A

PROJECT REPORT

ON

"*RISK MANAGEMENT*"

UNDERTAKEN AT

"*THE AKSHAYA PATRA FOUNDATION*"

IN PARTIAL FULFILMENT OF

POST GRADUATE DIPLOMA IN MATERIAL MANAGEMENT

MIT SCHOOL OF DISTANCE EDUCATION,

PUNE.

GUIDED BY

PRABHAKAR TN

SUBMITTED BY

GOVINDA VERMA

Registration No._MIT2017000850_

MIT SCHOOL OF DISTANCE EDUCATION

PUNE-411 038

YEAR 2017-2019

To,
The Director
MIT School of Distance Education, Pune

Respected Sir,

This is to inform you to kindly exempt me from submitting the certificate from my organization for Project Work due to the reason mentioned below.

1. **As per the Rules of the Organization**

Thanking you in Anticipating of your approval to my request

Regards,

Govinda Verma

MIT2017000850

DECLARATION

I here by declare that this project report entitled "**RISK MANAGEMENT"** is a bonafide record of the project work carried out by myself during the academic year 2017-2019, in partial fulfillment of the requirements for the award of **POST GRADUATE DIPLOMA IN MATERIAL MANAGEMENT (PGDMTM)** of **MIT School of Distance Education, Pune.**

This work has not been undertaken or submitted elsewhere in connection with any other academic course.

(Name of Student and Signature)

GOVINDA VERMA

ACKNOWLEDGEMENT

I would like to take this opportunity to express my sincere thanks and gratitude to **Prabhakar TN of The Akshaya Patra Foundation** for giving me an opportunity to perform this project in the esteem organization and it has indeed been a great learning and enjoyable experience.

I would like to express my deep sense of gratitude and profound thanks to all staff members of **The Akshaya Patra Foundation** for their kind support and cooperation which helped me in gaining lots of knowledge and experience to do my project work successfully.

At last but not least, I am thankful to my **Family** and **Friends** for their moral support, endurance and encouragement during the course of the project.

GOVINDA VERMA

Student ID- MIT2017000850

ABSTRACT

This project is written on topic- Risk management as how to manage your assigned task in typical situation and how to handle risks.

TABLE OF CONTENTS

Introduction of the Organization

Chapter-1

The Akshaya Patra Foundation is a not-for-profit organisation headquartered in Bengaluru, India. This organisation strives to eliminate classroom hunger by implementing the Mid-Day Meal Scheme in the government schools and government-aided schools. Alongside, Akshaya Patra also aims at countering malnutrition and supporting the right to education of socio-economically disadvantaged children.

Since 2000, Akshaya Patra has been concerting all its efforts towards providing fresh and nutritious meals to children on every single school day. It is continuously leveraging technology to multiply its reach. The state-of-the-art kitchens have become a subject of study and have attracted curious visitors from around the world.
Its partnership with the Government of India and various State Governments, along with the persistent support from corporates, individual donors, and well-wishers have helped its to grow from serving just 1,500 children in 5 schools in 2000 to serving 2.2 million children per day.

Today, Akshaya Patra is the world's largest (not-for-profit run) Mid-Day Meal Programme serving wholesome food every school day to over 2.2 million children from 70 Kitchen in 22000+ schools across 15 states & 2 UTs in India.

The Growth of The Akshaya Patra Foundation – A Quick Overview

On 28 November 2001, the Supreme Court of India passed a mandate, "*Cooked mid-day meal is to be provided in all the Government and Government-aided primary schools in all the states*."
And, Akshaya Patra was also called upon to provide testimonies to the Supreme Court.
By the time the Ministry of Human Resource Development - Department of School Health and Education extended its support to the initiative in 2003, Akshaya Patra was already reaching out to 23,000 children.

Today, Akshaya Patra has 68 kitchens spread across 15 states & 2 UTs in India, a result of the successful partnership with the Government of India, various State Governments and generous supporters.

Chapter-2- Organizational Profile

There are Vision and Mission of Akshaya Patra

Vision:- NO CHILD IN INDIA SHALL BE DEPRIVED OF EDUCATION BECAUSE OF HUNGER.

Mission:- TO FEED 5 MILLION CHILDREN BY 2025

Through Mid-Day Meal Programme, its attempt is to feed the millions of children in India who lack the means, but, have the zeal to learn and achieve. By feeding them one wholesome meal a day, we give them the nourishment and motivation they need to pursue an education for a better future. It is endeavor to reach out to every child at the grass root level of the society.

Mid Day Meal Programme Implementation

While implementing the mid-day meal programme, the Central and State Governments work hand in hand. Central Government issues guidelines to be followed by State Governments while executing the scheme. However, there are some states that have issued guidelines different from Central Guidelines.

A National Steering-cum-Monitoring Committee (NSMC) is set up to monitor the programme, assess its impact and provide policy advice to Central and State Governments. Central assistance in the form of subsidies is released upon submission of the committee's Annual Work Plan by the Programme Approval Board.

Steering-cum-Monitoring Committees are also set up at a state level to monitor the programme. A nodal department is authorized to take responsibility. Implementation cells are organized by the nodal department and one officer is appointed at each district and block level to oversee effective implementation of the programme.

The Panchayats / Urban Local Bodies are in charge of the scheme in states where primary education is entrusted to them.

Objectives of Mid Day Meal :-

Would you be able to learn if hunger was your classroom companion?
Classroom hunger affects children's ability to learn and grow. To solve this challenge, Akshaya Patra began the Food for Education initiative which is continuously making an effort to enable children from over 13,000 schools in India.

On August 15, 1995, National Programme of Nutritional Support to Primary Education (NP-NSPE) was launched as a Centrally Sponsored Scheme and in the year 2001, the Supreme Court of India ordered all the state governments and union territories to implement Mid-Day Meal Scheme and provide cooked meals to school children from Government and Government-aided schools.

With support from the central and state governments, Akshaya Patra began operating its Mid-Day Meal Programme in 2000 and has inculcated a set of rules and guidelines related to child health and growth, the quantity of calories and proteins required for children from specific age groups, the quantity of grains that can be allotted to each child, and so forth. With an effective Public-Private Partnership model, we have been able to serve mid-day meals for 23 years.

The objectives of Mid-Day Meal as issued by the government:

- Improving the nutritional status of children in classes I-V in Government, Local Body and Government aided schools, and EGS and AIE centres
- Encouraging children, belonging to disadvantaged sections, to attend school more regularly and help them concentrate on classroom activities
- Providing nutritional support to children of primary stage in drought affected areas during summer vacation

While focusing on improving nutritional level and attendance, Akshaya Patra also aims to address two Sustainable Development Goals: Zero Hunger and Quality Education.

NGOs play an important role in the expansion of the Mid-Day Meal Scheme. The State Governments partner with NGOs like The Akshaya Patra Foundation to implement the Mid-Day Meal Programme in order to increase the number of children they reach out to. Thus many NGOs work towards countering hunger and malnutrition.

This Public-Private Partnership (PPP) has proved instrumental in improving the quality and reach of the programme. There are many facets which the Government considers when selecting a non-profit to partner with. Such organisations must be transparent and 'of proven integrity'. Below are the NP-NSPE 2004 criteria for choosing an NGO

Other Initiatives:-

The organisation has taken many other feeding and social initiatives other than Mid Day Meals Program. Here are some of the feeding initiatives and social initiatives that are undertaken by Akshaya Patra.

