involves changes. If the management system is not helping the company achieve its objectives, something must be altered.

- **Improvement** – There are two different factors here, adapting and continually improving. Adapting requires the risk management framework to address both external and internal changes within a process to improve value. Continually improving requires maintaining and evolving integration, therefore improving the effectiveness of the risk management framework.

Notice any similarities?

The ISO 31000 framework shares a lot of the same descriptor words as the ISO 31000 principles! While it may seem redundant, these similarities point to how closely linked the strategy's objectives are (the principles) and how those objectives can be reached (the framework).

Types of Risks

You may be surprised to know that risk can affect the workplace either negatively or positively. This is because risk, in this context, is expressed through the **sources** of risk, **potential** events, the **consequences** of taking any risks, and the **likelihood** of those consequences coming to fruition. With that being said, the definition of risk within an industry is quite a bit more ambiguous than what we may attribute as risky behavior normally.

There are three different categories of risk that ISO 31000 specifies:

1. **A hazard risk is classified as a negative outcome to an uncertain event.**
    1. Hazard risks are more than just work-related injuries and illnesses. Remember, it's an outcome with a negative effect on the company. This can mean anything from marketing risks to financial risks.
    2. Try using the hierarchy of hazards to mitigate these hazard risks, at least for the safety related risks.
2. **A control risk is defined by its innate sense of uncertainty. It is the uncertainty of an event occurring, but also not knowing what the consequences hold if it does take place.**
    1. Control risks are a bit more difficult to tackle as both sides are unknown. What it comes down to is project management and critical decision-making.
    2. Remember that sometimes risks must be taken!
3. **The last risk option is referred to as opportunity. This is when an uncertain event occurs, and positive consequences follow.**
    1. Taking an opportunity risk, while uncertain if it will happen, the outcome is known within reason. However, there are some companies that have a higher risk tolerance than others.
    2. Opportunity risks may present themselves as workers needing and wanting a new space to accommodate their growing department. The positive consequences result in happier and healthier employees that are safer and more satisfied with their jobs.

Recognizing these types of risks and establishing a standard tolerance level for approaching risks is critical for creating a robust risk management program. Without this, risk treatment and the collaboration that goes into a risk management process will lack a basic understanding of risk level.

The Risk Management Process

The risk management process is iterative due to the often-repetitive nature of select steps to generate different risk management outcomes. The risk management process utilizes the systematic application of policies and procedures in relation to communication, establishing context, and monitoring, treating, reviewing, and documenting risk within workplace objective and activities.

The diagram that ISO 31000 provides for visualizing the risk management process has several different pieces. The very center is where it all begins. Risk assessment, risk treatment, and the scope, context, and criteria of the business' efforts in risk management is located there. The next layer involves communication and consultation as well as monitoring and review. The last part of this diagram is the recording and reporting section.

Think of this diagram as proceeding from the inside out, where the identified risk is focused on first. The farther out the layers go in this diagram, the more information the user has obtained to work with. All of which eventually leads them to making a calculated decision for the company.

Workplace Safety & Risk Management

Workplace safety is defined as the level of safety, health, and well-being employees are subject to in their working environment. OSHA and other regulatory organizations take this subject very seriously by either enforcing safety guidelines for unique environments or creating new voluntary standards that have been proven to decrease workplace accidents.

With that being said, workplace safety and risk management go hand in hand when it comes to business operations. You can't have one without the other, and because of that, it is important to establish and follow the risk management program guidelines put out by ISO 31000.

Hazard Risk Assessment

Remember when we discussed the center of the risk management process that ISO outlines? Within the center of risk assessment there are three different categories:

1. Risk Identification
2. Risk Analysis

3. Risk Evaluation

Once these three components have been identified and defined, the user must then figure out who exactly is at risk, as well as document all their findings. These are the basic steps of a hazard risk assessment, you can learn more about it in our risk assessment article here.

Readers may please note that D. L. Shah Trust brings out two e-journals on a fortnightly basis. These are mailed to those persons or institutions who are desirous of receiving them:
These two e-journals are:
1. Safety Info
2. Quality Info

If you or your friends or colleagues wish to receive these journals, you may send us an email requesting for the same. There is no charge for these journals. Our e-mail address is:

dlshahtrust@yahoo.co.in **or** haritaneja@hotmail.com **or** dlshahtrust@gmail.com

You can also access these journals on our website: www.dlshahtrust.org

Published by : D. L. Shah Trust, **Room No. 16, 1st Floor, Gool Mansion,** **Homji Street, Mumbai 400 001** **email: dlshahtrust@yahoo.co.in** **Ph: 022-22672041** **Subscription: Free on request** **(soft copy only)**	**Edited by : Hari K Taneja, Trustee,** **D. L. Shah Trust** **email: dlshahtrust@gmail.com** **Phone: 022-2309 6529** **Subscription: Free on request** **(soft copy only)**