- Anganwadi feeding
- Disaster relief
- Feeding expecting and lactating mothers
- Feeding programmes in old-age homes
- Feeding programmes in special schools
- Feeding runaway children
- Feeding the homeless & Covid Time feeding
- Subsidized lunch for the economically disadvantaged

History of The Akshaya Patra Foundation :-

Looking out of a window, one day in Mayapur, a village near Calcutta, His Divine Grace A. C. Bhaktivedanta Swami Prabhupada saw a group of children fighting with stray dogs over scraps of food. From this simple, yet heart-breaking incident was born a determination that no child within a radius of ten miles from our center should go hungry.

His inspiring resolve sowed the seeds of The Akshaya Patra Foundation. With the vision: "*No child in India shall be deprived of education because of hunger,"* Akshaya Patra started the Mid-Day Meal Programme in June 2000 by serving mid-day meals to 1,500 children across five government schools in Bengaluru, Karnataka. A humble beginning, yet, the initial days of implementing the programme was not a smooth sail. Soon came the helping hands of Mohandas Pai, who took the initiative of donating the first vehicle to transport food to the schools.

Chapter-3- Project Objectives & Scope

There are five objectives of Risk Management.

Now let's look at how these steps are carried out in a more digital environment.

Step 1: Identify the Risk

The first step is to identify the risks that the business is exposed to in its operating environment. There are many different types of risks – legal risks, environmental risks, market risks, regulatory risks, and much more. It is important to identify as many of these risk factors as possible. In a manual environment, these risks are noted down manually.

If the organization has a risk management solution employed all this information is inserted directly into the system. The advantage of this approach is that these risks are now visible to every stakeholder in the organization with access to the system. Instead of this vital information being locked away in a report which has to be requested via email, anyone who wants to see which risks have been identified can access the information in the risk management system. **Single item will be delivered in Lucknow due to load issue.**

Step 2: Analyze the risk

Once a risk has been identified it needs to be analyzed. The scope of the risk must be determined. It is also important to understand the link between the risk and the different factors within the organization. To determine the severity and seriousness of the risk it is necessary to see how many businesses function the risk effects. There are risks which can bring the whole business to a standstill if actualized, while there are risks which will only be minor inconveniences in analyzed. In a manual risk management environment, this analysis must be done manually.

When a risk management solution is implemented one of the most important basic steps is to map risks to different documents, policies, procedures, and business processes. This means that the system will already have a mapped risk framework which will evaluate risks and let you know the far-reaching effects of each risk.

Step 3: Evaluate or Rank the Risk

Risks need to rank and prioritize. Most risk management solutions have different categories of risks, depending on the severity of the risk. A risk that may cause some inconvenience is rated lowly, risks that can result in catastrophic loss are rated the highest. It is important to rank risks because it allows the organization to gain a holistic view of the risk exposure of the whole organization. The business may be vulnerable to several low-level risks but it may not require upper management intervention. On the other hand, just one of the highest rated risks is enough to require immediate intervention.

Step 4: Treat the Risk

Every risk needs to be eliminated or contained as much as possible. This is done by connecting with the experts of the field to which the risk belongs to. In a manual environment, this entails contacting each and every stakeholder and then setting up meetings so everyone can talk and discuss the issues. The problem is that the discussion is broken into many different email threads, across different documents and spreadsheets, and many different phone calls.

In a risk management solution, all the relevant stakeholders can be sent notifications from within the system. The discussion regarding the risk and its possible solution can take place from within the system. Upper management can also keep a close eye on the solutions being suggested and the progress being made from within the system. Instead of everyone contacting each other to get updates, everyone can get updates directly from within the risk management solution.

Step 5: Monitor and Review the risk

Not all risks can be eliminated – some risks are always present. Market risks and environmental risks are just two examples of risks that always need to be monitored. Under manual systems monitoring happens through diligent employees. These professionals must make sure that they keep a close watch on all risk factors. Within a digital environment, the risk management system monitors the entire risk framework of the organization. If any factor or risk changes, it is immediately visible to everyone. Computers are also much better at continuously monitoring risks than people.

The first step to defining risk management goals and risk management objectives is to define your organization's shared vision. Once the shared vision is articulated, overall risk management goals and objectives must be defined.

While a vision statement is often aspirational, the goals and objectives should ordinarily describe in simple terms what is to be accomplished. They should be actionable by the organization. They should be defined in the context of the organization’s business strategy.

For example, some common risk management objectives chosen by companies to frame their ERM approach include the following:

- Develop a common understanding of risk across multiple functions and business units so we can manage risk cost-effectively on an enterprise-wide basis.
- Achieve a better understanding of risk for competitive advantage.
- Build safeguards against earnings-related surprises.
- Build and improve capabilities to respond effectively to low probability, critical, catastrophic risks.
- Achieve cost savings through better management of internal resources.

- Allocate capital more efficiently.

Risk management goals and objectives should be consistent with and supportive of the enterprise's business objectives and strategies. Therefore, the organization's business model provides an important context for risk management.

For example:

- It targets the markets and geographies in which the firm does business.
- It specifies the products and services it provides to those markets, the channels it uses to access those markets and the characteristics by which it differentiates its products and services in the eyes of the customer.
- It is built on many important elements: on the processes through which the entity converts materials and labor into products and services; on the employees the entity hires, trains and retains; on the suppliers and customers with which the organization does business; and on the shareholders and lenders that supply it capital.

Business risks are inherent in all of these elements. As the enterprise executes its strategy, it creates and increases its exposures to uncertainty. Therefore, business objectives and strategies provide the context for understanding the risks the enterprise desires to take. COSO affirmed this point by establishing "objective setting" as a component of the ERM framework.

When defining risk management goals and objectives, management should ask "tough questions," such as those listed below:

- What are our business objectives and strategies? What are our financial targets, e.g., profitability, size and revenue growth? What values do we want to build and reinforce?
- What markets do we choose? What relative market position do we seek? What is our business model for winning in our chosen markets?
- What specific possible future events do we face? Are they related?
- How sensitive are our strategies, markets, earnings and cash flow to the occurrence of future events?
- How risky are our tangible and intangible assets for creating value? What are the loss drivers affecting those assets?
- Which specific future events could, if they occurred, affect our organization's ability to achieve its objectives relating to quality, innovation, timeliness, safety, compliance, etc., and to execute its strategies successfully? Which events would affect our market share?
- How capable are we of responding to events beyond our control that may happen in the future?
- Do we know what our expected returns are, as adjusted for risk? Do risk-adjusted returns vary by business unit? By major product? By geography?
- Finally, if we decide to accept the exposures inherent in our business model that give rise to our existing risks, do we have sufficient capital to absorb significant unforeseen losses should they occur?

The above questions provide a powerful context for defining risk management goals and objectives. Following is an example of a statement of risk management vision, mission, goals and objectives:

Vision

Contribute to the creation, optimization and protection of enterprise value by managing our business risks as we create value in the marketplace.\

Mission

Create a comprehensive approach to anticipate, identify, prioritize, manage and monitor the portfolio of business risks impacting our organization. Put in place the policies, common processes, competencies, accountabilities, reporting and enabling technology to execute that approach successfully.

Goals and Objectives

(1) Design and execute a global business risk management process integrated with our strategic management process:

- Integrate business risk management with our strategy formulation and business planning processes;
- Articulate our strategies so that they are understood throughout our organization;
- Establish KPIs designed to drive behaviors consistent with our strategy; and
- Reward effective articulation and management of key risks.

(2) Ensure that process ownership questions are addressed with clarity so that roles, responsibilities and authorities are properly understood.

(3) Design and execute a global process to monitor and reassess the top quartile risk profile and identify gaps in the management of those risks, based upon changes in business objectives and in the external and internal operating environment.

(4) Define risk management strategies and clear accountabilities and action steps for building and executing risk management capabilities and improving them continuously.

(5) Continuously monitor the information provided to decision-makers in order to assist them as they manage key risks and protect the interests of shareholder

Business always comes with risk and to manage this risk, you need to hire the proper experts. The objectives of risk management are-

1. To lower the unwanted surprises in future.
2. It will make your plans risk-proof.
3. It'll help you to spot trouble before it pops up.

4. It'll also help in better decision making as the data will be properly examined.
5. Aids in better communication between teams.

The objective of a well-managed risk management program is to provide a repeatable process for balancing cost, schedule, and performance goals within program funding. This is especially true on programs with designs that approach or exceed the state-of-the-art or have tightly constrained or optimistic cost, schedule, and performance goals. Without effective risk management the Program Management Office (PMO) may find itself doing crisis management, a resource-intensive process that is typically constrained by a restricted set of available options. Successful risk management depends on the knowledge gleaned from assessments of all aspects of the program coupled with appropriate mitigations applied to the specific root causes and consequences

A key concept here is that the government shares the risk with the development, production, or support contractor (if commercial support is chosen), and does not transfer all risks to the contractor. The PMO always has a responsibility to the system user to develop a capable and supportable system and cannot absolve itself of that responsibility. Therefore, all program risks, whether primarily managed by the program office or by the development/support contractor, are of concern and must be assessed and managed by the program office. Once the program office has determined which risks and how much of each risk to share with the contractor, it must then assess the total risk assumed by the developing contractor (including subcontractors). The PMO and the developer must work from a common risk management process and database. Successful mitigation requires that government and the contractor communicate all program risks for mutual adjudication. Both parties may not always agree on risk likelihoods, and the government Program Manager (PM) maintains ultimate approval authority for risk definition and assignment. A common risk database available and open to the government and the contractor is an extremely valuable tool. Risk Mitigation involves selection of the option that best provides the balance between performance and cost. Recall that schedule slips generally and directly impact cost. It is also possible that throughout the system life cycle there may be a need for different near-term and long-term mitigation approaches

An effective risk management process requires a commitment on the part of the PM, the PMO and the contractor to be successful. Many impediments exist to risk management implementation, however, the program team must work together to overcome these obstacles. One good example is the natural reluctance to identify real program risks early for fear of jeopardizing support of the program by decision makers. Another example is the lack of sufficient funds to properly implement the risk mitigation process. However, when properly resourced and implemented, the risk management process supports setting and achieving realistic cost, schedule, and performance objectives and provides early identification of risks for special attention and mitigation.
PMs have a wide range of supporting data and processes to help them integrate and balance programmatic constraints against risk. The Acquisition Program Baseline (APB) for each program defines the top-level cost, schedule, and technical performance parameters for that program. Additionally, acquisition planning documents such as Life-Cycle Cost Estimates

(LCCE), Systems Engineering Plans (SEP), Integrated Master Schedule (IMS), Integrated Master Plans (IMP), Test and Evaluation Master Plans (TEMP) and Technology Readiness Assessment (TRA) provide detailed cost, schedule, and technical performance measures for program management efforts. Since effective risk management requires a stable and recognized baseline from which to access, mitigate, and manage program risk it is critical that the program use an IMP/IMS. Processes managed by the contractor, such as the IMP, contractor IMS, and Earned Value Management (EVM), provide the PM with additional insight into balancing program requirements and constraints against cost, schedule, or technical risk.

Risk management is easily one of the most important aspects of protecting a business, and growing it larger. Yet, it's also one of the least discussed or taught to business owners. Why is this? Perhaps it's because the entrepreneur inherently understands risk so well. If their business fails, it feels personal. If sales goals falling short, it hits close to the wallet. However, understanding the risks are one thing, proactively doing something about them is a whole other side of things that risk management can provide.

If you, the business owner, develop a systematic way of analyzing your risks and coming up with risk management plans, then you will be implementing what is referred to as Enterprise Risk Management. Thus, while risk management is so important to an entrepreneur, it's often one of the biggest opportunities to drive a fledgling business into a successful company.

Enterprise Risk Management is a strategic, business discipline that helps an organization achieve its goals be systematically understanding the risk impact and implementing a plan to manage those risks. It includes the methods and processes used by businesses to manage risks and seize opportunities related to the achievement of their objectives. Small and medium sized businesses have unique risks and opportunities, such as strategic market placement and growth.

ERM provides a framework for identifying inherent risks and opportunities that are specific to that organization and relevant to its objectives. It includes assessing those risks in terms of likelihood and impact if it happens. It also provides a structured approach to creating a plan for moving the business away from risk and towards those opportunities.

Purpose of risk management is to minimize the threats and increase the opportunity. Overall increase ROI. Objectives are:

1. Minimize threats and enhance opportunities.
2. Identify, evaluate, mitigate and control risks.
3. Determine key risk indicators (KRI) and key performance indicators (KPI) to align effort to meet organizational strategic goals.
4. Do SWOT analysis to determine e overall organization's strength, weaknesses, opportunity and threats
5. Although not a part traditionally, but contribute overall for business continuity.
6. Find the major threats to an organization or projects or any business area and align resources to reduce the impact

By establishing the framework for the management of risks, the basic parameters within which risks must be managed are defined. Consequently, the scope for the rest of the Risk Management process is also set. It includes the definition of basic assumptions for the organization's external and internal environment and the overall objectives of the Risk Management process and activities. Although the definition of scope and framework are fundamental for the establishment of Risk Management, they are independent from the particular structure of the management process, methods and tools to be used for the implementation.

In order to define an efficient framework it is important to:

- understand the background of the organization and its risks (e.g. its core processes, valuable assets, competitive areas etc.);
- evaluate the Risk Management activities being undertaken so far;
- develop a structure for the Risk Management initiatives and controls (countermeasures, security controls etc.) to follow.

This approach is useful for:

- clarifying and gaining common understanding of the organizational objectives;
- identifying the environment in which these objectives are set;
- specifying the main scope and objectives for Risk Management, applicable restrictions or specific conditions and the outcomes required;
- developing a set of criteria against which the risks will be measured;
- defining a set of key elements for structuring the risk identification and assessment process.

Definition of external environment

This step includes the specification of the external environment in which the organization operates and the definition of the relationship between this environment and the organization itself.

The external environment typically includes:

- the local market, the business, competitive, financial and political environment;
- the law and regulatory environment;
- social and cultural conditions;
- external stakeholders.

It is also very important that both the perceptions and values of the various stakeholders and any externally generated threats and/or opportunities are properly evaluated and taken into consideration.

Definition of internal environment

As in every significant business process, the most critical prerequisite is to understand the organization itself.

Key areas that must be evaluated in order to provide a comprehensive view of the organization's internal environment include:

- key business drivers (e.g. market indicators, competitive advances, product attractiveness, etc.);
- the organization's strengths, weaknesses, opportunities and threats;
- internal stakeholders;
- organization structure and culture;
- assets in terms of resources (such as people, systems, processes, capital etc);
- goals and objectives and the strategies already in place to achieve them.

Generating the Risk Management context

In business terms, Risk Management as a process should provide a balance between (all kinds of) costs, benefits and opportunities. Therefore, it is necessary to draw the appropriate framework and to correctly set the scope and boundaries of the Risk Management process.

Setting the Risk Management context involves defining the:

- organization, process, project or activity (to be assessed) and establishing its goals and objectives;
- duration of the project, activity or function;
- full scope of the Risk Management activities to be carried out specifying any including inclusions and exclusions;
- roles and responsibilities of various parts of the organization participating in the Risk Management process;
- dependencies between the project or activity and other projects or parts of the organization;

Formulation of Risk Criteria

The criteria by which risks will be evaluated have to be decided and agreed. Deciding whether risk treatment is required, is usually based on operational, technical, financial, regulatory, legal, social, or environmental, criteria or combinations of them. The criteria should be in line with the scope and framework defined above. Furthermore they should be closely related to the organization's internal policies and procedures and support its goals and objectives.

Important criteria, to be considered, are:

- impact criteria and the kinds of consequences that will be considered;

- criteria of likelihood;
- the rules that will determine whether the risk level is such that further treatment activities are required.

It is very common, that criteria identified during these steps are further developed or even modified during later phases of the Risk Management process.

Principles of Risk Management:-

There are risk management principle by international standardization organization and by project management body of knowledge. A combined view of principles identified by ISO and PMBK is as follow-

1. Organizational context
2. Involvement of stakeholders
3. Organizational objectives
4. Reporting
5. Roles and Responsibility
6. Support Structure
7. Early warning indicators
8. Review Cycles
9. Supportive culture
10. Continual improvement

Risk Management- Construction Style

BT :- Build and Transfer

BTO :- Build, Transfer, Operate

BOT :- Build , Operate and Transfer

BOOT :- Build, Own, Operate and Transfer

BOONT :- Build, Own, Operate, and No Transfer

Chapter-4-Data Analysis & Interpretation

We use many different terms to describe common risk management concepts. For example risk, threat, hazard and in insurance peril are all used interchangeably but this often causes significant confusion.

To manage this some countries and organizations have attempted to develop standards for the purpose of defining a common risk management language. Examples of such standards include the Australian/New Zealand Standard (AS/NZS 4360:1995). Other countries such as the UK, Canada and South Africa have also developed similar standards. Some leading risk management organizations have also developed standards. This includes AIRMIC, ALARM, IRM, and the International Standardization Organization (ISO).

It is worth noting that often people identify risk in a negative light, equating it with threat to some goal or objective. However business is built upon risk and without it there would be no possibility to make profit - which is commonly recognized as a reward for taking a risk.

Enterprise risk management is the recognition that it is often best to approaching the management of risk from an integrative stand point. Business risk comes in many forms and these forms are often changing. For example legislation evolves, competition develops and technologies are made redundant.

However a biannual survey conducted by AON indicates that the following are currently the top risks concerning top managers in 100 of Europe's top companies;

1. Loss of Reputation
2. Business Interruption
3. Failure to Change
4. Product Liability / Tampering
5. Impact of Regulation / Legislation
6. Physical Damage
7. Employee Accidents
8. Terrorism
9. Corporate Governance
10. Professional Indemnity

And

Risk management is the process of identifying, assessing and controlling financial, legal, strategic and security risks to an organization’s capital and earnings. These threats, or risks,

could stem from a wide variety of sources, including financial uncertainty, legal liabilities, strategic management errors, accidents and natural disasters.

If an unforeseen event catches your organization unaware, the impact could be minor, such as a small impact on your overhead costs. In a worst-case scenario, though, it could be catastrophic and have serious ramifications, such as a significant financial burden or even the closure of your business.

To reduce risk, an organization needs to apply resources to minimize, monitor and control the impact of negative events while maximizing positive events. A consistent, systemic and integrated approach to risk management can help determine how best to identify, manage and mitigate significant risks.

At the broadest level, risk management is a system of people, processes and technology that enables an organization to establish objectives in line with values and risks.

A successful risk assessment program must meet legal, contractual, internal, social and ethical goals, as well as monitor new technology-related regulations. By focusing attention on risk and committing the necessary resources to control and mitigate risk, a business will protect itself from uncertainty, reduce costs and increase the likelihood of business continuity and success. Three important steps of the risk management process are risk identification, risk analysis and assessment, and risk mitigation and monitoring.

Identifying risks

Risk identification is the process of identifying and assessing threats to an organization, its operations and its workforce. For example, risk identification may include assessing IT security threats such as malware and ransomware, accidents, natural disasters and other potentially harmful events that could disrupt business operations.

Risk analysis and assessment

Risk analysis involves establishing the probability that a risk event might occur and the potential outcome of each event. Risk evaluation compares the magnitude of each risk and ranks them according to prominence and consequence.

Risk mitigation and monitoring

Risk mitigation refers to the process of planning and developing methods and options to reduce threats to project objectives. A project team might implement risk mitigation strategies to identify, monitor and evaluate risks and consequences inherent to completing a specific project, such as new product creation. Risk mitigation also includes the actions put into place to deal with issues and effects of those issues regarding a project.

Risk management is a nonstop process that adapts and changes over time. Repeating and continually monitoring the processes can help assure maximum coverage of known and unknown risks.

here are five commonly accepted strategies for addressing risk. The process begins with an initial consideration of risk avoidance then proceeds to three additional avenues of addressing risk (transfer, spreading and reduction). Ideally, these three avenues are employed in concert with one another as part of a comprehensive strategy. Some residual risk may remain.

Risk avoidance
Avoidance is a method for mitigating risk by not participating in activities that may negatively affect the organization. Not making an investment or starting a product line are examples of such activities as they avoid the risk of loss.
Risk reduction
This method of risk management attempts to minimize the loss, rather than completely eliminate it. While accepting the risk, it stays focused on keeping the loss contained and preventing it from spreading. An example of this in health insurance is preventative care.
Risk sharing
When risks are shared, the possibility of loss is transferred from the individual to the group. A corporation is a good example of risk sharing — a number of investors pool their capital and each only bears a portion of the risk that the enterprise may fail.
Transferring risk
Contractually transferring a risk to a third-party, such as, insurance to cover possible property damage or injury shifts the risks associated with the property from the owner to the insurance company.
Risk acceptance and retention
After all risk sharing, risk transfer and risk reduction measures have been implemented, some risk will remain since it is virtually impossible to eliminate all risk (except through risk avoidance). This is called residual risk.

Risk management standards set out a specific set of strategic processes that start with the objectives of an organization and intend to identify risks and promote the mitigation of risks through best practice. Standards are often designed by agencies who are working together to promote common goals, to help to ensure high-quality risk management processes. For example, the ISO 31 000 standard on risk management is an international standard that provides principles and guidelines for effective risk management.

While adopting a risk management standard has its advantages, it is not without challenges. The new standard might not easily fit into what you are doing already, so you could have to introduce new ways of working. And the standards might need customizing to your industry or business.

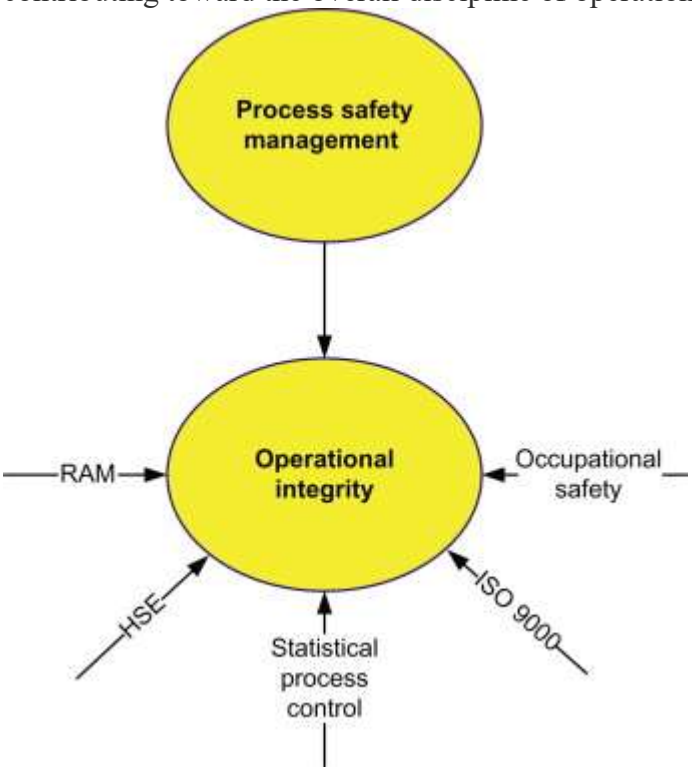
Facilities in the process industries typically handle large quantities of hazardous materials. The consequences of an incident involving these materials can be very serious, so it is critical that management in those industries develop and implement risk management programs. The contents of this book provide guidance as to how this can be done. Risk management covers a broad range of issues, including technical analysis, the development and use of management systems, and human behavior, so the scope of this book is broad. And the goals of risk management programs go beyond safety—which is why the title of this book was changed

from *Process Safety Management* to *Process Risk and Reliability Management*. An effective risk management program considers not just safety, but also environmental impacts, economic losses, and more nebulous topics such as company reputation.

Risk management is part of the larger topics of Operational Integrity and Operational Excellence. A facility which has a high level of operational integrity is one that performs as expected in an atmosphere of "no surprises." The facility exhibits integrity in all aspects of its operation. These programs incorporate not just process safety but also many other technical initiatives that companies have been pursuing during the last two decades in order to improve safety, environmental performance, and profitability. A partial list of such initiatives includes:

1. RAM (reliability, availability, and maintainability) programs that focus on achieving maximum profitability.
2. HSE programs covering the broad spectrum of Health, Safety, and Environmental (HSE) work.
3. Statistical process control.
4. Quality standards such as ISO 9000.
5. Occupational and behavior-based safety programs that help improve the actions and behaviors of individuals.

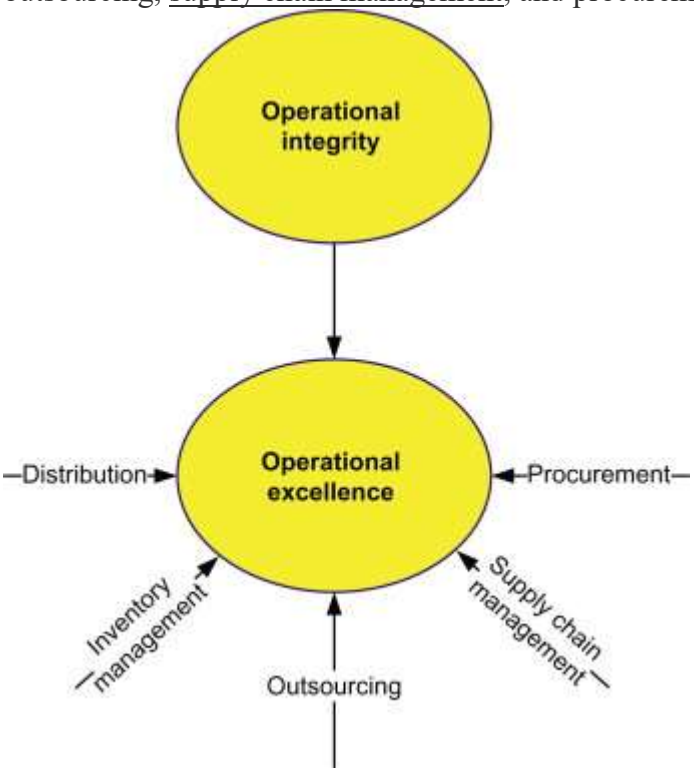
Each of these topics—along with many others not listed above—can be thought of as contributing toward the overall discipline of operational integrity, as illustrated in Figure 1.1.



In addition to the incorporation of a wide range of management techniques that are shown in Figure 1.1, operational integrity can be applied to a much wider variety of industries than is

the case with process safety management. Operational Integrity Management (OIM) can be used not only in chemical facilities and refineries, but also in transportation, pipelines, and offshore oil and gas.

Many companies are also developing operational excellence programs. The manner in which these can relate to operational integrity is shown in Figure 1.2. Operational integrity is made up of technical initiatives; operational excellence incorporates nontechnical management systems that can affect safety and operability. These include distribution, inventory management, outsourcing, supply chain management, and procurement.



Decision-making under conditions of large uncertainty is an issue that poses serious questions about the decisional chain, its complexities, the consequent responsibilities, and, ultimately, the difficulties of identifying the “right” decision to make. This paper addresses these issues from a civil protection perspective, i.e., from the point of view of an organization which often operates under highly uncertain conditions in the management of the risk cycle. Three main participants in the decision-making process are identified: scientists, political decision-makers (PDMs), and technical decision-makers (TDMs). They provide different contributions to the risk management, with frequent and intricate interactions that, however, can cause distortions in the distinction of the roles to be played, and thus of the responsibilities to be taken. In addition to scientists and decision-makers, there are other participants playing important roles in the risk cycle, and thus influencing decisions within the civil protection system, such as the technical community of professionals, the mass media, the magistrates, and the citizens. PDMs and TDMs, as well as scientists, are directly involved in the decision-making process. Professionals, journalists, magistrates, and citizens can indirectly condition decisions and their implementation. Examples are reported for all of these categories. Participants in the decisional process who understand their role and responsibilities can contribute to a more efficient and effective civil protection

system, reducing the occurrence of errors and incidents, if they act within the bounds of their expertise, but avoid to adhere too rigidly to their role. How to develop a correct and fruitful interaction among all the actors is a primary target for a mature civil protection system.

Global Risk Management System Through Lessons From the Great East Japan Earthquake

Nissan's risk management is unique in that "Locations spread over the world fully support Japan at the time of emergency" through its global alliance with Renault. For example, Nissan's Global Vehicle Production Technology Center in Zama City, Kanagawa Prefecture keeps digital drawing data of molds for all Nissan car parts. When the Iwaki factory stopped operation, the data was transferred to the US factories and alternate production of engine parts for the Japanese market started immediately.

Nissan's global risk management system with lessons from the Great East Japan Earthquake now contains the following developments: First, the basic tools of risk management rules, methodology of risk assessment, or risk map format are shared. Second, actual actions are coordinated globally on a job basis. Third, for exchanging information and opinions, global risk management meetings are organized annually, domestic risk management meetings twice annually, and information exchange with Renault and a joint venture in China once or twice a year. Fourth, values are expected to be produced through risk management operations in each region and each company. In other words, risk assessment is made through the viewpoint of each region and each company. "Risks for the entire group" at the global headquarters are not pushed down towards the global companies. Similarly, the risk maps from the companies are not consolidated into a global version risk map. The global risk management system at Nissan is thus a loose coordination with the basic risk management processes shared globally.

Risk management is predicated on risk characterization, as previously discussed. In the risk management process there is an integration of activities for assessing disposal, storage, transportation, conditioning, and proliferation concerns against a wide range of waste classification factors, such as toxicity, mobility, integrity, and reactivity. The purpose of classification is to facilitate an understanding of the magnitude of risks and to simplify the management of multiple elements in a diverse system. Table 4 summarizes the management activities and classification factors that are considered in characterizing the potential adverse impact on public health. Figure 7 represents a framework for evaluating the acceptability of long-term waste disposal options. In addition to assessing the potential of exposure to hazardous substances released from a repository by natural processes (e.g., water intrusion, earthquake, or volcanic activity), it indicates a need to evaluate the potential impact from intentional or unintended human intrusion (e.g., well drilling).

Risk management decisions should be based on a wide range of issues relevant to risk analysis, including medical opinion, epidemiology, and professional judgment, along with socioeconomic factors and technical feasibility. A premium on enhancing communication and obtaining

feedback from those engaged in the components of risk analysis and management is recommended.

Risk Management Measures (RMM)

RMMs include any action that is introduced during manufacture or use of a substance (either in a pure state or in a mixture) in order to prevent, control, or reduce exposure of humans and/or the environment. RMMs, and their proper implementation, are of critical importance for the safe use of substances. Examples of RMMs include the following:

- Engineering controls – refer to the design of process plant and equipment to isolate substance emission sources, maximize substance containment, and prevent contact between workers and the hazardous substance. Examples include the use of local and/or general exhaust ventilation (i.e., mechanical and/or passive), isolation controls, wastewater treatment, and sewage/waste treatment. The use of engineering controls for the reduction of worker (and consumer) exposures is considered to be the most effective, and most strongly recommended, RMM.
- Administrative controls – are management tools that seek to reduce exposure opportunity, control the way the work is carried out, limit exposure duration, and ensure that the work activity is carried out in a predetermined way. Examples include personnel rotations and schedule adjustments to reduce exposure time/opportunity and worker training to recognize chemical hazards as well as techniques, etc., to reduce/eliminate exposures. Effectiveness of administrative controls is often dependent on worker compliance and consistent supervisory enforcement. They support engineering controls in reducing the potential for exposure.
- Personal protective equipment (PPE) – includes protective clothing, appropriate (i.e., impervious) gloves, particulate and organic vapor respirators, and eye protection (e.g., goggles). PPE is the lowest ranked RMM option because its effectiveness depends to a large extent on its appropriate selection, use, and maintenance and (worker) compliance. PPE protects only the individual wearer and does not prevent the exposure or contamination of the wider working environment. Nevertheless, it may be the best available option for infrequent tasks of short duration and for maintenance tasks or emergency situations. As with administrative controls, PPE may also be used to complement implemented engineering controls.

Regulatory Risk Management:-

Regulatory risk management is the last step, but also the one that has received more attention. These activities usually focus on the manufacturing and/or marketing of the hazardous substances, imposing specific conditions or limitations that may even represent total banning. There are two main regulatory risk management lines: one of proactive nature, setting controls or conditions prior to the manufacturing and marketing, and the other of reactive nature, limiting and controlling substances already in the market.

Proactive risk management lines are usually applied to groups of substances of particular concern, trying to avoid or minimize, beforehand, their risks. The most typical model is the use of positive lists or premarketing authorization systems. Before manufacturing, using, or marketing the substance, industry needs to demonstrate an acceptable level of risk for that particular use. Positive lists means that only the substances included in the list can be utilized for that particular use; premarketing authorization requires a concrete application with the specific use patterns and conditions, usually at the company level. Both alternatives can be combined; for example, in the case of pesticides, biocides, or pharmaceuticals many regulatory schemes include a two-step approach, first with the inclusion of the active substance in a positive list, and second with the specific marketing authorization for the formulated commercial product. Proactive risk management may also be based on specific measures or even information requirements. The special measures for the national or international transport of dangerous goods, the particular packaging and storage requirements, or even the information requirements for classification and labeling, SDS, etc. can be considered also in this category of regulatory risk management.

Proactive risk management is based on generic policy decisions, and it is in many cases related to concerns, not to actual risks; although the consequence is a risk analysis requirement. In fact, these policy lines require industry to demonstrate a safe use through risk assessments in order to commercialize these substances/products. For example, pharmaceuticals, pesticides, biocides, food additives, etc. are assumed to be, by default, of concern and/or to require particular attention, and consequently are broadly regulated through positive lists and premarketing authorization requirements. Consequently, these substances/products require the inclusion in the positive list or an authorization. Similarly, hazard-based criteria can be used for setting generic concerns. Transport, packaging, and storage requirements are directly associated with particular hazard classification classes and categories, and are usually oriented to the minimization of the risk associated to accidental unintended releases, not to the intended use.

On the contrary, reactive risk management is typically the outcome of a substance specific risk assessment on a marketed substance or product. When the outcome of such assessment identifies that the risks are not properly handled by the business sector, the authority establishes mandatory limitations such as the restriction of certain uses, the implementation of some control measures, or even a total ban. Restrictions for marketing and/or use are typical reactive risk management practices. Depending on the identified risks, the restriction may affect specific products, general product categories, or certain uses. In same cases, the final aim can be the total ban and substitution by other alternatives, but if the total ban cannot be implemented yet, time-limited exceptions are included to promote the development of the alternatives. In some cases, less stringent options may also be effective; for example, obligatory labeling requirements or inclusion in ‘gray lists’ imposing additional regulatory controls.

As already mentioned, a key element for risk management decisions is the comparison of the risk and the impacts, including the socioeconomic impacts. The regulatory decision requires in many cases to set the balance between the risks and the benefits or a comparative assessment of the risk of the substance/activity and that of the possible chemical and technological alternatives. In fact, management decisions must often balance the benefits of interventions for human health and environment and the costs of restrictions for the economy. There are efforts, both sides of the Atlantic, for improving the coordination between the risk assessment and the socioeconomic analysis. In the United States, the NRC Framework for Risk-Based Decision-Making intends to make economics and risk–risk tradeoffs more central in the analysis; encouraging the use of similar methods between disciplines (such as the explicit incorporation of uncertainty and variability and the development of default assumptions and criteria for the departure in economic analyses) and promoting collaboration between risk assessors and regulatory economists. The aim is to facilitate cooperation and understanding, overcoming the many regulatory, legislative, and logistical constraints that in many cases complicate the simultaneous consideration of costs of control and benefits. Similar proposals have been suggested in Europe by the DG SANCO Scientific Committees in the opinion on Improvement of Risk Assessment in View of the Needs of Risk Managers and Policy Makers. These frameworks also provide the opportunity for improved public participation. The focus of inquiry is broader to the relevant elements for society and the consideration of potential risk–risk tradeoffs are made a central part of the assessment. Stakeholders (such as local communities and citizens' organizations) may also bring particular knowledge about the benefits, costs, and implementation of risk management options to a discussion.

Chapter-5 –Conclusions/Findings:-

The RMI and LAC indexes in conjunction with semi structured interviews with risk management practitioners, vulnerable groups, and experts have proved to be a quick and effective method of assessing vulnerability in a particular system through an examination of the strengths and weaknesses of its risk management structure. Although this methodology does not provide a quantitative measure of existing vulnerability, it provides qualitative and actionable assessments that allow for policy and practical improvements to strengthen the overall risk management and disaster response mechanisms. Through its application to heatwaves and drought hazards in London, the following observations and recommendations are made with regards to risk management and vulnerability assessment:

- Vulnerability to climate change hazards is a dynamic function of both physical as well as social factors. Both types of indicators need to be taken into account when measuring vulnerability.
- Disaster risk management directly impacts vulnerability and requires multiagency coordination from organizations involved not only in disaster response but also risk reduction (such as social services).
- Disaster management plans need built-in mechanisms to ensure that they move beyond their role as risk management regimes to best-practice guidelines for local actors.
- Climate change hazards need greater prioritization and given further policy and financial support by governments in order to decrease vulnerability and risk.

Abstract
Disaster risk management for cultural heritage is needed in the light of increasing vulnerability of cultural heritage to disasters due to natural as well as human induced hazards. However, this requires robust governance mechanisms at national as well as local levels both in the sectors of disaster risk management and cultural heritage conservation. The chapter will elaborate on the essential pre-requisites for achieving this, which include greater collaboration between agencies responsible for disaster risk management, cultural heritage conservation and development. It also calls for not just formalized institutional systems but also traditional governance systems that are rooted in local communities, necessitating community engagement in disaster risk management of cultural heritage. The chapter concludes by enumerating on the importance of good governance achieved through collaboration, transparency, accountability and social justice.

Establish Broad Risk Management Goals

Risk management goals are statements of the intended purpose and the end result that risk management is intended to achieve. The goals can be expressed in different ways, for example, to ensure that the intake of a certain chemical hazard by a vulnerable population group does not exceed a defined acceptable daily intake (ADI) or provisional tolerable weekly intake (PTWI) or to achieve a specified reduction in exposure of a population group to a chemical hazard within a certain time period. For example, Germany has set a goal to reduce acrylamide exposure via food by taking an as low as reasonably achievable (ALARA) approach (see Evaluate the Options).

Risk analysis and management began around the middle of the 20th century in different industries with different approaches such as:

- In the 1960s—the aerospace industry with quantitative risk assessment methods and the nuclear industry with a probabilistic risk assessment approach;
- In the 1970s—the chemical industry with quantitative risk assessment and the Seveso directive;
- In the 1980s—the oil and gas industry with quantitative risk assessment and safety case.

By definition, risk is the combination of a hazardous event and its consequence. To analyze and evaluate risk, the qualitative and quantitative approach can be performed. In fact, when risk is assessed and evaluated based on qualitative methods, such assessment is performed qualitatively based on specialist opinion regarding a risk matrix with the frequency and consequence criterion established.

There are different configurations of risk matrix and such configuration must reflect the law and companies' risk policy. In fact, before making an appropriate risk matrix it is necessary to define clearly the frequency or probability category as well as severity. The discussion between risk specialists regarding the best risk matrix is usually a difficult one: frequency or probability, but in reality most of the time it is easier for the specialist who takes part in risk analysis to predict frequency rather than probability concerning the causes of accidents. Fig. 6.1 shows an example of a risk matrix with four severity categories and six frequency categories. Again, the risk matrix configuration must fit well to companies and their process, and in some cases it is necessary to use a different risk matrix for different processes in the same company.

		FREQUENCY CATEGORY					
		A (extremely remote)	B (remote)	C (Little frequence)	D (Frequent)	E (Very frequent)	F (Extremely frequent)
		At least 1 between 1000 and 100,000 years	At least 1 between 50 and 1000	At least 1 between 30 and 50 years	At least 1 between 5 and 30 years	At least 1 in 5 years	At least 1 in 1 year
SEVERITY CATEGORY	IV	M	NT	NT	NT	NT	NT
	III	M	M	NT	NT	NT	NT
	II	T	T	M	M	M	M
	I	T	T	T	M	M	M

Individual risk is calculated from the sum of all risks of each accident scenario in a plant facility, and is expressed in terms of the number of deaths per year. To define the number of deaths in each accident scenario, it is necessary to carry out a Consequence and Effect analysis (CEA) to predict such a number based on the effect on employees in a vulnerable area. Such a calculation considers the consequences (radiation, toxic level, pressure wave) and tolerance that are defined by PROBIT equations. This will be discussed in more detail with examples of a CEA.

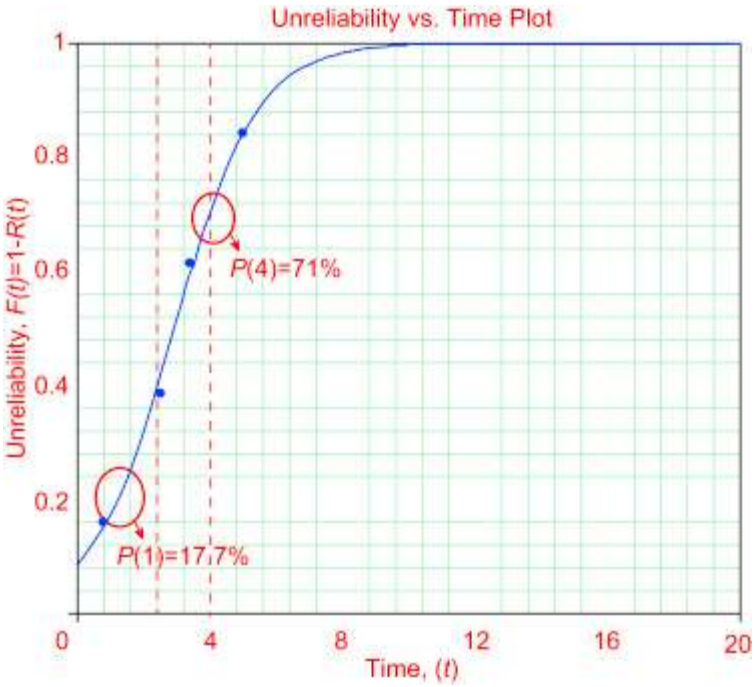
Remarkably, in some countries only societal risk is a decision criterion for acceptance of new projects; individual risk is not. Regardless of how many deaths occur during a plant installation, if such an accident does not affect the community outside the plant, the project is accepted. From a safety point a view, this makes no sense and means that projects with a low level of safety are accepted by authorities when they are located in places where no community is present, or where there will be no significant effect on the community.

Furthermore, in most of cases in individual risk calculation, such risk is considered independent of time. That means the calculated risk remains constant for a long period of time. This is unrealistic because initiating events are mostly equipment failures that are dependent on time and are better represented by cumulative density function distribution. Consequently, the probability of failure increases over a long period of time, and this results in the associated risk increasing over a period of time. To keep risk at an acceptable level, inspection and preventive maintenance are required so that failure in layers of protection and equipment with possible unsafe failures may be detected.

Societal risk is the frequency of death per year to which a community outside the industrial area is exposed. Societal risk is usually represented by the F–N curve that shows the cumulative expected number of fatalities on each frequency level. Such a curve represents the combination of the expected number of deaths and the frequency, and is thus a cumulative curve, which takes into account all the hazard scenarios from one or more specific hazard sources in the plant facility, which may affect the community outside the plant facility area. ALARP is also represented by the F–N curve to define when societal risk is acceptable or not. A high level of reliability on layers of protection and equipment can also help to mitigate risk, as well as the implementation of preventive maintenance to keep a high level of reliability and availability of such devices.

wo of the most important concepts in quantitative risk analysis are the probability and frequency of an event. The probability of failure is the inverse of reliability. Reliability is the probability of equipment, products, or services operating successfully over a specific period of time, and is the mathematical complement of the probability of cumulative failure.

Thus, in risk analysis, the probability of event occurrence can be assessed by cumulative density functions (CDFs), or, in other words, unreliability time, as shown in Fig. 6.5. In this way, the quantitative methods for defining probability density functions (PDFs) and CDFs (unreliability) discussed in Chapter 1 will be used in risk analysis to define the probability of failure over time.

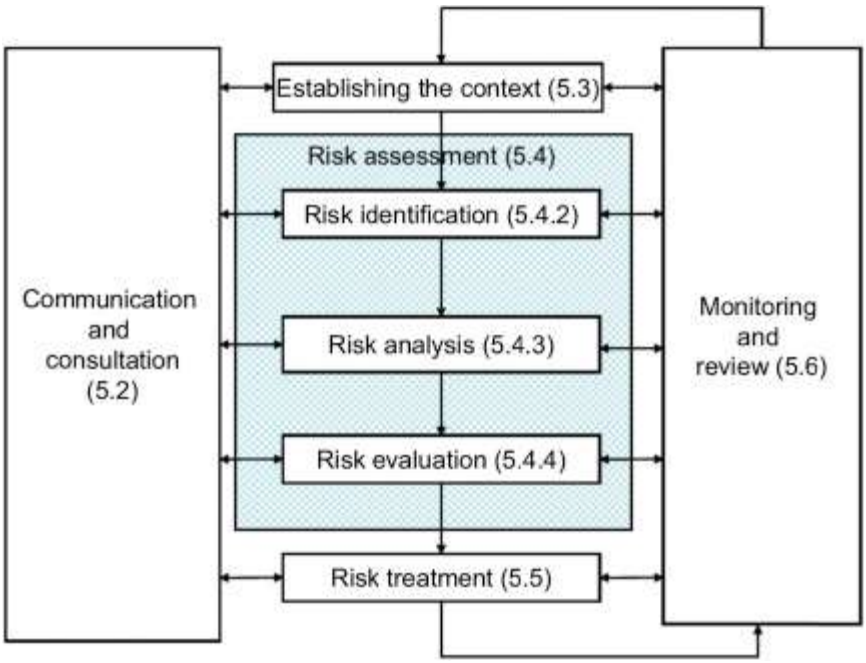


it is clear that depending on the time considered in risk analysis, the probability of failure will be different. The probability is higher if no maintenance on equipment is performed to reestablish a part of reliability. Thus if 1 year is used the probability of failure is 17.7%, but if 4 years is used the probability of failure is 71%. Such concept will be applied to the quantitative risk methods in the following sections.

To define, assess, and mitigate risk, the risk management process is vital. In fact, risk management is applied to maintain process risk under acceptable levels and avoid whenever possible incidents and accidents. Based on ISO 31000 standard, risk management is established based on the Plan, Do, Check and Act (PDCA) concept, which encompasses different steps such as:

- Mandate and commitment: requires risk management policy establishment at strategic level and such policy will drive all goals and indexes throughout the organization.
- Design of a framework: supports the first step more effectively and will guarantee that the risk policy is adequate for the company taking into account the internal and external organization's context.
- Implementing risk management: comprises four phases, which are risk assessment, risk treatment, risk communication, and risk monitoring and review.

Fig. 6.6 shows the risk management process based on ISO 31000 concepts.


Establishing the context (5.3)
Risk assessment (5.4)
Risk identification (5.4.2)
Risk analysis (5.4.3)
Risk evaluation (5.4.4)
Risk treatment (5.5)
Communication and consultation (5.2)
Monitoring and review (5.6)

Chapter-6-Suggestion/Recommendations

To mitigate process risk, different layers of protection with significant reliability are applied to assure that in case of unsafe process conditions the system will return to a safe condition. Therefore, the acceptable risk level in industrial processes relies on multiple layers of protection.

There are different types of layers of protection such as design features, control systems, safety protection functions, and emergency response plans. The best approach to maintain an acceptable risk level is to start risk management during the design phase. Moreover, it is also necessary to implement risk analysis recommendation throughout the asset phases and update risk analysis whenever a process modification takes place. In fact, during the project phase, there are increased flexibilities for modifications to incorporate new ideas to improve asset safety rather than during the operational phase.

The major approach to inherently safer process designs is divided into the following categories (Crow and Louvar, 2002):

- Intensification
- Substitution
- Attenuation
- Simplification

Intensification means minimizing risk whenever possible based on less hazardous equipment and products. Substitution means replace whenever it is possible the current equipment for more safety equipment and products. Attenuation means processes should be designed to mitigate the effects of accidents. Simplification means establishing process control as simple as possible for case of incidents and accident.

An additional important concept related with risk management is risk perception, which means how much employees and other affected parties like communities are aware of the risks to which they are exposed. Risk perception is related to risk communication and is a very important task of risk management. In fact, risk communication is difficult to apply because of the requirements of different groups of employees and even society. A powerful tool to communicate risk is *safety dialogue*, which is a discussion about a safety-related issue carried out for a particular employee. The main objective is to make groups aware of such issues and enable discussion. To communicate process risk to operators a safety dialogue is appropriate because it enables discussion about risks rather than an electronic message. In the same way, whenever a meeting is conducted with the community, in most cases such communication is about emergency procedures that are very important to the community in case of an accident. Whenever possible the communication management team must be involved in such a process because they know the best ways to communicate and to deal with information within the company.

Risk communication has a high influence on risk perception but does not guarantee that risk perception will trigger preventive behavior in the workplace because this depends on safety

culture as well. In addition, even though employees and society realize the risk they are exposed to, there is a third factor that influences their behavior: their risk profile. In general terms, risk profile can be aversive, neutral, or searching and varies from person to person depending on the situation and people's attitudes. Such a risk profile is very important to understand a leader's attitude to prevent and mitigate risks.

Finally, risk analysis results have to be considered in an emergency plan and such plan must be part of risk management. An emergency plan is a set of activities carried out in case of an accident, as well as resources and responsibilities for each task. A well-defined emergency plan is essential to have a good emergency response in case of accidents, but in addition it is necessary to carry out practical exercises in emergency plan application regarding an accident scenario. Thus it is very important to take into account the risk analysis results in the emergency plan otherwise the emergency response team will not be prepared to effectively respond to a predicted accident scenario. However, risk analysis does not cover all accident scenarios but the challenge is to be prepared for all possible events, even natural catastrophes and terrorist attacks.

THANKS